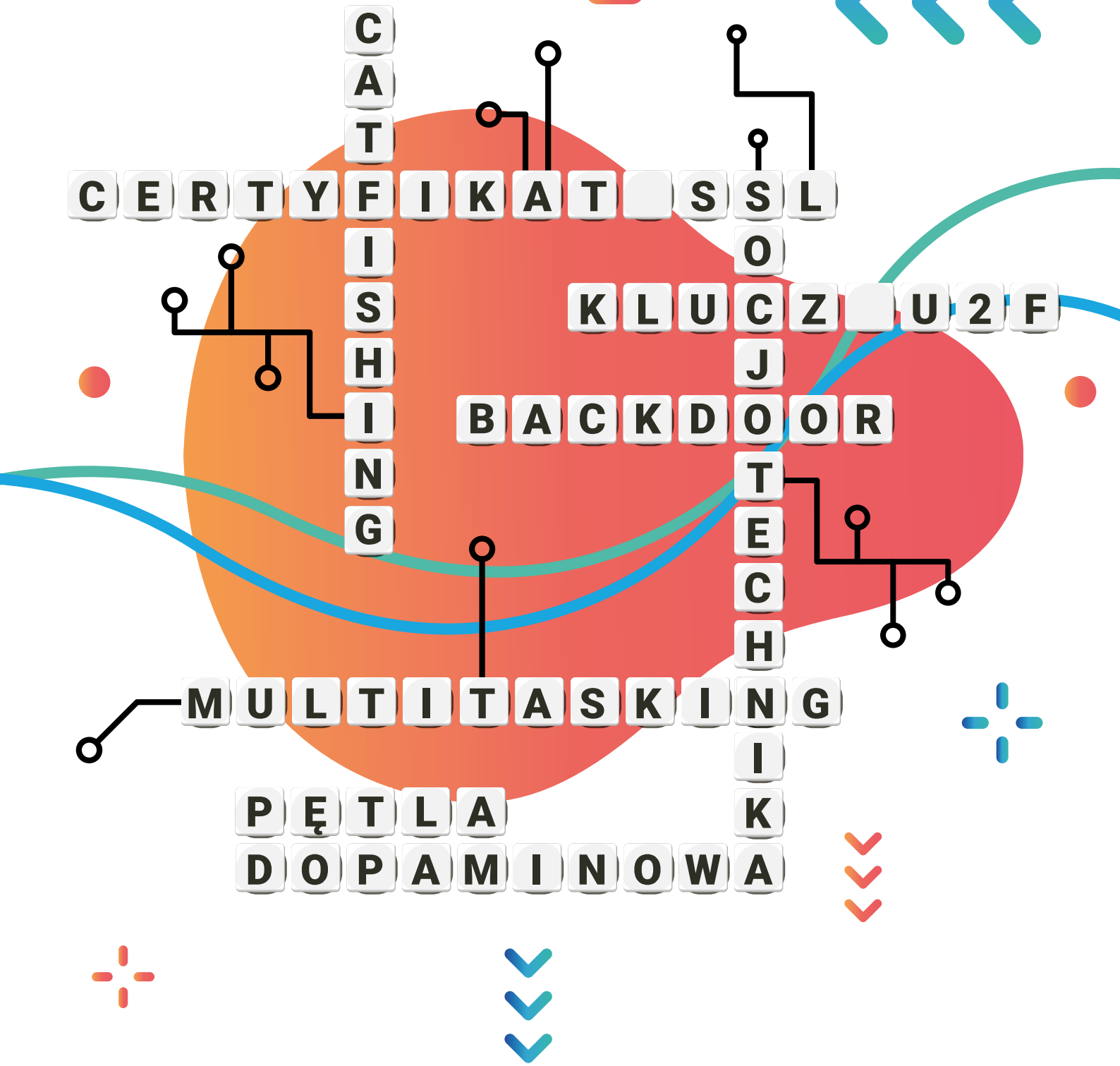
ABC cyberbezpieczeństwa 2.0



OGÓLNOPOLSKA SIEĆ EDUKACYJNA ose NASK

Autorki: Katarzyna Gańko, Diana Kania

Opieka merytoryczna: **Karol Bojke, Anna Borkowska, Joanna Dębek, Filip Marczewski, Bartosz Michałowski, Iwona Prószyńska, Szymon Sidoruk, Paweł Srokosz, Aleksandra Szczęsna, Dominik Tybura, Marta Witkowska**

Opracowanie graficzne i skład: **Aneta Witecka**

© NASK – Państwowy Instytut Badawczy
Warszawa 2025

ISBN: 978-83-68356-41-0

Wydanie II uzupełnione

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

„ABC cyberbezpieczeństwa 2.0” powstało na podstawie publikacji „ABC cyberbezpieczeństwa” autorstwa Katarzyny Gańko, Diany Kani i Emilii Troszczyńskiej-Roszczyk, wydanej w 2022 r. przez Państwowy Instytut Badawczy NASK. Opracowane wówczas hasła w tym wydaniu zostały zaktualizowane i znacząco uzupełnione, z zachowaniem pierwotnej koncepcji.

Projekt finansowany ze środków Ministerstwa Cyfryzacji

Spis treści

Wstęp ... 8

A ... 9

Administrator ... 9
Aktualizacja ... 9
Anonimowość w sieci ... 10
Aplikacja ... 11
Atak APT ... 11
Atak BLE Spam i bluejacking ... 12
Atak DDoS ... 13
Atak DoS ... 13
Atak siłowy ... 14
Atak słownikowy ... 15
Awatar ... 16

B ... 17

Backdoor ... 17
Backup ... 17
Bankowość internetowa ... 18
Bańka informacyjna ... 19
Baza danych ... 20
Bezpieczne przesyłanie plików ... 21
Biały wywiad (OSINT) ... 22
BLIK ... 23
Bluetooth ... 24
Bomba logiczna ... 25
Bot ... 25
Botnet ... 26
Browser hijacker ... 27
Business Email Compromise (BEC) ... 27

C ... 29

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) ... 29
Catfishing ... 30
CERT Polska ... 31
Certyfikat SSL ... 31
Chatboty AI ... 32
Cheap fake ... 33
Child grooming ... 33
Chmura ... 35
Clickbait ... 36
Clickjacking ... 37
Cracking ... 38
Credential stuffing ... 38
CRP (stopień alarmowy) ... 39
Cryptojacking ... 40
CSIRT ... 41
Cyberbezpieczeństwo ... 41
Cyberporwanie ... 43
Cyberprzemoc ... 44
Cybersquatting ... 45
Cyberstalking ... 46
Cyfrowy ślad ... 47

D 49

Dane osobowe 49
Deepfake 50
Dezinformacja 51
Digital self-harm 52
Dobrostan cyfrowy 53
Domowa sieć W-Fi 54
Doomsurfing 55
Doxing 56
Dyżurnet.pl 57
Dzień Bezpiecznego Internetu (DBI) 58

E 59

E-mail 59
E-uzależnienia 59
Ekran blokady 61
Emotikon, emoji 62
Europejski Miesiąc Cyberbezpieczeństwa (ECSM) 62
Exploit 63

F 64

Fact-checking 64
Fałszywe domeny 64
Fałszywe informacje 65
Fałszywe inwestycje 66
Fałszywe oferty wakacyjne 67
Fałszywe panele logowania 68
Fałszywe reklamy 69
Filtry kontroli rodzicielskiej 70
Firewall 71
Flaming 72
Flooding 72
FOMO 73
Fonoholizm 74

G 77

Gaming 77
Generator hasła 78
Geolokalizacja 79
Gray hat 79

H 81

Haktywista 81
Happy slapping 81
Hardening 82
Hasło 83
Hazard w internecie 84
Hejt 85
Helpline 86
Higiena cyfrowa 87
Hotline 88

I 89

Incydent bezpieczeństwa 89
Influencerzy 89
Infostealer 90

Internet ... 91
Internet rzeczy (IoT) ... 92
IP ... 93

J ... 95

Jailbreak ... 95
Jamming ... 95
JavaScript injection ... 96
JOMO ... 96

K ... 98

Keylogger ... 98
Klucz U2F ... 98
Kompetencje cyfrowe ... 99
Komunikacja bliskiego zasięgu (NFC) ... 100
Komunikatory internetowe ... 100
Kongres OSE ... 101
Kradzież danych ... 102
Kradzież tożsamości ... 103
Kradzież własności intelektualnej ... 104
Kryptowaluty ... 105

L ... 107

LAN (Local Area Network) ... 107
Lateral reading ... 107
Likejacking ... 108
Link ... 109
Lista ostrzeżeń przed niebezpiecznymi stronami ... 109
Login ... 110
Lootbox ... 110

M ... 112

Malware (złośliwe oprogramowanie) ... 112
Man-in-the-middle ... 112
Maskarada ... 113
Media społecznościowe ... 114
Menedżery haseł ... 115
Mikropłatności ... 116
mOchrona ... 116
Mowa nienawiści ... 117
Multitasking ... 118

N ... 119

Nadużywanie nowych technologii ... 119
Naruszenia prawa autorskiego ... 120
Naruszenia prywatności ... 121
NASK ... 122
„Nastolatki" (raport) ... 122
Netykieta ... 123
Nieautoryzowany dostęp ... 124
Niebezpieczne kontakty ... 125
Nielegalne treści ... 126
Nomofobia ... 126
Nudging ... 127

O ... 129

Ochrona urządzeń mobilnych ... 129
Odporność cyfrowa ... 129
Offline challenge ... 130
Ogólnopolska Sieć Edukacyjna (OSE) ... 131
Oprogramowanie antywirusowe ... 131
Oprogramowanie reklamowe (adware) ... 132
Oprogramowanie szpiegujące (spyware) ... 133
Oprogramowanie szyfrujące ... 134
Oszustwa internetowe ... 134
OUCH! ... 135
Oversharing ... 136

P ... 137

Pan European Game Information (PEGI) ... 137
Password spraying ... 138
Patotreści ... 139
Pętla dopaminowa ... 140
Phishing ... 141
Phubbing ... 142
Pliki cookie ... 143
Płatności biometryczne ... 144
Płatności internetowe ... 144
Podatność bezpieczeństwa ... 146
Podatność zero-day ... 146
Polskie Centrum Programu Safer Internet (PCPSI) ... 147
Problemowe używanie internetu (PUI) ... 147
Propaganda ... 148
Prywatność w sieci ... 149
Przeciążenie informacją ... 150

Q ... 151

Quishing ... 151

R ... 152

Ransomware ... 152
Regulamin ... 152
Romance scam ... 153
Rozporządzenie o ochronie danych osobowych (RODO) ... 154
Rozszerzona rzeczywistość (AR) ... 154
Równowaga online–offline ... 155

S ... 157

Scam ... 157
Seksting ... 157
Self generated sexual content ... 158
Separacja tożsamości ... 159
Sextortion ... 159
Sharenting ... 160
Skimming ... 161
Smombie ... 161
Snubbing w mediach społecznościowych ... 162
Social media sabbatical ... 163
Socjotechnika ... 164
Spam ... 164
Spoofing ... 165

Spray & pray ... 166
Stalking ... 167
Stealware ... 168
Stres cyfrowy ... 168
Szkodliwe treści ... 169
Sztuczna inteligencja ... 170
Szyfrowanie end-to-end ... 171

T ... 173

Techniczny Reprezentant Szkoły (TRS) ... 173
Teorie spiskowe ... 173
Troll parenting ... 174
Trolling w sieci ... 174
Tryb incognito ... 175
Typosquatting ... 176

U ... 177

Unboxing w grach cyfrowych ... 177
User experience (UX) ... 177
Usługi bezpieczeństwa OSE ... 178
Ustawa o krajowym systemie cyberbezpieczeństwa ... 178
Uwierzytelnianie dwuskładnikowe ... 179
Uwierzytelnianie wieloskładnikowe ... 180
Uzależnienie od gier komputerowych ... 180
Użytkownik ... 181

V ... 182

Viral ... 182
Virtual Private Network (VPN) ... 182

W ... 184

Wideokonferencje ... 184
Wirtualna rzeczywistość (VR) ... 184
Wirus komputerowy ... 186
Wizerunek online ... 186
Wtyczka (plug-in, add-on) ... 188
Wyciek danych ... 188
Wyzwanie (challenge) ... 189

Z ... 191

Zabezpieczenia biometryczne ... 191
Zachowania ryzykowne ... 191
Zakupy online ... 192
Zbiórki charytatywne online ... 193
Zero trust security ... 194
Zespół ds. nadużyć (zespół abuse) ... 194
Zielonka kłódka ... 195

Bibliografia ... 196

Wstęp

Cyfrowy świat nie stoi w miejscu – zmienia się z dnia na dzień, a my codziennie uczymy się, jak poruszać się w internecie bezpiecznie i czerpać z nowych technologii to, co najlepsze. Niestety, oszuści też stale doskonalą swoje techniki. Niektóre zagrożenia znikają, a w ich miejsce powstają nowe, bardziej zaawansowane i przemyślane. Jak nie dać się zaskoczyć? Jedno pozostaje niezmienne – liczą się: czujność, rozwaga w działaniu, znajomość cyberzagrożeń, umiejętność reagowania na niebezpieczne sytuacje online i przeciwdziałanie szkodliwym zjawiskom. Tylko i aż tyle…

W Ogólnopolskiej Sieci Edukacyjnej (OSE) doskonale wiemy, jak łatwo zgubić się w cyfrowym gąszczu, dlatego wracamy z wersją 2.0 bezpłatnego poradnika „ABC cyberbezpieczeństwa”!

Nasza publikacja „ABC cyberbezpieczeństwa 2.0” to ułożone alfabetycznie pigułki wiedzy. Krótkie, ale treściwe hasła pomogą zrozumieć zagrożenia czyhające w sieci oraz poznać dobre nawyki wspierające bezpieczeństwo i równowagę online–offline. To propozycja zarówno dla tych, którzy stawiają pierwsze kroki w internecie, jak i dla osób już wtajemniczonych, pragnących podejmować bardziej świadome decyzje związane z wykorzystaniem urządzeń cyfrowych.

Czym jest catfishing? Jak uchronić się przed e-uzależnieniami? Gdzie zgłosić fałszywe domeny i panele logowania? Jak nie wpaść w pętlę dopaminową? Czy warto zadbać w sieci o separację tożsamości? Co zrobić, gdy nasze dane wyciekły i jak reagować na incydenty bezpieczeństwa? Na te i inne pytania znajdziecie odpowiedź w 220 hasłach opatrzonych obszerną bibliografią.

Wiele z tych haseł ukazało się w aktualnościach z cyklu „ABC cyberbezpieczeństwa” i „ABC cyberbezpieczeństwa 2.0”, które publikowaliśmy na naszej platformie e-learningowej OSE IT Szkoła od kwietnia do czerwca 2022 r. i od stycznia do sierpnia 2024. W tym wydaniu poradnika odświeżyliśmy i zaktualizowaliśmy hasła, dodaliśmy nowe definicje, uporządkowaliśmy wszystko – od A do Z!

Mamy nadzieję, że nasza publikacja „ABC cyberbezpieczeństwa 2.0” będzie dla Was praktycznym przewodnikiem, a nawet podręcznym niezbędnikiem. Życzymy inspirującej lektury i… samych cyberbezpiecznych chwil przed ekranami urządzeń!

A

Administrator

Czy wiecie, kto nadzoruje działanie stron internetowych, baz danych i serwerów, odpowiada za konfigurację urządzeń (m.in. routerów, access pointów, switchy) i oprogramowania? Kto tworzy lokalne sieci komputerowe, zarządza nimi, dba o ich prawidłowe funkcjonowanie, bezpieczeństwo, wydajność i dostępność? Tą osobą jest administrator.

Do obowiązków administratora należy także ochrona sieci przed atakami, wdrażanie polityk bezpieczeństwa, udzielanie dostępów do określonych zasobów sieci oraz zapobieganie dostępom nieautoryzowanym. Na tym jednak nie koniec: administratorzy dbają także o regularne tworzenie kopii zapasowych, zarządzają kontami użytkowników, na bieżąco rozwiązują problemy techniczne związane z działaniem systemów i nadzorują codzienną pracę sieci. Mają sporo na głowie!

Ważnym zadaniem administratora jest również reagowanie na zgłoszenia użytkowników, dotyczące m.in. naruszeń prawa do prywatności i/lub bezpieczeństwa w sieci (np. hejtu w komentarzach na forach dyskusyjnych czy zamieszczanych na stronach szkodliwych treści). W takich przypadkach administratorzy mają możliwości i obowiązek usuwania niepożądanych materiałów czy blokowania cyberagresorów. Pamiętajcie: jeśli zauważycie w internecie coś, co Was zaniepokoi, bezzwłocznie skontaktujcie się z administratorem, np. za pomocą formularza kontaktowego lub specjalnego centrum pomocy, które znajdziecie np. w serwisach społecznościowych.

W Ogólnopolskiej Sieci Edukacyjnej (OSE) administratorami są Techniczni Reprezentanci Szkół (TRS), którzy pełnią rolę administratorów szkolnych sieci LAN, konfigurują urządzenia, instalują nowe wersje oprogramowania oraz na bieżąco współpracują z Centrum Kontaktu OSE (tel.: +48 22 182 55 55, e-mail: wsparcietechniczne_ose@nask.pl).

Aktualizacja

Systematyczne aktualizacje oprogramowania – czyli instalacje jego nowszych, poprawionych wersji – to podstawa! Pozwalają chronić urządzenia i dbać o Wasze bezpieczeństwo w sieci. Nowe wersje programów czy aplikacji zwykle naprawiają błędy zauważone np. w trakcie testów penetracyjnych, zawierają nowe funkcjonalności czy zmiany w interfejsie, wpływają również na wygodę użytkowania sprzętów i poprawiają ich wydajność.

Jak się pewnie domyślacie, dla cyberbezpieczeństwa ważne są zwłaszcza usprawnienia związane z prywatnością i ochroną. Producenci oprogramowania na bieżąco reagują na nowe zagrożenia pojawiające się w cyberprzestrzeni i dzięki aktualizacjom pomagają np. zwiększyć odporność aplikacji na ataki. Jak to działa w praktyce? Aktualizacje „łatają" luki w oprogramowaniu, pozwalające cyberprzestępcom na wykonanie działań, których nie przewidział twórca danego programu, aplikacji lub urządzenia. Wykorzystanie takich podatności może mieć poważne skutki, jak choćby wyciek danych czy uzyskanie nieautoryzowanego dostępu do systemu przez oszusta, prowadzące np. do ingerencji w kod oprogramowania. Zdecydowanie lepiej jest poświęcić chwilę na aktualizację, niż borykać się z takimi konsekwencjami!

Dzięki regularnym aktualizacjom oprogramowania możecie czuć się pewnie, korzystając z aplikacji bankowych czy innych programów przechowujących dane osobowe lub istotne informacje. „Łatki" bezpieczeństwa utrudniają oszustom kradzież haseł i danych logowania, pomagają unikać złośliwego oprogramowania (malware) i być na bieżąco z usprawnieniami, które ułatwiają codzienne korzystanie z systemu lub aplikacji.

Jak nie przegapić kolejnych aktualizacji? Niektóre instalują się automatycznie w tle, poprawiając bezpieczeństwo i stabilność systemu bez ingerencji użytkownika. Inne wymagają ręcznej akceptacji – wówczas pojawiają się w formie powiadomień: „Zaktualizuj teraz" albo „Nowa

wersja aplikacji dostępna". Nigdy nie warto odkładać ich na później: każda pominięta łatka zwiększa ryzyko ataku!

Dbanie o aktualizacje to prosty i skuteczny sposób, by uniknąć wielu problemów, od spowolnienia urządzenia po poważne włamania. To inwestycja w bezpieczeństwo, która praktycznie nic nie kosztuje, a może uratować nasze dane przed kradzieżą.

Więcej o aktualizacjach dowiecie się z aktualności na stronie ose.gov.pl: „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!" i „Bezpieczni w sieci z OSE: podatności i luki bezpieczeństwa".

Anonimowość w sieci

W internecie nic nie ginie – znacie to powiedzenie? Korzystając z sieci, wszyscy pozostawiamy za sobą cyfrowe ślady – np. adres IP (Internet Protocol), wyszukiwania w przeglądarce, dane geolokalizacyjne i inne. Z kolei dzięki tzw. ciasteczkom (pliki cookies) serwery stron śledzą naszą aktywność w online. Wszystkie te informacje mogą trafić w niepowołane ręce i służyć m.in. do szpiegowania czy kradzieży tożsamości.

Z pomocą przychodzą narzędzia, które pozwalają zachować anonimowość w sieci oraz utrudniają cyberprzestępcom dotarcie do wrażliwych danych:

- Łączenie się z internetem za pomocą VPN (Virtual Private Network) – tzw. sieci tunelowej. Dzięki temu rozwiązaniu strony internetowe „nie widzą" Waszego rzeczywistego urządzenia, a Wasze połączenie z internetem staje się trudniejsze do wyśledzenia.

- Korzystanie z trybu incognito w przeglądarce i tymczasowych skrzynek poczty e-mail. Gdy jesteśmy w trybie prywatnym, przeglądarka nie zapisuje historii odwiedzanych stron, „ciasteczek" ani danych logowania, co minimalizuje ilość informacji, jakie pozostawiamy po sobie w systemie.

- Używanie szyfrowania end-to-end w komunikatorach internetowych. Dzięki niemu treść rozmów jest zaszyfrowana w taki sposób, że tylko nadawca i odbiorca mogą ją odczytać – dostępu do przesyłanych wiadomości nie ma nawet dostawca usługi.

Chcąc zachować anonimowość online, zwracajcie również uwagę na publikowane treści, m.in. w mediach społecznościowych (nigdy nie udostępniajcie tam np. skanów dokumentów lub innych wrażliwych informacji!). Im mniej danych ujawniacie, tym trudniej będzie je wykorzystać do wyłudzeń, kradzieży tożsamości czy innych przestępczych działań. Nawet pozornie nieistotne informacje, takie jak miejsce zamieszkania, zdjęcia z wakacji czy data urodzenia, mogą być wykorzystane w niepożądany sposób.

Warto pamiętać, że anonimowość ma też aspekt społeczny i moralny. Osoby, które ukrywają swoją tożsamość w sieci, często czują większą swobodę w wypowiadaniu opinii. Niestety, bywa to wykorzystywane w negatywny sposób – pozornie anonimowe komentarze mogą przybierać formę hejtu, obraźliwych wpisów czy cyberprzemocy. Dlatego warto pamiętać, że anonimowość nie oznacza braku odpowiedzialności. W sieci, podobnie jak w realnym świecie, nasze słowa mają konsekwencje, a anonimowość powinna służyć ochronie prywatności, a nie krzywdzeniu innych.

Czy da się na dobre zniknąć z internetu? Nie do końca, jednak ważnym krokiem w stronę anonimowości jest świadome korzystanie z prawa do bycia zapomnianym, wynikającego z rozporządzenia unijnego RODO (Ogólnego rozporządzenia o ochronie danych). Dokument ten daje osobom fizycznym, a zatem nam wszystkim, prawo żądania od administratora niezwłocznego usunięcia naszych danych osobowych i innych materiałów, które nas dotyczą. Warto jednak pamiętać, że zawsze gdzieś może się zachować kopia jakiejś informacji.

Jeśli chcecie dowiedzieć się więcej o anonimowości w internecie, koniecznie zajrzyjcie do e-kursu „Cyberprzemoc – anonimowość w sieci" dostępnego na platformie OSE IT Szkoła oraz aktualności „Jak cię widzą, tak cię piszą… Zadbaj o swój wizerunek w sieci" na stronie kompetencjecyfowe.gov.pl.

Aplikacja

Nawigacja, krokomierz, rozkład jazdy autobusów, serwisy streamingowe, komunikatory, bankowość mobilna, czytnik e-booków – z tych i innych aplikacji chętnie korzystamy na swoich urządzeniach przenośnych, takich jak smartfony czy tablety. Aplikacje ułatwiają nam wiele codziennych czynności: używanie poczty e-mail, kontakty z bliskimi, załatwianie formalności, zakupy czy oglądanie filmów lub seriali.

Na pewno znacie zalety aplikacji: należą do nich wygoda, powszechny dostęp, sprawne działanie, angażujące funkcje, możliwość personalizacji i zmiany ustawień.

Jeśli zależy Wam na bezpiecznym korzystaniu z aplikacji, musicie pamiętać o kilku zasadach. Przede wszystkim pobierajcie apki tylko z oficjalnych, bezpiecznych źródeł, czyli ze sklepów z aplikacjami przeznaczonymi dla odpowiednich systemów operacyjnych (najpopularniejsze to Google Play dla systemu Android i App Store dla systemu iOS). Pamiętajcie też o ograniczeniu uprawnień aplikacji – np. odmowie dostępu do danych lokalizacyjnych czy innych danych na urządzeniu i rozważnym dokonywaniu mikropłatności. Wreszcie – nie podawajcie swoich danych na nieznanych urządzeniach, logujcie się do nich tylko ze swojego smartfona czy tabletu.

Pamiętajcie, że każda aplikacja może mieć luki, które zagrażają Waszej prywatności. Z tego powodu regularnie przeglądajcie apki na swoim smartfonie i instalujcie aktualizacje zalecane przez producenta. Od jakiegoś czasu nie korzystacie z którejś aplikacji? Natychmiast ją usuńcie!

Jeśli jesteście rodzicami – polecamy Wam naszą aplikację ochrony rodzicielskiej mOchrona, która skutecznie pomaga w kształtowaniu dobrych postaw związanych z użytkowaniem sieci oraz diagnozowaniu potencjalnych problemów i zagrożeń.

Porady dotyczące bezpiecznego korzystania z aplikacji znajdziecie w aktualności „Bezpieczni w sieci z OSE: aplikacje mobilne" na stronie ose.gov.pl.

Atak APT

Jednym z poważniejszych zagrożeń w sieci są ataki, za które odpowiadają zorganizowane grupy specjalistów – zwłaszcza teraz, gdy mówimy nie tylko o bezpieczeństwie użytkowników, ale też bezpieczeństwie informatycznym całego państwa. Należą do nich zaawansowane, długotrwałe ataki (APT, ang. *Advanced Persistent Threat*), wykorzystywane przez podmioty stanowiące zagrożenie dla kraju. Takie ataki, zwane też atakami ukierunkowanymi, nierzadko mogą powodować szkody dla stabilności gospodarczej i politycznej państwa oraz inne istotne zakłócenia.

Ataki APT dotyczą głównie firm oferujących dostęp do nowoczesnych technologii czy zajmujących się badaniami, różnego rodzaju platform rządowych, firm energetycznych i wszystkich instytucji kluczowych z punktu widzenia bezpieczeństwa lub obronności kraju. Istotne jest jednak, by przeciętni użytkownicy internetu również mieli świadomość tego zagrożenia.

Warto wiedzieć, że ataki APT są perfekcyjnie zaplanowane i ukierunkowane na konkretną instytucję, co więcej – mogą trwać naprawdę długo. Przestępcy korzystają z różnych form tego ataku: mogą albo wykradać poufne dane, albo niszczyć dane cyfrowe lub urządzenia fizyczne. Używają też zaawansowanych technik obchodzenia zabezpieczeń (EAT – ang. *Advanced Evasion Techniques*), dzięki czemu niezauważenie funkcjonują w atakowanym systemie przez wiele tygodni lub miesięcy. Oszustom zależy przede wszystkim na zdobyciu szeroko rozumianej wartości intelektualnej, nierzadko przechowywanej wewnątrz sieci wewnętrznej atakowanych jednostek.

Atak APT rozpoczyna się od poznania ofiary – poszukiwania informacji na jej temat w internecie i przygotowania odpowiednich narzędzi oraz dotarcia do osób wewnątrz organizacji, które mają dostęp do cennych danych. W dalszej kolejności następuje instalacja oprogramowania typu backdoor, a więc wtargnięcie i uzyskanie dostępu do systemu danej firmy czy instytucji. Zbieranie istotnych informacji może następnie trwać do skutku lub dopóki atak nie zostanie wykryty.

Środkiem zaradczym po raz kolejny będą tu świadome działania: stosowanie aktualizowanych na bieżąco programów antywirusowych oraz innych zabezpieczeń użytkowanych systemów. Ważna jest też świadomość, że bezpieczeństwo formy zależy od skutecznej ochrony każdego jej ogniwa, w tym także jej wszystkich pracowników. Warto więc szkolić ich w zakresie cyberbezpieczeństwa i prowadzić akcje informacyjne – nie tylko na temat ataków APT.

Źródła:

„Encyklopedia cyberbezpieczeństwa: APT”, (2022), artykuł w serwisie instytutcyber.pl.

„Zaawansowane długotrwałe ataki (APT)”, (b.r), artykuł w serwisie 4consult.com.pl.

Atak BLE Spam i bluejacking

Z pewnością często korzystacie w swoich smartfonach (i innych urządzeniach elektronicznych) z modułu Bluetooth, który umożliwia bezprzewodową komunikację krótkiego zasięgu pomiędzy sprzętami. Dzięki niemu możecie np. sparować opaskę sportową z telefonem lub łączyć się z drukarkami, słuchawkami czy głośnikami.

Choć ta technologia zdecydowanie ułatwia życie, musicie wiedzieć, że niesie za sobą także ryzyko pewnych zagrożeń, wśród których można wymienić bluejacking (od ang. *Bluetooth* i *hijacking* – porwanie). Ten typ ataku polega na przesyłaniu niechcianych wiadomości z linkami lub reklamami za pośrednictwem modułu Bluetooth z jednego urządzenia do drugiego – które można wykryć, wyszukując dostępne sprzęty w pobliżu. Ogólnie rzecz biorąc, bluejacking jest jednym z typów ataków DoS (od ang. *Denial of Service* – odmowa dostępu), których celem jest uniemożliwienie działania systemu komputerowego lub usługi sieciowej.

W większości przypadków bluejacking jest wykorzystywany dla zabawy lub w celu nawiązania kontaktu z nieznajomymi, ale pamiętajcie: przesyłane w ten sposób linki mogą prowadzić np. do malware (złośliwego oprogramowania), stron phishingowych lub innych niebezpiecznych treści.

Jednym z przykładów bluejackingu, który być może przestraszył także i Was, był atak BLE (Bluetooth Low Energy) Spam, prowadzony swego czasu w warszawskim metrze. Jego ofiarą padali masowo użytkownicy smartfonów, laptopów i tabletów. Na czym polegał atak? Oszust, wykorzystując specjalne oprogramowanie i pasmo Bluetooth, rozsyłał setki monitów z informacją o parowaniu nieistniejącego sprzętu (np. słuchawek). Powiadomienia spływały co chwilę, zapełniając bufor pamięci urządzeń i w ostateczności doprowadzając do zawieszania systemów operacyjnych (zarówno Android, jak i iOS).

Jako że zasięg tego ataku wynosił nawet do 50 m, okazywało się, że wiele osób naraz traciło możliwość korzystania ze swoich urządzeń. Na szczęście pasażerowie metra byli bezpieczni – ich dane nie były wykradane (mogli utracić jedynie np. nagrywaną w momencie ataku wiadomość głosową). I choć finalnie atak nie okazał się poważnym zagrożeniem, zwrócił uwagę na bardzo istotne zagadnienie – w dzisiejszych czasach nie potrzeba wcale zaawansowanego sprzętu, by sparaliżować działanie urządzeń cyfrowych na określonym terenie. Warto przy tym pamiętać, że producenci na bieżąco wypuszczają poprawki do oprogramowania, które zmniejszają skuteczność również takich ataków.

Jak się chronić? Jedyne, co możecie zrobić, to wyłączać moduł Bluetooth, gdy z niego nie korzystacie, i sprawdzać, czy Wasze urządzenie jest widoczne dla innych sprzętów w okolicy. Pomoże to jeszcze lepiej zadbać o bezpieczeństwo i… oszczędzać baterię w smartfonie.

Więcej o BLE Spam przeczytacie w artykule „Ktoś od miesiąca zawiesza smartfony w warszawskim metrze. Jak to robi?" w serwisie niebezpiecznik.pl.

Atak DDoS (ang. *Distributed Denial of Service*)

Ataki typu DDoS (z ang. rozproszona odmowa usługi) to jedne z najczęstszych ataków na systemy komputerowe lub usługi sieciowe. Najprościej rzecz ujmując, ich celem jest zajęcie wszystkich wolnych zasobów komputera. Takie działanie cyberprzestępców ma uniemożliwić korzystanie z urządzenia i dostępnych na nim zasobów, a co za tym idzie – blokować funkcjonowanie usługi online (np. strony internetowej czy poczty e-mail znajdującej się na hostingu). Warto wiedzieć, że tego typu atak częściej niż w osoby fizyczne wymierzany jest w instytucje.

Rozpoznanie ataku DDoS jest możliwe po pewnych sygnałach: strona ładuje się bardzo wolno lub wcale, nagle wzrasta ilość ruchu, pojawiają się nietypowe połączenia z wielu losowych adresów IP, a usługi zależne od serwera również przestają działać.

Ataki DDoS przeprowadzane są z wielu miejsc jednocześnie, za pomocą urządzeń zainfekowanych specjalnym oprogramowaniem, połączonych w sieci zwane botnetami. Bywa, że właściciele tych komputerów nie mają świadomości, że ich urządzenie podłączone do sieci jest wykorzystywane przez niepowołane osoby. Aby nie stać się mimowolnym uczestnikiem takiego ataku, należy stosować podstawowe zasady cyberhigieny: dbać o aktualizacje sprzętu i oprogramowania, weryfikować przed kliknięciem linki otrzymane z nieznanych źródeł, zwracać szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych i nie uruchamiać ich, jeśli budzą nasze wątpliwości, a także nie instalować aplikacji i programów spoza oficjalnych sklepów i stron producentów oprogramowania.

Atak DoS (ang. *Denial of Service*)

Jak dobrze wiecie, cyberprzestępcy nie ustają w próbach utrudniania nam życia. Jedną ze stosowanych przez nich metod jest uniemożliwianie działania systemu komputerowego lub usługi sieciowej. Taki atak określa się mianem DoS (z ang. odmowa dostępu).

DoS polega na ciągłym wysyłaniu określonych typów pakietów na adres IP atakowanego serwisu, którego efektem jest przeciążenie łącza internetowego. Przestępcy mogą też wykorzystywać luki w oprogramowaniu lub niedoskonałości protokołów internetowych, angażując zasoby atakowanego serwisu (np. serwera), co skutkuje blokadą dostępu do niego lub zawieszaniem aplikacji, która próbuje wykonać trudną operację. Przeciążenie danej usługi (dużą ilością ruchu, żądań lub danych) wypełnia całą dostępną pamięć, wyczerpuje przestrzeń dyskową, spowalnia przetwarzanie informacji, a więc uniemożliwia normalne funkcjonowanie np. serwisu internetowego.

Ataki DoS mogą występować w różnych formach, ale wszystkie mają wspólny mianownik, jakim jest zakłócenie usługi w wyniku przeładowania sieci. Wyróżniamy m.in.:

- Ataki DDoS (ang. *Distributed Denial of Service*, rozproszona odmowa usługi), w których przestępcy wysyłają ruch z wielu lokalizacji jednocześnie, np. z wielu komputerów lub serwerów pozostających pod kontrolą atakującego. Bywa też, że komputery zwykłych użytkowników są infekowane wirusem, pozwalającym na określony typ aktywności w internecie bez wiedzy właściciela urządzenia. Oszust może zdalnie uruchamiać atak DoS na wskazany serwis właśnie przy użyciu tych „komputerów zombie".

- Ataki DRDoS (ang. *Distributed Reflected Denial of Service*, rozproszona odbita odmowa dostępu), wykorzystujące tzw. wzmocnienie odbicia – polegające na podszywaniu się przez atakującego pod adres IP celu i wysyłaniu żądań. Serwer odpowiada wówczas na większą niż normalnie liczbę zapytań, co wysyca łącze internetowe i skutkuje jego zablokowaniem. Ta metoda nie wymaga infekowania urządzeń wirusem, wystarczy odpowiednio spreparowane żądanie wysłane na przypadkowe adresy IP w internecie.

Jak rozpoznać objawy ataku DoS? Przede wszystkim Wasza witryna lub usługa nagle spowolni swoje działanie lub stanie się niedostępna. Wówczas pomocne okażą się narzędzia do analizy ruchu, które wykryją np. nietypowe wzorce ruchu na stronie lub podejrzane ilości ruchu pochodzące z zakresu jednego adresu IP.

Ataki DoS wpływają na stan dostępności danej witryny. Przerwy w dostępie (bo tym właśnie są efekty tych ataków dla zwykłych użytkowników) mogą skutkować utratą zaufania do marki, spadkiem liczby użytkowników lub nawet uszkodzeniem fizycznych elementów obsługujących konkretne zasoby. Jedyną metodą ochrony jest instalowanie specjalnego oprogramowania zabezpieczającego. Warto też mieć plan reakcji w przypadku wykrycia ataku DoS.

Źródło:

„Czym jest atak DoS”, (2022), artykuł w serwisie instytutcyber.pl.

Atak siłowy

Używacie prostych haseł typu 123456, qwerty, ania1? A może logujecie się tym samym hasłem do różnych witryn w sieci? Zmieńcie to! W takich przypadkach jesteście narażeni na atak siłowy (z ang. *brutal force* – „brutalna siła”), co wcale nie oznacza, że ktoś będzie chciał zmusić Was przemocą do podania danych do logowania. Jeśli Wasze hasło jest krótkie i przewidywalne, złodziej wykradnie je bez Waszej wiedzy – i w to kilka sekund. W jaki sposób?

Atak siłowy polega na zgadywaniu metodą prób i błędów: haseł, kodów PIN, kluczy szyfrowania. W tym celu przestępcy wykorzystują komputery z dużą mocą obliczeniową, a także kombinacje haseł składających się z liter, cyfr i znaków specjalnych. Złamanie słabego, przewidywalnego szyfru to tylko kwestia czasu.

Warto wiedzieć, że w ramach ataku siłowego istnieje kilka sposobów na przejęcie Waszych danych uwierzytelniających. Jednym z nich jest atak słownikowy, polegający na tym, że przestępcy wykorzystują popularne słowa i frazy, ale też hasła uzyskane podczas wycieków danych, po to, by przewidzieć możliwe kombinacje. Tworząc hasła, korzystajcie więc z nieoczywistych połączeń słownych, co zmniejszy szansę złodziei na złamanie Waszego zabezpieczenia.

Inną metodą stosowaną w ramach ataku siłowego jest credential stuffing (z ang. upychanie poświadczeń). Złodzieje po uzyskaniu Waszych danych uwierzytelniających do któregoś z kont będą próbowali użyć ich na innych platformach. Pamiętajcie więc, by nie korzystać z tego samego hasła dla różnych witryn!

Podpowiadamy, jak jeszcze bronić się przed atakiem siłowym.

- **Silne hasło** – to podstawa! CERT Polska rekomenduje stosowanie unikatowych haseł składających się z przynajmniej pięciu słów. Mogą to być zmodyfikowane cytaty z frazą w obcym języku, np. DwaBialeLatajace**Sophisticated**Króliki. Jakich haseł na pewno powinniście się wystrzegać? Sprawdźcie listę najpopularniejszych haseł opublikowaną przez CERT Polska. Znajdziecie tam przykłady zabezpieczeń, które można łatwo złamać.

- **Więcej niż hasło** – wszędzie, gdzie się da, stosujcie uwierzytelnianie dwuskładnikowe lub wieloskładnikowe, czyli oprócz hasła logujcie się do witryny dodatkowymi składnikami, np. kodem otrzymanym SMS-em, odciskiem palca czy kluczem U2F.

- **Generatory haseł** – możecie z nich korzystać podczas tworzenia losowych kombinacji różnych znaków, które mają Wam zapewnić silne zabezpieczenie.

- **Czujność** – na stronie bezpiecznedane.gov.pl możecie sprawdzić, czy Wasze hasła wyciekły. Jeśli tak, koniecznie zmieńcie swoje dane uwierzytelniające!

Więcej o zasadach tworzenia silnych haseł i ochrony przed atakami przeczytacie na stronie CERT Polska w poradniku „Kompleksowo o hasłach", a także w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: wyciek danych".

Atak słownikowy

Na pewno wielokrotnie słyszeliście, jak ważne jest używanie silnych haseł, które zabezpieczają Wasze konta pocztowe, bankowe czy społecznościowe. Jeśli jednak nie wzięliście tych ostrzeżeń poważnie i wciąż używacie oczywistych, łatwych do złamania zabezpieczeń, narażacie się na ataki słownikowe (ang. *dictionary attack*), będące odmianą ataków siłowych.

Cyberprzestępcy, chcąc złamać Wasze hasło, wykorzystują powszechnie używane frazy – liczą na to, że z pośpiechu, wygody lub (niestety) lenistwa skorzystaliście z oczywistych ciągów liter lub cyfr. Jeśli używacie haseł takich jak „12345", „qwerty", „zaq123wsx" lub wplatacie w nie ważne daty (np. urodzenia) czy imiona, ułatwiacie oszustom zadanie. Co ważne, ataki słownikowe to niejedyne incydenty, które zagrażają Waszym hasłom, a tym samym bezpieczeństwu Waszych kont. Dane logowania mogą zostać upublicznione także w wyniku wycieku – osoby nieuprawnione wchodzą wówczas w posiadanie poufnych informacji na Wasz temat.

Ataki słownikowe mogą bazować na gotowych lub zmodyfikowanych (np. w zakresie wielkości liter lub dodawania znaków specjalnych) listach pochodzących z wycieków danych lub publicznych zestawień najpopularniejszych haseł. Bywa też, że oszuści korzystają ze słowników branżowych i próbują włamywać się na konta np. na forach inwestycyjnych, używając listy haseł zawierających frazy dotyczące tej konkretnej dziedziny (Łużak, 2024).

Warto znać różne typy ataków słownikowych – należą do nich credential stuffing (czyli zautomatyzowane próby logowania wykorzystujące skradzione w sieci loginy i hasła przypisane do konkretnych użytkowników) oraz password spraying (czyli próby uzyskania dostępu do kilku kont w jednej domenie przy użyciu listy popularnych haseł).

Czy Wasze hasła należą do tych najczęściej używanych przez użytkowników? Sprawdźcie je w polskiej wersji słownika haseł dostępnej na stronie cert.pl. Na liście znajduje się około miliona haseł ujawnionych w wyciekach, posortowanych od najpopularniejszych do tych rzadszych.

Aby ochronić się przed atakami słownikowymi (i wszelkimi próbami łamania Waszych haseł), musicie pamiętać o kilku ważnych zasadach:

- Nie używajcie w hasłach danych osobowych ani innych informacji, które jednoznacznie się z Wami kojarzą.
- Unikajcie potocznych zwrotów, nazwisk celebrytów, nazw restauracji i innych oczywistych fraz (np. kolejnych liter na klawiaturze), uważajcie na frazy notowane w słowniku haseł.
- Stosujcie unikalne hasła dla wszystkich swoich kont.
- Twórzcie hasła składające się z min. 14 znaków, najlepiej będące zdaniem złożonym z przynajmniej pięciu słów. Jako inspiracja mogą posłużyć Wam cytaty, przysłowia lub fragmenty piosenek, które jednak zmienicie w sprytny i znany tylko Wam sposób (np. Wlazł**Kostek**NaMostekI**Stuka**).
- Używajcie generatorów haseł bez obaw, że zapomnicie swoje szyfry. Pomogą Wam menedżery haseł, które przechowują i automatycznie wpisują Wasze zabezpieczenia, gdy chcecie się zalogować.
- Tam, gdzie to możliwe, stosujcie uwierzytelnianie dwuskładnikowe lub wieloskładnikowe. Jeśli przestępcy uda się odgadnąć Wasze hasło, nadal będzie potrzebował drugiego

elementu niezbędnego do weryfikacji tożsamości, np. hasła generowanego przez specjalną aplikację lub odcisku Waszego palca. Z założenia tym dodatkowym składnikiem jest „coś, co znacie", „coś, co macie" lub „coś, czym jesteście", więc nikt oprócz Was nie powinien móc zalogować się na Wasze konto, nawet posiadając hasło.

Więcej porad znajdziecie w poradniku CERT Polska „Kompleksowo o hasłach". Zajrzyjcie też do aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe".

Źródło:

Łużak T., (2024), „Atak słownikowy – na czym polega i jak się przed nim chronić?", artykuł w serwisie netia.pl.

Awatar

Jak być rozpoznawalnym w internecie, a jednocześnie nie pokazywać zbyt wiele? Z pomocą jak zwykle przychodzi technologia, dzięki której możemy stworzyć swojego reprezentanta w wirtualnym świecie.

Zapewne nie raz spotkaliście się w sieci – na forach dyskusyjnych, w grach czy mediach społecznościowych – z ikonką, obrazkiem, grafiką, które mają oddać wizerunek jakiegoś użytkownika sieci. To awatar – dzięki niemu możemy zaznaczyć swoją obecność online bez pokazywania rzeczywistego wizerunku. Awatar może przybierać różne formy: człowieka podobnego (bądź nie) do nas, zwierzęcia, maskotki – ograniczeniem jest tylko nasza wyobraźnia. Istnieją specjalne narzędzia do tworzenia tego typu postaci.

Tak było jeszcze do niedawna, bo wraz z rozwojem sztucznej inteligencji (ang. *artificial intelligence*, AI) pojawiła się możliwość wygenerowania awatara AI. To odpowiednik nas samych, postać, która wygląda, mówi, porusza się jak my. Jest też w stanie w czasie rzeczywistym reagować na daną sytuację. Wyobraźcie sobie, że jesteście nauczycielem i za pomocą swojego awatara przeprowadzacie wirtualne lekcje: tłumaczycie trudne koncepcje, wykonujecie symulacje i udzielacie odpowiedzi na pytania. Na pewno znacie takie rozwiązania z filmów. Dziś są one dostępne dzięki sztucznej inteligencji. Ponadto awatary AI możemy generować w grach komputerowych. Dzięki nim gracze mogą tworzyć bardzo realistyczne (lub fikcyjne, ale nadal dające poczucie autentyczności) postacie i reagować na działania innych członków rozrywki online. Takie możliwości daje np. wirtualna rzeczywistość (ang. *virtual reality*, VR).

Użycie awatarów w formie obrazka lub grafiki może wiązać się z niewielkimi zagrożeniami, np. z fałszywym przekonaniem, że jesteśmy w sieci całkowicie anonimowi. Większe ryzyko dostrzega się w rozwoju awatarów AI i związanej ze sztuczną inteligencją technologii deepfake, za pomocą której tworzy się zmanipulowane filmy. Z tego rozwiązania korzystają też internetowi oszuści. Są oni w stanie wygenerować np. nagranie z udziałem znanego polityka lub celebryty zawierające nieprawdziwe, niewiarygodne informacje lub przeprowadzić cyberporwanie, wykorzystując zmanipulowany film, który przedstawia rzekomo uprowadzoną bliską nam osobę.

Ochroną przed cyberatakami tego typu jest dbanie o swoją prywatność w sieci. Z rozwagą twórzcie więc swój cyfrowy ślad i wszędzie, gdzie to możliwe, stosujcie ustawienia prywatności, szczególnie w mediach społecznościowych. Nie każdy musi mieć dostęp do publikowanych przez Was informacji. Korzystajcie też z prawa do bycia zapomnianym – jeśli w sieci znajdują się dotyczące Was treści, możecie prosić o ich usunięcie. Takie prawo wynika z Ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Ponadto pamiętajcie, że zbytnie zaangażowanie w świat VR i utożsamianie się ze swoim wirtualnym reprezentantem może kształtować Wasze postawy, przekonania i odczucia. W korzystaniu z nowych technologii należy więc zachować umiar.

B

Backdoor

To pojęcie możemy przetłumaczyć jako „tylne drzwi” lub „furtka”. Co ma wspólnego z bezpieczeństwem w sieci? Backdoor to nic innego jak umyślnie pozostawiona luka w zabezpieczeniach systemu komputerowego. Celem tego działania jest późniejsze wykorzystanie „szczeliny” w oprogramowaniu do bardzo niebezpiecznych działań. Backdoor może zostać pozostawiony przez malware – złośliwe oprogramowanie, cyberprzestępcę, ale też umyślnie stworzony przez autora danego programu, np. w celu serwisowania systemu.

Backdoor może być ukryty w wielu miejscach: w aplikacjach, systemach operacyjnych, urządzeniach IoT (internet rzeczy) czy w oprogramowaniu wbudowanym w sprzęt, np. routera lub dysku twardego. Niestety „tylne drzwi” mogą być ogromnym zagrożeniem. To furtka do:

- kradzieży danych – haseł i innych poufnych informacji, dokumentów, zdjęć;
- instalacji złośliwego oprogramowania;
- przejęcia kontroli nad zainfekowanym systemem – np. do wykorzystania go w atakach typu DDoS.

Jak chronić się przed backdoorem? Zawsze powinniście pamiętać o zasadach bezpiecznego korzystania z urządzeń cyfrowych:

- Nie ignorujcie komunikatów o dostępnych aktualizacjach. To nie tylko poprawki błędów, ale przede wszystkim łatki bezpieczeństwa, które zamykają znane luki. Zaktualizowany system, program (w tym antywirusowy) będzie znacznie trudniejszy do sforsowania.
- Stosujcie silne hasła, a wszędzie, gdzie to możliwe – uwierzytelnianie dwuskładnikowe (2FA) lub uwierzytelnianie wieloskładnikowe (MFA). Nawet jeśli ktoś pozna Wasze hasło, bez drugiego i trzeciego składnika (np. kodu z aplikacji lub SMS-a i odcisku palca) nie dostanie się do Waszego konta czy urządzenia.
- Korzystajcie z zapory sieciowej firewall – to jeden z prostszych i skuteczniejszych sposobów zabezpieczenia sieci przed włamaniem, infekcją wirusami komputerowymi i próbami szpiegowania. Pamiętajcie, że Wasze domowe routery często mają wbudowane firewalle, ale należy sprawdzić, czy są aktywne.
- Pobierajcie oprogramowanie, aplikacje i inne narzędzia tylko ze sprawdzonych źródeł – instalowanie plików z nieoficjalnych, podejrzanych stron, na których znajdują się np. „darmowe wersje premium”, to prosta droga do infekcji sprzętu i otwarcia furtki cyberprzestępcom.
- Weryfikujcie **linki** otrzymane z nieznanych źródeł przed kliknięciem – zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych i nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości. Pamiętajcie, że **phishing** to sposób na uzyskanie dostępu do Waszych danych!

Źródło:

„Co to jest Backdoor?”, (b.r.), artykuł na stronie nflo.pl.

Backup

Urządzenia cyfrowe to dla wielu z nas prawdziwe kopalnie wspomnień – zdjęć, filmów i innych plików, mających wartość sentymentalną. Co w sytuacji, gdy utracicie Wasz sprzęt lub znajdujące się na nim pliki? Wtedy przyda się backup! To kopia zapasowa danych przechowywana w innych miejscach niż ich oryginalne wersje. Dzięki temu rozwiązaniu możecie zabezpieczyć

ważne materiały przed utratą, np. na skutek usunięcia plików, kradzieży lub zainfekowania sprzętu malware – złośliwym oprogramowaniem. Najprościej mówiąc, backup to taki cyfrowy plan B, który pozwoli Wam szybko i bez zbędnego stresu odzyskać utracone dane.

Jak przygotować się do stworzenia backupu? Na początek określcie, które dane są dla Was najcenniejsze. Zazwyczaj będą to: zdjęcia i filmy, dokumenty (np. umowy, prace twórcze), pliki projektowe, ważne wiadomości e-mail. Dobrą praktyką jest także tworzenie kopii całych systemów operacyjnych – dzięki temu, w razie awarii, szybko przywrócicie pełne środowisko pracy.

W kolejnym kroku wybierzcie miejsce do przechowywania. Macie kilka opcji:

- **Nośniki fizyczne** (np. dyski zewnętrzne czy pendrive'y) – dają pełną kontrolę nad danymi i działają offline, ale są podatne na uszkodzenia lub zgubienie.
- **Chmura** – umożliwia dostęp do danych z dowolnego miejsca i automatyczną synchronizację. Wybierając usługę chmurową, postawcie na sprawdzonego dostawcę.
- **Serwery NAS** (ang. *Network Attached Storage*) – to urządzenia podłączone do sieci, które pozwalają na tworzenie kopii zapasowych z wielu urządzeń. Dobre rozwiązanie dla firm i domów, gdzie potrzebny jest dostęp z różnych lokalizacji.

Jeśli przechowujecie kopie zapasowe na fizycznych nośnikach lub w chmurze, warto je zaszyfrować. Dzięki temu tylko Wy będziecie mieć dostęp do swoich danych, nawet jeśli nośnik trafi w niepowołane ręce.

I jeszcze podpowiedź, podczas zabezpieczania swoich danych stosujcie zasadę 3-2-1: 3 kopie danych – trzy wersje backupu w różnych lokalizacjach; 2 różne typy nośników – np. dysk zewnętrzny i chmura; 1 kopia offline – odłączona od internetu, odporna na ataki ransomware.

Zastanawiacie się, jak często robić backup? Najlepiej ustalić stały harmonogram tworzenia kopii zapasowych. Możecie wybrać: automatyczne backupy – wygodne i bezobsługowe, dostępne w wielu usługach chmurowych, lub ręczne backupy – dają większą kontrolę, ale wymagają systematyczności (np. raz w tygodniu). W przypadku często aktualizowanych plików warto robić kopie na bieżąco.

Nie zapominajcie też o regularnym testowaniu możliwości odzyskania danych, najlepiej co kilka miesięcy. To szczególnie ważne przed wymianą sprzętu lub dużą aktualizacją systemu.

Backup to łatwe i mało kosztowne rozwiązanie, które w przypadku niekorzystnych zdarzeń losowych może zaoszczędzić Wam wiele czasu, nerwów i pieniędzy. Dlatego warto wyrobić w sobie nawyk tworzenia kopii zapasowych.

Jak przygotować się do stworzenia backupu? Więcej informacji znajdziecie w aktualnościach „Zrób kopię zapasową!", „Bezpieczni w sieci z OSE na wakacje: kopie zapasowe" na stronie ose.gov.pl oraz w tekście „Masz już swój plan B?" dostępnym na platformie OSE IT Szkoła. Zajrzyjcie też do biuletynu „OUCH! – Czy robisz kopie zapasowe" opublikowanego na stronie CERT Polska.

Bankowość internetowa

Razem z wieloma innymi dziedzinami życia do internetu przeniosło się też zarządzanie naszymi finansami. Nie musicie już iść do banku, by wpłacić pieniądze na rachunek czy zrobić przelew, nie czekacie na papierowy wyciąg z konta – kontrolę nad swoimi środkami możecie mieć praktycznie 24 godziny na dobę dzięki bankowości internetowej. Na czym to polega?

Dzięki bankowości internetowej macie dostęp do usług bankowych za pośrednictwem sieci, a dokładnie strony Waszego banku. Po zalogowaniu, czyli podaniu loginu i hasła, macie dostęp nie tylko do historii transakcji czy ustawień swojego konta, ale też możecie robić przelewy, płacić rachunki, ustawiać zlecenia stałe itp. To samo – i jeszcze więcej – umożliwia bankowość mobilna, z której skorzystacie dzięki hasłu na swoim smartfonie. W apce macie szerszy wachlarz

dostępnych płatności, np. zapłacicie tu BLIK-iem czy uwierzytelnicie transakcje. Takie aplikacje są intuicyjne i łatwe w obsłudze, nie musicie się ich bać!

Choć korzystanie z bankowości internetowej i/lub mobilnej jest wygodne i przyjemne, pamiętajcie o podstawowych zasadach bezpieczeństwa. Dzięki temu unikniecie przykrych sytuacji, gdy oszust próbuje wyłudzić Wasze dane osobowe lub pożyczkę na Wasze nazwisko. Jak się przed tym zabezpieczyć?

- Używajcie silnych haseł albo zabezpieczeń biometrycznych.
- Ustawcie uwierzytelnianie dwuskładnikowe, dzięki czemu będziecie mieć pewność, że tylko Wy macie dostęp do Waszego konta.
- Ustalcie niewielkie dzienne limity transakcji, które uniemożliwią złodziejowi przelanie dużych kwot naraz. Jeśli planujecie większe zakupy, takie limity można szybko zmienić na wyższe!
- Ustawcie w aplikacji bankowej powiadomienia o każdej transakcji – wtedy od razu zauważycie podejrzany ruch na koncie. W takiej sytuacji od razu skontaktujcie się z bankiem.
- Weryfikujcie e-maile i SMS-y od banku, nawet jeśli na pierwszy rzut oka wydaje Wam się, że są prawdziwe. Wiadomości, w których ktoś prosi Was o szybkie działanie czy podanie danych osobowych, mogą świadczyć o phishingu!
- Zwracajcie też uwagę na rzekomych konsultantów bankowych, którzy informują Was telefonicznie o dziwnej transakcji lub braku dostępu do konta. W takich przypadkach rozłączcie się i zadzwońcie na infolinię banku, żeby potwierdzić tożsamość Waszego rozmówcy (coraz częściej możecie zrobić to też w aplikacji). Pamiętajcie: dzwoniący do Was konsultant nie powinien prosić o podawanie danych osobowych – z założenia wie, do kogo dzwoni i nie musi tego weryfikować. Podawania danych będą wymagać tylko fałszywi konsultanci.
- Na bieżąco śledźcie ostrzeżenia przed oszustwami publikowane w mediach społecznościowych i komunikatach na stronie Waszego banku oraz CERT Polska.
- Zanim dokonacie płatności w internecie, postarajcie się sprawdzić, czy strona, na której się znajdujecie, jest prawdziwa, a domena w pasku adresu jest poprawna, np. nie zawiera literówek.
- Pamiętajcie też o podstawowych zasadach cyberhigieny: używajcie programu antywirusowego i aktualizujcie go na bieżąco (bez obaw korzystajcie także z wbudowanych antywirusów, które aktualizują się automatycznie!). Nie podawajcie nikomu swoich danych dostępowych do bankowości internetowej, uważajcie na szkodliwe oprogramowanie, które możecie pobrać np. jako załącznik do nieoczekiwanego maila.

Szczegółowych informacji o bezpieczeństwie bankowości internetowej szukajcie na stronie cert.pl w poradniku „Kompleksowo o hasłach” i w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: BLIK i płatności internetowe” oraz „Bezpieczni w sieci z OSE na wakacje: bankowość mobilna”.

Bańka informacyjna

Wiedzieliście, że w sieci łatwo można wpaść w tzw. bańkę informacyjną (filtrującą)? Co więcej – sami się w niej zamykamy! Z bańką informacyjną możecie mieć do czynienia wtedy, gdy w internecie otrzymujecie wyselekcjonowane wiadomości, wybrane dla Was w wyniku działania określonych algorytmów. Jak to się dzieje? Algorytmy dobierają informacje podobne do tych, których wcześniej szukaliście – możliwie najbardziej atrakcyjne i odpowiadające Waszym potrzebom. Zwykle bazują też na wiedzy zgromadzonej o użytkowniku przez dany portal, np. na podstawie Waszej historii wyszukiwania.

Jakie mogą być skutki utknięcia w bańce filtrującej? Wśród nieprzyjemnych konsekwencji można wymienić m.in.: zamknięcie na nowe pomysły, tematy i ważne wiadomości, ograniczenie dostępu do innych punktów widzenia niż własny, jak również większą podatność na manipulację, propagandę i dezinforamcję.

Warto pamiętać, że w sieci trudno jest uciec przed fałszywymi informacjami, które mogą do nas trafić na wiele sposobów – poprzez media, liderów opinii bądź zwykłych użytkowników internetu, ale także przez boty, czyli zautomatyzowane konta w mediach społecznościowych. Jeśli lubicie „sensacyjne wiadomości" i często klikacie w „szokujące nagłówki", z pewnością takie treści będą do Was często trafiały i zamykały Was w bańce informacyjnej. Dlatego warto nauczyć się demaskować każdy przejaw dezinformacji, by nie wpaść w otchłań zmanipulowanych treści, a przede wszystkim nie przyczyniać się do szerzenia nieprawdy, np. poprzez udostępnianie postów. Jak to zrobić?

- **Odróżniajcie informację od opinii** – informacja to coś, co można zweryfikować, a opinia to czyjś punkt widzenia. Jeśli źródło jest anonimowe, traktujcie je z ostrożnością – wiarygodność może być wątpliwa.
- **Korzystajcie z zaufanych źródeł** – takich jak renomowane media, eksperci, sprawdzeni dziennikarze czy organizacje fact-checkingowe. Ale pamiętajcie, nawet najlepsi mogą się pomylić, więc zanim uznacie coś za pewnik, poszukajcie pierwotnego źródła.
- **Nie ulegajcie emocjom** – jeśli coś brzmi zbyt sensacyjnie, prawdopodobnie zostało podkoloryzowane. Zatrzymajcie się i pomyślcie, zanim klikniecie i udostępnicie dalej.
- **Traktujcie media społecznościowe z przymrużeniem oka** – to nie serwisy informacyjne i każdy może tam napisać, co chce. Dlatego warto podchodzić do treści publikowanych w social mediach z dystansem i zdrowym rozsądkiem.

Skorzystajcie z naszych materiałów, w których znajdziecie niezbędne informacje na temat ochrony przed nieprawdziwymi treściami. Na stronie OSE IT Szkoła, oprócz kursu „(Dez)informacja, czyli w co wierzyć w internecie?" i zawartych w nim scenariuszy, znajdziecie: ulotkę „Fake newsy, bańki informacyjne, teorie spiskowe", konspekt zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole", infografikę „Jak rozpoznać fake newsa?". Sięgnijcie też po aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: metody i techniki dezinformacji" oraz „Bezpieczni w sieci z OSE: dezinformacja w mediach społecznościowych".

Baza danych

Czy wiecie, że każdego dnia korzystacie z różnych baz danych? Robicie to m.in. podczas używania wyszukiwarek internetowych, sprawdzania rozkładów jazdy pociągów lub autobusów, a nawet… wypłacania pieniędzy z bankomatu!

Większość systemów informatycznych wykorzystuje właśnie bazy danych – czym więc one są? Bazą danych nazywamy zbiór informacji zapisanych według ściśle określonych reguł. Celem gromadzenia danych jest ich późniejsze wykorzystanie, dlatego dzięki określonym zasadom możemy zachowywać porządek na etapie ich przechowywania, a także poprawnie je interpretować.

Zapewne wielokrotnie słyszeliście o wyciekach danych z baz, które zawierały dane osobowe, wrażliwe informacje na temat pacjentów, ich historii leczenia czy szczegóły dotyczące zakupów online. Tego typu dane mogą zostać wykorzystane nie tylko do uzyskiwania informacji na temat konkretnej osoby, ale również do przeprowadzania oszustw, prześladowania ofiar czy wyłudzeń.

Pamiętajcie, jeśli zauważycie, że Wasze dane zostały ujawnione, przeskanujcie komputer za pomocą programu antywirusowego – to pomoże wykryć ewentualne zagrożenia. Następnie natychmiast zmieńcie wszystkie hasła do swoich kont – poczty e-mail czy mediów społecznościowych. Ponadto wszędzie, gdzie to możliwe, włączcie dodatkowe zabezpieczenia – uwierzytelnianie dwuskładnikowe. Koniecznie zawczasu zastrzeżcie swój numer PESEL, by zapobiec np. próbom wyłudzenia kredytu na Wasze nazwisko – możecie to zrobić np. w aplikacji mObywatel.

Trzymajcie rękę na pulsie, upublicznienie poufnych informacji, dostępnych w różnego rodzaju bazach danych i serwisach internetowych, to częste incydenty bezpieczeństwa. Dlatego regularnie sprawdzajcie, czy Wasze dane nie wyciekły, np. na stronie bezpiecznedane.gov.pl. Śledźcie też komunikaty administratorów danych, którzy mają obowiązek informować klientów o wycieku. I bądźcie na bieżąco z informacjami o cyberzagrożeniach – zaglądajcie np. na Facebooka CERT Polska.

Więcej o wyciekach danych przeczytacie na stronie ose.gov.pl w naszej aktualności „Bezpieczni w sieci z OSE: wyciek danych". Skorzystajcie też z kursów e-learningowych zamieszczonych na platformie OSE IT Szkoła – dzięki bezpłatnym materiałom zdobędziecie wiedzę na temat baz danych oraz zasad ich tworzenia.

Bezpieczne przesyłanie plików

W dobie cyfryzacji przesyłanie – często dużych – plików stało się nieodłącznym elementem naszej pracy i codziennego życia. Opcji jest wiele: możecie korzystać z rozwiązań chmurowych, platform umożliwiających współdzielenie dokumentów lub internetowych narzędzi do transferu dużych plików. Niezależnie od tego, czy dzielicie się dokumentami z kolegami z pracy, czy wysyłacie zdjęcia do znajomych, ważne jest, abyście zadbali o bezpieczeństwo przesyłanych danych.

Podstawową metodą ochrony plików przed nieautoryzowanym dostępem jest ich szyfrowanie. Dzięki niemu Wasze dane będą zabezpieczone, a nawet jeśli plik zostanie przechwycony, nie będzie można go odczytać bez odpowiedniego klucza. Wybierajcie platformy, które oferują szyfrowanie end-to-end – będziecie wówczas mieć pewność, że przesyłane pliki będą zaszyfrowane nie tylko podczas przesyłania, ale także w momencie ich przechowywania na serwerach. Warto wiedzieć, że wiele platform pozwala na ograniczenie czasu, przez jaki odbiorca może mieć dostęp do pliku. Ustawiając datę wygaśnięcia dostępu, minimalizujecie ryzyko, że przesyłane dokumenty, zdjęcia czy inne treści zostaną niewłaściwie użyte w przyszłości. Możecie także skorzystać z jednorazowych linków, które wygasają po pierwszym otwarciu.

Jeśli nie chcecie szyfrować swoich plików (lub nie macie na to czasu, zwłaszcza gdy przesyłacie pliki sporych rozmiarów), możecie przynajmniej spakować pliki do archiwum – czyli do formatu .rar, .zip, .7zip – i opatrzyć je hasłem. Bez znajomości tego klucza uruchomienie pliku i jego wypakowanie będzie niemal niemożliwe.

Unikajcie przesyłania poufnych dokumentów za pośrednictwem tradycyjnej poczty e-mail czy niezaszyfrowanych komunikatorów. Co więcej, zanim wyślecie komuś swój plik, upewnijcie się, że trafia on do właściwej osoby. W przypadku wątpliwości skontaktujcie się z odbiorcą i potwierdźcie jego tożsamość, np. przez telefon.

Bezpieczeństwo plików zależy także od aktualności oprogramowania, z którego korzystacie. Regularnie aktualizujcie system operacyjny, przeglądarki, aplikacje oraz programy antywirusowe, aby zabezpieczyć się przed nowymi zagrożeniami. Pamiętajcie też o innych zasadach bezpiecznego poruszania się w sieci:

- Używajcie tylko oprogramowania pochodzącego z oficjalnych, sprawdzonych źródeł.
- Korzystajcie z silnych zabezpieczeń (hasła i uwierzytelniania dwuskładnikowego lub wieloskładnikowego) oraz VPN (ang. *Virtual Private Network*) – sieci, która szyfruje połączenie internetowe, chroniąc dane przed przechwyceniem.
- Udostępniajcie pliki tylko tym osobom, które rzeczywiście potrzebują do nich dostępu.
- Jeśli otrzymujecie od kogoś link do pobrania plików, skontaktujcie się z nadawcą (najlepiej telefonicznie) i upewnijcie się, czy to faktycznie on przesłał Wam jakieś treści.

Źródło:

Górecki M., (2021), „Bezpieczne przesyłanie dużych plików", artykuł w serwisie politykabezpieczenstwa.pl.

B

Biały wywiad, OSINT

OSINT (z ang. *open-source intelligence*) oznacza biały wywiad, czyli wyszukiwanie, gromadzenie i analizowanie informacji z różnych, ogólnodostępnych źródeł na temat firm, organizacji, osób. W przeciwieństwie do czarnego wywiadu, który wykorzystuje nielegalne metody pozyskiwania wiadomości – np. oprogramowanie szpiegujące, podsłuchy telefoniczne, socjotechnikę – biały wywiad jest legalny. Z założenia osoby stosujące OSINT działają zgodnie z prawem, choć warto podkreślić, że biały wywiad mogą też prowadzić cyberprzestępcy. Ważny jest cel gromadzenia informacji i sposób ich wykorzystania.

Nie jest tajemnicą, że OSINT wykorzystują służby, firmy, organizacje, ale też pracodawcy lub osoby prywatne. Zbiór danych, odpowiednio zinterpretowanych, może stanowić bardzo ważne źródło wiedzy. Czy trudno jest pracować w białym wywiadzie? I tak, i nie. Czasem potrzebne informacje mamy dosłownie na wyciągnięcie ręki, bo np. wszelkie materiały można znaleźć w sieci, a czasem trzeba poszukać głębiej, np. w rejestrach państwowych, a te nie zawsze są dostępne online. Cała sztuka polega jednak na uporządkowaniu okruchów informacji, ich analizie oraz przygotowaniu spójnego i wiarygodnego zbioru danych.

W kontekście białego wywiadu nie sposób nie wspomnieć o konieczności ochrony prywatności w sieci. Spróbujcie wykonać OSINT na swoim przykładzie i wyszukać online informacje na swój temat.

Jeśli korzystacie z mediów społecznościowych, a Wasze profile są otwarte, na pewno przekonacie się, jak wiele wiadomości o sobie udostępniacie. Każdy detektyw OSINT bez trudu ustali Waszą datę urodzenia, miejsce pracy, a nawet historię zatrudnienia. Pozna Waszych znajomych, członków rodziny, ulubione miejsca, które odwiedzacie, aktywności poza domem i pracą. Zainteresowani Waszym życiem bez problemu ustalą też adres zamieszkania czy numer telefonu, poznają firmowe dokumenty, np. sprawozdania, także adres IP Waszego komputera czy metadane z opublikowanych w sieci zdjęć (np. dane geolokalizacyjne). Dużo informacji, prawda? Pomyślcie, co może się stać, jeśli trafią one w niepowołane ręce.

Cyberprzestępcy potrafią zrobić użytek z każdej wiadomości. Znając wiele szczegółów z Waszego życia, mogą np. przygotować precyzyjny atak phishingowy, uwiarygodnić cyberporwanie czy przeprowadzić doxing, czyli zebrać informacje o Was i upublicznić te wpływające na bezpieczeństwo i wizerunek.

Jak bronić się przed białym wywiadem? Przede wszystkim dbajcie o swoje cyfrowe ślady zostawiane w sieci. Oto kilka zasad, które warto wdrożyć:

- **Zastanówcie się, zanim coś opublikujecie!** W internecie nic nie ginie, z rozwagą dzielcie się więc informacjami o sobie. Na pewno nie udostępniajcie w sieci prywatnych informacji typu numer telefonu, adres zamieszkania, e-mail.
- **Pamiętajcie o ukrytych danych**. Zdjęcia, filmy i inne dokumenty mogą zawierać informacje o ich autorze, czasie utworzenia czy lokalizacji. Kontrolujcie, jakie dane udostępniacie przy okazji aktywności w sieci. Pomocne może być wyłączenie funkcji geolokalizacji w smartfonie.
- **Wybierajcie konto prywatne zamiast publicznego**. W mediach społecznościowych dbajcie o ustawienia prywatności – nie każdy musi mieć dostęp do publikowanych przez Was treści.
- **Bądźcie asertywni.** Reagujcie, jeśli ktoś bez Waszej zgody udostępnił w internecie materiał zdradzający szczegóły z Waszego życia lub przedstawiający Was w niekorzystnym świetle. Ustalcie wcześniej z rodziną i znajomymi zasady zamieszczania online wspólnych zdjęć i filmików.
- **Chrońcie się przed kradzieżą danych.** Uważajcie na phishing, stosujcie silne hasła, uwierzytelnianie dwuskładnikowe, aktualizujcie aplikacje i oprogramowanie, w tym

antywirusowe. Pamiętajcie też o wylogowaniu się z urządzenia, blokadzie telefonu, jeśli go nie używacie.

- **Zapoznajcie się z polityką prywatności.** Za każdym razem, gdy zaczynacie korzystać z nowego portalu lub aplikacji, przeczytajcie zasady ochrony prywatności. Niektóre z nich zawierają zapisy dotyczące dostępu do zbyt wielu Waszych informacji, np. galerii zdjęć czy listy kontaktów w telefonie.
- **Korzystajcie z prawa do bycia zapomnianym.** Zawsze możecie prosić o usunięcie z internetu materiałów, które Was dotyczą. Takie prawo wynika z rozporządzenia unijnego RODO (Ogólnego rozporządzenia o ochronie danych).

Źródło:

„Co to jest OSINT (biały wywiad) i jak przebiega?", (2024), artykuł w serwisie bezpiecznyinternet.edu.pl.

BLIK

Wraz z rozwojem e-usług swoją ofertę wzbogaca też bankowość internetowa. Pojawiają się nowe formy płatności online – jedną z nich jest BLIK. Aby skorzystać z tego udogodnienia, nie potrzebujecie karty płatniczej, a tym bardziej portfela. Trzeba jedynie zainstalować na swoim smartfonie aplikację banku, w którym posiadacie konto. Za każdym razem, gdy będziecie chcieli dokonać płatności BLIK-iem, wystarczy, że wygenerujecie 6-cyfrowy kod, który jest aktywny przez ok. dwie minuty. Następny krok to wpisanie kodu we wskazanym miejscu podczas płatności. Na końcu akceptujecie całą operację w aplikacji banku i gotowe!

BLIK-iem możecie nie tylko płacić za zakupy w sklepach online, ale też wypłacać gotówkę z bankomatu oraz rozliczać się z innymi przelewem na telefon. Ta szybka, intuicyjna i z zasady bezpieczna forma płatności mobilnych stała się bardzo popularna, co oczywiście nie umknęło uwadze cyberprzestępców.

W oszustwie na BLIK schemat działania złodziei jest bardzo podobny. Włamują się na czyjeś konto w mediach społecznościowych, podszywają się pod prawowitego właściciela profilu i próbują wyłudzić kod BLIK od jego znajomych. Wysyłają wiadomość za pomocą komunikatora, w której zazwyczaj piszą o nagłej sytuacji, prosząc o pożyczkę. Obiecują szybki zwrot pieniędzy, ale oczywiście kontakt z oszustem się urywa po otrzymaniu kodu BLIK i zatwierdzeniu całej transakcji przez ofiarę.

Pamiętajcie, że transakcji dokonanych za pomocą kodu BLIK nie można cofnąć. Aby ustrzec się przed działaniem cyberprzestępców, trzymajcie się podstawowych zasad bezpieczeństwa w sieci.

- Nie klikajcie w linki przesłane w nietypowych wiadomościach i e-mailach, nie odpowiadajcie na dziwne SMS-y – to może być phishing, czyli próba wyłudzenia poufnych danych, np. logowania do serwisów społecznościowych.
- Stosujcie silne hasła, a najlepiej uwierzytelnianie dwuskładnikowe (hasło i kod np. SMS lub klucz U2F).
- Chrońcie swoje urządzenia mobilne przed nieuprawnionym dostępem. Stosujcie blokadę ekranu nieużywanego sprzętu, włączcie w ustawieniach opcję szyfrowania urządzeń mobilnych (złodziej nie będzie mógł dostać się do pamięci urządzenia) i zdalne zarządzanie sprzętem (daje ona możliwość blokady dostępu do smartfona, wyczyszczenia jego pamięci lub namierzenia lokalizacji), co jest przydatne szczególnie w przypadku kradzieży.
- Nie działajcie pod wpływem emocji. Jeśli znajomy pisze do Was z prośbą o kod BLIK, upewnijcie się, czy rzeczywiście potrzebuje Waszej pomocy. Wystarczy zadzwonić i porozmawiać.

- Ostrzeżcie innych przed działaniem oszusta. Gdy tylko zorientujecie się, że ktoś włamał się na Wasze konto w mediach społecznościowych, natychmiast poinformujcie o tym swoich znajomych. Wyślijcie wiadomość, ale też napiszcie post o tym zdarzeniu.

Więcej o bezpiecznych płatnościach znajdziecie w artykułach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: BLIK i płatności internetowe" i „Bezpieczni w sieci z OSE na wakacje: bankowość mobilna". Śledźcie też bieżące informacje o popularnych oszustwach na stronie Waszego banku oraz CERT Polska.

Bluetooth

Używamy obecnie różnych technologii bezprzewodowych, np. Wi-Fi i NFC (ang. *Near Field Communication* – komunikacja bliskiego zasięgu). Do tej listy wielu z nas zapewne dopisuje też Bluetooth. Wiedzieliście, że możemy korzystać z niego już od 1999 r.? Jest to bardzo popularny standard komunikacji umożliwiający wymianę danych między urządzeniami znajdującymi się w bliskim zasięgu – do 10 m w pomieszczeniach. W moduł Bluetooth wyposażona jest większość sprzętów codziennego użytku: smartfony, tablety, laptopy, inteligentne zegarki, głośniki, drukarki, a nawet aparaty słuchowe, piloty do telewizora i lodówki.

Do komunikacji między urządzeniami Bluetooth wykorzystuje fale radiowe o ultrawysokiej częstotliwości (2,4 miliarda fal na sekundę, czyli 2,4 GHz) i specjalne chipy, które umożliwiają nadawanie i odbieranie sygnałów radiowych. Aby połączenie mogło dojść do skutku, sprzęty muszą mieć wspólny klucz szyfrowania, co zagwarantuje bezpieczną komunikację. Po sparowaniu urządzenia mogą przesyłać między sobą dane, takie jak małe pliki (tekstowe, dźwiękowe, graficzne) czy sygnały sterujące (np. oświetleniem w inteligentnym domu).

Bluetooth pozwala na wygodne słuchanie muzyki bez użycia słuchawek przewodowych, monitorowanie aktywności przy pomocy opasek i zegarków, prowadzenie rozmów przez zestawy głośnomówiące, korzystanie z głośników, myszek, klawiatur, samochodowych systemów audio – a to wszystko bez zaplątywania się w kable. Bezprzewodowość to niejedyna zaleta tej technologii: musimy wspomnieć też o łatwości konfiguracji, niskim zużyciu energii oraz uniwersalności takiego rozwiązania (Bluetooth jest dostępny na wielu urządzeniach i umożliwia różne rodzaje połączeń).

Dzięki mechanizmom szyfrowania i autoryzacji Bluetooth wydaje się bezpieczną technologią, jednak w dzisiejszych czasach nie można zapominać o zasadzie ograniczonego zaufania. Zdarzają się bowiem ataki typu bluejacking, które polegają na przesyłaniu pomiędzy urządzeniami niechcianych wiadomości z linkami lub reklamami za pośrednictwem modułu Bluetooth. Inne ataki mogą wykorzystywać luki w protokole Bluetooth i w jego budowie, co w konsekwencji prowadzi do nieautoryzowanego dostępu do urządzenia. Jak się przed tym chronić?

- Wyłączajcie Bluetooth, gdy z niego nie korzystacie.
- Wyłączajcie wykrywanie Waszego urządzenia z Bluetooth dla obcych sprzętów w pobliżu.
- Nie przechowujcie istotnych informacji na urządzeniach wyposażonych w moduł Bluetooth.
- Nie pozostawiajcie urządzenia z Bluetooth bez kontroli.

Na koniec ciekawostka! Nazwa Bluetooth (ang. *blue* – niebieski i *tooth* – ząb) pochodzi od króla duńskiego Haralda Sinozębnego, który w X w. zasłynął zjednoczeniem Skandynawii. Ideą powstania Bluetooth również było jednoczenie technologii – telefonii komórkowej, komputerów, drukarek itd. Nazwę zaproponował Jim Hardash z Intela, jednej z firm zainteresowanych tą bezprzewodową komunikacją (brano pod uwagę także nazwy RadioWire i PAN).

Źródła:

Olszewski D., (2022), „Czy łączność bezprzewodowa Bluetooth jest bezpieczna?", artykuł w serwisie computerworld.com.

Vega N., (2017), „Co łączy króla wikingów, bezprzewodowe słuchawki i samochodowy zestaw głośnomówiący?", artykuł w serwisie businessinsider.com.

Bomba logiczna

Co wspólnego ma wybuch ładunku z cyberbezpieczeństwem? Ta analogia wykorzystana jest do opisania rodzaju złośliwego oprogramowania (malware), jakim jest bomba logiczna.

Tykająca bomba eksplodująca w najmniej oczekiwanym momencie? Dosłownie! „Detonacja" podstępnego oprogramowania może nastąpić po spełnieniu określonych warunków, np. po uruchomieniu przeglądarki, programu lub aplikacji przez konkretnego użytkownika, otwarciu lub usunięciu pliku. Szczególnym rodzajem bomby logicznej jest bomba czasowa, która aktywuje się w określonym przez przestępców czasie, np. w danym dniu tygodnia lub o konkretnej godzinie.

Ten rodzaj cyfrowego ataku jest niebezpieczny, ponieważ po zainstalowaniu złośliwego oprogramowania na Waszym urządzeniu przez dłuższy czas możecie nie zauważać oznak zagrożenia. Ładunek czeka w uśpieniu do momentu, w którym bomba logiczna zostanie aktywowana. Wtedy zaczynają się problemy. W wyniku uruchomienia szkodliwego kodu możecie stracić swoje dane. Ponadto przestępcy mogą zmienić Wasze hasła dostępu, przejąć kontrolę nad komputerem czy dokonać ataku DoS, czyli zablokować dostęp do określonych programów lub aplikacji poprzez wysyłanie ogromnej liczby zapytań.

Jak się bronić przed bombą logiczną? Korzystajcie ze sprawdzonych programów antywirusowych. Dbajcie o regularne aktualizacje oprogramowania, także antywirusowego. Pobierajcie oprogramowanie tylko ze sprawdzonych źródeł. Ponadto uważajcie na ataki phishingowe, w szczególności weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą wasze wątpliwości.

Źródło:

Łużak T., „Bomba logiczna, czyli liczy się czas", (2025), artykuł na stronie netia.pl.

Bot

To program mający na celu wykonywanie pewnych czynności za człowieka. Przykładów wykorzystania botów można wymienić wiele, a wraz z rozwojem nowych technologii na pewno będzie ich przybywać. Niezależnie, czy zdajecie sobie z tego sprawę, czy nie – programy te wykorzystywane są m.in. w automatycznych systemach obsługi klientów online (chatbot), do zbierania informacji (czyli tzw. indeksujące boty) czy obsługi inteligentnych domów.

Jednym słowem boty mają za zadanie ułatwiać nam wiele aspektów codziennego funkcjonowania. Przykładowo sklepy internetowe wykorzystują je do szybkiego odpowiadania na pytania klientów. Użytkownicy otrzymują potrzebne informacje bez konieczności kontaktu z obsługą, a pracownicy nie muszą odbierać telefonów czy odpisywać na e-maile. Warto pamiętać, że oprogramowanie typu bot może być wykorzystywane zarówno do pozytywnych, jak i negatywnych działań.

Zalety związane z wykorzystaniem botów:

- pomagają w wykrywaniu nietypowych zachowań i potencjalnych zagrożeń w sieci;
- umożliwiają automatyczne reagowanie na incydenty bezpieczeństwa;
- wspierają analizę danych, takich jak logi systemowe czy alerty, co przyspiesza identyfikację problemów.

B

Przykładowe zagrożenia związane z botami:

- mogą być wykorzystywane do tworzenia botnetów, które służą do przeprowadzania ataków typu DDoS (ang. *Distributed Denial of Service*) (boty DDoS);
- potrafią skopiować zawartość wybranej strony internetowej i stworzyć jej wierną kopię (boty zbierające dane, tzw. scraper bots);
- pozwalają na masowe i zautomatyzowane przeprowadzanie kampanii phishingowych, w celu np. rozprzestrzeniania malware – złośliwego oprogramowania (boty spamujące).

Jednym ze sposobów ochrony przed botami jest stosowanie CAPTCHA. To test, który pokazuje, czy osoba próbująca uzyskać dostęp do danej strony internetowej, nie jest robotem. Mechanizm ten chroni też przed tworzeniem fałszywych kont, przeciążeniem serwera czy spamem.

Więcej wiadomości na temat botów znajdziecie w materiałach dostępnych na platformie OSE IT Szkoła: aktualności „Dzień Bota – dowiedz się więcej o sztucznej inteligencji!" oraz kursach e-learningowych o sztucznej inteligencji.

Źródło:

„Co to jest bot?", (b.r.), artykuł na stronie nflo.pl.

Botnet

Kolejnym zagrożeniem w sieci, które powinniście zapamiętać, jest botnet, czyli grupa komputerów-zombie zainfekowanych szkodliwym oprogramowaniem, choć nie tylko. Atakujący może mieć też pod kontrolą inne urządzenia: routery, kamery do monitoringu czy elementy IoT (internetu rzeczy).

Dlaczego botnet jest niebezpieczny? Ponieważ umożliwia przestępcom przejmowanie kontroli nad wieloma (czasem nawet nad tysiącami!) „zarażonymi" urządzeniami jednocześnie i wykorzystywanie ich np. do wykradania danych osobowych, rozsyłania spamu lub wirusów czy przeprowadzania ataków typu ransomware bądź DDoS. Ponadto wszystkie te operacje dzieją się bez wiedzy i zgody właścicieli sprzętów, którzy są nieświadomi, do czego wykorzystuje się ich urządzenia.

Jak nie dopuścić do infekcji komputera i nie dać się wciągnąć w niebezpieczną sieć? Przede wszystkim postawcie na profilaktykę.

- Dbajcie o regularne aktualizacje – systemu, programów i oprogramowania antywirusowego.
- Zabezpieczajcie swoje konta i urządzenia silnymi hasłami, a najlepiej uwierzytelnianiem dwuskładkowym.
- Zadbajcie o zaporę sieciową (firewall) – sprawdźcie, czy jest włączona.
- Weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą wasze wątpliwości.
- Uważajcie na phishing i wszelkie próby przekierowania Was na strony z niebezpiecznym oprogramowaniem do pobrania.

Źródło:

„Co to jest Botnet?", (b.r.), artykuł na stronie nflo.pl.

Browser hijacker

Wyobraźcie sobie, że Wasze dziecko wbrew swojej woli trafia na witrynę ze szkodliwymi treściami albo w jego zakładkach z zaufanymi stronami pojawiają się nagle te nieodpowiednie dla młodych użytkowników sieci. Może to być wynik działania złośliwego oprogramowania (malware) – browser hijacker, którego nazwę można przetłumaczyć jako „porywacz przeglądarek".

Browser hijacker przejmuje kontrolę nad przeglądarką internetową, zmienia jej ustawienia i zarządza nią bez udziału użytkownika. W efekcie może się nagle okazać, że Wasza strona główna została zmieniona lub otwierają się witryny, których nie zamierzaliście odwiedzać – najczęściej przeładowane reklamami czy nieodpowiednimi treściami. W ten sposób przestępcy czerpią zyski z liczby wejść na daną stronę. Co więcej, „porywacz przeglądarek" uniemożliwia dostanie się na platformy z oprogramowaniem antywirusowym czy antyszpiegowskim.

Takie działania znacznie utrudniają korzystanie z internetu, a nawet bywają bardzo niebezpieczne. Oprócz problemów z przeglądaniem sieci browser hijacker może bowiem zawierać oprogramowanie szpiegujące, np. keyloggery, które śledzą ruch użytkownika i wykradają dane.

Jak dochodzi do zainfekowania sprzętu browser hijackerem? Najczęściej podczas pobierania programów, plików i „przydatnych" dodatków z nieznanych źródeł. Złośliwe oprogramowanie ukrywa się też w załącznikach lub linkach przesyłanych w wiadomości phishingowej.

Aby uniknąć tego typu zagrożenia, aktualizujcie system i przeglądarki, korzystajcie z programów antywirusowych oraz pobierajcie oprogramowanie tylko z legalnych stron. Nie otwierajcie też załączników od nieznanych nadawców oraz nie klikajcie bezrefleksyjnie w otrzymane linki. Ponadto uważajcie na natarczywe reklamy – np. te w formie bannerów lub wyskakujących okien przeglądarki internetowej – mogą one uruchomić instalację „porywacza"!

Źródło:

Łużak T., „Browser hijacker – ataki w przeglądarkach wykorzystywanych przez pracowników. Czym grożą?", (2025), artykuł na stronie netia.pl.

Business Email Compromise (BEC)

Cyberprzestępcy stosują różne metody, by wyłudzić pieniądze lub poufne informacje. Ich ataki wymierzone są nie tylko w instytucje czy osoby prywatne, ale również w firmy – zarówno mniejsze, jak i te duże. Jedną z popularnych praktyk jest *Business Email Compromise* (BEC), czyli „oszustwo na dyrektora", które najczęściej bazuje na kampaniach wykorzystujących phishing.

Każdego dnia otrzymujemy dziesiątki wiadomości e-mail – zarówno na konta prywatne, jak i służbowe. Wśród nich może pojawić się wiadomość od cyberprzestępców, którzy próbują zdobyć poufne informacje lub uzyskać dostęp do firmowych finansów. Wykorzystują nieuwagę i uśpioną czujność pracowników. Jak działają?

Dobrze przygotowują się do ataku: zbierają informacje o firmie, pracownikach – głównie wyższego szczebla – i kontrahentach. Następnie przygotowują fałszywe wiadomości e-mail, w których podszywają się pod prezesa danej firmy lub podają się za członków organizacji, z którymi firma współpracuje. W kolejnym kroku mailem wysyłają dyrektorom finansowym, głównym księgowym czy prawnikom – najczęściej osobom decyzyjnym – polecenie pilnego uregulowania zaległej płatności lub zmiany numeru rachunku, na który mają być przekazywane pieniądze. Niestety, niejednokrotnie okazuje się, że prośby od rzekomego szefa lub partnera biznesowego zwykle spełniane są bez zbędnej zwłoki. Jak więc bronić się przed BEC?

- Zachowujcie czujność i kierujcie się zasadą ograniczonego zaufania. Na pewno nie powinniście ulegać presji czasu i autorytetu.
- Unikajcie otwierania załączników i nieprzemyślanego klikania w linki w wiadomościach e-mail, które budzą Wasze wątpliwości.

B

- Sprawdzajcie, czy adres e-mail, z którego otrzymaliście wiadomość, jest poprawny, zwróćcie też uwagę na domenę. Pamiętajcie jednak, że przestępcy są w stanie uzyskać dostęp do poczty innego pracownika i nawet nietypowe maile mogą wyglądać bardzo wiarygodnie.
- Weryfikujcie prośby dotyczące zmiany numeru konta oraz potwierdzajcie transakcje finansowe, szczególnie te opiewające na większe kwoty. Najlepiej skontaktować się telefonicznie z osobą, która rzekomo wysłała taką wiadomość, aby potwierdzić zasadność danego działania.

Wszelkie oszustwa możecie zgłosić na policję, a incydenty bezpieczeństwa komputerowego również do CERT Polska, korzystając z formularza dostępnego na stronie incydent.cert.pl.

Źródło:

„Oszustwa typu BEC”, (2023), artykuł na stronie gov.pl.

C

C

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Zakładacie konto na portalu lub forum dyskusyjnym, uzupełniacie formularz online, zmieniacie hasło do poczty e-mail – procedura już niemal zakończona, ale jeszcze… „Potwierdź, że nie jesteś robotem". To tzw. CAPTCHA: rodzaj dodatkowego zabezpieczenia, znanego jako uwierzytelnianie typu wywołanie – reakcja. CAPTCHA polega na wyświetleniu prostego testu, który ma za zadanie sprawdzić, czy użytkownik próbujący się logować jest człowiekiem, a nie komputerem włamującym się na konto chronione hasłem.

Na pewno nie raz spotkaliście się z różnymi typami CAPTCHA: może to być np. prośba o wykonanie prostego działania matematycznego, przepisanie zniekształconego tekstu z obrazka, podanie odpowiedzi na wyświetlone pytanie, dopasowanie brakującego elementu układanki albo wskazanie określonych elementów na wyświetlonym zdjęciu. Choć rozwiązanie to może wydawać się uciążliwe, pozwala w znacznym stopniu zabezpieczyć nasze informacje, wrażliwe dane i ochronić przed nieautoryzowanym dostępem do kont. Zastosowanie tego mechanizmu chroni m.in. przed tworzeniem sztucznych kont przez automaty (boty), dużą liczbą zapytań do serwera, spamem w formularzach kontaktowych czy reklamami w komentarzach na blogach.

Choć CAPTCHA jest sprawdzonym zabezpieczeniem, cyberprzestępcy opracowali sposoby na jej omijanie, a nawet wykorzystanie w atakach socjotechnicznych. Jednym z niebezpiecznych oszustw jest tzw. fałszywa CAPTCHA, która wygląda jak standardowy test, lecz wymaga od użytkownika wykonania określonych działań poza stroną internetową. Użytkownik może zostać poproszony o skopiowanie ciągu znaków do schowka i uruchomienie go w systemie, co w rzeczywistości powoduje uruchomienie złośliwego kodu.

Taki atak działa poprzez wykorzystanie dobrze znanych skrótów klawiaturowych: Ctrl+C (kopiowanie) i Ctrl+V (wklejanie), a także Win+R, które otwiera okno „Uruchom" w systemie Windows. Jeśli użytkownik postępuje zgodnie z instrukcją, nieświadomie wykonuje polecenia cyberprzestępców, otwierając dostęp do swojego systemu dla złośliwego oprogramowania.

Jak się chronić? Podstawową zasadą bezpieczeństwa jest świadomość zagrożeń i ostrożność w sieci. Pamiętajcie: żadna prawdziwa CAPTCHA nie będzie wymagała opuszczania strony internetowej ani wykonywania działań systemowych, takich jak uruchamianie programów czy kopiowanie kodów do schowka. Jeśli natraficie na podobne instrukcje, natychmiast przerwijcie proces i opuśćcie stronę.

Cyberprzestępstwa w dużej mierze bazują na socjotechnice, wykorzystując nieuwagę i brak świadomości użytkowników na temat zagrożeń związanych z cyfrowym światem. Dlatego warto zawsze zachować czujność i traktować podejrzane polecenia z dużą ostrożnością. Weryfikowanie wiarygodności stron internetowych, stosowanie oprogramowania zabezpieczającego oraz unikanie klikania w nieznane linki to podstawowe kroki, które mogą uchronić nas przed niebezpiecznymi atakami w sieci.

Na koniec ciekawostka. CAPTCHA kojarzy Wam się pewnie z testem Turinga, który może pomóc odróżnić człowieka od komputera. I słusznie! Zabezpieczenie to od samego początku – po raz pierwszy w znanej dziś formie zostało użyte w 2000 r. – miało zapobiegać automatycznemu korzystaniu ze stron internetowych (w tym atakom na nie) i działalności botów. W oryginalnym założeniu CAPTCHA to dowolne zadanie, z którym człowiek poradzi sobie łatwo, a komputer nie będzie w stanie go wykonać.

Chcecie dowiedzieć się więcej o teście Turinga i botach? Zajrzyjcie do kursów dotyczących sztucznej inteligencji na OSE IT Szkole! Więcej o CAPTCHA przeczytacie w aktualności na stronie ose.gov.pl „Bezpieczni w sieci z OSE: CAPTCHA" oraz cert.pl „Uwaga, fałszywa CAPTCHA, czyli nie daj się zainfekować".

C

Catfishing

Poznanie drugiej połówki online nikogo już nie dziwi. Portale randkowe to dla wielu szansa na zbudowanie nowej relacji. Niestety, nie wszystkie internetowe znajomości kończą się happy endem, szczególnie że przestępcy nie mają skrupułów i wykorzystają każdą okazję do realizacji swoich niecnych celów. Fascynacja czy zauroczenie nowo poznaną osobą dodatkowo potrafi uśpić naszą czujność. Trafieni strzałą Amora, możemy nie zorientować się, że znajomy z internetu wcale nie jest tym, za kogo się podaje. Tworzenie fałszywych profili w celu złowienia potencjalnej ofiary w sidła miłości to catfishing.

Czym dokładnie jest? Catfishing to podszywanie się w internecie pod istniejącą lub nieistniejącą osobę. Oszust najczęściej kradnie czyjąś tożsamość, tworzy fałszywe konto i umieszcza na nim cudze zdjęcia. Przyciąga potencjalną ofiarę, prezentując idealny obraz swojej osoby, rozkochuje ją w sobie, a następnie dopuszcza się przestępstwa. Wyłudza od niej pieniądze czy ważne dane, może też ją szantażować, grożąc ujawnieniem pozyskanych wcześniej intymnych materiałów.

Jak rozpoznać catfishing? Kilka szczegółów powinno wzbudzić Wasze podejrzenia:

- **Zbyt piękne, aby było prawdziwe.** Idealny wygląd, wymarzona praca, częste podróże, wystawny tryb życia… Warto krytycznie ocenić, czy taki profil w mediach społeczno-ściowych jest prawdziwy. Sprawdźcie, kiedy został założony, czy jego właściciel ma wielu znajomych, czy fotografuje się z nimi. Pomocne może być też skorzystanie z opcji wyszukiwania obrazem w sieci. Być może znajdziecie prawdziwe źródło zdjęć wykorzystanych przez potencjalnego oszusta.
- **Rozmowa tak, ale nie wideo.** Oszust chętnie nawiązuje kontakt na czacie, telefoniczny czy mailowy, ale jak ognia unika spotkania online z włączoną kamerą, nie mówiąc już o randce w realu? Takie zachowanie może oznaczać, że próbuje ukryć swoją prawdziwą tożsamość.
- **Zbytnia wylewność.** Jeśli nowo poznana osoba bardzo szybko deklaruje miłość, dzieli się swoimi sekretami i poufnymi informacjami, to znak, by zachować ostrożność. Na pewno nie należy odwzajemniać się ujawnianiem wrażliwych danych o sobie.
- **Prośba o intymne materiały.** To kolejny znak, że znajomość zmierza w złą stronę. Przesłane zdjęcia, filmiki o charakterze erotycznym (seksting) mogą posłużyć oszustowi do szantażu (sextortion), a w konsekwencji – wyłudzania pieniędzy!
- **Prośba o pieniądze.** Jeśli internetowy znajomy prosi Was o pieniądze na leczenie czy spłatę długów, uważajcie! Zazwyczaj chodzi o większe sumy, dlatego zanim przelejecie swoje oszczędności, zastanówcie się, czy należy pożyczać pieniądze osobie, której nawet nie widzieliście na oczy.

Catfishing nie jest przestępstwem. Podawanie zmyślonych danych w sieci nie podlega karze. Natomiast karalne są działania będące skutkiem catfishingu. Przestępstwem jest kradzież tożsamości zmierzająca do wyrządzenia osobie, której wizerunek jest wykorzystany, szkody majątkowej lub osobistej. Karze podlegają też: wyłudzenie pieniędzy, kradzież danych, w tym osobowych, szantaż lub nękanie w sieci (cyberstalking). Jeśli doświadczyliście catfishingu i cyberataków, koniecznie zgłoście ten fakt na policję! Pamiętajcie, żeby wcześniej skopiować oraz zabezpieczyć całą korespondencję – to ważny dowód w sprawie.

O zagrożeniach związanych z budowaniem relacji online przeczytacie w naszych aktualnościach na stronie ose.gov.pl: „Uwaga na romance scam!”, „Walentynki online? Sexting – niebezpieczny trend”, „Wirtualna miłość – realne zagrożenie”, „Bezpieczni w sieci z OSE na wakacje: catfishing i letnie kontakty online”. Polecamy również poradniki przygotowane przez ekspertów NASK: „Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online” i „Internetowe love II – randkowanie, AI i cyberbezpieczeństwo”.

CERT Polska

O tym, jak szkodliwe i nieprzyjemne w skutkach potrafią być incydenty w sieci, przekonało się już wielu użytkowników nowych technologii. Gdzie zgłosić niebezpieczną domenę wyłudzającą pieniądze, podejrzane SMS-y i e-maile, złośliwe oprogramowanie (malware) lub fałszywy sklep internetowy? Z pomocą przychodzi CERT Polska (ang. *Computer Emergency Response Team Polska*) – czyli zespół reagowania na incydenty działający w strukturach NASK – Państwowego Instytutu Badawczego. Od 2018 r. zespół CERT Polska realizuje część zadań CSIRT NASK.

Do zadań CERT Polska należą:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- prowadzenie testów bezpieczeństwa – badanie rozwiązań cyfrowych i ich podatności na ataki oraz nielegalne wykorzystanie;
- reagowanie na otrzymane zgłoszenia;
- wydawanie komunikatów o zidentyfikowanych niebezpieczeństwach (np. wykrytych lukach w systemach informatycznych) oraz sposobach, jak sobie z nimi radzić;
- publikowanie artykułów o najpopularniejszych formach ataków oraz sposobach ochrony przed cyberzagrożeniami;
- współpraca z podobnymi jednostkami na całym świecie czy prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa.

Zespół CERT Polska opracowuje też narzędzia zwiększające bezpieczeństwo wszystkich internautów. Przykładem jest moje.cert.pl, dzięki któremu każdy – od osoby prywatnej po dużą instytucję – może bezpłatnie zweryfikować, czy jego zasoby sieciowe (np. strona internetowa) są odpowiednio chronione. Umożliwia skanowanie domen pod kątem zagrożeń, informuje o wyciekach danych i ostrzega przed niebezpiecznymi witrynami. Regularne korzystanie z serwisu to prosty sposób na zwiększenie poziomu cyberbezpieczeństwa.

Więcej o działaniach CERT Polska dowiecie się ze strony cert.pl.

Certyfikat SSL

Choć może nie zawsze sobie to uświadamiacie, strony www są zabezpieczane za pomocą specjalnego standardu szyfrowania. To w uproszczeniu certyfikaty SSL (ang. *Secure Sockets Layer*), które zapewniają poufność danych przesyłanych przez internet i są używane do szyfrowania połączeń m.in. z pocztą elektroniczną i różnymi serwisami. Certyfikaty SSL wykorzystywane są także w celu zabezpieczenia ruchu pomiędzy urządzeniami internetu rzeczy. Zastosowań tych certyfikatów jest jeszcze więcej – dzięki nim zabezpieczane są też aukcje internetowe, transakcje dokonywane w bankowości internetowej czy płatności online.

Jak działa certyfikat? Gdy nawiązujecie połączenie z witryną internetową chronioną protokołem SSL, ustalany jest algorytm i klucz szyfrowania, które w kolejnym etapie służą do przesyłania danych. Następnie serwer wysyła przeglądarce kopię swojego certyfikatu, przeglądarka sprawdza ważność certyfikatu i przesyła wiadomość do serwera, który wysyła potwierdzenie do rozpoczęcia szyfrowanej sesji SSL.

Z certyfikatów mogą korzystać zarówno firmy i instytucje, jak i użytkownicy indywidualni. Koniecznie powinny je uwzględniać serwisy pocztowe, strony banków i instytucji finansowych, sklepy internetowe, serwisy aukcyjne, strony internetowe administracji publicznej, aplikacje typu klient–serwer czy systemy przetwarzające dane na temat zdrowia pacjentów. Dlaczego to takie ważne? Certyfikat potwierdza, że przetwarzane dane osobowe, hasła czy numery kart płatniczych nie zostaną przechwycone przez osoby trzecie. Certyfikat SSL bazuje na szyfrowaniu asymetrycznym, tzn. za pomocą klucza publicznego. Im taki klucz jest dłuższy, tym trudniej odszyfrować przesyłane dane.

C

O tym, że połączenie z serwerem jest szyfrowane, informuje zielona kłódka przy adresie strony. Po kliknięciu w nią można uzyskać szczegółowe informacje na temat certyfikatu. Czy kłódka zawsze oznacza, że witryna jest bezpieczna? Niestety nie – certyfikat bardzo łatwo jest uzyskać i można zrobić to za darmo. Kłódka to sygnał, że połączenie jest szyfrowane, jednak tego samego nie można już powiedzieć o danych, które finalnie trafiają do serwera.

Certyfikaty SSL wykorzystujemy także w Ogólnopolskiej Sieci Edukacyjnej – Techniczni Reprezentanci Szkół instalują je na komputerach i urządzeniach przenośnych (tablety, smartfony) w sieci placówki korzystającej z usług bezpieczeństwa OSE. Instalacja certyfikatów gwarantuje możliwość prawidłowego i bezpiecznego korzystania z zasobów sieci.

Źródło:

„Co to jest certyfikat SSL, podstawowe informacje o certyfikatach SSL", artykuł w serwisie instytutcyber.pl.

Chatboty AI

Nowe technologie rozwijają się w zaskakująco szybkim tempie, a niektóre rozwiązania sprawiają, że zaczynamy funkcjonować inaczej niż dotychczas. Przykładem niezwykłego osiągnięcia twórców cyfrowych rozwiązań, które już zmieniły organizację pracy w wielu firmach, są chatboty AI. Za ich pośrednictwem możemy komunikować się z maszyną – tak jak z człowiekiem! Jak to możliwe?

Takie chatboty to rodzaj sztucznej inteligencji (AI – ang. *artificial intelligence*), która została wytrenowana na bardzo dużych zbiorach danych tekstowych, by móc odpowiadać na nasze pytania i tworzyć różne teksty, jeśli ją o to poprosimy. Wystarczy wprowadzić polecenie zwane promptem, a duży model językowy (ang. *Large Language Mode*l, LLM) wygeneruje odpowiedź najlepszą z możliwych. Rozmawiając z chatbotem, mamy wrażenie, że prowadzimy konwersację z człowiekiem. Model ten potrafi bowiem rozumieć kontekst, prowadzić logiczne wnioskowanie, tworzyć spójne wypowiedzi na dany temat.

Fundamentem działania chatbotów są głębokie sieci neuronowe, które wzorowane są na ludzkim mózgu. W uproszczeniu można powiedzieć, że sztuczne neurony wychwytują sygnał, przetwarzają go i przekazują kolejnym w sieci. W ten sposób model się uczy. Z czasem jego umiejętności są coraz lepsze, ponieważ im większe zbiory danych przeanalizuje, tym jego sposób komunikacji i interakcji staje się bardziej zrozumiały i naturalny.

Gdzie chatboty mogą być wykorzystywane? W wielu dziedzinach, mogą pomagać np. w systemach wsparcia klienta, generowaniu różnych tekstów: artykułów, recenzji, e-maili, przemówień (przykładów jest wiele), a także wspomagać proces edukacyjny. Modele AI mogą też być dla nas wsparciem i źródłem nowych pomysłów. Pytaliście je już: Co warto ugotować w upalny dzień? Jak rozwinąć swój biznes? Prosiliście, żeby ułożyły Wam plan dnia, napisały CV lub przygotowały scenariusz zajęć? A może chcieliście, żeby w prosty sposób wytłumaczyły Wam zawiłe terminy? Polecamy sprawdzić odpowiedzi – możecie się mile zaskoczyć.

Pamiętajcie jednak, że duże modele językowe mają swoje ograniczenia. Na tym etapie rozwoju nie możemy im bezgranicznie ufać. Chatboty potrafią się mylić, podawać błędne informacje, zmyślać, jeśli czegoś nie wiedzą (czyli mieć… halucynacje). Mogą też czerpać wiedzę z nieaktualnych danych. Podchodźcie więc krytycznie do generowanych przez nie odpowiedzi. Co więcej, uważajcie też na przekazywanie im danych osobowych i innych wrażliwych informacji. Pod żadnym pozorem nie udostępniajcie w promptach swoich haseł, danych uwierzytelniających, informacji dotyczących kont bankowych i informacji medycznych. Jeśli prosicie chatbota np. o napisanie wniosku czy innego urzędowego pisma, używajcie pseudonimu zamiast prawdziwego imienia i nazwiska. Lepiej nie ryzykować!

Sprawdźcie sami, jak działa Chat GPT, Copilot, Gemini czy PLLuM stworzony w NASK. Szerokim łukiem omijajcie nieznane platformy!

Chcecie dowiedzieć się więcej, czym jest AI i w jakich obszarach może być stosowana? Skorzystajcie z bezpłatnych kursów e-learningowych o sztucznej inteligencji dostępnych na platformie OSE IT Szkoła.

Źródło:

Watemborski M., (2023), „Chat GPT – co to jest, jak działa, i do czego może być przydatny", artykuł w serwisie tech.wp.pl.

Cheap fake

Powoli przyzwyczajamy się do tego, że w dzisiejszych czasach żadne zdjęcie czy nagranie nie może być już stuprocentowym dowodem, że coś istnieje lub się wydarzyło. Za pośrednictwem internetu oraz mediów społecznościowych docierają do nas setki informacji, które nie zawsze są prawdziwe i mogą zawierać zmanipulowane treści i materiały. Sprawy nie ułatwia nieustanny rozwój technologii – coraz trudniej rozpoznać, czy np. filmik z serwisu społecznościowego jest prawdziwy, czy nie. Dlatego warto krytycznie podchodzić do treści publikowanych w sieci, szczególnie tych, które wydają się nam nieprawdopodobne.

Tworzeniu sfałszowanych materiałów – a co za tym idzie: szerzeniu dezinformacji – sprzyjają osiągnięcia sztucznej inteligencji. Technikę obróbki obrazów z wykorzystaniem algorytmów nazywamy deepfake (od ang. *deep learning* – systemy głębokiego uczenia maszynowego i *fake* – fałsz). Oszuści, fabrykując obraz, korzystają z prawdziwych próbek głosu, filmów i zdjęć. W nasze ręce trafia wtedy np. filmik z udziałem polityka, który wypowiada się na kontrowersyjne tematy lub przyznaje się do wyimaginowanych przewinień.

Odmianą takich zmanipulowanych materiałów jest też cheap fake (ang. *cheap* – tani i *fake* – fałsz). Są to treści audiowizualne, które zostały sfabrykowane przy użyciu o wiele mniej zaawansowanych technologii niż w przypadku deepfake. Powstają np. w efekcie zmiany pierwotnego kontekstu, ale też spowolnienia lub przyspieszenia oryginalnego nagrania czy zastosowania programów graficznych.

Metody obrony przed zmanipulowanymi treściami – zarówno deepfake, jak i cheap fake – są podobne. Musicie ufać intuicji i próbować ocenić wartość takich nagrań (audio i wideo). Sprawdzajcie, czy:

- na nagraniu nie pojawia się migotanie twarzy, czy nie przebija się oryginalny obraz;
- kolory i cienie na nagraniu wyglądają naturalnie;
- czy osoba występująca w filmiku mruga i nie przyjmuje nietypowych póz;
- dźwięk jest zsynchronizowany z obrazem.

Chcecie dowiedzieć się więcej o dezinformacji i sposobach na odróżnianie prawdy od nieprawdy w sieci? Zajrzyjcie do naszego bezpłatnego kursu e-learningowego „(Dez)informacja, czyli w co wierzyć w internecie" dostępnego na platformie OSE IT Szkoła oraz aktualności na stronie ose.gov.pl: „Czy to nagranie może kłamać? Uwaga na deepfake" i „Zanim uwierzysz – sprawdź".

Źródło:

„Pojęciownik Demagoga", (2022), artykuł w serwisie demagog.pl.

Child grooming

Internet to dla dzieci i młodzieży przestrzeń, w której spędzają wiele godzin każdego dnia. Co robią online? Przeważnie wykorzystują sieć pozytywnie – do słuchania muzyki, oglądania filmów i seriali, grania w gry online, kontaktowania się ze znajomymi i rodziną za pomocą komunikatorów, przeglądania serwisów społecznościowych, nauki i poszerzania wiedzy w ramach hobby (Ładna i in., 2025). W internecie szukają też nowych znajomości. Niektóre

C

z nich przeradzają się w trwałe przyjaźnie, ale bywa, że są też źródłem problemów, gdy ktoś trafi na internetowych przestępców, próbujących wyłudzić cenne dane lub pieniądze. Niestety, na tym niebezpieczeństwa się kończą: młodzi użytkownicy sieci narażeni są także na kontakt z osobami uwodzącymi małoletnich.

Uwodzenie dziecka w internecie – z wykorzystaniem nowoczesnych technologii komunikacyjnych – określane jest mianem child grooming. Działanie to może zaczynać się pozornie niewinnie: od zwykłej wiadomości, zaproszenia do przyjacielskiego kontaktu lub komentarza komplementującego wygląd dziecka bądź nastolatka pod postem.

Uwodzenie dziecka w sieci to długotrwały proces, podczas którego sprawca zaprzyjaźnia się z osobą małoletnią, zdobywa jej zaufanie, buduje więź emocjonalną. Cel takiej relacji jest jeden: sprawca zmierza do wykorzystania dziecka w świecie realnym lub produkcji nielegalnych treści z jego udziałem. To szczególnie niebezpieczne w kontekście danych z badania NASK „Nastolatki", z których wynika, że co dziewiąty nastolatek (11%) zdecydował się na podjęcie bezpośrednich kontaktów z nieznajomymi osobami dorosłymi poznanymi w internecie (Ładna i in., 2025).

Oto sygnały, które mogą świadczyć, że dziecko padło ofiarą child groomingu:

- spędza dużo czasu na rozmowach online z osobami, których nie znacie, i unika rozmów o tym, z kim się kontaktuje;
- ogranicza kontakty z dotychczasowymi znajomymi;
- przynosi do domu nowe sprzęty, kosmetyki, dostaje od kogoś doładowania w grach lub inne gadżety i prezenty;
- jest zamknięte w sobie, wycofane, zachowuje się inaczej niż zwykle;
- posiada, ogląda lub otrzymuje materiały pornograficzne oraz porusza tematy związane z seksualnością;
- używa zwrotów i języka typowego dla osób dorosłych (Kwaśnik, 2023).

Należy podkreślić, że child grooming jest przestępstwem, które należy zgłosić na policję! W tym celu zabezpieczcie wszelkie dowody: zrzuty ekranu i inne dane, które pozyskaliście od dziecka. Zgłoście się do administratora strony (jeśli jakiekolwiek materiały zostały opublikowane w sieci) z prośbą o usunięcie nielegalnych treści. Możecie też skorzystać z pomocy działającego w NASK zespołu Dyżurnet.pl, do którego zgłosicie nielegalne treści, szczególnie związane z seksualnym wykorzystywaniem dzieci.

Co jeszcze możecie zrobić? Jeśli Wasze dziecko doświadczyło uwodzenia w sieci, otoczcie je szczególną opieką – stwórzcie warunki do szczerej, wspierającej rozmowy. Na pewno nie obwiniajcie dziecka za całą sytuację! W wielu przypadkach wymagana będzie pomoc specjalisty.

Zapobiegajcie też podobnym sytuacjom – rozmawiajcie z dzieckiem o zagrożeniach związanych z zawieraniem nowych znajomości w internecie oraz o potrzebie ochrony prywatności w sieci. Zawczasu skonfigurujcie ustawienia prywatności w mediach społecznościowych, ustawcie profil dziecka jako niewidoczny dla osób spoza listy znajomych, zablokujcie możliwość przesyłania wiadomości od obcych. Wspólnie usuńcie z sieci wszystkie materiały (zdjęcia, filmiki), które mogą być wykorzystane przez osoby o złych intencjach.

Na stronie gov.pl znajdziecie materiały edukacyjne na temat groomingu z cykl „Bądź z innej bajki": animację, podcast oraz broszurę. Pedagogom polecamy również powiązany tematycznie z animacją scenariusz lekcji „Złapani w sieć. Złota Rybka i niebezpieczne kontakty online" oraz poradnik dla nauczycieli „Sexting i nagie zdjęcia w sieci". Z kolei rodzice mogą skorzystać z naszego poradnika „Sexting i nagie zdjęcia. Twoje dziecko i ryzykowne zachowania online" – materiały dostępne są na platformie OSE IT Szkoła. Ponadto przeczytajcie naszą aktualność na ose.gov.pl: „Bezpieczni w sieci z OSE: child grooming".

Źródła:

Kwaśnik A., (2023), „Sexting i nagie zdjęcia. Twoje dziecko i ryzykowne zachowania online”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Chmura

Choć nazwa ta pewnie przywołuje Wam na myśl głównie meteorologiczne skojarzenia, to w kontekście internetu i nowych technologii jako chmurę (a dokładniej chmurę obliczeniową) rozumiemy technologię, która umożliwia przechowywanie, przetwarzanie i zarządzanie danymi bez konieczności posiadania własnych serwerów czy infrastruktury IT (technologii informacyjnych). Zamiast tego korzysta się z zasobów udostępnianych przez internet przez zewnętrznych dostawców – takich jak przestrzeń dyskowa, moc obliczeniowa czy aplikacje.

W zależności od potrzeb i sposobu zarządzania zasobami, wyróżniamy kilka typów chmury:

- **chmura prywatna** – przeznaczona dla jednej osoby lub organizacji;
- **chmura publiczna** – dostępna dla wielu użytkowników;
- **chmura hybrydowa** – łączy elementy chmury prywatnej, publicznej lub wspólnotowej;
- **chmura wspólnotowa** – współdzielona przez kilka organizacji o podobnych celach i wymaganiach.

Chmury obliczeniowe mogą być wykorzystywane w różnym celu, dlatego można wyodrębnić kilka modeli świadczenia usług chmurowych, takich jak: **IaaS** (ang. *infrastructure as a service*) – infrastruktura jako usługa, **PaaS** (ang. *platform as a service*) – platforma jako usługa, **SaaS** (ang. *software as a service*) – oprogramowanie jako usługa, **SecaaS** (ang. *security as a service*) – cyberbezpieczeństwo jako usługa czy **DRaaS** (ang. *disaster recovery as a service*) – odzyskiwanie po awarii jako usługa.

Dla przeciętnego użytkownika narzędzi cyfrowych taka wirtualna przestrzeń jest niezwykle przydatna. Pozwala m.in. na tworzenie backupu, czyli kopii zapasowych swoich danych. Ale co zrobić, by nasze zasoby były bezpieczne w chmurze? Warto pamiętać o kilku zasadach:

- **Silne hasło i dodatkowa warstwa zabezpieczeń.** Korzystajcie ze wszystkich dostępnych mechanizmów ochrony danych. Ustawcie mocne, unikalne hasło i – jeśli to możliwe – aktywujcie uwierzytelnianie dwuskładnikowe. Nigdy nie udostępniajcie też swoich danych logowania innym osobom!
- **Ostrożność przy udostępnianiu plików**. Jeśli dzielicie się z innymi użytkownikami plikami zapisanymi w chmurze, upewnijcie się, czy przypadkowo nie są one dostępne publicznie. Regularnie sprawdzajcie, kto ma dostęp do Waszych zasobów i w razie potrzeby ograniczcie uprawnienia.
- **Zasada ograniczonego zaufania**. Przed rozpoczęciem korzystania z usług chmurowych dokładnie zapoznajcie się z ustawieniami prywatności i zabezpieczeń. Sprawdźcie np., czy osoby, którym udostępniacie pliki, mogą je dalej przekazywać bez Waszej wiedzy.
- **Kontrolowanie terminów**. Monitorujcie daty ważności umów lub subskrypcji związanych z usługą chmurową. Po ich wygaśnięciu dostęp do danych może zostać ograniczony.

Więcej o chmurze dowiecie się z biuletynu „OUCH! – Bezpieczne przechowywanie danych w chmurze” oraz aktualności na stronie ose.gov.pl „Bezpieczni w sieci z OSE: przechowywanie danych w chmurze”.

C

Clickbait

Czy zdarzyło się Wam kiedyś kliknąć w artykuł tylko z powodu sensacyjnego tytułu lub miniaturki, która wyolbrzymiała faktyczną treść materiału bądź w ogóle do niej nie pasowała? Jeśli tak, to zetknęliście się z clickbaitem. Wyrażenie to powstało z połączenia angielskich słów *click* (kliknięcie) i *bait* (przynęta). Celem clickbaitów jest wyróżnienie się w morzu innych konkurencyjnych doniesień medialnych i skuteczne przyciągnięcie uwagi użytkownika, który – zachęcony zaskakującym przekazem – wejdzie w dany artykuł. Uwaga! Niektóre clickbaity mogą wpływać na szerzenie się dezinformacji w sieci! Ale nie tylko – przekazy, które prowokują do reakcji: kliknięcia w link, pobrania załącznika, zalogowania się w oknie danej strony, to częsta pułapka zastawiana przez cyberprzestępców.

Na clickbaitowe treści, linki, zdjęcia możecie natknąć się wszędzie: w wiadomościach e-mail i SMS, na fałszywych stronach podszywających się pod te oryginalne, w mediach społecznościowych, w komentarzach pod postami, w reklamach o treści szokującej lub emocjonalnej. Po kliknięciu w clickbaitowy odnośnik ofiara może trafić na stronę phishingową, złośliwy formularz logowania albo pobrać na swoje urządzenie malware (złośliwe oprogramowanie).

Jak nie dać się złapać na przynętę zarzucaną przez cyberprzestępców?

- **Zachowajcie dystans**. Uważajcie na nagłówki bazujące na emocjach – strachu, ciekawości lub gniewie. Gdy coś „aż prosi się o kliknięcie", to właśnie wtedy warto powstrzymać się od działania.
- **Sprawdzajcie źródło**. Przyjrzyjcie się dokładnemu adresowi strony, na której znaleźliście się po kliknięciu w odnośnik. Dziwna domena typu: .tk, .top, .ru czy .xyz to sygnał ostrzegawczy! Podobnie jak niepasujące subdomeny, np. bank.security.login.example.com, oraz dodatkowe elementy w adresie, np. paypal-secure.com zamiast paypal.com.
- **Nie dajcie się zwieść zielonej kłódce**. Kłódka w przeglądarce obok adresu zaczynającego się od https nie jest już gwarancją bezpieczeństwa. Oznacza jedynie, że strona posiada certyfikat TLS, czyli że połączenie z serwerem jest szyfrowane. Taki certyfikat można uzyskać za darmo, chroni on przed podsłuchaniem naszej wymiany informacji z właścicielem strony – jednak jeśli właścicielami są cyberprzestępcy, zielona kłódka nic nie zmienia.
- **Nie klikajcie bezmyślnie w linki**. Nie dajcie się też „złapać" na linki ukryte w e-mailach – zamaskowane pod hiperłączami czy przyciskami. Przed kliknięciem zawsze najeżdżajcie myszką na odnośnik, aby zobaczyć, dokąd naprawdę prowadzi.
- **Zadbajcie o aktualizacje**. Systemu, oprogramowania, programu antywirusowego i przeglądarki internetowej. Nowoczesne przeglądarki coraz skuteczniej blokują podejrzane strony, ale wymagają aktualnych baz bezpieczeństwa.

Jeśli cokolwiek wzbudzi Wasze podejrzenia – reagujcie! Potencjalnie niebezpieczną stronę służącą do wyłudzeń danych i środków finansowych możecie zgłosić za pośrednictwem formularza internetowego dostępnego na stronie incydent.cert.pl lub za pomocą usługi „Bezpiecznie w sieci" w aplikacji mObywatel. Niepokojące SMS-y, zawierające Waszym zdaniem groźne linki, przesyłajcie do CERT Polska na numer 8080, korzystając z funkcji „przekaż" albo „udostępnij".

Clickbait stanie się mniej skuteczny, jeśli będziecie się kierować zdrowym rozsądkiem i nauczycie się odróżniać wiarygodne źródła od manipulacji. Krytyczne myślenie w połączeniu z podstawową wiedzą o cyberhigienie to skuteczna tarcza przeciw atakom socjotechnicznym.

Chcecie dowiedzieć się więcej o dezinformacji oraz ochronie przed manipulacją w internecie? Przeczytajcie aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: fake newsy", „Zanim uwierzysz, sprawdź!", „Bezpieczni w sieci z OSE: metody i techniki dezinformacji". Skorzystajcie też z naszych materiałów, w których znajdziecie niezbędne informacje na temat ochrony przed nieprawdziwymi treściami. Na stronie OSE IT Szkoła, oprócz kursu „(Dez)informacja, czyli w co

wierzyć w internecie?" i zawartych w nim scenariuszy, znajdziecie: ulotkę „Fake newsy, bańki informacyjne, teorie spiskowe", konspekt zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole", infografikę „Jak rozpoznać fake newsa?".

Clickjacking

Cyberprzestępcy zastawiają na nas różne pułapki, jeśli w nie wpadniemy, możemy wiele stracić. Jedną z nich jest clickjacking. To wyjątkowo podstępny sposób na wyłudzenie naszych danych lub pieniędzy. Zagrożenie to można przetłumaczyć jako „przechwytywanie kliknięć". Jak dokładnie dochodzi do oszustwa? Klikając w przycisk „zaloguj", „potwierdź" lub „pobierz", w rzeczywistości klikacie w element ukryty pod widoczną warstwą interfejsu, która stanowi tylko fasadę dla niebezpiecznej strony.

Do clickjackingu często dochodzi bez wiedzy użytkownika, ponieważ przestępcy skrupulatnie ukrywają niebezpieczne odnośniki, najczęściej linki, pod elementami graficznymi potencjalnie bezpiecznej witryny. Oszuści mogą też przygotować całą stronę np. z atrakcyjną ofertą – darmowym oprogramowaniem lub grą – a pod nią ukryć groźne odsyłacze.

Co się stanie, jeśli padniecie ofiarą clickjackingu? Niepostrzeżenie możecie np. pobrać na swoje urządzenie oprogramowanie szpiegujące typu keylogger, monitorujące Waszą aktywność, lub inny złośliwy program (malware). Nieświadomie możecie też podać swoje dane uwierzytelniające (np. do bankowości internetowej) w fałszywym panelu logowania.

Warto wiedzieć, że odmianą ataku typu clickjacking jest likejacking. Polega on na manipulacji przyciskiem „Lubię to" w mediach społecznościowych, co sprawia, że użytkownicy „polubią" zupełnie inną stronę, zwiększając jej oglądalność. Istnieje też gorszy, ale równie prawdopodobny scenariusz likejackingu: po pechowym kliknięciu Wasz profil zostanie zainfekowany, konto może stać się widoczne dla wszystkich (dojdzie do zmiany ustawień prywatności), na tablicy pojawi się post o tym, że lubicie fałszywą stronę, a do Waszych znajomych trafi spam.

Zła wiadomość jest taka, że jako zwykli użytkownicy internetu możemy mieć trudność w wykryciu clickjackingu. Z reguły przestępcy umieszczają przygotowaną przez siebie niebezpieczną stronę w kodzie HTML za pomocą „ramki" – iframe, co sprawia, że jest ona praktycznie niewidoczna. Cała nadzieja w twórcach i administratorach witryn, którzy poprzez eliminację luk w kodzie strony i dodanie odpowiednich skryptów, zapobiegają większości prób ataku tego typu.

Jako użytkownicy sieci możemy się jednak bronić przed clickjackingiem, zachowując szczególną ostrożność.

- Bacznie obserwujcie odwiedzane strony. Jeśli nagle, po kliknięciu w jakiś button, zauważycie zmianę w wyglądzie witryny albo otrzymacie dziwną prośbę, np. o podanie danych logowania, podczas gdy miejsce, w którym się znajdujecie, tego nie wymaga – natychmiast opuście taką stronę.
- Często śledźcie pasek przeglądarki. W każdej chwili możecie zostać przekierowani na fałszywą stronę. Literówki, dodatkowe lub brakujące znaki w adresie to również sygnał, że znajdujecie się w oknie złośliwej witryny.
- Regularnie aktualizujcie swoje przeglądarki internetowe. Niektóre z nich zawierają wtyczki (plug-in), które mają pomóc w rozpoznaniu ukrytej strony.

Pamiętajcie, jeśli natkniecie się na podejrzaną witrynę, koniecznie zgłoście to do CERT Polska – możecie to zrobić za pośrednictwem formularza internetowego na stronie incydent.cert.pl.

Źródło:

Rożnowski J., (2024), „Na czym polega atak clickjacking? Jak się zabezpieczyć?", artykuł w serwisie semcore.pl.

C

Cracking

Cracking to termin, który pochodzi od angielskiego słowa *crack* – „łamać" i oznacza dziedzinę informatyki zajmującą się łamaniem zabezpieczeń oprogramowania. Cracking to też sam proces łamania danego zabezpieczenia komputerowego, np. hasła czy systemu zabezpieczeń.

Jeśli chodzi o łamanie zabezpieczeń oprogramowania, jest to proceder skomplikowany i wymaga profesjonalnej wiedzy. Jego początków można się dopatrywać w latach 80. XX w., czyli w czasach, kiedy pojawiły się komputery Atari i Commodore. Wówczas producenci zaczęli wprowadzać mechanizmy chroniące przed nielegalnym kopiowaniem programów. Oczywiście w odpowiedzi na te działania pojawiły się też osoby, które analizowały i łamały nakładane zabezpieczenia. Jak dokładnie działa cracker w przypadku forsowania zabezpieczeń oprogramowania? Dąży on do uzyskania dostępu do określonych zasobów bez korzystania z kodu źródłowego. Aby to osiągnąć, wykorzystuje tzw. inżynierię wsteczną, polegającą na przekształceniu skomplikowanego programu ponownie na język programowania.

Dziś najczęściej przełamywane są zabezpieczenia czasowe (tzw. wersje trial oprogramowania) czy pliki z kluczem. Cracking umożliwia użytkownikowi dostęp do pełnej wersji programu bez konieczności wniesienia opłaty. Wystarczy, że cracker przygotuje program, zwany crackiem, który automatycznie usuwa zabezpieczenia.

Warto pamiętać, że cracking jest nielegalny – za takie działania grozi odpowiedzialność karna, co dokładnie opisane jest w ustawie o prawie autorskim i prawach pokrewnych. Ponadto crack może być zainfekowany malware (złośliwym oprogramowaniem), za pomocą którego przestępcy uzyskują dostęp do naszych danych osobowych, haseł, loginów czy numerów kart płatniczych. Cracking to niebezpieczny proceder – może zakłócać działanie systemów komputerowych, a w skrajnych przypadkach prowadzić do ataków na infrastrukturę krytyczną, taką jak sieci energetyczne, systemy transportowe czy placówki medyczne, co ma istotny wpływ na bezpieczeństwo państwa.

Jako zwykli użytkownicy internetu również powinniśmy się chronić przed crackingiem. Przede wszystkim należy zachować podstawowe zasady bezpieczeństwa w sieci. Niech Was nie skuszą darmowe pliki, gry, aplikacje pobierane z nieznanych źródeł! Ponadto chrońcie swoje dane – stosujcie silne hasła, najlepiej uwierzytelnianie dwuskładnikowe lub wieloskładnikowe, czyli oprócz hasła logujcie się do usług cyfrowych dodatkowymi składnikami, np. kodem otrzymanym SMS-em i odciskiem palca. Pamiętajcie też o regularnych aktualizacjach Waszych aplikacji oraz oprogramowania, także antywirusowego. Wszelkie błędy i luki w zabezpieczeniach zwiększają szanse przestępców na przeprowadzenie skutecznego ataku!

Credential stuffing

Mówiąc o zasadach bezpieczeństwa w internecie, należy przede wszystkim pamiętać o konieczności stosowania unikalnych haseł we wszystkich miejscach, gdzie zakładacie konta (media społecznościowe, serwisy internetowe, e-sklepy, poczta elektroniczna itd.). Przestrzegając tej zasady, znacząco ograniczycie ryzyko ataku typu credential stuffing, który polega na wykorzystaniu skradzionych w sieci danych logowania, przypisanych do konkretnych użytkowników.

Jak przestępcy wchodzą w posiadanie naszych loginów i haseł? Zwykle dzieje się to w związku z wyciekiem danych z popularnych portali i baz danych. W ręce oszustów mogą trafić wówczas adresy e-mail powiązane z hasłami. Mając takie dane, można podejmować zautomatyzowane próby logowania do wielu różnych portali, licząc, że wykradzione hasło będzie pasować więcej niż do jednego konta przypisanego do danego adresu. Credential stuffing to atak zautomatyzowany, dlatego warto zawczasu zadbać o bezpieczeństwo i włączyć uwierzytelnianie dwuskładnikowe.

Stosując to samo hasło do logowania do różnych kont, musicie liczyć się z tym, że Wasze dane nie są bezpieczne. Weźmy prosty przykład: jeśli przestępcy udało się wykraść hasło do poczty elektronicznej, będzie liczył na to, że tego samego zabezpieczenia używacie np. w serwisie

zakupowym, gdzie podaliście dane swojej karty kredytowej. Jeśli ma rację – możecie stracić oszczędności, a nawet paść ofiarą kradzieży tożsamości.

Pierwszą oznaką, że macie do czynienia z credential stuffingiem, mogą być powtarzające się powiadomienia (np. mailowe) o próbach logowania do Waszych kont na innych urządzeniach. Niepokój powinny wzbudzić też informacje o próbach logowania z nieznanych lokalizacji lub przeglądarek, z których nie korzystacie.

Aby chronić się przed atakiem typu credential stuffing, trzeba pamiętać o podstawowych zasadach dotyczących silnych haseł:

- Używajcie fraz składających się z co najmniej 14 znaków. Unikajcie oczywistych kombinacji liter i cyfr, nie wykorzystujcie kojarzących się z Wami danych (np. daty urodzenia) ani potocznych zwrotów, nazwisk celebrytów itd.
- Tworząc hasło, korzystajcie z długich, sprytnie zmienionych fraz, które będą łatwe do zapamiętania dla Was, a trudne do złamania dla przestępców (np. WlazłKostekNa-MostekIStuka). Siłę hasła wzmocnią też obcojęzyczne wtręty (np. DwaBialeLatajace-SophisticatedKroliki).
- Sprawdźcie listę najpopularniejszych haseł opublikowaną przez CERT Polska i wystrzegajcie się jak ognia podanych tam propozycji.
- Stosujcie unikalne hasła do wszystkich kont, do których się logujecie.
- Używajcie generatorów haseł i menedżerów haseł, dzięki którym nie będziecie musieli pamiętać wszystkich swoich zabezpieczeń.
- Tam, gdzie to możliwe, korzystajcie z uwierzytelniania dwuskładnikowego, czyli dodatkowego kroku, który pomoże zweryfikować Waszą tożsamość podczas logowania.
- Co jakiś czas sprawdzajcie, czy Wasze hasła nie wyciekły – np. na stronie bezpiecznedane.gov.pl. Gdy zorientujecie się, że Wasze dane zostały upublicznione, przede wszystkim użyjcie oprogramowania antywirusowego, żeby sprawdzić bezpieczeństwo swojego komputera. Następnie bezzwłocznie zmieńcie dotychczasowe hasła do logowania, w tym również hasła pokrewne, które łatwo zgadnąć.

Więcej o cechach dobrego hasła przeczytacie na stronie CERT Polska w poradniku „Kompleksowo o hasłach", a także w naszych aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: wyciek danych".

CRP (stopień alarmowy)

Spotkaliście się kiedyś w mediach lub internecie z określeniem „stopień BRAVO-CRP" i zastanawialiście się, co to takiego? Śpieszymy z wyjaśnieniami. Termin ten jest związany z cyberbezpieczeństwem kraju, a dokładniej dotyczy ataków wymierzonych w systemy teleinformatyczne. Stopnie alarmowe CRP (ang. *Cyber Response Planning*) zostały określone w ustawie o działaniach antyterrorystycznych i są wprowadzane w sytuacjach, gdy pojawia się wzmożone zagrożenie w cyberprzestrzeni.

Wyróżniamy cztery stopnie alarmowe CRP: ALFA-CRP, BRAVO-CRP, CHARLIE-CRP i DELTA-CRP. Każdy kolejny stopień odzwierciedla wyższy poziom zagrożenia:

- ALFA-CRP – pierwszy stopień alarmowy oznacza niski poziom zagrożenia. Można go wprowadzić w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia.
- BRAVO-CRP – drugi, podwyższony stopień alarmowy wprowadza się w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, jednak konkretny cel ataku nie jest zidentyfikowany.

- CHARLIE-CRP – trzeci, wysoki stopień alarmowy można wprowadzić w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel cyberataku o charakterze terrorystycznym lub w przypadku uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu tego typu.
- DELTA-CRP – czwarty, najwyższy stopień alarmowy jest stosowany po wystąpieniu cyberataku terrorystycznego lub po uzyskaniu informacji o końcowej fazie przygotowywania takiego zdarzenia, a zebrane dane wskazują jednocześnie na nieuchronność takiego zdarzenia.

Stopnie alarmowe wprowadza, zmienia i cofa – w drodze rozporządzenia – Prezes Rady Ministrów zgodnie z przepisami ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Każdego dnia powinniście pamiętać o zachowaniu bezpieczeństwa w sieci, a w sytuacjach, gdy zostanie wprowadzony któryś stopień alarmowy CRP, swoją czujność warto jeszcze dodatkowo wzmocnić.

Więcej o stopniach alarmowych CRP dowiecie się z aktualności „Stopnie alarmowe i stopnie alarmowe CRP" dostępnej na stronie Ministerstwa Spraw Wewnętrznych i Administracji.

Źródło:

„ALFA, BRAVO, CHARLIE, DELTA – stopnie alarmowe CRP", (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

Cryptojacking

Wydajność Waszego sprzętu znacznie spadła: niegdyś superszybki komputer lub tablet nagle spowolnił, częściej używa wentylatora? Bateria w telefonie wyczerpuje się nadzwyczaj szybko? A może Wasze rachunki za prąd drastycznie wzrosły? Sprawdźcie, czy nie padliście ofiarą cryptojackingu!

Cryptojacking (zwany też złośliwym wydobywaniem kryptowalut) to cyberzagrożenie, na które narażony jest każdy użytkownik internetu. Atak polega na przejęciu mocy obliczeniowej urządzenia ofiary. W ten sposób przestępcy nielegalnie wykorzystują zasoby cudzego sprzętu do wydobywania kryptowalut. Warto podkreślić, że samo „kopanie" wirtualnych monet jest legalne, ale wymaga dużych nakładów finansowych, m.in. budowania farm komputerów z niezwykle wydajnymi komponentami i zużywania ogromnej ilości energii elektrycznej. Przestępcy wymyślili więc, że do wydobycia elektronicznego pieniądza posłużą się siecią urządzeń cyfrowych zainfekowanych szkodliwym oprogramowaniem.

Ofiary cryptojackingu zazwyczaj nie wiedzą, że ich urządzenie zostało zaatakowane i służy do wydobywania kryptowalut. Malware (złośliwe oprogramowanie) zostało zaprojektowane tak, by działać w tle. Skutkiem tego ataku jest szybkie zużycie sprzętu, a w konsekwencji skrócenie jego żywotności, oraz wzrost rachunków za prąd.

W jaki sposób przestępca przeprowadza atak?

- Phishing – to jedna z najpopularniejszych metod uzyskania dostępu do naszych danych czy zainfekowania sprzętu. Oszuści podszywają się pod inne osoby lub firmy, wysyłają wiadomości i nakłaniają odbiorcę, by ten pod presją czasu np. kliknął w przesłany link. Postępowanie zgodnie z instrukcją cryptojackera może m.in. spowodować pobranie i zainstalowanie malware, w wyniku którego Wasze urządzenie dołączy do tysiąca innych pracujących nad wydobywaniem kryptowaluty.
- „Drive-by mining" – to metoda, która polega na zakażaniu witryn internetowych złośliwym kodem. Użytkownik sieci, przeglądając daną stronę, zazwyczaj nie ma świadomości, że właśnie jego komputer lub smartfon dołączył do jednej z wielu „koparek" wirtualnych monet. Co istotne – proceder może trwać nawet po opuszczeniu przez Was zainfekowanej strony.

- Wirusy i szkodliwe aplikacje – pobieranie bezpłatnego oprogramowania lub aplikacji pochodzących z niewiarygodnych źródeł zawsze wiąże się z ryzykiem cyberataku. Wraz z zainstalowaniem darmowych narzędzi możecie wpuścić do systemu złośliwe oprogramowanie, które ukrywa oprogramowanie ułatwiające cryptojackerowi atak.

Pozbycie się szkodliwego oprogramowania bywa trudne – w niektórych przypadkach konieczne może się okazać sformatowanie dysku. Warto więc zrobić wszystko, by nie dopuścić do zainfekowania sprzętu.

Przede wszystkim wyposażcie się w sprawdzone oprogramowanie antywirusowe, dbajcie o regularne aktualizacje, pobierajcie programy tylko z wiarygodnych źródeł oraz uważajcie na ataki phishingowe. Obserwujcie też, jak zachowuje się Wasz sprzęt: czy nie traci na wydajności, czy nie zużywa się zbyt szybko. Ponadto zaglądajcie do „Menadżera zadań" – obserwujcie, czy w tle działają programy lub przeglądarki stron internetowych, z których akurat nie korzystacie. Zachowajcie czujność!

CSIRT

Czy wiecie, że o bezpieczeństwo naszego kraju dbają specjalnie utworzone zespoły CSIRT (ang. *Computer Security Incident Response Team*), a dokładnie trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego? Na mocy ustawy o krajowym systemie cyberbezpieczeństwa rolę CSIRT poziomu krajowego pełnią Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON).

Koordynowanie oraz obsługa zgłoszonych incydentów, sprawne zarządzanie ryzykiem, a także skuteczne reagowanie na wszelkie niebezpieczne sytuacje zagrażające bezpieczeństwu sieci i systemów informatycznych – to główne zadania CSIRT.

Warto wspomnieć, że obowiązki CSIRT NASK zostały powierzone zespołowi CERT Polska i Dyżurnet.pl. Oprócz rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo sieci, a także aktywnego reagowania na zagrożenia, CSIRT NASK prowadzi również działalność badawczą z zakresu metod wykrywania incydentów bezpieczeństwa. Ponadto realizuje wiele projektów informacyjno-edukacyjnych, mających na celu poprawę świadomości użytkowników sieci w zakresie bezpieczeństwa teleinformatycznego. Zachęcamy do lektury raportów z działalności CERT Polska zawierających dane o popularnych cyberzagrożeniach, z którymi każdego roku stykają się polscy internauci.

CSIRT NASK przyjmuje zgłoszenia od podmiotów publicznych, operatorów usług kluczowych, dostawców usług cyfrowych, ale też od wszystkich obywateli, którzy przekazując tego typu informacje, przyczyniają się do zwiększenia bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej.

Jak zgłosić incydent bezpieczeństwa? Możecie to zrobić na stronie incydent.cert.pl. Bądźcie bezpieczni w sieci!

Cyberbezpieczeństwo

W dobie powszechnej cyfryzacji cyberbezpieczeństwo stało się kluczowym elementem ochrony naszych danych, tożsamości i prywatności. Codziennie korzystamy z internetu, przesyłamy wrażliwe informacje, robimy zakupy online, a także przechowujemy ważne dane w chmurze. Niestety, na każdym kroku jesteśmy narażeni na różne niebezpieczeństwa, takie jak phishing, wycieki danych, zainfekowanie urządzeń wirusami czy innym szkodliwym oprogramowaniem.

Cyberbezpieczeństwo to zbiór praktyk, technologii i procesów mających na celu ochronę systemów komputerowych, sieci oraz danych przed atakami, uszkodzeniami czy nieautoryzowanym dostępem. Obejmuje ono zarówno działania podejmowane przez firmy i instytucje, jak i środki, które możemy wdrożyć jako indywidualni użytkownicy.

C

W dzisiejszym świecie cyberprzestępcy stale ulepszają swoje metody, szybko się uczą, jak wykorzystywać różnorodne techniki do łamania zabezpieczeń. Bezpieczeństwo w sieci to dynamiczna dziedzina, która wymaga ciągłego dostosowywania się do nowych zagrożeń i wyzwań. Stale musimy mieć oczy i uszy szeroko otwarte!

Jakie są najczęstsze zagrożenia, z jakimi możecie spotkać się w internecie?

- Phishing: atak polegający na podszywaniu się pod zaufaną instytucję lub osobę w celu wyłudzenia danych osobowych, takich jak hasła czy numery kart kredytowych. Zazwyczaj odbywa się poprzez fałszywe e-maile i inne wiadomości (np. wysyłane za pośrednictwem komunikatorów) oraz podczas rozmów telefonicznych z rzekomymi „przedstawicielami banków".
- Malware (złośliwe oprogramowanie): obejmuje wirusy i inne programy, które infekują komputery, aby kraść dane, niszczyć pliki lub szantażować użytkowników.
- Ransomware: oprogramowanie, które blokuje dostęp do systemu lub danych i wymaga okupu za ich odblokowanie. Tego typu ataki mogą być szczególnie groźne, jeśli nie posiadamy kopii zapasowych danych.
- Ataki DDoS (ang. *Distributed Denial of Service*): polegają na przeciążeniu serwera lub sieci, co prowadzi do ich czasowego unieruchomienia. Chociaż ataki DDoS są zazwyczaj skierowane przeciwko firmom, to ich skutki mogą odczuć także indywidualni użytkownicy, zwłaszcza jeśli korzystają z tych samych zasobów sieciowych.

Ochrona przed cyberzagrożeniami nie musi być skomplikowana. Wprowadzenie kilku prostych nawyków może znacząco zmniejszyć ryzyko stania się ofiarą cyberprzestępców.

- Silne i unikalne hasła. Używanie silnych, unikalnych haseł to podstawa cyberbezpieczeństwa. Hasła powinny mieć co najmniej 14 znaków, dobrze, jeśli składają się z kilku słów. Ważne jest także, aby nie używać tego samego hasła do różnych kont. W przypadku dużej liczby kont warto rozważyć korzystanie z menedżera haseł, który pomoże w ich tworzeniu i przechowywaniu.
- Uwierzytelnianie dwuskładnikowe i wieloskładnikowe. Włączenie tego zabezpieczenia wszędzie tam, gdzie jest to możliwe, stanowi dodatkową warstwę ochrony. Nawet jeśli ktoś pozna Wasze hasło, do zalogowania będzie potrzebował dodatkowego elementu znanego tylko Wam, np. kodu wygenerowanego przez aplikację czy odcisku palca.
- Aktualizacje. Regularne aktualizowanie systemów operacyjnych, programów – w tym programu antywirusowego – i aplikacji jest kluczowe dla ochrony przed znanymi lukami w zabezpieczeniach. Producenci regularnie publikują łatki, które eliminują te zagrożenia, więc warto mieć włączone automatyczne aktualizacje.
- Ostrożność w korzystaniu z poczty elektronicznej. Uważajcie na e-maile od nieznanych nadawców, zwłaszcza te zawierające linki lub załączniki. Jeśli macie wątpliwości, czy wiadomość jest autentyczna, skontaktujcie się bezpośrednio z nadawcą lub instytucją, która rzekomo wysłała e-mail.
- Backup. Regularne tworzenie kopii zapasowych danych ochroni Was przed ich utratą w wyniku ataków ransomware czy awarii sprzętu. Kopie zapasowe powinny być przechowywane w różnych lokalizacjach, np. na zewnętrznym dysku twardym oraz w chmurze.
- Świadomość zagrożeń. Edukacja jest kluczem do skutecznej ochrony przed cyberzagrożeniami. Bądźcie na bieżąco z nowinkami dotyczącymi cyberbezpieczeństwa i regularnie sprawdzajcie, czy Wasze dane nie wyciekły w wyniku naruszeń bezpieczeństwa.

Pamiętajcie: cyberbezpieczeństwo to nie tylko technologia, ale także nasze codzienne nawyki. Wprowadzenie podstawowych zasad ochrony danych osobowych, takich jak tworzenie silnych

haseł, regularne aktualizacje czy ostrożność w korzystaniu z poczty elektronicznej, znacząco zmniejsza ryzyko cyberataku. Warto pamiętać, że w świecie cyfrowym to właśnie użytkownik jest pierwszą linią obrony przed zagrożeniami.

Chcecie dowiedzieć się więcej na temat sposobów ochrony przed zagrożeniami? Zaglądajcie na stronę ose.gov.pl i platformę OSE IT Szkoła, gdzie znajdziecie wiele pomocnych treści – aktualności, kursy e-learningowe, poradniki i inne materiały. Zapraszamy Was także na strony: nask.pl, cert.pl i dyzurnet.pl!

Cyberporywanie

Cyberporwanie lub wirtualne porwanie to zdarzenie, do którego w rzeczywistości nie doszło, choć przestępcy robią wszystko, aby osoby, które dowiedziały się o rzekomym uprowadzeniu bliskiej osoby, uwierzyły w przerażającą historię i zapłaciły okup. Oszuści do swoich celów coraz częściej wykorzystują zdobycze sztucznej inteligencji (ang. *artificial intelligence*, AI). Zanim jednak zaatakują, śledzą każdy ruch ofiary w sieci i zbierają informacje na jej temat. Ale zacznijmy od początku.

Wyobraźcie sobie, że dostajecie telefon lub wiadomość z nagraniem, na którym Wasz syn lub córka błaga o pomoc, bo doszło do porwania. Następnie porywacze grożą, że jeśli nie zapłacicie okupu, już nigdy nie zobaczycie swojego dziecka. Zaaranżowana sytuacja może wyglądać bardzo realistycznie. Wszystko za sprawą wykorzystania technologii AI, która skutecznie zaciera różnice między rzeczywistością a fikcją. Niestety, stworzenie mrożącego krew w żyłach scenariusza nie jest takie trudne – potrzebne narzędzia są ogólnodostępne.

Jak dochodzi do manipulacji? AI potrafi naśladować głos każdej osoby. Wystarczy jej próbka nagrania oryginalnej wypowiedzi, by mogła sklonować czyjś głos, a następnie wygenerować żądaną przez oszustów wypowiedź ofiary brzmiącą niezwykle wiarygodnie. To samo AI może zrobić z nagraniem wideo – jeśli dostarczymy jej próbkę głosu, filmik i zdjęcia jakiejś osoby, stworzy – korzystając z technologii deepfake – zmanipulowany materiał, na którym „na własne oczy" przekonamy się, że doszło do porwania.

Scenariuszy takiego upozorowanego działania może być wiele. I choć skutków cyberporwania nie można porównywać do prawdziwego zdarzenia, bo ostatecznie okazuje się, że rzekoma ofiara jest bezpieczna, to nie zmienia to faktu, że bliscy w danym momencie przeżywają ogromną tragedię. Ponadto działając pod wpływem gróźb i w nadziei na szybki powrót bliskiej osoby, mogą zapłacić okup, a tym samym stracić cały majątek, bo przecież życie i zdrowie najbliższych nie ma ceny.

Jak bronić się przed cyberporwaniem? Przede wszystkim należy dbać o swój cyfrowy ślad w sieci, szczególnie ten zostawiany świadomie. Posty, komentarze, zdjęcia, filmiki, oznaczenia geolokalizacyjne, zdradzające, gdzie dokładnie się znajdujecie, także publikowane w mediach społecznościowych materiały rodzinne, które ujawniają Wasze powiązania – te wszystkie okruchy informacji przestępcy skrzętnie zbierają i wykorzystują do przeprowadzenia wirtualnego porwania. Stworzenie wstrząsającej historii, w którą ktoś uwierzy, jest łatwiejsze, gdy oszust zna Wasze plany i szczegóły z Waszego życia, a przede wszystkim wie, gdzie dokładnie przebywacie. Cyberporwanie najlepiej przeprowadzić, jak będziecie za granicą, z dala od bliskich, którzy łatwo mogliby zdemaskować oszustwo.

Aby zminimalizować groźbę cyberporwania, warto też trzymać się kilku innych zasad bezpieczeństwa w internecie:

- Dbajcie o swoją prywatność w sieci – stosujcie ustawienia prywatności, szczególnie w mediach społecznościowych. Nie każdy musi mieć dostęp do publikowanych przez Was informacji.
- Nie udostępniajcie zdjęć swoich dzieci w internecie – sharenting to popularny wśród rodziców trend. Jednak publikowanie w sieci fotografii dziecka, a przy okazji wielu informacji na jego temat, takich jak: imię, wiek, data urodzin, nazwa szkoły lub przedszkola, do którego chodzi – realnie zagraża jego bezpieczeństwu.

C

- Uważajcie na phishing – i inne próby wyłudzenia danych osobowych czy uwierzytelniających. Pozyskane informacje mogą być pomocne w przeprowadzeniu wirtualnego porwania.
- Korzystajcie z prawa do bycia zapomnianym – jeśli w sieci znajdują się dotyczące Was treści, możecie prosić o ich usunięcie. Takie prawo wynika z rozporządzenia unijnego RODO (Ogólnego rozporządzenia o ochronie danych).

Jak się zachować, gdy otrzymacie informację o porwaniu najbliższej osoby? Niezależnie od tego, czy uprowadzenie jest prawdziwe, czy wirtualne – choć tego w pierwszej chwili nie będziecie w stanie stwierdzić – zachowajcie spokój, nie przekazujcie przestępcom żadnych informacji, które mogłyby im pomóc w dalszym uwiarygodnianiu swoich działań. Podczas rozmowy z rzekomymi sprawcami przestępstwa spróbujcie skontaktować się z potencjalnie uprowadzoną osobą, ustalcie, czy jest bezpieczna. Powiadomcie policję o całym zdarzeniu.

Więcej praktycznych wskazówek, jak dbać o swoją prywatność w sieci, znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: ochrona danych osobowych”, „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci”.

Cyberprzemoc

Internet przynosi nam wiele korzyści, ale naraża też na niebezpieczeństwa. Jednym z nich jest cyberprzemoc. Czym jest to zjawisko, jak się przejawia i jak się bronić przed agresją w sieci?

„Cyberzemoc to przemoc z użyciem urządzeń elektronicznych, najczęściej telefonu bądź komputera. Bywa określana także jako cyberbullying: nękanie, dręczenie, prześladowanie w internecie. Niezależnie od nazwy jej celem zawsze jest wyrządzenie krzywdy drugiej osobie. Cyberprzemoc to – podobnie jak przemoc tradycyjna – regularne, podejmowane z premedytacją działanie wobec słabszego, który nie może się bronić” (Borkowska, 2023).

Dane z raportu NASK „Nastolatki” nie pozostawiają złudzeń – młodzi użytkownicy internetu spędzają online średnio 5 godzin (bez jednej minuty) dziennie, a w dni wolne od zajęć – 5 godzin i 16 minut. W sieci doświadczają też różnych form agresji. Co trzeci badany nastolatek był wyzywany, ośmieszany, poniżany czy straszony. Przy czym młodzi ludzie rzadko proszą dorosłych o pomoc, gdy padną ofiarą cyberprzemocy. Te same badania pokazują, że aż 47% badanych zadeklarowało, że w ogóle nie podjęło żadnych działań i nikomu nie powiedziało o problemie (Ładna i in., 2025).

Niestety, cyberprzemoc nie kończy się wraz z wyłączeniem komputera – np. raz udostępnione w sieci krzywdzące treści mogą krążyć online miesiącami, stale przypominając ofierze o wyrządzonej szkodzie. Ponadto wirtualnym atakom trudniej jest zapobiegać, bo szybko się rozprzestrzeniają, a ich sprawcy są na ogół anonimowi. Co przeżywają ofiary cyberprzemocy?

Osoby dotknięte przemocą w sieci często czują się samotne, bezradne i zastraszone. Obawiają się upokorzenia i kompromitacji, co może prowadzić do lęku, smutku, a nawet depresji. Często zmagają się też z poczuciem winy, trudnościami w relacjach społecznych, spadkiem samooceny oraz problemami w nauce. Ponadto odczuwają dolegliwości zdrowotne, takie jak bóle głowy, brzucha, mają problemy ze snem itp. W skrajnych przypadkach mogą mieć myśli lub podejmować próby samobójcze (Borkowska, 2023).

Dręczenie, hejt, wykluczenie z grona znajomych, ośmieszanie w sieci może dotknąć każdego, stąd tak ważna jest profilaktyka. Po pierwsze, warto tłumaczyć uczniom, czym tak naprawdę jest cyberprzemoc, bo niektórzy (17%) nie potrafią nawet jednoznacznie stwierdzić, czy doświadczyli cyfrowej agresji (Ładna i in., 2025). Po drugie, należy uczyć, jak radzić sobie z atakami w internecie oraz gdzie można uzyskać profesjonalną pomoc. Niezwykle ważna jest także edukacja świadków przemocy w zakresie tego, co mogą zrobić, by przerwać obserwowane akty nękania w sieci i tym samym wspierać ofiary cyberbullyingu.

W edukacji i wychowywaniu istotne jest wyposażanie dzieci w umiejętności społeczne, które pomagają ograniczać ryzyko angażowania się przez nie w cyberprzemoc. Kluczowe są: samokontrola, regulacja emocji, empatia, zdolność patrzenia z perspektywy innych oraz przestrzeganie norm społecznych – zarówno online, jak i offline.

A jak reagować, gdy dziecko/uczeń padnie ofiarą cyberprzemocy? Najważniejsze to okazać mu zrozumienie i wsparcie. Postarajcie się wspólnie przeanalizować sytuację i zrozumieć, co się wydarzyło. Równocześnie zabezpieczcie dowody cyberprzemocy – warto zachować lub wydrukować wiadomości e-mail, SMS, MMS, rozmowy z komunikatorów internetowych, wpisy i komentarze z portali społecznościowych, blogów czy stron internetowych. Zgromadzone materiały mogą pomóc w identyfikacji sprawcy, usunięciu szkodliwych treści przez administratora serwisu, a także będą istotnym źródłem informacji dla osób zaangażowanych w rozwiązanie sprawy.

Pamiętajcie – cyberprzemoc to naruszenie prawa! Każdy taki przypadek – uporczywe nękanie, podszywanie się pod inną osobę, kradzież tożsamości, groźby, publikowanie niedozwolonych materiałów – należy zgłaszać odpowiednim służbom, w tym policji. W usunięci z sieci szkodliwych treści pomoże działający w NASK zespół Dyżurnet.

Skorzystajcie z naszych materiałów edukacyjnych na temat przemocy w sieci, dostępnych na stronie OSE IT Szkoła: kursów e-learningowych, animacji, poradników (w tym zboru felietonów „O cyberprzemocy i hejcie w sieci”), scenariuszy lekcji, plakatów, infografik. Zachęcamy też do lektury aktualności na ose.gov.pl: „Bezpieczni w sieci z OSE: cyberbullying”.

Źródła:

Borkowska A., (2023), „Cyberprzemoc w szkole. Poradnik dla nauczycieli”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Cybersquatting

Cybersquatting określany jest często jako piractwo domenowe czy spekulacja domenami. Nazwa tego cyberzagrożenia pochodzi od angielskiego słowa squatting, dosłownie oznaczającego „czaić się”, a powszechnie używanego do nazwania procederu zamieszkiwania opuszczonego domu lub mieszkania bez zgody właściciela. Z przestępcami praktykującymi cybersquatting jest podobnie. Wykupują oni niezarejestrowane domeny łudząco podobne w nazwie do znanych stron lub zawierające inne rozszerzenie niż oryginalna witryna, np. com, .com.pl, .eu czy .pl. Następnie próbują odsprzedać takie domeny za dużo większą kwotę firmom, pod które się podszywają. Warto wspomnieć, że ofiarami tego procederu padają nie tylko duże, znane marki, ale też mniejsze przedsiębiorstwa.

Jaki jest cel działania cybersquattera? Próbuje on przede wszystkim uzyskać korzyści majątkowe, ale może też działać na szkodę firmy, np. publikując na swojej stronie, która kojarzy się z daną marką, treści godzące w jej dobre imię. Może też wykorzystać spreparowaną witrynę łudząco podobną do tej oryginalnej w celu wyłudzenia od użytkowników danych uwierzytelniających (loginów, haseł) czy zainfekowania naszego sprzętu złośliwym oprogramowaniem (malware). To oznacza, że niepostrzeżenie możemy pobrać na swoje urządzenie np. ransomware, adware czy spyware, ułatwiając tym samym cyberprzestępcom dostęp do naszych danych. Jak się chronić przed cybersquattingiem?

Jeśli jesteście właścicielami firmy:

- Zarejestrujcie nazwę swojej domeny jako znak towarowy. Wtedy będziecie mieli wyłączne prawo do wykorzystywania danej nazwy, a jeśli ktoś będzie chciał się nią posłużyć, łatwiej wygracie sprawę przed sądem.

C

- Możecie też zarejestrować swoją domenę w kilku wariantach, korzystając z różnych rozszerzeń oraz kilku wersji pisowni (np. „mojsklep.pl", „moj-sklep.com"). Pamiętajcie przy tym, żeby na czas przedłużyć ważność domeny.
- Korzystajcie z usług związanych z monitoringiem domen, dzięki którym szybko wykryjecie próbę podszywania się pod Waszą firmę.

Jeśli jesteście użytkownikami sieci, uważajcie na: fałszywe domeny, które podszywają się pod znane podmioty, firmy i instytucje, oraz akcje phisingowe i przesyłane w wiadomościach (SMS, e-mail, na komunikatorach) linki – mogą one przenieść Was na niebezpieczne strony.

Pamiętajcie, że cybersquatting zgodnie z zapisami art. 5 Ustawy o zwalczaniu nieuczciwej konkurencji jest niezgodny z prawem i oznacza działanie polegające na wprowadzaniu w błąd co do tożsamości przedsiębiorstwa.

Macie podejrzenie, że jakaś witryna internetowa służy do wyłudzenia danych lub pieniędzy? Koniecznie zgłoście to do CERT Polska za pomocą formularza na stronie incydent.cert.pl. Eksperci ocenią, czy wpisać ją na listę ostrzeżeń przed niebezpiecznymi stronami. Z kolei niepokojące SMS-y, zawierające potencjalnie groźne linki, przesyłajcie na numer 8080, korzystając funkcji „przekaż" albo „udostępnij".

Źródło:

„Cybersquatting w praktyce – na czym polega? Jak się przed nim zabezpieczyć?", (2023), artykuł w serwisie netia.pl.

Cyberstalking

To internetowa odmiana stalkingu, która polega na uporczywym, celowym nękaniu drugiej osoby za pomocą narzędzi cyfrowych (np. przy wykorzystaniu serwisów społecznościowych czy komunikatorów). Ten rodzaj cyberprzemocy może mieć swoje źródło zarówno w świecie online, jak i offline.

Cyberstalkingiem określamy m.in. nękanie poprzez wielokrotne wysyłanie komuś w sieci lub przy użyciu nowych technologii niechcianych materiałów i informacji, cyberdręczenie, kradzież tożsamości, nielegalny monitoring, śledzenie, rozsyłanie wiadomości w imieniu innej osoby, ale wbrew jej woli. Działania stalkera wywołują u ofiary: strach, panikę, wstyd, poczucie winy. Ponadto osoby doświadczające prześladowania tracą poczucie bezpieczeństwa i zaufanie do ludzi. Mogą też cierpieć na zaburzenia lękowe, a nawet popaść w depresję.

Co robić, jeśli Wy lub ktoś z Waszych bliskich znalazł się na celowniku cyberstalkera? Przede wszystkim nie odpowiadajcie na wiadomości napastnika. Jeśli znacie jego tożsamość – natychmiast zablokujcie mu dostęp do swoich profili w mediach społecznościowych. Ponadto zgłoście sprawę administratorowi platformy, za pomocą której otrzymujecie niechciane wiadomości.

Pamiętajcie, żeby zawsze dbać o profilaktykę, która może Was uchronić przed cyberstalkerem:

- **Minimalizujcie swój cyfrowy ślad.** Udostępniajcie w sieci jak najmniej informacji o sobie, w tym dotyczących Waszej geolokalizacji. Przestępca na pewno skrzętnie zbierze wszystkie wiadomości, aby Was osaczyć, szczególnie te wpływające na bezpieczeństwo i wizerunek.
- **Dbajcie o prywatność w sieci**. Korzystajcie z ustawień prywatności w portalach społecznościowych, nie wszyscy muszą mieć dostęp do publikowanych przez Was treści.
- **Bądźcie asertywni.** Reagujcie, gdy ktoś bez Waszej zgody zamieszcza w internecie treści naruszające Waszą prywatność lub przedstawiające Was w negatywnym świetle. Warto wcześniej ustalić z bliskimi zasady dotyczące udostępniania online wspólnych zdjęć i filmików.
- **Róbcie porządki.** Usuwajcie historię przeglądania i wyszukiwania, pliki cookies czy nieużywane konta w mediach społecznościowych i innych serwisach.

- **Zabezpieczajcie swoje profile i urządzenia.** Używajcie silnych haseł, uwierzytelniania dwuskładnikowego oraz dbajcie o aktualizację oprogramowania i aplikacji. Uważajcie też na phishing – weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem, zwracajcie uwagę na rozszerzenie pliku załączników do wiadomości mailowych i nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości.
- Korzystajcie z prawa do bycia zapomnianym. Zawsze możecie prosić o usunięcie z internetu materiałów, które Was dotyczą. Takie prawo wynika z rozporządzenia unijnego RODO (Ogólnego rozporządzenia o ochronie danych).

Cyberstalking jest przestępstwem! Wszelkie przejawy uporczywego nękania zgłaszajcie na policję. Wcześniej zabezpieczcie jednak dowody celowego działania sprawcy: e-maile, SMS-y, MMS-y, wiadomości w komunikatorach, wpisy na stronach internetowych, komentarze do wpisów lub do zdjęć w serwisach społecznościowych, na blogach itp.

Jeśli potrzebujecie wsparcia w kryzysie, skorzystajcie z pomocy specjalisty. Pomoc znajdziecie też, dzwoniąc na bezpłatne linie pomocowe – helpline, np. pod numer 116 111 (116111.pl) – anonimowy telefon zaufania dla dzieci lub 116 123 – kryzysowy telefon zaufania dla dorosłych.

Cyfrowy ślad

Wszyscy zostawiamy w internecie swój cyfrowy ślad – odciska go każda aktywność w sieci. Nasze dane (m.in. wpisywane w formularzach e-sklepów, wysyłane w wiadomościach czy przekazywane razem z komentarzami w mediach społecznościowych) trafiają do baz danych i chmur obliczeniowych, a tam… zaczynają żyć własnym życiem.

Swój cyfrowy ślad możemy zostawiać celowo – gdy wysyłamy e-maile, komentujemy posty w mediach społecznościowych, publikujemy zdjęcia czy filmy. Bierne ślady to m.in. informacja o systemie operacyjnym, adresie IP, używanej przeglądarce internetowej, ale też dane geolokalizacyjne czy godzina i data wykonania zdjęcia dodanego do posta w social mediach. Nawet jeśli wydaje nam się, że pozostajemy anonimowi, udostępniamy informacje o swoich kliknięciach, które mogą być analizowane, rejestrowane i przechowywane. Profilowane reklamy i bańki informacyjne to dopiero początek – dziś jeszcze nie do końca wiemy, jak nasze dane będą wykorzystywane w przyszłości!

Z internetu nie tak łatwo wymazać raz opublikowane treści na nasz temat, choć to możliwe. Przysługujące każdemu prawo do bycia zapomnianym, związane z unijnym rozporządzeniem RODO (Ogólnym rozporządzeniem o ochronie danych), pomaga np. w usunięciu danych osobowych z wyszukiwarek i innych platform internetowych. Warto jednak pamiętać, że zawsze gdzieś może się zachować kopia jakiejś informacji.

Kompromitujące zdjęcie z młodości, zabawny post, który nie przetrwał próby czasu, publikowanie kontrowersyjnych treści, nienawistnych komentarzy – to wszystko może sprawić, że budowana przez lata reputacja w sekundę legnie w gruzach. Wystarczy, że przyszły pracodawca, znajomy czy niedoszła miłość trafi na materiał, po obejrzeniu którego wyrobi sobie o nas niezbyt pochlebną opinię, przez co zamknie się przed nami wiele drzwi. Dlatego już od początku swojej aktywności w sieci należy zadbać o własną cyfrową wizytówkę, bo ta będzie nam towarzyszyć przez długi czas.

Czy można zminimalizować swój cyfrowy ślad? Tak!

- **Bądźcie uważni w mediach społecznościowych.** Dostosujcie ustawienia prywatności i rozważnie dzielcie się treściami w internecie.
- **Używajcie trybu prywatnego (incognito, In Private) w przeglądarkach.** Dzięki temu uchronicie się przed zapisywaniem Waszej historii przeglądania, danych w formularzach czy tzw. ciasteczek.
- **Pamiętajcie o ukrytych danych.** Zdjęcia, filmy i inne dokumenty mogą zawierać informacje o ich autorze, czasie utworzenia czy lokalizacji. Zanim coś opublikujecie, sprawdźcie, jakie

C

dane dodatkowo udostępniacie. Pomocne może być wyłączenie funkcji geolokalizacji w smartfonie.

- **Reagujcie na publikacje bez Waszej zgody.** Jeśli ktoś bez konsultacji z Wami udostępnił w internecie materiał, np. stawiający Was w niekorzystnym świetle, warto poprosić o jego usunięcie. Najlepiej wcześniej ustalić ze znajomymi i rodziną zasady zamieszczania online wspólnych zdjęć oraz materiałów wideo.
- **Pamiętajcie o regularnych porządkach.** Pozbywajcie się nieużywanych kont lub adresów e-mail oraz sprawdźcie, czy aplikacje, z których korzystacie, nie mają dostępu do zbyt wielu Waszych danych.

Chcecie dowiedzieć się więcej o cyfrowym śladzie i ochronie swojego wizerunku online? Sięgniecie do aktualności na stronach ose.gov.pl i OSE IT Szkoła: „Cyberbezpieczna biblioteczka: cyfrowy ślad" i „Bezpieczni w sieci z OSE na wakacje: oversharing i cyfrowy ślad" oraz publikacji Dyżurnet.pl „Cyfrowy ślad małego dziecka".

D

Dane osobowe

Zgodnie z definicją Komisji Europejskiej dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej. Skomplikowane, prawda? Mówiąc prościej, to m.in. imię i nazwisko, adres zamieszkania, adres e-mail zawierający istotne dane (np. nazwisko@firma.com), numer dowodu tożsamości czy dane geolokalizacyjne (np. ustawienia lokalizacji w telefonie komórkowym) i adres IP.

Naszymi danymi osobowymi, niestety, coraz częściej interesują się cyberprzestępcy. Dlatego trzeba je szczególnie chronić – zwłaszcza w internecie. Jak możecie to zrobić?

- **Zachowajcie czujność i przestrzegajcie zasady ograniczonego zaufania.** Szereg rozwiązań oferowanych w sieci wymaga rejestracji, która wiąże się z przekazaniem swoich danych osobom trzecim. Jeśli zdecydujecie się na założenie jakiegoś konta internetowego lub korzystanie z aplikacji mobilnej, uważnie przeczytajcie ich politykę prywatności. Zastanówcie się, czy nic nie budzi Waszych wątpliwości i czy na pewno dana strona potrzebuje wymaganych danych, a także czy podanie ich nie przyniesie w przyszłości kłopotów. Pamiętajcie także o weryfikowaniu otrzymanych linków przed kliknięciem, nawet jeśli pochodzą od znajomych.
- **Używajcie silnych i unikatowych haseł.** Skorzystajcie również z możliwości uwierzytelniania dwuskładnikowego lub wieloskładnikowego. Takie zabezpieczenie zapewni konieczność dodatkowej weryfikacji osoby logującej się do wirtualnych usług (m.in. bankowości internetowej czy portali społecznościowych), będzie więc dla Was kolejną warstwą ochrony.
- **Zadbajcie o ustawienia przeglądarki.** Zmieńcie opcje prywatności w ustawieniach przeglądarki lub włączcie tryb incognito. Umożliwi to ograniczenie zakresu udostępnianych informacji, a także używania i przechowywania plików cookies.
- **Sprawdzajcie instalowane aplikacje**. Zanim zdecydujecie się na pobranie i korzystanie z danego programu, upewnijcie się, czy nie jest fałszywy i czy za jego pośrednictwem przestępca nie podszywa się pod producenta oryginalnej wersji. W tym celu warto zweryfikować m.in. opinie innych użytkowników oraz widoczną w sklepie liczbę pobrań. Sprawdzajcie też, do jakich danych mają dostęp poszczególne aplikacje.
- **Dbajcie o swój sprzęt – aktualizujcie oprogramowanie i program antywirusowy.**
- **Kontrolujcie swój cyfrowy ślad.** Publikujcie w sieci jak najmniej informacji na swój temat oraz dobrze się zastanówcie, czy dana treść, post, filmik lub komentarz powinny znaleźć się w sieci – raz wrzucone zasoby mogą nigdy nie zniknąć i w przyszłości zostać wykorzystane.
- **Korzystajcie z prawa do bycia zapomnianym**. Wielu użytkowników sieci nie zdaje sobie sprawy z przysługującego im prawa do bycia zapomnianym, które jest jedną z gwarancji prawa do prywatności. Oznacza to, że osobom fizycznym przysługuje prawo do usunięcia swoich danych, jeśli wycofają zgodę o przetwarzaniu danych osobowych i nie występują inne zasadne podstawy do ich zachowania, tj. nie są one już niezbędne do celów, do jakich zostały pobrane, lub nie muszą być w inny sposób przetwarzane.
- **Zwracajcie uwagę na otrzymywane SMS-y czy e-maile.** Cyberprzestępcy wykorzystują takie wiadomości m.in. do ataku phishingowego, którego celem może być wyłudzenie nie tylko danych osobowych, ale i np. danych dostępowych do bankowości elektronicznej. Kradzież danych bywa dotkliwsza niż utrata rzeczy materialnych!

Musicie też wiedzieć, że bazy danych (zgromadzone np. w serwisach zakupowych czy bankach) wyciekają, a więc stają się publicznie dostępne. Możecie sprawdzić, czy Wasze dane logowania

i inne prywatne informacje nie dostały się w ręce cyberprzestępców – wejdźcie np. na stronę haveibeenpwned.com lub bezpiecznedane.gov.pl i wpiszcie tam swój adres e-mailowy. Jeśli doszło do wycieku, koniecznie zmieńcie hasło we wskazanych serwisach, a także wszędzie, gdzie używaliście podobnego hasła.

Więcej informacji o ochronie danych osobowych znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: phishing" i „Bezpieczni w sieci z OSE: ochrona danych osobowych".

Źródło:

„Ochrona danych zgodnie z RODO", (2025), artykuł na stronie europa.eu.

Deepfake

Dotychczas bywaliśmy nieufni wobec zdjęć, które w obecnych czasach łatwo przecież przerobić, a więc zmanipulować. Niestety to samo dotyczy też… filmów. Być może spotkaliście się już w sieci ze sfabrykowanymi nagraniami, stworzonymi przy użyciu prawdziwych próbek głosu, wideo i zdjęć. Film z udziałem znanego polityka lub celebryty zawierający nieprawdziwe, niewiarygodne informacje? Uwaga, to może być deepfake!

Deepfake (od ang. *deep learning* – systemy głębokiego uczenia maszynowego oraz *fake* – fałsz) bazuje na zaawansowanych algorytmach uczenia maszynowego, w szczególności technice zwanej deep learning oraz modelach generatywnych, np. GAN (ang. *Generative Adversarial Networks*). System „uczy się" wyglądu i głosu konkretnej osoby na podstawie dostępnych materiałów (zdjęć, filmów, nagrań dźwiękowych), a następnie generuje nowe treści, które do złudzenia przypominają oryginał.

Pierwsze deepfake'i miały charakter rozrywkowy, ale szybko stały się narzędziem dezinformacji, manipulacji i cyberprzestępstw. W erze masowego dzielenia się treściami online fałszywe wideo może rozprzestrzenić się błyskawicznie i wywołać realne skutki. Takie materiały rozpowszechniają nieprawdziwe wiadomości, sieją dezinformację, manipulują opinią publiczną. Są też w stanie zniszczyć reputację konkretnych osób – to główny cel tego rodzaju działań.

Gdzie można natknąć się na deepfake'i?

- **Polityka i dezinformacja** – fałszywe przemówienia liderów państw mogą siać zamęt, podważać zaufanie do instytucji i destabilizować sytuację społeczną.
- Media społecznościowe – fałszywe wideo z udziałem influencerów lub znanych osób może szybko zdobyć miliony wyświetleń i wpływać na opinię publiczną.
- **Cyberprzestępczość** – deepfake'i mogą posłużyć do wyłudzania pieniędzy, np. za sprawą spreparowanych nagrań wykorzystywanych w atakach phishingowych.
- **Przemoc w sieci** – technologia bywa wykorzystywana do tworzenia deepfake'ów o charakterze pornograficznym, co jest formą cyberprzemocy.

Choć technologia się rozwija, nadal istnieją pewne sygnały ostrzegawcze, które mogą świadczyć o tym, że mamy do czynienia z deepfake'em:

- **Nienaturalne ruchy twarzy** – zwróć uwagę na oczy (rzadkie mruganie, martwe spojrzenie), usta (źle zsynchronizowana mowa) czy brak płynnych zmian mimiki.
- **Zniekształcenia i artefakty** – nieostrości, dziwne przejścia w okolicach uszu, włosów czy szyi mogą świadczyć o sztucznie wygenerowanym obrazie.
- **Niespójność głosu** – choć syntezatory mowy są coraz lepsze, spreparowane nagrania nadal mogą zawierać nienaturalne pauzy lub akcenty.
- **Brak źródła** – jeśli wideo pojawiło się nagle i nie zostało potwierdzone przez żadne wiarygodne media lub instytucje – warto je dokładnie sprawdzić.

Choć przeciętny użytkownik internetu nie jest w stanie zatrzymać rozwoju deepfake'ów, może nauczyć się funkcjonować w świecie, gdzie takie treści istnieją. Jak to zrobić?

Po pierwsze: **zachowajcie czujność i sceptycyzm**. Zanim uwierzycie w to, co widzicie, odpowiedzcie sobie na pytania: Czy materiał pochodzi z wiarygodnego źródła? Czy zawiera kontrowersyjne, szokujące treści, które mogą wzbudzać silne emocje?

Po drugie: **sprawdzajcie informacje**. Korzystajcie z narzędzi fact-checkingowych, takich jak serwisy Demagog (demagog.org.pl), Sprawdzam AFP (sprawdzam.afp.com) czy Fact-checking PAP (pap.pl/fact-checking). W przypadku podejrzanego wideo spróbujcie je zweryfikować w niezależnych mediach.

Po trzecie: **zabezpieczcie swoje dane i wizerunek**. Nie publikujcie zbyt wielu zdjęć i filmów w wysokiej jakości, szczególnie w mediach społecznościowych. Im więcej materiałów z Waszym udziałem w sieci, tym łatwiej stworzyć wiarygodny deepfake.

Po czwarte: **zgłaszajcie podejrzane materiały**. Jeśli podejrzewacie, że materiał może być deepfake'iem, zgłoście go do administratora platformy lub odpowiednich służb. Możecie skorzystać też z formularza dostępnego na stronie Państwowego Instytutu Badawczego NASK: zglos-dezinformacje.nask.pl.

Chcecie dowiedzieć się więcej? Sięgnijcie do kursu e-learningowego „Dezinformacja, czyli w co (nie) wierzyć w internecie" na platformie OSE IT Szkoła oraz aktualności na stronie ose.gov.pl: „Jak nie wpaść w pułapkę fake newsów" i „Czy to nagranie może kłamać? Uwaga na deepfake!".

Źródło:

„Nauczyciel w świecie deepfake – czy uwierzyłbyś swoim oczom?", (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

Dezinformacja

Dezinformacji przyświeca jeden cel: szerzenie nieprawdziwych lub zmanipulowanych wiadomości. To forma przekazu bazująca na różnego rodzaju treściach, które wprowadzają odbiorców w błąd, a dodatkowo skłaniają ich do podejmowania określonych działań.

Dezinformacja celowo destabilizuje sytuację w państwie, a także wywiera destrukcyjny wpływ na obywateli – wykorzystuje się ją do wyrządzania krzywdy zarówno pojedynczym osobom (np. politykom czy celebrytom, dziennikarzom i nie tylko), ale też grupom czy organizacjom. Takie działania mają wywołać niepewność lub wrogość oraz podsycać negatywne emocje. Warto wiedzieć, że dezinformacja nastawia przeciwko sobie różne grupy społeczne i tworzy obraz świata niezgodny z rzeczywistością.

Z jakimi narzędziami dezinformacji możecie zetknąć się w internecie?

- **Wątpliwe, fałszywe wiadomości**, które zazwyczaj powołują się na nieistniejące lub niezbyt wiarygodne źródła, np. naocznych świadków. Najczęściej informują o jakimś sensacyjnym wydarzeniu, wykorzystując w tym celu krzykliwy nagłówek i nacechowany emocjonalnie język.
- **Podszywanie się pod instytucje/podmioty publiczne**. Oszuści korzystają tutaj z łudząco podobnych lub identycznych logotypów, zdjęć profilowych, nazw, aliasów i innych elementów charakterystycznych dla danej instytucji. Liczą na to, że przeczytamy sfabrykowaną wiadomość pobieżnie i uwierzymy w nią jak w oficjalny komunikat.
- **Deepfake**. To technika obróbki obrazu, wykorzystująca zdobycze sztucznej inteligencji, w której na podstawie prawdziwych próbek głosu, filmów i zdjęć powstaje nowy sfabrykowany materiał, łudząco przypominający prawdziwe treści.
- **Manipulowanie dowodami i danymi**. Ta forma dezinformacji polega na przedstawieniu sfabrykowanych zdjęć i filmów. Materiały te często przedstawiają szokujące wydarzenia

lub inne sytuacje budzące skrajne emocje. Są przy tym wyrwane z kontekstu, co sprawia, że odbiorca nie ma pełnych informacji i nie może ocenić prawdziwości danego materiału.

- **Teorie spiskowe**. Najprościej rzecz ujmując, są to wszelkie próby objaśniania świata, sprzeczne z powszechnie uznaną wersją wydarzeń. Mają zasiać niepewność w społeczeństwie, utwierdzić ludzi w przekonaniu, że za określonymi sytuacjami i zdarzeniami stoją spiskowcy. Dają złudne poczucie bezpieczeństwa w niepewnej sytuacji.

Pamiętajcie: dezinformacja karmi się naszymi lękami i uprzedzeniami. Ci, którzy rozprzestrzeniają fałszywe wiadomości, grają na emocjach, wiedzą, że uwagę odbiorców przykuwają szokujące nagłówki i złe informacje. Zależy im, żeby te treści jak najszybciej dotarły do jak największej liczby osób. Zastanówcie się więc dwa razy, zanim udostępnicie w sieci niesprawdzony news!

Warto wiedzieć, że za dezinformacją stoją m.in. internetowi trolle i boty, a także – czasem nieświadomie – liderzy opinii, politycy, służby poszczególnych krajów, a także… my sami (zwłaszcza gdy bezrefleksyjnie komentujemy lub udostępniamy niezweryfikowane treści).

Choć walka z dezinformacją jest trudna, na szczęście nie jesteśmy z góry skazani na niepowodzenie. Jak rozpoznawać fałszywe treści w sieci?

1. **Sprawdźcie autora, datę i źródło**. Podchodźcie nieufnie do materiałów, w których brakuje tych podstawowych informacji. Zwracajcie uwagę na datę – być może news jest nieaktualny.
2. **Korzystajcie z rzetelnych źródeł i starajcie się potwierdzić informację w kilku źródłach**. Im więcej źródeł, tym większa pewność, że wiadomość jest prawdziwa!
3. **Nie wyrabiajcie sobie zdania na dany temat wyłącznie po lekturze nagłówka artykułu**. Leady często zawierają sensacyjne informacje – tylko po to, by przykuć uwagę odbiorców.
4. **Zastanówcie się, czy dana wiadomość bazuje na faktach, czy na opiniach**. Sprawdźcie, czy jej autor popiera swoje twierdzenia dowodami i nie odnosi się do własnych odczuć.
5. **Spróbujcie popatrzeć na informację z szerszej perspektywy**. Zastanówcie się, jak na ocenę wiarygodności informacji wpływają Wasze poglądy. Może niektóre wiadomości przyjmujecie bezkrytycznie?
6. **Przeczytajcie informację (artykuł, post itd.) uważnie**. Jeśli znajdziecie błędy językowe albo Waszą uwagę zwróci emocjonalny język, najprawdopodobniej macie do czynienia ze zmanipulowaną wiadomością.
7. **Przeanalizujcie okoliczności**. Fake newsy często są wyrwane z szerszego kontekstu, dzięki czemu jeszcze łatwiej mogą wprowadzić odbiorców w błąd. Zawsze zwracajcie uwagę na miejsce, czas i okoliczności przekazu danej informacji.

Pomocne informacje znajdziecie w aktualności „Jak nie wpaść w pułapkę fake newsów" nastronie ose.gov.pl oraz w kursie e-learningowym „Dezinformacja, czyli w co (nie) wierzyć w internecie" i w pakiecie materiałów dotyczących fałszywych wiadomości: ulotce „Fake newsy, bańki informacyjne, teorie spiskowe", konspekcie zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole" i grafice „Jak rozpoznać fake newsa?" dostępnym na platformie OSE IT Szkoła.

Digital self-harm

Cyfrowy świat wiąże się nie tylko z pozytywnymi doświadczeniami, ale też z cyberzagrożeniami – w tym z cyberprzemocą, zwaną również cyberbullyingiem. Internet to miejsce, w którym dochodzi zarówno do wielu aktów agresji, jak i autoagresji. Digital self-harm, czyli cyfrowe samookaleczenie, to przykład psychicznego znęcania się w sieci nad sobą. Jakie są przyczyny takiego zachowania i jak wyrządzanie sobie krzywdy online wpływa na zdrowie i samopoczucie?

Przywykliśmy do tego, że autorami nieprzychylnych komentarzy na forach czy w mediach społecznościowych są inni użytkownicy sieci, a my możemy łatwo paść ofiarą ich działań: hejtu,

mowy nienawiści. Tymczasem psychologowie zwracają uwagę na nową formę cyberprzemocy, która polega na samodzielnym, anonimowym publikowaniu z fikcyjnych kont krzywdzących treści na swój temat.

Znęcanie się nad sobą dotyczy głównie nastolatków i może mieć różne podłoże: czasem to forma zabawy, sposób na zwrócenie na siebie uwagi, znalezienie pocieszenia, uzyskanie wymuszonych komplementów, próba udowodnienia, że jest się odpornym na ataki, a czasem to wyraz głębszych problemów, np. z depresją czy regulacją emocji.

Digital self-harm to akt poniżania, zastraszania, nękania siebie w sieci. Takie zachowanie może więc wpływać na poczucie własnej wartości, powodować problemy związane ze zdrowiem psychicznym, a nawet prowadzić do myśli samobójczych. Może mieć również wpływ na życie zawodowe, codzienne funkcjonowanie czy kwestie wizerunkowe.

Jeśli dostrzeżecie, że ktoś w Waszym otoczeniu jest zaangażowany w cyfrowe samookaleczenie, podejmijcie odpowiednie kroki:

- Rozmawiajcie – okażcie zainteresowanie problemem, z którym mierzy sią dana osoba, spróbujcie ustalić powody ryzykownego zachowania i spytajcie, jak możecie pomóc.
- Wykażcie się empatią – nie krytykujcie i nie oceniajcie. Starajcie się wczuć w sytuację emocjonalną osoby dokonującej aktów samoagresji.
- Zaoferujcie profesjonalną pomoc – zaproponujcie pomoc psychologa lub terapeuty, który udzieli wsparcia w radzeniu sobie z emocjami i negatywnymi myślami.
- Reagujcie – jeśli podejrzewacie, że czyjeś życie lub zdrowie jest zagrożone, skontaktujcie się z odpowiednimi służbami, np. linią wsparcia dla osób w kryzysie lub policją.

Pamiętajcie, że istnieją różne zespoły i linie pomocowe – to przede wszystkim Dyżurnet.pl (dyzurnet.pl) i telefony zaufania (helpline), np.: 800 100 100 dla rodziców i nauczycieli, 116 111 dla dzieci i młodzieży czy Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka 800 12 12 12.

Źródło:

Sreenivas S., (2023), „What Is Digital Self-Harm?”, artykuł w serwisie webmd.com.

Dobrostan cyfrowy

Urządzenia cyfrowe zajmują coraz więcej miejsca w naszym życiu. Można powiedzieć, że ekrany stały się nieodłączną częścią codziennego funkcjonowania. Smartfon mamy zawsze w zasięgu ręki, niejednokrotnie uczymy się i pracujemy przy komputerze, natomiast w czasie wolnym załatwiamy sprawy online lub po prostu korzystamy z urządzeń dla rozrywki. Nasze – a w szczególności młodych – zamiłowanie do nowych technologii potwierdzają badania. Z raportu NASK „Nastolatki” wynika, że spędzają oni w internecie 4 godziny i 59 minut w dni powszednie oraz 5 godzin i 16 minut w weekendy (Ładna i in., 2025).

Popularność nowych technologii sprawiła, że zaczęliśmy baczniej przyglądać się ich wpływowi na nasze życie. Okazuje się, że im więcej czasu zabierają nam urządzenia cyfrowe, tym większe prawdopodobieństwo wystąpienia problemów ze zdrowiem i codziennym funkcjonowaniem. Ból głowy, szyi, zmęczenie, zaburzenia snu – to przykłady fizycznych objawów nadużywania ekranów. Niekontrolowane korzystanie z sieci ma też wpływ na zdrowie psychiczne. Często mierzymy się ze stresem cyfrowym, przeciążeniem informacją, FOMO (ang. *Fear of Missing Out*), czyli lękiem przed odłączeniem, PUI – problemowym używaniem internetu, a nawet e-uzależnieniami.

Pewnie zgodzicie się z tym, że z nowych technologii trudno jest dziś zrezygnować, warto jednak zadbać o równowagę online–offline, inaczej mówiąc o swój dobrostan cyfrowy (ang. *digital well-being*). Czym dokładnie jest i jak go osiągnąć?

D

Każdego dnia staramy się dbać o swoje dobre samopoczucie – psychiczne i fizyczne. Na drodze do osiągnięcia zadowolenia z życia należy zwrócić uwagę również na dobrostan cyfrowy. Odnosi się on do zdrowego i zrównoważonego sposobu korzystania z nowych technologii: smartfonów, komputerów i internetu. Oznacza to takie użytkowanie urządzeń, by były one dla nas wsparciem w rozwoju i codziennym funkcjonowaniu, a nie wpływały na nas negatywnie.

Utrzymanie higieny cyfrowej to wyzwanie. Warto je podjąć, by osiągnąć dobrostan cyfrowy. Oto kilka kroków, które pomogą Wam czerpać korzyści z wykorzystania nowych technologii:

- **Kontrolujcie czas spędzany w sieci.** Pilnujcie, by aktywności z urządzeniem cyfrowym nie wpływały na Wasze codzienne obowiązki, nie przysłaniały potrzeby budowania relacji poza siecią, nie wpływały na jakość odpoczynku. Zadbajcie o równowagę w sieci i poza nią. W kontroli czasu spędzanego z urządzeniem pomogą Wam aplikacje do zarządzania sposobem korzystania z telefonu.
- **Dbajcie o pozytywne doświadczenia online.** Unikajcie kontaktów ze szkodliwymi treściami, bądźcie wyczuleni na wszelkie próby siania dezinformacji. Skupiajcie się na pozytywnych i wartościowych przekazach, dbajcie też o dobre interakcje w sieci. Ponadto reagujcie na przejawy hejtu i cyberprzemocy.
- **Zwiększcie swoje bezpieczeństwo.** Przede wszystkim chrońcie swoją prywatność w sieci, strzeżcie się przed cyberprzestępcami, szczególnie uważajcie na phishing, fałszywe panele logowania czy fałszywe domeny, a tym samym na próby wyłudzenia od Was cennych informacji, takich jak: loginy, hasła (np. do bankowości internetowej), numery karty płatniczej, PESEL czy numer dowodu osobistego. Jeśli natkniecie się w sieci na stronę, która wzbudza podejrzenia, zgłoście ją do CERT Polska, wypełniając formularz dostępny na stronie incydent.cert.pl.
- **Ograniczcie multitasking.** Praktykujecie cyfrowy multitasking, czyli np. oglądacie film, a w tym samym czasie scrollujecie media społecznościowe, robicie zakupy online i odpisujecie na e-maile? Starajcie się nie korzystać ze zbyt wielu ekranów naraz! Przebodźcowanie nadmiarem informacji wiąże się m.in. z uwolnieniem hormonów stresu, a przewlekły stres powoduje wyczerpanie ciała i umysłu, w tym problemy ze snem. Podczas wykonywania zadań wymagających skupienia usuńcie urządzenia z zasięgu wzroku, wyłączcie powiadomienia, zadbajcie o regenerujące przerwy – krótki spacer czy obserwowanie widoków za oknem.
- **Zadbajcie o zdrowy sen.** Wyciszenie umysłu przed snem oraz poranne, powolne wejście w nowy dzień to sprawa kluczowa dla zdrowia. Zadbajcie o to, aby w tych rytuałach nie towarzyszył Wam telefon. Nie korzystajcie ze smartfonów co najmniej godzinę przed zaśnięciem i zaraz po przebudzeniu.
- **Planujcie aktywności offline.** Spotkania z przyjaciółmi, dobra książka, spacer, rower, sport, rozwijanie pasji… pomysłów na spędzenie czasu poza siecią jest wiele. Odłączajcie się od internetu tak często, jak to możliwe!

Źródła:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy", Warszawa: Państwowy Instytut Badawczy NASK.

Śliwowski K., (2022), „Jak dbać o swój cyfrowy dobrostan", artykuł w serwisie otwartezasoby.pl.

Domowa sieć Wi-Fi

W dzisiejszych czasach stabilne i szybkie łącze internetowe jest kluczowe dla komfortu korzystania z sieci. W domu, gdzie wiele urządzeń jednocześnie korzysta z internetu, warto dobrze zaplanować swoją sieć, aby zapewnić jej stabilność i bezpieczeństwo.

Mówiąc najprościej, Wi-Fi (ang. *Wireless Fidelity*) to standardy stworzone do budowy bezprzewodowych sieci komputerowych. Łączycie swoje sprzęty z internetem bez użycia kabla? Korzystacie z Wi-Fi! To rozwiązanie jest wygodne i idealne dla urządzeń mobilnych, takich jak laptopy, smartfony czy tablety. Wiele nowoczesnych urządzeń smart: odkurzacze, oczyszczacze powietrza, termostaty czy nawet żarówki, również łączy się z internetem przez Wi-Fi.

Domowa sieć może składać się zarówno z połączeń przewodowych (kable ethernetowe), jak i bezprzewodowych (Wi-Fi). Nieodłącznymi elementami sieci są też modem i router – pierwszy łączy urządzenia z internetem, a drugi dystrybuuje sygnał w całym domu. Przy większej liczbie urządzeń przydatny okaże się też switch, czyli przełącznik służący do rozgałęziania sieci, a także wzmacniacz sygnału Wi-Fi.

Co musicie zrobić, aby zbudować stabilną sieć w domu? Urządzenia, które wymagają niezawodnego połączenia, takie jak komputery stacjonarne, telewizory Smart TV czy konsole do gier, podłączajcie do sieci za pomocą kabli. Pozwoli to na uzyskanie stabilniejszego połączenia bez ryzyka zakłóceń. Dobrze zaplanowana sieć domowa zapewni płynne korzystanie z internetu przez wszystkich domowników, niezależnie od liczby urządzeń. Zastanówcie się też, czy wszystkie domowe sprzęty naprawdę wymagają połączenia z internetem – zdarza się, że właśnie słabo zabezpieczone urządzenia stają się bramą umożliwiającą przeniknięcie do Waszej sieci… intruzów. Dodatkowo pamiętajcie o tym, by router umieścić w centralnym miejscu i z dala od przeszkód takich jak ściany czy metalowe przedmioty.

Nie możecie zapominać też o bezpieczeństwie domowej sieci Wi-Fi, które jest kluczowe, aby chronić się przed cyberatakami. Oto kilka prostych kroków:

- **Zmieńcie domyślne hasło.** Domyślne hasło od dostawcy usług internetowych łatwo złamać. Ustawcie silne, unikalne hasło składające się z co najmniej 14 znaków, które będzie łatwe do zapamiętania dla Was i niemożliwe do odgadnięcia dla osób postronnych.
- **Zmieńcie nazwę sieci (SSID).** Domyślna nazwa sieci może sugerować, że właściciel nie dba o bezpieczeństwo. Ustawcie nazwę, która nie zawiera Waszych danych osobowych.
- **Stwórzcie sieć dla gości.** Możecie utworzyć osobną sieć Wi-Fi dla gości, aby ograniczyć dostęp do swoich głównych urządzeń. Ułatwi to także kontrolę nad hasłem do sieci.
- **Wyłączcie rozgłaszanie SSID.** Ukrycie nazwy sieci (SSID) sprawi, że nie będzie ona widoczna dla osób w pobliżu, co utrudni potencjalnym intruzom jej znalezienie.
- **Rozważcie korzystanie z VPN.** Jeśli chcecie dodatkowo zabezpieczyć swoją prywatność, możecie korzystać z VPN (ang. *Virtual Private Network*) – sieci tunelowej, która szyfruje ruch w internecie. Zapewni to dodatkową ochronę przed śledzeniem Waszej aktywności online.

Doomsurfing

Czy zwróciliście kiedyś uwagę, jakie treści śledzicie w internecie z największym zainteresowaniem? Okazuje się, że często poświęcamy nadmierną uwagę na przyswajanie negatywnych, niepokojących wiadomości z mediów, ciągłe scrollowanie serwisów internetowych czy mediów społecznościowych w poszukiwaniu katastroficznych informacji, teorii spiskowych, negatywnych relacji. To zjawisko to doomsurfing. Termin pochodzi od dwóch angielskich słów: *doom*, oznaczającego fatum, oraz *surfing*, czyli przeglądanie sieci.

Doomsurfing nasila się zwłaszcza podczas ważnych, krytycznych wydarzeń – mogliśmy zetknąć się z nim np. w czasie pandemii, gdy na bieżąco śledziliśmy informacje o liczbach zachorowań i zgonów na COVID, czy po wybuchu wojny w Ukrainie, gdy większość z nas zaczynała dzień od sprawdzenia aktualnych doniesień. Niestety okazuje się, że nałogowe przeczesywanie sieci w poszukiwaniu najświeższych newsów nie przynosi ulgi i nie daje odpowiedzi na nurtujące nas pytania, a jedynie może wywołać poczucie lęku, bezradności czy nawet stany depresyjne.

D

Jak chronić się przed skutkami doomsurfingu? Przede wszystkim zastanówcie się, ile czasu spędzacie na czytaniu sensacyjnych internetowych wiadomości. Czy zdarzyło się, że jakaś informacja wpłynęła na pogorszenie Waszego samopoczucia w danym momencie? Warto być na bieżąco, ale czasami lepiej ograniczyć liczbę przyswajanych wiadomości, bo ich nadmiar nie przyniesie nam nic dobrego.

Tylko jak to zrobić?

- Korzystajcie z jednego lub dwóch źródeł wiadomości, które zapewniają rzetelną analizę sytuacji, a nie powielają niesprawdzone, sensacyjne informacje.
- Postarajcie się ograniczyć scrollowanie – zwłaszcza to dla zabicia czasu. Wybierzcie moment w ciągu dnia, w których sprawdzacie najnowsze informacje – nie róbcie tego co chwilę. Ważne tylko, aby nie był to moment przed snem.
- Analizujcie przedstawione w mediach informacje. Wiemy, że nie zawsze jest na to czas, ale postarajcie się przynajmniej sprawdzić, kto stoi za ich rozpowszechnianiem – czy to znany i ceniony ekspert, czy przypadkowa osoba.
- Pamiętajcie, że część informacji w sieci trafia do nas tylko dlatego, że wcześniej szukaliśmy podobnych. Tak działają algorytmy, które podsuwają nam to, czym jesteśmy zainteresowani. Jeśli więc wydaje Wam się, że internet aktualnie żyje tylko jednym tematem, dlatego trzeba się nim zajmować – w rzeczywistości może być zupełnie inaczej. To zjawisko tzw. bańki informacyjnej, czyli zamknięcia w otoczeniu treści o określonym wydźwięku.
- Szukajcie też pozytywnych informacji – nawet jeśli giną one często w natłoku tych negatywnych, nadal są dostępne. To z pewnością sprawi, że poczujecie się lepiej.

Pamiętajcie również o higienie cyfrowej i o tym, aby czas spędzany przed ekranem regularnie równoważyć aktywnościami offline.

Więcej informacji o doomsurfingu znajdziecie w aktualności „Doomsurfing – jak wyrwać się z błędnego koła śledzenia złych informacji" na stronie ose.gov.pl.

Źródło:

„Zadbaj o siebie z OSE: doomsurfing", (2025), artykuł na stronie ose.gov.pl.

Doxing

Niemal każdego dnia zostawiamy w sieci cyfrowy ślad: zamieszczając materiały w mediach społecznościowych, publikując komentarze na forach lub po prostu przeglądając konkretne strony. Ale czy wiecie, że z okruchów informacji porozrzucanych w sieci ktoś może stworzyć zbiór danych na Wasz temat, a następnie opublikować online wszystkie wiadomości – najczęściej te wpływające na bezpieczeństwo i wizerunek?

Takie działanie to doxing (znane też jako doxxing, doksing). Oznacza śledzenie i gromadzenie informacji w sieci na temat określonej osoby lub organizacji w celu analizy zebranych danych, a następnie ich upublicznienia. Termin ten powstał z połączenia skrótu dox (docs), utworzonego od angielskiego słowa documents (dokumenty), oraz compiling/releasing (przetwarzać, upubliczniać). Czy doxing może być niebezpieczny? Nawet bardzo!

Doxer szuka wstydliwych zdjęć lub filmików, kontrowersyjnych wypowiedzi, danych osobowych i wrażliwych. W tym celu wciela się w cyfrowego detektywa, który legalnie uzyskuje informacje z sieci, ale też w cyberprzestępcę wykorzystującego oprogramowanie szpiegujące bądź socjotechnikę, by zmanipulować ofiarę i uzyskać interesujące go dane.

W dobie rozwoju sztucznej inteligencji OSINT (z ang. *open-source intelligence*), czyli biały wywiad – wyszukiwanie, gromadzenie i analizowanie informacji z różnych, ogólnodostępnych

źródeł na temat firm, organizacji, osób – staje się o wiele mniej kosztowny dla oszustów, przez co bardziej powszechny.

Jak zatem chronić się przed doxingiem? Przede wszystkim dbajcie o swoją prywatność w sieci!

- Z rozwagą dzielcie się w internecie informacjami o sobie. Nie udostępniajcie prywatnych danych typu numer telefonu, adres zamieszkania, e-mail.
- Kontrolujcie, jakie dane zdradzacie nieświadomie. Zdjęcia, filmy i inne dokumenty mogą zawierać informacje o ich autorze, czasie utworzenia czy lokalizacji. Ponadto nie publikujcie zdjęć, z których można pozyskać istotne informacje – biletów lotniczych, dokumentów tożsamości czy kart kredytowych (nawet ich fragmentów).
- W mediach społecznościowych dbajcie o ustawienia prywatności – nie każdy musi mieć dostęp do publikowanych przez Was treści.
- Reagujcie, jeśli ktoś bez Waszej zgody udostępnił w internecie materiał zdradzający szczegóły z Waszego życia. Ustalcie z rodziną i znajomymi zasady zamieszczania online wspólnych zdjęć i filmików.
- Zapoznajcie się z polityką prywatności za każdym razem, gdy zaczynacie korzystać z nowego portalu lub aplikacji. Niektóre z nich zawierają zapisy dotyczące dostępu do zbyt wielu Waszych informacji, np. galerii zdjęć czy listy kontaktów w telefonie.
- Korzystajcie z prawa do bycia zapomnianym. Zawsze możecie prosić o usunięcie z internetu dotyczących Was materiałów – nieaktualnych, nieistotnych lub takich, które naruszają Wasz wizerunek. Takie prawo wynika z Ogólnego rozporządzenia o ochronie danych – RODO.
- Bądźcie też wyczuleni na phishing i wszelkie próby wyłudzenia danych osobowych czy uwierzytelniających.

Więcej przydatnych informacji znajdziecie na stronie ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: doxing”.

Dyżurnet.pl

Internet otwiera nam okno na świat, w sieci możemy uczyć się, rozwijać, kontaktować z innymi ludźmi. Jednak co wtedy, gdy online spotka nas – lub nasze dzieci czy uczniów – coś nieprzyjemnego, np. natkniemy się na treści, których nie chcieliśmy zobaczyć? W takich przypadkach pomocą służy Dyżurnet.pl. To zespół ekspertów Państwowego Instytutu Badawczego NASK działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

Dyżurnet.pl m.in. obsługuje linię telefoniczną i serwis internetowy, umożliwiając zgłaszanie i analizę przypadków dystrybucji, rozpowszechniania lub przesyłania materiałów przedstawiających seksualne wykorzystywanie dzieci, w skrócie CSAM (z ang. *child sexual abuse materials*), przez internet.

Zgłoszenia o potencjalnie nielegalnych treściach możecie przekazywać za pomocą formularza, na adres mailowy dyzurnet@dyzurnet.pl lub pod numerem telefonu 801 615 005. Jeśli zgłoszona treść dotyczy materiałów przestawiających seksualne wykorzystywanie dzieci, twardej pornografii, rasizmu i ksenofobii czy innych nielegalnych treści, zespół Dyżurnet.pl podejmuje odpowiednie działania (np. zgłasza sprawę na policję). Specjaliści reagują również na szkodliwe treści, zagrażające bezpieczeństwu dzieci. W takim przypadku najczęściej kontaktują się z administratorem, który moderuje np. wskazane posty na forach.

Szczegółowych informacji o zgłaszaniu nielegalnych treści i działaniach Zespołu Dyżurnet.pl szukajcie na stronie dyzurnet.pl.

D

Dzień Bezpiecznego Internetu (DBI)

Czy wiecie, które daty w corocznym kalendarzu są szczególnie ważne dla bezpieczeństwa w sieci? To na pewno październik będący Europejskim Miesiącem Cyberbezpieczeństwa (ECSM), ale też pierwsza połowa lutego, gdy obchodzimy Dzień Bezpiecznego Internetu. Celem tej akcji jest inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i nastolatków do sieci, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online, a także promocja pozytywnego wykorzystywania internetu. Dzień Bezpiecznego Internetu obchodzimy od 2004 r. z inicjatywy Komisji Europejskiej. Od lat różnorodne wydarzenia z okazji DBI organizowane są nie tylko w Europie, ale na całym świecie.

Organizatorem DBI w naszym kraju jest Polskie Centrum Programu Safer Internet (PCPSI), które jako Państwowy Instytut Badawczy NASK tworzymy z Fundacją Dajemy Dzieciom Siłę. Centralnym punktem naszych obchodów jest doroczna konferencja z udziałem ekspertów, ale i szkół, organizacji pozarządowych czy przedstawicieli biznesu, którzy angażują się w DBI.

Więcej informacji, w tym nagrania z wystąpień ekspertów podczas konferencji, znajdziecie na stronie saferinternet.pl.

E

E-mail

Chyba każdy internauta ma przynajmniej jeden adres e-mailowy. To właśnie on pozwala nam korzystać z wielu możliwości, jakie oferuje dostęp do sieci. E-mail to poczta elektroniczna (ang. *electronic mail*), dzięki której komunikujemy się przez internet. Określenie to stosujemy też do samej wiadomości elektronicznej.

Posiadając swój osobisty adres mailowy, możecie przesyłać wiadomości i otrzymywać je od innych, odbierać newslettery czy zakładać konta w różnych mediach społecznościowych oraz sklepach internetowych. Aby korzystać z poczty elektronicznej, wystarczy urządzenie (np. komputer, smartfon) z dostępem do internetu i skrzynka, którą można założyć bezpłatnie. Ważne, by zabezpieczyć ją silnym, unikalnym hasłem, a także skorzystać z uwierzytelniania dwuskładnikowego (2FA), czyli oprócz hasła będziecie logować się do poczty dodatkowymi składnikami, np. kodem otrzymanym SMS-em.

Nie zapominajcie też o czujności! Wielu oszustów wykorzystuje wiadomości elektroniczne w swoich kampaniach phishingowych. Mogą w nich podszywać się pod Waszych znajomych, zaufane instytucje czy firmy. Otrzymując wiadomość na wirtualną skrzynkę, zawsze bądźcie ostrożni. Uważajcie na te oznaczone jako spam, weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości. Zawsze sprawdzajcie, czy nadawca rzeczywiście jest tym, za kogo się podaje, i nie ma złych intencji.

Co powinno wzbudzić Waszą podejrzliwość?

- Wiadomość napisana niepoprawnym językiem (choć dziś dzięki narzędziom bazującym na sztucznej inteligencji nie jest trudno wygenerować poprawny tekst).
- Wiadomość nakłaniająca do nieprzemyślanego i szybkiego działania, np. udostępnienia wrażliwych danych, takich jak loginy, hasła czy numery kart płatniczych.
- Ton wypowiedzi, w którym nadawca ostrzega Was, że wydarzy się coś złego, jeśli natychmiast nie wykonacie jego polecenia.
- Adres nadawcy zawierający błędy czy rzadko spotykane rozszerzenia, np. zamiast popularnego w Polsce .pl, .com, .eu widnieje dziwna domena typu: .tk, .top, .ru czy .xyz.

Pamiętajcie, że nasze skrzynki pocztowe często skrywają wiele cennych informacji. Skany dokumentów, dane uwierzytelniające do różnych kont, dane medyczne i inne poufne treści powinny być usuwane z poczty. Warto też pamiętać o separacji tożsamości, czyli tworzeniu osobnej skrzynki mailowej np. do spraw urzędowych i kont w sklepach internetowych. Oddzielne konta e-mail pomagają zminimalizować skutki ewentualnego wycieku danych.

Chcecie dowiedzieć się więcej o poczcie elektronicznej? Zajrzyjcie do kursu e-learningowego „Techniki internetu" dostępnego na naszej platformie OSE IT Szkoła oraz aktualności „Bezpieczni w sieci z OSE: poczta e-mail", którą znajdziecie na stronie ose.gov.pl.

E-uzależnienia

Internet, komputer, smartfon, smartwatch, gry online – nowe technologie na dobre zagościły w naszym życiu. Badania NASK prowadzone od 2014 r. pokazują, że młodzi ludzie spędzają bardzo dużo czasu z urządzeniami ekranowymi podłączonymi do sieci. Według danych z raportu „Nastolatki" młodzież korzysta z sieci średnio 4 godziny i 59 minut w dni powszednie oraz 5 godzin i 16 minut w weekendy (Ładna i in., 2025).

Choć narzędzia cyfrowe ułatwiają nam codzienne funkcjonowanie, zapewniają rozrywkę, pomagają w pracy, nauce, podtrzymywaniu kontaktów, to ich nadużywanie może prowadzić

do poważnych problemów. Zaburzenie cyfrowej higieny powoduje m.in. stres elektroniczny, przeciążenie informacją czy problemowe używanie internetu (PUI). Na czubku góry lodowej ukazującej skutki niekontrolowanego korzystania z internetu i urządzeń znajdują się e-uzależnienia.

E-uzależnienie, należące do szerszej kategorii uzależnień behawioralnych (czynnościowych), to z jednej strony uzależnienie od urządzeń cyfrowych, takich jak: komputery, tablety czy smartfony (fonoholizm), z drugiej – uzależnienie od czynności, które wykonujemy za pomocą tych urządzeń. Możemy więc mówić o uzależnieniu np. od: internetu, zakupów w sieci, gier lub hazardu online, mediów społecznościowych czy oglądania w internecie szkodliwych treści, np. pornograficznych (por. Makaruk, Włodarczyk, Skoneczna 2019).

Światowa Organizacja Zdrowia (WHO) szczególne zagrożenie dostrzega w uzależnieniu od gier online (gaming disorder). Z tego też powodu zostało ono wpisane na listę Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych (ICD-11). Zaburzenie to również znajduje się w grupie uzależnień behawioralnych. Z kolei uzależnienie od internetu nie znalazło się na liście chorób czy zaburzeń psychicznych, co nie znaczy, że nie wpływa ono negatywnie na nasze zdrowie. Wręcz przeciwnie – niekontrolowany przymus korzystania z sieci jest przyczyną wielu problemów.

Warto podkreślić, że nadużywanie urządzeń cyfrowych czy internetu nie musi od razu oznaczać, że jesteśmy uzależnieni. Zanim padnie taka diagnoza, potrzebna jest dłuższa obserwacja i określenie, czy cyfrowe nawyki zaburzają nasze funkcjonowanie psychofizyczne, czy prowadzą do życiowych problemów.

Jak rozpoznać czy ktoś – Wy lub Wasze dziecko – wpadł w sidła e-uzależnienia? Należy zwrócić uwagę na kilka symptomów:

- brak kontroli nad czasem spędzanym online, nieudane próby ograniczenia aktywności w sieci, nawet jeśli wiążą się z tym jakieś konsekwencje (np. wyrzucenie z pracy, problemy w szkole, rezygnacja z ważnych szans);
- izolowanie się od znajomych, rodziny, zrywanie kontaktów zawartych poza siecią, problemy z budowaniem relacji offline;
- wzrastająca tolerancja na działanie czynnika uzależniającego – z czasem zaabsorbowanie cyfrowym światem staje się coraz większe;
- występowanie objawów odstawienia: zmiany nastroju, gdy urządzenia cyfrowego nie ma w zasięgu ręki (smutek, lęk, złość, agresja, stany depresyjne) i reagowanie euforią, gdy odzyska się dostęp do sieci;
- problemy z koncentracją, przemęczenie, niewyspanie i związane z tym pogorszenie wyników w nauce lub pracy;
- zaniedbywanie codziennych obowiązków, pasji i hobby, a także potrzeb fizjologicznych (posiłki, toaleta) na rzecz aktywności online;
- użytkowanie sieci i urządzeń cyfrowych jako jedynej strategii radzenia sobie ze stresem, emocjami, formy ucieczki od problemów;
- problemy zdrowotne: bóle czy zawroty głowy, ból pleców, karku, nadgarstków, oczu, problemy ze snem, pogorszenie wzroku (por. Izdebski, Kotyśko, 2016; Rowicka, Kongres OSE 2023).

Osoba, która ma problem z e-uzależnieniem, rzadko potrafi poradzić sobie z nim sama. Potrzebuje wsparcia najbliższych i pomocy specjalistów – psychologa lub psychiatry. Gdzie szukać ratunku? Na portalu uzaleznieniabehawioralne.pl znajdziecie bazę wiedzy, skontaktujecie się ze specjalistami z poradni online lub znajdziecie placówkę oferującą terapię e-uzależnień (Witkowska, 2023). Warto także dbać o profilaktykę! Najlepszą metodą jest zachowywanie cyfrowej higieny i rozsądne korzystanie z urządzeń ekranowych.

Źródła:

Izdebski, P., Kotyśko, M., (2016), „Problemowe korzystanie z nowych mediów", w: B. Habrat (red.), „Zaburzenia uprawiania hazardu i inne tak zwane nałogi behawioralne" (s. 219–250), Warszawa: Instytut Psychiatrii i Neurologii, za: Makaruk K., Włodarczyk J., Skoneczna P., (2019), „Problematyczne używanie internetu przez młodzież. Raport z badań", Warszawa: Fundacja Dajemy Dzieciom Siłę.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy", Warszawa: Państwowy Instytut Badawczy NASK.

Rowicka M., (2023), „Kongres OSE 2023. E-uzależnienia", wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Witkowska M., (2023), „FOMO i problemowe używanie internetu. Poradnik dla nauczycieli", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ekran blokady

Choć nie zawsze zdajecie sobie z tego sprawę, jednym z ważniejszych zabezpieczeń Waszych urządzeń (smartfonów, tabletów, laptopów) jest ekran blokady. Być może wcale go nie lubicie – wpisywanie hasła jest dla Was irytujące, często zapominacie PIN? Gwarantujemy: warto znosić tę „niewygodę"!

W zależności od używanego sprzętu macie do wyboru kilka zabezpieczeń. Aby odblokować ekran za każdym razem, gdy włączacie lub wybudzacie urządzenie, możecie: wpisać czterocyfrowy PIN, narysować wzór – połączyć w dowolnej kolejności kropki układające się w kwadrat 3x3, wpisać hasło, użyć czytnika linii papilarnych, mechanizmu rozpoznawania twarzy lub funkcji Smart Lock (zezwolić na odblokowywanie urządzenia tylko w określonych miejscach, np. w domu).

Wybierając rodzaj blokady ekranu, rozważcie kilka kwestii:

- Jeśli zdecydujecie się na PIN, unikajcie oczywistych kombinacji cyfr (np. 1111, 1234) i ważnych dla Was liczb (np. tworzących datę urodzenia). Podobną ostrożność zachowajcie też w przypadku hasła: nie stawiajcie na popularne ciągi liter (np. qwerty, asdf, haslo, password) i związane z Wami frazy. Sprawdźcie listę najpopularniejszych haseł opublikowaną przez CERT Polska i jeśli znajdziecie na niej swój szyfr – zmieńcie go natychmiast!
- Uważajcie również na wzór, który rysujecie na ekranie. Wiecie, że możliwych jest ok. 150 milionów możliwych kombinacji, a najczęściej wykorzystywanych jest tylko… 15 najpopularniejszych wzorów? Oznacza to, że złamanie tego zabezpieczenia zajmuje maksymalnie 90 sekund (WEC Communication, 2017). Wystrzegajcie się wzorów w kształcie liter i innych oczywistych połączeń kropek. Jeśli zdecydujecie się na wzór, uważajcie, czy nikt nie zagląda Wam przez ramię, gdy rysujecie swój szyfr. Dbajcie też o czystość ekranu – ślad po wprowadzonym rysunku będzie cenną podpowiedzią dla złodzieja, któremu uda się ukraść Wasz telefon.
- Skuteczną, choć nie niezawodną metodą zabezpieczeń wydaje się biometria. Odcisk palca czy skan tęczówki oka są unikalne dla każdego człowieka i trudno je podrobić.
- Ciekawym sposobem zabezpieczania urządzenia jest Smart Lock (dla użytkowników urządzeń z systemem Android). Niepotrzebne są PIN-y i hasła: smartfon będzie odblokowany, gdy wyczuje – za pomocą modułu Bluetooth, GPS i przedniej kamery – że znajduje się w określonym miejscu lub wykryje twarz użytkownika. Jeśli znajdziecie taką opcję w ustawieniach swojego sprzętu, ograniczcie liczbę możliwych prób odblokowywania ekranu.

Pamiętajcie: liczy się Wasze bezpieczeństwo, dlatego warto ograniczyć złodziejom i oszustom możliwość uzyskania dostępu do Waszych urządzeń. Postawcie na silne zabezpieczenie, nawet

jeśli będzie to oznaczało wpisywanie długiego hasła lub rysowanie skomplikowanego wzoru na ekranie!

Dowiedzcie się więcej na temat silnych haseł – szczegółowe informacje znajdziecie na stronie CERT Polska w poradniku „Kompleksowo o hasłach" oraz w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe" i „Bezpieczni w sieci z OSE: bezpieczeństwo urządzeń mobilnych".

Źródło:

WEC Communication, (2017), „Sprawdzamy, która metoda blokady ekranu jest najbezpieczniejsza", artykuł w serwisie media.wec24.pl.

Emotikon, emoji

Kolorowe symbole w telefonie – serduszka, ognie, śmieszne buźki, zwierzątka i owoce – których wcześniejszym wcieleniem były buźki robiące różne miny, wydają się nieszkodliwym dodatkiem do rozmów online. Ale w cyfrowym świecie emoji to nie tylko dekoracje. To język emocji, aluzji, relacji i czasem… ukrytych przekazów. Komunikacja za pomocą emoji jest dla młodych ludzi wygodna, szybka i bezpieczna. Umożliwia wyrażenie tego, czego nie chcą lub nie potrafią powiedzieć słowami. Dodatkowo tworzy poczucie wspólnoty i wtajemniczenia. Znajomość kodów emoji to dziś część kultury internetowej młodzieży – jak slang, tylko bardziej dynamiczny i trudniejszy do uchwycenia przez dorosłych.

Emoji w sieci działają jak mimika w rozmowie: podkreślają nastrój, łagodzą przekaz, sugerują żart lub flirt. Okazuje się, że mogą też służyć do przekazywania treści, których dzieci nie powiedziałyby wprost. Przykład? „Bakłażan", „wiśnie" i „brzoskwinia" nie odnoszą się wśród młodzieży do warzyw i owoców, zamiast tego symbolizują intymne części ciała. „Płomień" oznacza, że ktoś wygląda „hot", „śnieg" to symbol kokainy, „liść" – marihuany, „winogrona" odnoszą się do gwałtu (przez skojarzenie angielskiego słowa *grape* – winogrona z *rape* – gwałt).

Niepokojące jest to, że część emoji wykorzystywana jest w wiadomościach, które mają ukryty, niebezpieczny przekaz. Na przykład „tęcza" nie zawsze oznacza poparcie dla różnorodności – bywa używana ironicznie, prześmiewczo lub jako oznaczenie zamkniętej grupy. Z kolei „pistolet", „bomba" czy „trumna" to symbole przemocy, które mogą być częścią zastraszania w sieci – nawet jeśli ich nadawcy twierdzą, że to żart.

Odczytanie tych znaczeń wymaga nie tylko znajomości symboli, ale też kontekstu: kto z kim rozmawia, w jakim stylu, jak długo się znają. To dlatego emoji mogą jednocześnie wydawać się zabawne i nieszkodliwe, a przy tym stać się zasłoną dla cyberprzemocy, presji seksualnej czy zachowań ryzykownych. Warto pamiętać, że dla dorosłych są dosłownym przedstawieniem tego, czego dotyczy rozmowa, a dla młodych – metaforą, niewerbalnym odzwierciedleniem tego, o czym nie można lub nie chce się napisać słownie.

Źródło:

„Ukryte znaczenie emocji – jak zrozumieć swoje dziecko?", (2025), artykuł na stronie ose.gov.pl.

Europejski Miesiąc Cyberbezpieczeństwa (European Cybersecurity Month, ECSM)

Ogólnoeuropejska kampania na rzecz bezpieczeństwa w sieci, zainicjowana w 2012 r. i koordynowana przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz Komisję Europejską, której celem jest zwiększanie świadomości o zagrożeniach online i sposobach skutecznej ochrony przed nimi.

Polską edycję ECSM organizuje Państwowy Instytut Badawczy NASK. Każdego roku akcja angażuje coraz szersze grono partnerów, a wydarzenia realizowane w jej ramach stają się okazją nie tylko do edukacji, lecz także do wspólnego działania na rzecz bezpiecznego cyfrowego środowiska.

W 2024 r. w Polsce odbyło się aż 127 wydarzeń w ramach ECSM, które dotarły łącznie do ponad 1,4 miliona odbiorców.

Kampania ma charakter otwarty – uczestniczyć mogą w niej instytucje publiczne, przedsiębiorstwa, organizacje pozarządowe, szkoły (także wyższe) oraz wszyscy użytkownicy internetu zainteresowani cyberbezpieczeństwem. Każdy może zgłosić własną inicjatywę: warsztaty, szkolenia, konferencje, konkursy, webinary czy kampanie informacyjne, realizowane online i stacjonarnie.

Więcej informacji można znaleźć na stronie bezpiecznymiesiac.pl.

Exploit

Uwaga! To kolejne niebezpieczeństwo, na jakie możecie być narażeni jako użytkownicy nowych technologii. Exploit to sposób wykorzystania istniejących błędów w oprogramowaniu. Cyberprzestępca poprzez lukę przejmuje kontrolę nad urządzeniem lub zmusza je do wykonania żądanej przez niego operacji.

Aby uchronić się przed konsekwencjami ataku tego typu, należy dbać o regularne aktualizacje oprogramowania. W ten sposób uniemożliwiamy wykorzystanie podatności, które zostały znalezione w starszych wersjach używanych przez nas programów.

Warto wiedzieć, że luki w oprogramowaniu, które pozwalają podejmować cyberprzestępcom niebezpieczne dla użytkowników działania, to tzw. podatności. Każda z nich ma swój numer w słowniku identyfikatorów zagrożeń CVE (ang. *Common Vulnerabilities and Exposures*), dostępnym na stronie cve.org. Obecnie w bazie znajduje się ponad 300 tys. wpisów – ta liczba stale rośnie!

F

Fact-checking

Fact-checking to angielski termin, który oznacza proces weryfikacji faktów w celu dokładnego sprawdzenia wiarygodności informacji. Może nie wiecie, ale są osoby, które dbają o prawdziwość przekazywanych wiadomości. Fact-checkerzy docierają do danych, statystyk, dokumentów źródłowych, merytorycznych analiz, wypowiedzi specjalistów z określonej dziedziny, by zweryfikować treści pojawiające się w mediach i internecie. Wykorzystują też różne narzędzia, umożliwiające np. zbadanie autentyczności filmów czy zdjęć. Organizacje fact-checkingowe walczą z dezinformacją i szkodliwą narracją, a także budują świadomość społeczną, przekazując odbiorcom rzetelne i sprawdzone informacje.

To szczególnie ważne zadanie w dobie rozwoju internetu i narzędzi cyfrowych – również tych wspieranych przez sztuczną inteligencję, które ułatwiają tworzenie oraz rozprzestrzenianie nieprawdziwych materiałów. Fałszywe treści są niebezpieczne, bo rozchodzą się w błyskawicznym tempie (głównie za pomocą mediów społecznościowych), zaburzają przepływ prawdziwych informacji i wpływają negatywnie na wiele aspektów naszego życia. Ponadto wzbudzają silne emocje (np. lęk, smutek, oburzenie, gniew), kształtują poglądy, postawy i nastroje społeczne, pogłębiają podziały, podsycają konflikty czy podważają autorytety i wiarygodność państwa (kompetencjecyfrowe.gov.pl, 2025).

Jeśli macie wątpliwości, czy jakieś informacje w sieci są prawdziwe, zaglądajcie na strony fact-checkingowe, takie jak: demagog.org.pl, pravda.org.pl, fakenews.pl czy pap.pl/fact-checking. Znajdziecie tu wiele zdementowanych informacji. Możecie też sami wcielić się w fact-checkera. Włączcie zdrowy rozsądek i z dystansem podchodźcie do materiałów publikowanych w sieci, a w szczególności do krzykliwych nagłówków. Jeśli coś budzi Wasze wątpliwości, starajcie się potwierdzić informację w kilku niezależnych źródłach.

Natknęliście się w internecie na materiał, który może być fałszywy? Zgłaszajcie to! Eksperci z Ośrodka Analizy Dezinformacji Instytutu NASK sprawdzą jego wiarygodność i ostrzegą innych przed ewentualną manipulacją. Wystarczy wypełnić formularz dostępny na stronie nask.pl/dezinfo.

Chcecie dowiedzieć się więcej o sposobach weryfikowania informacji w sieci? Skorzystajcie z naszego bezpłatnego kursu dla nauczycieli „(Dez)informacja, czyli w co wierzyć w internecie”, który znajdziecie na platformie OSE IT Szkoła.

Źródło:

„Ochrona przed dezinformacją”, (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

Fałszywe domeny

Oszuści stosują różne metody, aby wyłudzić od internautów dane osobowe, dane uwierzytelniające czy pieniądze. Jedną z nich jest tworzenie stron internetowych podszywających się pod znane podmioty, firmy i instytucje. Co je odróżnia? Zazwyczaj niewiele – może to być błąd w nazwie domeny (np. zero – „0” zamiast litery „O”), nietypowe rozszerzenie lub dodatkowy element w adresie strony.

Bądźcie czujni, bardzo łatwo jest wpaść w sidła przestępców i przez nieuwagę zalogować się w oknie fałszywej strony banku, bramce płatności internetowej, e-sklepie, mediach społecznościowych czy witrynie instytucji łudząco podobnej do tej prawdziwej. Dlatego zawsze zwracajcie szczególną uwagę na adresy stron internetowych, na których wpisujecie swoje hasła i loginy!

Co jeszcze możecie zrobić, by nie dać się oszukać?

- Uważajcie na typosquatting – fałszywa domena może mieć w nazwie prawie niewidoczny błąd. Zamienianie, celowe pomijanie lub przestawianie kolejnością liter to powszechny

zabieg. Zwracajcie też uwagę na podobne znaki – „rn", „vv", „l" wyglądają jak „m", „w", „1". Ponadto przyglądajcie się szczegółom: wypatrujcie niepotrzebnych kropek czy dodatkowych łączników.

- Zwróćcie uwagę, czy adres nie zawiera rzadko spotykanych rozszerzeń, np. zamiast popularnego w Polsce .pl, .com, .eu widnieje dziwna domena typu: .tk, .top, .ru czy .xyz.
- Poświęćcie szczególną uwagę witrynom z długimi lub niepasującymi subdomenami, np. bank.security.login.example.com, oraz z dodatkowymi elementami w adresie, np. paypal-secure.com zamiast paypal.com.
- Zawsze śledźcie adres w pasku przeglądarki. Może się zdarzyć, że klikniecie w link zamaskowany pod przyciskiem lub elementem strony i niepostrzeżenie zostaniecie przekierowani na niebezpieczną witrynę.
- Nie dajcie się zwieść zielonej kłódce w przeglądarce obok adresu zaczynającego się od https – ten znak nie jest już gwarancją bezpieczeństwa. Oznacza jedynie, że strona posiada certyfikat TLS, czyli że połączenie z serwerem jest szyfrowane. Taki certyfikat można uzyskać za darmo, chroni on przed podsłuchaniem naszej wymiany informacji z właścicielem strony – jednak jeśli właścicielami są cyberprzestępcy, zielona kłódka nic nie zmienia.

Na nielegalne strony, służące do wyłudzenia danych lub pieniędzy, oszuści często zwabiają nas podstępem, stosując phishing. Dlatego weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości.

Jeśli traficie na fałszywą domenę, zgłoście to do CERT Polska. Wystarczy wypełnić formularz dostępny na stronie incydent.cert.pl. Możecie też przesłać wiadomość SMS zawierającą potencjalnie groźny link. W tym celu skorzystajcie z funkcji „przekaż" albo „udostępnij" i wyślijcie wiadomość na numer 8080. Możecie też skorzystać z usługi „Bezpiecznie w sieci" w aplikacji mObywatel.

Pamiętajcie – nie musicie mieć pewności, że jakaś domena jest fałszywa – wystarczy, że nabierzecie podejrzeń. Eksperci NASK przyjmą i przeanalizują każde zgłoszenie, a jeśli potwierdzą, że witryna wyłudza dane, zamieszczą ją na liście ostrzeżeń przed niebezpiecznymi stronami.

Więcej informacji znajdziecie na stronie ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: lista ostrzeżeń przed fałszywymi stronami".

Fałszywe informacje

Nie jest tajemnicą, że internet to skarbnica wiedzy, ale też źródło fałszywych, nieprawdziwych wiadomości, nierzadko o sensacyjnym, szokującym charakterze. Popularne, a zarazem szkodliwe, zmanipulowane newsy przyciągają uwagę krzykliwymi nagłówkami i emocjonalnym językiem, co sprawia, że czytamy je chętnie i równie chętnie się nimi dzielimy – np. w mediach społecznościowych.

Ale czy wiecie, że fałszywe wiadomości najczęściej mają za zadanie dezinformować, wprowadzać odbiorców w błąd? Niejednokrotnie są też narzędziem do przeprowadzenia ataków phishingowych. Zawarte w nich linki mogą Was przekierowywać do fałszywych witryn internetowych, których celem jest wyłudzenie Waszych danych lub kradzież środków finansowych. Jak zatem nie wpaść w pułapkę fałszywych informacji?

Prawdą jest, że jesteśmy przeciążeni informacjami, które każdego dnia docierają do nas z internetu. Konsumujemy treści szybko, pobieżnie i nie zawsze weryfikujemy, co jest prawdą, a co fałszem. W natłoku informacji warto jednak pamiętać o kilku kluczowych zasadach ochrony przed zmanipulowanymi newsami:

- **Oddzielajcie informację o opinii** – informację można zweryfikować, natomiast opinia to subiektywna wypowiedź.

- **Korzystajcie ze sprawdzonych źródeł** – szukajcie informacji w mediach o ugruntowanej pozycji, na kanałach ekspertów, stronach fact-checkingowych. Widomości pochodzące z anonimowych źródeł są zwykle mniej wiarygodne. Zanim uznacie coś za pewne, postarajcie się dotrzeć do źródła.
- **Nie rozpowszechniajcie fałszywych newsów** – jeśli będziecie chcieli przekazać dalej jakiś materiał, np. o sensacyjnym tytule, krzykliwym nagłówku, zastanówcie się dwa razy, czy warto powielać niewiarygodne treści.
- **Zgłaszajcie fałszywe materiały** – eksperci z Ośrodka Analizy Dezinformacji Instytutu NASK sprawdzą ich wiarygodność i ostrzegą innych przed manipulacją. Jak zgłosić podejrzaną treść? Wystarczy wypełnić formularz dostępny na stronie zglos-dezinformacje.nask.pl (kompetencjecyfrowe.gov.pl, 2025).

Więcej wiadomości o fałszywych treściach i dezinformacji znajdziecie na stronie ose.gov.pl w aktualności „Jak nie wpaść w pułapkę fake newsów?". Skorzystajcie też z naszych bezpłatnych materiałów e-learningowych: kurs „(Dez)informacja, czyli w co wierzyć w internecie" znajdziecie na platformie OSE IT Szkoła, natomiast kurs „Fake news, teorie spiskowe, manipulacje w sieci" dostępny jest na platformie bezpieczniwsieci.edu.pl.

Źródło:

„Ochrona przed dezinformacją", (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

Fałszywe inwestycje

Fałszywe inwestycje online, znane również jako oszustwa inwestycyjne, są jednym z najczęstszych zagrożeń w cyfrowym świecie. Cyberprzestępcy wykorzystują różne techniki, aby przekonać ofiary do zainwestowania pieniędzy w fikcyjne projekty, co może prowadzić do dużych strat finansowych.

Oszuści kuszą przede wszystkim szybkim, łatwym i gwarantowanym zarobkiem, reklamami z udziałem znanych osób, firm czy portali biznesowych – okazuje się, że to niejednokrotnie wystarcza, byśmy powierzyli im swoje oszczędności. Katalog ich metod jest jednak znacznie bogatszy: przestępcy wykorzystują w swoich działaniach także fałszywe wpisy użytkowników lub reklamy w serwisach społecznościowych, reklamy w wyszukiwarkach oraz bezpośredni kontakt poprzez wiadomość SMS.

Oferta oszustów wydaje się warta rozważenia – zachwalają oni specjalne platformy internetowe, za pomocą których można rzekomo inwestować w kryptowaluty lub akcje firm. Po kliknięciu w link użytkownik przechodzi do strony, na której wypełnia formularz, a następnie „przedstawiciel firmy" kontaktuje się z nim telefonicznie i nakłania do wykonania przelewu na poczet inwestycji. Początkowo ofiara przelewa małe kwoty, ale jako że na platformie może obserwować wyraźne zyski, zaczyna robić coraz większe wpłaty. Pieniądze te nie są jednak inwestowane, a bezpowrotnie trafiają na konto przestępców…

Na co powinniście uważać, gdy natkniecie się na podejrzane reklamy inwestycji?

- **Kury znoszące złote jaja nie istnieją.** Jeśli jakaś oferta wydaje się wyjątkowo korzystna, najpewniej nie jest prawdziwa. Pamiętajcie, że w rzeczywistości wysokie zyski wiążą się zazwyczaj z wysokim ryzykiem.
- **Brak transparentności to istotny sygnał ostrzegawczy.** Fałszywe inwestycje często ukrywają szczegóły dotyczące projektu lub sposobu generowania zysków. Jeśli firma nie podaje konkretnych informacji lub unika odpowiedzi na pytania – wycofajcie się!
- **Nacisk na natychmiastowe działanie nigdy nie wróży niczego dobrego.** Oszuści często wywierają presję, sugerując, że oferta jest ograniczona czasowo i wymaga szybkiego działania. Ma to skłonić ofiary do podejmowania pochopnych decyzji.

Na szczęście można się skutecznie bronić przed fałszywymi inwestycjami. Skorzystajcie z naszych miniporad:

- **Sprawdzajcie wiarygodność.** Przed zainwestowaniem w jakikolwiek projekt poszukajcie w internecie opinii na jego temat, sprawdźcie, czy firma jest zarejestrowana i regulowana przez odpowiednie instytucje finansowe.
- **Ostudźcie emocje.** Oszuści często wykorzystują sztuczki socjotechniczne, aby nakłonić do inwestycji. Działajcie na podstawie racjonalnych analiz, a nie emocjonalnych impulsów.
- **Korzystajcie z zaufanych źródeł.** Inwestujcie tylko przez sprawdzone i renomowane platformy inwestycyjne. Unikajcie ofert, które pojawiają się w nieznanych miejscach, np. na forach internetowych czy w wiadomościach e-mail od nieznajomych.
- **Bądźcie na bieżąco.** Śledźcie informacje o najnowszych zagrożeniach i metodach wykorzystywanych przez oszustów. Im więcej wiecie o potencjalnych zagrożeniach, tym trudniej Was oszukać!
- **Nie udostępniajcie podejrzanych ofert.** Nie chcecie przecież narazić znajomych na straty.

A co, jeśli podejrzewacie, że padliście ofiarą fałszywej inwestycji? Natychmiast zgłoście to odpowiednim służbom, takim jak policja czy organizacje zajmujące się przestępstwami finansowymi. Pamiętajcie: jeśli chcecie zacząć inwestować pieniądze, poradźcie się specjalisty finansowego, np. w swoim banku!

Źródło:

„Uważaj na fałszywe inwestycje w sieci"– informacje na stronie cert.pl.

Fałszywe oferty wakacyjne

Letnie wyjazdy przyciągają nas obietnicami pięknych widoków, luksusowych hoteli, bogactwem atrakcji, a często także kusząco niską ceną. Czekaliśmy na ten czas cały rok, więc jak tu nie skorzystać? Niestety, wakacyjny boom to również okres wzmożonej aktywności cyberprzestępców, którzy podsuwają fałszywe oferty.

Oszustwa wakacyjne polegają na oferowaniu fikcyjnych usług – od biletów lotniczych, przez zakwaterowanie, aż po wynajem samochodów i całe wycieczki. Wyobraźcie sobie, że płacicie za rezerwację, a na miejscu okazuje się, że Wasze nazwisko nie figuruje na liście pasażerów, apartament nie istnieje, a hotel nigdy o Was nie słyszał. Taki scenariusz może nie tylko zniszczyć wakacyjne plany, ale też poważnie nadszarpnąć Wasz budżet. Cyberprzestępcy najczęściej chcą wyłudzić od Was pieniądze lub dane osobowe, a czasem są to bardziej złożone operacje, które mogą obejmować kradzież tożsamości czy dostęp do Waszych kont bankowych.

Nie oznacza to jednak, że powinniście rezygnować z wakacji lub podchodzić do ich planowania z obawą. Istnieją sposoby, aby rozpoznać fałszywe oferty. Oto kilka wskazówek:

- **Wyjątkowo atrakcyjna cena.** Jeśli oferta wydaje się zbyt korzystna, aby była prawdziwa, sprawdźcie, czy nie jest tylko przynętą. Porównajcie ceny rynkowe – jeśli oferta znacząco odbiega od średniej, może być to sygnał ostrzegawczy.
- **Niepewne opinie.** Czytanie opinii przed zakupem powoli staje się już standardem, ale zwróćcie uwagę na ich wiarygodność. Jeśli recenzji jest mało albo brzmią podobnie, mogą być fałszywe i stworzono je tylko po to, aby wzbudzić Wasze zaufanie.
- **Niejasny opis i zdjęcia.** Odpowiedzcie sobie na pytanie: „Czy oferta opisana jest w sposób niemal bajkowy, ale brakuje potwierdzenia na zdjęciach?". Jeśli fotografie są niewyraźne, jest ich mało lub wydają się bardziej komputerową wizualizacją niż prawdziwym miejscem, powinna Wam się zapalić czerwona lampka.
- **Presja czasu.** Jeśli oferta „znika za chwilę" i wymaga szybkiej decyzji albo obejmuje dodatkowy rabat za natychmiastową płatność, może to być kolejna wskazówka, że coś jest nie tak.

- **Podejrzane formy płatności.** Zwracajcie uwagę na sposób, w jaki macie dokonać płatności. Upewnijcie się, że strona płatności jest autentyczna i że nie podajecie więcej danych, niż to konieczne.

Czy możecie zrobić coś jeszcze? Tak – ostrożności nigdy za wiele!

- **Korzystajcie ze sprawdzonych dostawców.** Starajcie się rezerwować bilety bezpośrednio przez linie lotnicze, a noclegi – na stronach hoteli. Jeśli korzystacie z pośredników, wybierajcie tych renomowanych lub dobrze ocenianych.
- **Sprawdzajcie wiarygodność nowej firmy.** Zwróćcie uwagę na to, czy strona wygląda profesjonalnie, czy zawiera regulamin, politykę prywatności i dane kontaktowe. Sprawdźcie również opinie innych klientów.
- **Unikajcie odpowiedzi na podejrzane wiadomości**. Nie klikajcie w linki w mailach czy SMS-ach od nieznanych nadawców. Mogą one prowadzić do złośliwych stron lub zawierać wirusy.
- **Sprawdzajcie rezerwacje.** Po dokonaniu zakupu upewnijcie się, że rezerwacja została prawidłowo zrealizowana. Sprawdźcie, czy wszystkie dane są poprawne i czy otrzymaliście potwierdzenie.

Zachowanie ostrożności może znacząco zmniejszyć ryzyko, że padniecie ofiarą wakacyjnego oszustwa. Jeśli jednak mimo wszystko stanie się coś niepokojącego, zbierzcie dowody i jak najszybciej zgłoście sprawę na policję. Pamiętajcie, że strona z oszukańczą ofertą może zniknąć, dlatego warto zabezpieczyć wszelkie potwierdzenia transakcji i zrzuty ekranu.

Więcej informacji znajdziecie na stronach cert.pl, bezpiecznymiesiac.pl oraz w aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE na wakacje: fałszywe oferty".

Fałszywe panele logowania

Tworzenie fałszywych stron, na które mają zalogować się użytkownicy sieci, to znany proceder. Cyberprzestępcy preparują panele logowania do popularnych witryn, w szczególności do poczty e-mail, bankowości internetowej i portali społecznościowych, by w ten sposób wyłudzić pieniądze lub uzyskać dostęp do Waszych danych.

Fałszywe panele logowania do złudzenia przypominają te oryginalne – wykorzystują tę samą szatę graficzną, logotypy, czcionki – ale konsekwencje zalogowania się w oknie spreparowanej strony mogą być fatalne.

Uzyskanie przez przestępców dostępu do e-konta bankowego wiąże się z utratą środków – często oszczędności życia. Włamanie się do Waszego e-maila oznacza otwarcie furtki do przesyłania spamu czy ataków phishingowych z Waszego adresu. To też droga do kradzieży wielu cennych danych. Pewnie nie pamiętacie, że to właśnie w skrzynce pocztowej przechowujecie np. skany dokumentów czy korespondencję zawierającą poufne informacje. Przejęte konto w portalu społecznościowym wykorzystywane jest natomiast do dalszych przestępczych działań: publikowania wpisów z linkami, które kierują do innych fałszywych paneli logowania, lub wysyłania wiadomości do znajomych z prośbą o pieniądze – kod BLIK czy przelew (najczęściej za pośrednictwem fałszywej bramki płatności).

Na co powinniście zwrócić uwagę, zanim wpiszecie login i hasło w panelu logowania?

- Adres internetowy fałszywej domeny zazwyczaj zawiera błąd w nazwie – literówkę lub zmienioną kolejność wyrazów (to typosquatting).
- Niepoprawna polszczyzna, brak polskich znaków, nieaktualny logotyp – to też sygnały, żeby opuścić daną stronę.
- Często próbując wejść w jakąś zakładkę w spreparowanym portalu, użytkownik zostaje przeniesiony na zupełnie inną stronę – śledźcie więc adres w pasku przeglądarki.

- Zielona kłódka obok adresu w przeglądarce nie gwarantuje już bezpieczeństwa. Certyfikat TLS oznaczający, że połączenie z serwerem jest szyfrowane, chroni przed podsłuchaniem naszej wymiany informacji z właścicielem strony. Jeśli jednak właścicielami strony są cyberprzestępcy, zielona kłódka nic nie zmieni.

Jak zawsze przed cyberzagrożeniami może Was uchronić zdrowy rozsądek. Nie klikajcie w przypadkowe linki, nie działajcie pod wpływem emocji, na bieżąco aktualizujcie swoje sprzęty, korzystajcie z oprogramowania antywirusowego.

Jeśli traficie na fałszywą stronę, zgłoście to do CERT Polska za pośrednictwem formularza dostępnego na stronie incydent.cert.pl. Eksperci przyjmą i przeanalizują każde zgłoszenie, a podejrzaną domenę zamieszczą na liście ostrzeżeń przed niebezpiecznymi stronami. Możecie też przesłać wiadomość SMS, zawierającą potencjalnie groźny link. W tym celu skorzystajcie z bezpłatnego numeru 8080 i funkcji „przekaż" albo „udostępnij".

Fałszywe reklamy

Co robicie, gdy chcecie znaleźć w sieci jakiś produkt czy interesującą Was informację? Najczęściej korzystacie z wyszukiwarki internetowej – to oczywiste. Ale czy wiecie, że cyberprzestępcy i w tym przypadku mogą próbować zwabić Was na specjalnie przygotowaną niebezpieczną stronę, za pomocą której przeprowadzą cyberatak? Jedną z podstępnych metod ich działania są fałszywe reklamy, które przekierowują nas na szkodliwe witryny – najczęściej dotyczące funduszy inwestycyjnych czy wykorzystujące wizerunki banków. Jak dokładnie działają oszuści?

Wykupują w popularnych wyszukiwarkach reklamy stron, produktów, które mogą się wiązać z najczęściej wpisywanymi w przeglądarkach słowami. Po kliknięciu w przygotowaną przez przestępców fałszywą reklamę zostaniecie przekierowani na szkodliwą stronę phishingową. Co dzieje się później? Scenariuszy może być wiele, w zależności od typu oszustwa. Jedno jest pewne – im dłużej zostaniecie na takiej stronie i wykonacie jakieś działanie – pobierzecie plik, wpiszecie hasło i login w fałszywym panelu logowania czy podacie swoje dane osobowe, narazicie się na duże straty.

CERT Polska ostrzega, że cyberprzestępcy coraz częściej wykorzystują fałszywe reklamy, by podszywać się pod producentów oprogramowania. Przygotowane przez oszustów witryny są łudząco podobne do tych oryginalnych, a w dodatku pojawiają się na pierwszych miejscach w wynikach wyszukiwania, co potrafi uśpić naszą czujność. W rzeczywistości służą do rozpowszechniania złośliwego oprogramowania (malware), które np. wykrada dane uwierzytelniające do serwisów, w tym do bankowości elektronicznej.

W kontekście fałszywych reklam warto też wspomnieć o stronach nakłaniających do inwestowania pieniędzy na giełdzie lub w kryptowaluty. Oszuści tworzą fałszywe witryny, na których reklamują intratne interesy. Osoby szukające zysku zostawiają tam swoje dane kontaktowe, po czym odzywa się do nich rzekomy przedstawiciel firmy inwestycyjnej i nakłania ofiary do ulokowania pieniędzy, które w rzeczywistości trafiają na konta przestępców.

Jak uchronić się przed fałszywymi reklamami?

- Uważajcie na typosquatting – adres internetowy fałszywej domeny zazwyczaj zawiera trudny do wychwycenia na pierwszy rzut oka błąd w nazwie, dokładnie sprawdzajcie więc każdą literę i każdy znak nazwy domeny.
- Zachowajcie czujność, nie klikajcie pochopnie w linki prowadzące do wyszukanej przez Was strony, nie dajcie się zgubić rutynowemu korzystaniu z wyszukiwarek. Dobrą praktyką jest samodzielne wpisywanie adresu strony internetowej w pasku.
- Jeśli przypadkiem znaleźliście się na portalu, na którym widnieje nieaktualny logotyp, treści napisane są niepoprawną polszczyzną, w opisach brakuje polskich znaków – niezwłocznie opuśćcie taką stronę.

- Pamiętajcie też, że zielona kłódka obok adresu w przeglądarce nie jest już gwarancją bezpieczeństwa. Certyfikat TLS oznaczający, że połączenie z serwerem jest szyfrowane, można łatwo uzyskać. Cyberprzestępcy również korzystają z tego rozwiązania.
- Uniwersalna rada: na bieżąco aktualizujcie swoje sprzęty, korzystajcie z oprogramowania antywirusowego, a także z oprogramowania typu bloker reklam.

Pamiętajcie, że fałszywą stronę możecie zgłosić do CERT Polska! Wystarczy wypełnić formularz dostępny na stronie incydent.cert.pl. Eksperci przyjmą i przeanalizują każde zgłoszenie, a podejrzaną domenę zamieszczą na liście ostrzeżeń przed niebezpiecznymi stronami. Możecie też przesłać wiadomość SMS, zawierającą potencjalnie groźny link. W tym celu skorzystajcie z bezpłatnego numeru 8080 i funkcji „przekaż" albo „udostępnij". Zespół CERT Polska w 2024 r. wytworzył łącznie 746 wzorców szkodliwych wiadomości, które przełożyły się na zablokowanie blisko 1,5 mln SMS-ów (CERT, 2025).

Więcej o szkodliwych witrynach przeczytacie w aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: lista ostrzeżeń przed fałszywymi stronami".

Źródła:

CERT Polska, (2025), „Raport roczny 2024 z działalności CERT Polska", Warszawa: Państwowy Instytut Badawczy NASK.

„Niebezpieczne reklamy w wyszukiwarkach – jak się nie dać złapać cyberoszustom?", (2023), artykuł na stronie gov.pl.

„Nowa kampania reklamowa ad hijacking za pośrednictwem Google Ads", (2023), artykuł na stronie cert.pl.

Filtry kontroli rodzicielskiej

Dzieci spędzają bardzo dużo czasu w internecie. Potwierdzają to badania NASK „Nastolatki" prowadzone co dwa lata od 2014 r. Według danych z 2024 r. młodzież korzysta z sieci 5 godzin dziennie (bez jednej minuty) w dni powszednie, a w weekendy 5 godzin i 16 minut. To bardzo dużo, choć mniej niż rekordowy wynik z 2022 r. (5 godz. 36 min w dni powszednie i 6 godzin i 16 minut w weekendy). Aż 4 na 10 dzieci otrzymuje swój własny telefon z dostępem do sieci jeszcze przed 9. urodzinami (Ładna i in., 2025). Niestety, wraz z możliwością korzystania z internetu, pojawia się obawa, że dziecko natknie się na niebezpieczne treści.

Eksperci są jednomyślni – samodzielne korzystanie z internetu i urządzeń wymaga odpowiedniego przygotowania. Po pierwsze, należy budować zdrowe nawyki cyfrowe dziecka. W tym przypadku ważna jest rozmowa na temat bezpieczeństwa w sieci i towarzyszenie najmłodszym w wędrówkach po internecie. Po drugie, trzeba zadbać o zabezpieczenia techniczne. Wsparciem dla rodziców w tym zakresie są rozwiązania technologiczne, które pomagają minimalizować ryzyko kontaktu dziecka ze szkodliwymi materiałami online. Badania pokazują, że średni wiek, w jakim dziecko pierwszy raz styka się z pornografią w sieci, to 11 lat i 3 miesiące (Ładna i in., 2025). Filtry kontroli rodzicielskiej to właśnie oprogramowanie, które ogranicza najmłodszym dostęp do szkodliwych, niebezpiecznych lub nieodpowiednich do ich wieku treści.

Wiele z dostępnych na naszych urządzeniach aplikacji posiada wbudowany tryb kids – to filtr, który pozwala na dostęp do treści przyjaznych dzieciom, a blokuje te adresowane do pełnoletnich użytkowników. Można też korzystać z narzędzi ochrony rodzicielskiej, czyli specjalnych aplikacji pomocnych w sprawowaniu kontroli nad materiałami docierającymi do dziecka z cyfrowego świata.

Jednym z takich narzędzi jest stworzona w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) bezpłatna aplikacja ochrony rodzicielskiej – mOchrona. Ułatwia ona ustalenie zasad dotyczących korzystania z internetu i różnych aplikacji oraz daje rodzicom dostęp do informacji o aktywności dziecka na jego urządzeniu. Jeśli jeszcze nie korzystacie z tego narzędzia, koniecznie pobierzcie

aplikację mOchrona na urządzenia mobilne z oficjalnych sklepów z aplikacjami, a także w wersji dla systemu Windows.

Pamiętajcie – zanim zdecydujecie się na instalację aplikacji ochrony rodzicielskiej na urządzeniu swoim i dziecka, koniecznie porozmawiajcie z synem lub córką o zasadności takiego rozwiązania. Dziecko powinno wiedzieć, z czego wynikają przyjęte zasady i dlaczego niektóre treści mogą być dla niego szkodliwe. Reguły używania internetu najlepiej jest ustalać wspólnie.

Więcej informacji o filtrach kontroli rodzicielskiej i naszej apce znajdziecie na stronie ose.gov.pl w: artykule „Bezpieczni w sieci z OSE: kontrola rodzicielska", wywiadzie „5 pytań o... aplikację mOchrona" oraz w zakładce mOchrona.

Źródło:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Firewall

Inaczej zapora sieciowa (lub ogniowa) to bardzo ważne urządzenie bądź oprogramowanie zabezpieczające sieć. Można powiedzieć, że jest to pierwsza linia obrony przed cyberzagrożeniami.

Jak działa firewall? Filtruje zarówno dane sieciowe przychodzące, jak i wychodzące z urządzeń cyfrowych. Każdy pakiet informacji przechodzący przez zaporę jest analizowany i porównywany z ustalonym zestawem reguł – jeśli nie spełnia wymogów bezpieczeństwa, zostaje automatycznie zablokowany. W ten sposób zapora znacząco utrudnia intruzom nieautoryzowany dostęp do zasobów Waszego komputera.

Istnieją różne rodzaje zapór:

- zapora sieciowa – chroni całą sieć lokalną i dba o to, by żadne niebezpieczne dane nie dostały się do środka;
- zapora aplikacyjna – pilnuje konkretnych programów, np. przeglądarki internetowej;
- firewall nowej generacji (ang. *next generation firewalls*, NGFW) – łączy różne metody ochrony, potrafi wykrywać ataki dzięki sztucznej inteligencji i analizować dane.

Rozwiązania sprzętowe stosuje się głównie w środowiskach firmowych, gdzie ochrona musi obejmować większe sieci i segmenty infrastruktury. Z kolei zapory programowe, instalowane bezpośrednio na komputerach czy serwerach, zapewniają indywidualną ochronę systemów użytkowników przed nieautoryzowanym dostępem.

W czasach rosnącej liczby cyberataków i pracy zdalnej coraz większą popularność zyskują także firewalle w chmurze, które filtrują ruch sieciowy za pośrednictwem serwerów dostawcy usług cloud security. Rozwiązanie to zapewnia elastyczność, szybkie wdrożenie i ochronę użytkowników niezależnie od lokalizacji.

Użytkownik nie musi robić wiele, aby z skorzystać z firewalla – wystarczy, że zapora jest włączona. Dzięki temu firewall jest jednym z najprostszych i najskuteczniejszych sposobów zabezpieczenia sieci przed włamaniem, infekcją wirusami i próbami szpiegowania.

Źródło:

„Co to jest firewall? Jak działa zapora sieciowa?", (2025), artykuł na stronie bezpiecznyinternet.edu.pl.

F

Flaming

Byliście świadkiem żarliwych dyskusji na forach lub w komentarzach publikowanych w mediach społecznościowych, które szybko przerodziły się w konflikt przesycony wulgaryzmami, obelgami, a nawet groźbami? Jeśli tak, prawdopodobnie mieliście okazję zaobserwować, jak działa flaming, czyli celowe „zaognianie" (od ang. *flame* – płomień) rozmowy w sieci. Flamerzy inicjują internetowe kłótnie, podczas których merytoryczne argumenty schodzą na dalszy plan, a próba przedstawienia flamerowi faktów zazwyczaj kończy się eskalacją agresywnego zachowania.

Warto wiedzieć, że flaming może być formą cyberprzemocy, jeśli przybiera formę regularnego, podejmowanego z premedytacją działania wobec słabszego, który nie może się bronić (Borkowska, 2023). Agresja słowna – poniżanie, wyzywanie, oczernianie w sieci, zamieszczanie komentarzy na forum internetowym lub na cudzych profilach w portalach społecznościowych w celu ośmieszenia, sprawienia przykrości lub wystraszenia innej osoby – to przejawy cyberprzemocy, która dotyka wielu internautów. Jak pokazują statystyki, co trzeci nastolatek spotyka się z różnymi formami agresji online, przy czym aż 47% młodych ludzi nikomu nie mówi o swoich przykrych doświadczeniach (Ładna i in., 2025). Sprawcy cyberprzemocy często czują się anonimowi, co sprawia, że mają złudne wrażenie bezkarności.

Flaming to też jawny przykład łamania zasad netykiety. Internetowe kłótnie oraz wszelkie przejawy „wojny na obelgi" czy agresji w sieci powinniście zgłaszać moderatorom strony, forum lub grupy dyskusyjnej – w celu ich usunięcia. Czego na pewno nie należy robić: wdawać się w utarczki słowne. Wtedy jest szansa, że flamer zniechęci się, gdy jego ataki pozostaną bez żadnej reakcji.

Więcej o zasadach netykiety przeczytacie w aktualnościach: „Netykieta, czyli jak zostać mistrzem słowa w internecie" na stronie ose.gov.pl oraz „Nie krzycz w internecie, czyli ściągawka z netykiety" na portalu OSE IT Szkoła.

Źródła:

Borkowska A., (2023), „Cyberprzemoc. Włącz blokadę na nękanie. Poradnik dla rodziców", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Flooding

Zdarzyło Wam się dostać wiele niepotrzebnych, a może identycznych, pustych lub celowo zniekształconych wiadomości e-mail lub SMS w krótkim odstępie czasu? A może irytowały Was powtarzające się komentarze albo ciągi znaków na forach internetowych? To tzw. flooding (od ang. *flood* – powódź), czyli atak spamerski ukierunkowany na jednego odbiorcę.

Z floodingiem spotkacie się zazwyczaj w mediach społecznościowych, na czatach i w różnego rodzaju komunikatorach. Może on przybrać formę np. tej samej wiadomości publikowanej w ramach jednej dyskusji lub grupy na forum albo wielokrotnie pojawiającego się komentarza na YouTubie z prośbą o subskrypcję danego kanału. Ten typ floodingu jest najczęściej wynikiem nieznajomości zasad netykiety albo niedbałego posługiwania się językiem.

Bardziej szkodliwy jest flooding stosowany celowo, prowadzący do zablokowania usługi, w obrębie której wielokrotnie wysyłane są pakiety identycznych danych. Hakerzy wykorzystują ten mechanizm w atakach typu DoS (ang. *Denial of Service*), uniemożliwiając działanie danego systemu lub usługi komputerowej.

Na flooding narażeni są również użytkownicy telefonów komórkowych i poczty elektronicznej. Skrzynki „zalewane" są wówczas dużą liczbą zbędnych wiadomości – mamy do czynienia z bombą pocztową (ang. *mail bombing*). Na szczęście tego typu ataki towarzyszą nam coraz

rzadziej: zarówno komunikatory pocztowe, jak i smartfony wyposażane są obecnie w skuteczne filtry antyfloodowe, które blokują niechciane wiadomości.

Zastanawiacie się pewnie, czym flooding różni się od spamu. W przypadku floodingu mamy do czynienia z jednym odbiorcą niechcianych bądź niezamawianych wiadomości, z kolei spam polega na masowej wysyłce takich treści do wielu osób jednocześnie. Co więcej, masowość spamu zazwyczaj opiera się na dużej liczbie odbiorców pojedynczej wiadomości w ramach jednej wysyłki, a w przypadku floodingu odwrotnie – mała liczba odbiorców otrzymuje dużo wiadomości w ramach jednej odsłony kampanii.

FOMO

Dorośli, ale też nastolatki spędzają bardzo dużo czasu w sieci. Potwierdzają to nasze obserwacje i badania NASK „Nastolatki". W dni powszednie młodzież korzysta z internetu 5 godzin dziennie (bez jednej minuty), a w weekendy 5 godzin i 16 minut (Ładna i in., 2025).

Bywa, że nie rozstajemy się ze smartfonem. Urządzenia ekranowe towarzyszą nam podczas posiłków, przed snem, zaraz po przebudzeniu. Zdarza się też, że wybudzamy się w nocy, żeby sprawdzić powiadomienia przychodzące z mediów społecznościowych. Ponadto potrafimy wpatrywać się w telefon w trakcie rozmowy z kimś, sięgać po smartfon w czasie nauki, pracy czy oglądania telewizji… Taka cyfrowa nadaktywność wpływa negatywnie na nasze funkcjonowanie.

Ból głowy, szyi, zmęczenie, problemy ze snem – to tylko niektóre fizyczne objawy nadużywania urządzeń. Brak kontroli nad czasem spędzanym online wpływa też na zdrowie psychiczne. Zarówno młodzi, jak i starsi mierzą się z wieloma problemami: stresem cyfrowym, przeciążeniem informacją, problemowym używaniem internetu (PUI).

Na liście skutków zbytniego przywiązania do internetu i urządzeń znajduje się też FOMO (ang. *Fear of Missing Out*), czyli lęk przed odłączeniem, dojmujące poczucie bezpowrotnej utraty czegoś ważnego, obawa przed wypadnięciem z obiegu w sytuacji, w której akurat nie możemy skorzystać z internetu.

Osoby z wysokim poziomem FOMO mogą reagować rozdrażnieniem, skarżyć się na poczucie pustki i nudy, a nawet wpadać w panikę czy reagować agresją, gdy nie mają dostępu do sieci i mediów społecznościowych. Ukojenie przynosi obecność smartfona oraz takie proste czynności, jak odblokowywanie urządzenia czy bezwiedne scrollowanie postów. Wysoki poziom FOMO skłania do coraz częstszego korzystania ze smartfona i social mediów, może więc doprowadzić do nadużywania nowych technologii i zwiększać ryzyko wystąpienia e-uzależnienia. *Fear of Missing Out* może dotknąć każdego, niezależnie od wieku, ale badania pokazują, że to nastolatki są na nie szczególnie narażone. Raport z badań „FOMO 2022. Polacy a lęk przed odłączeniem" potwierdza, że jedynie 6% młodych ludzi nie odczuwa lęku przed odłączeniem od sieci, a aż 28% nastolatków doświadcza wysokiego poziomu FOMO (Jupowicz-Ginalska i in., 2022).

Duże nasilenie FOMO sprawia, że dzieci tracą z oczu realne przyjaźnie, hobby, zainteresowania. Przez wzmożoną aktywność w sieci, nierzadko do późnych godzin wieczornych, opuszczają się w nauce, mają problemy z koncentracją, zdrowiem, spóźniają się na lekcje, wagarują, zaniedbują codzienne obowiązki. Wysoki poziom FOMO wiązany jest również z obniżeniem nastroju, poczuciem przygnębienia, spadkiem samooceny, a nawet stanami depresyjnymi. To efekt porównywania siebie i swojego życia z wizją świata przedstawianą przez innych internautów na profilach w mediach społecznościowych.

Jak przeciwdziałać temu zjawisku? Przede wszystkim warto postawić na profilaktykę, czyli uczyć dzieci i młodzież ustalania właściwych proporcji między życiem online i offline. Dbanie o cyfrowy dobrostan to również pokazywanie, jak ważna jest higiena cyfrowa i kształtowanie zdrowych nawyków w tym zakresie. Szukając dróg do zachowania równowagi w korzystaniu z internetu i urządzeń ekranowych, warto pamiętać o kilku uniwersalnych kwestiach:

- **Trzymajcie się zasady małych kroków** – wprowadzajcie zmiany powoli i systematycznie. Nagła rezygnacja z urządzeń cyfrowych może skończyć się niepowodzeniem,

co zniechęci do podejmowania kolejnych prób. Lepiej planować cele, które będą możliwe do osiągnięcia, np. zamiast namawiać dzieci do usuwania kont w mediach społecznościowych, zachęćcie je do wylogowania się z ulubionego serwisu na jeden dzień.

- **Zaplanujcie czas poza siecią** – warto podzielić czas wolny na kilka innych aktywności poza internetem. Nie zapominajcie przy tym o elastyczności – jeśli jakiś punkt na Waszej liście się nie sprawdził, możecie go skorygować w dowolnym momencie i dostosować plan dnia do aktualnych potrzeb.
- **Celebrujcie sukcesy, rozmawiajcie o trudnościach** – najważniejsze jest wsparcie. Rozmawiajcie z dziećmi o problemach, z jakimi mierzą się podczas wprowadzania zasad higieny cyfrowej. Na pewno nie należy krytykować czy oceniać ich aktywności online. Pamiętajcie natomiast o docenieniu każdego, nawet najmniejszego sukcesu.
- **Podejmujcie wyzwania w grupie** – namawiajcie dzieci do wspólnego równoważenia aktywności online–offline. Może się okazać, że im więcej osób, tym więcej pomysłów na poradzenie sobie z danym wyzwaniem. Nie bez znaczenia jest też wsparcie rówieśników, na które można liczyć podczas prób wprowadzania zdrowych nawyków cyfrowych.
- **Rozmawiajcie o różnicach między realnym światem, a tym kreowanym w mediach społecznościowych** – to, z czym dziecko styka się w portalach społecznościowych, jest często ubarwione, wystylizowane, wykreowane na potrzeby czyjegoś wizerunku. Porównywanie się z wyidealizowanymi zdjęciami i profilami zawsze wypada na naszą niekorzyść. Urealniajcie oczekiwania dziecka, pomóżcie mu dostrzec tę różnicę. Zapytajcie, jakie przeżycia towarzyszą mu podczas przeglądania profili innych.

Więcej informacji na temat FOMO znajdziecie w aktualnościach na ose.gov.pl: „Temat lekcji: FOMO i problemowe używanie internetu wśród uczniów”, „Niebezpieczne zjawiska w internecie: FOMO” oraz w wywiadzie „5 pytań o… FOMO i problemowe używanie internetu”, a także w tekście na OSE IT Szkole: „Temat lekcji: nadużywanie internetu”. Skorzystajcie też z naszych bezpłatnych materiałów edukacyjnych dostępnych na platformie OSE IT Szkoła: kursu e-learningowego „Zrozumieć FOMO” czy scenariuszy zajęć – z serii „#stopfomo”, „Jak się nie zaplątać w sieci?”, „Otwórz oczy – internet to nie wszystko. Śpiąca Królewna i FOMO”. Ponadto polecamy nasze poradniki: dla rodziców „FOMO i nadużywanie nowych technologii” i nauczycieli „FOMO i problemowe używanie internetu”. Koniecznie sięgnijcie też po materiały (kursy, scenariusze lekcji, komiksy) opracowane w ramach kampanii edukacyjnej „FOMOwscy i JOMOwscy”.

Źródła:

Jupowicz-Ginalska i in., (2022), „FOMO 2022. Polacy a lęk przed odłączeniem”, Warszawa: Wydział Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Fonoholizm

Telefon ułatwia życie – to pewne! Ale czy wiecie, że za jego sprawą niepostrzeżenie możecie wpaść w pułapkę nadużywania nowych technologii? Wszystko przez to, że współczesne smartfony, oprócz możliwości wykonywania połączeń i wysłania wiadomości, oferują szereg funkcjonalności, a przede wszystkim ułatwiają dostęp do sieci – o każdej porze i praktycznie z każdego miejsca.

Chętnie korzystamy z możliwości, jakie daje nam urządzenie mobilne, które zawsze jest w zasięgu ręki. Dzięki smartfonom i licznym aplikacjom możemy dziś robić zakupy, realizować przelewy, wizyty lekarskie, liczyć kalorie, kroki, uczyć się języków czy spędzać czas na rozrywce. Smartfon zastąpił też wiele przedmiotów codziennego użytku. Aparat fotograficzny, kamera, budzik, kalendarz, notatnik, odtwarzacz muzyki – to wszystko trzymamy dosłownie w jednej kieszeni.

Można powiedzieć, że smartfony towarzyszą nam przez większość czasu w ciągu dnia. Z raportu NASK „Nastolatki" wynika, że aż 93% nastolatków korzysta z internetu właśnie przez telefon. Z czego co trzeci badany (31%) ma trudność z rozstaniem się z urządzeniem choćby na chwilę, a 5 na 100 (5%) – ma z tym duży problem (Ładna i in., 2025).

Warto wiedzieć, że zbyt częste i intensywne korzystanie z telefonu może prowadzić do uzależnienia. Fonoholizm to nałogowe używanie telefonu komórkowego (smartfona), które należy do grupy uzależnień behawioralnych, czyli czynnościowych. Choć fonoholizm jako jednostka chorobowa jest wpisany na listę Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych (ICD-11) w ogólnej świadomości funkcjonuje jako rodzaj e-uzależniania. To z jednej strony uzależnianie od urządzenia cyfrowego, w tym przypadku smartfona, a z drugiej – od czynności, które wykonujemy za jego pomocą.

Jak rozpoznać, że ktoś wpadł w sidła fonoholizmu? Częste używanie nie oznacza jeszcze nadużywania. Aby stwierdzić problem, potrzebna jest dłuższa obserwacja i określenie, czy cyfrowe nawyki zaburzają nasze funkcjonowanie psychofizyczne, czy prowadzą do trudnych sytuacji życiowych.

Oto kilka symptomów, które mogą świadczyć o nałogowym korzystaniu ze smartfona:

- odczuwanie ciągłego przymusu korzystania z urządzania;
- nieustanne zerkanie na ekran w poszukiwaniu nowych powiadomień, ciągłe nasłuchiwanie dźwięku połączeń lub powiadomień, a nawet słyszenie dźwięków fantomowych;
- posiadanie telefonu zawsze przy sobie i reagowanie złością i frustracją, gdy nie można z niego skorzystać;
- strach przed rozładowaniem się telefonu (konieczność noszenia przy sobie ładowarki);
- unikanie bezpośrednich kontaktów z innymi ludźmi, spotkań towarzyskich;
- wydłużanie się czasu spędzanego przed ekranem telefonu, oszukiwanie bliskich co do czasu korzystania z urządzenia;
- zaniedbywanie codziennych obowiązków, poświęcanie czasu na sen, by spędzić go z telefonem;
- utwierdzanie innych, że wszystko mamy pod kontrolą, a telefon jest nam potrzebny z praktycznych powodów (gov.pl, b.r.).

Fonoholizm niesie za sobą wiele negatywnych konsekwencji dla zdrowia i funkcjonowania. Problemy ze snem i koncentracją, przemęczenie, izolowanie się od innych, a nawet depresja – to skutki braku kontroli nad czasem, jaki poświęcamy na korzystanie z urządzenia. Walka z nałogiem polega na podjęciu długofalowych działań.

Fonoholizm dotyczy Was lub kogoś bliskiego? Skorzystajcie z rad specjalisty, który pomoże Wam zmierzyć się z problemem i podpowie, jak w praktyce wdrażać zdrowe cyfrowe nawyki. Informacje na temat wsparcia uzyskacie np. na portalu uzaleznieniabehawioralne.pl. Znajdziecie tu bazę wiedzy, skontaktujecie się ze specjalistami z poradni online lub wyszukacie placówkę oferującą terapię e-uzależnień. Postawicie też na działania profilaktyczne – każdego dnia dbajcie o równowagę między czasem spędzanym z urządzeniem a aktywnościami offline.

Więcej porad związanych ze zdrowym korzystaniem z telefonów znajdziecie na stronie ose.gov.pl w aktualnościach „Dzień bez Telefonu Komórkowego – czy to możliwe?" oraz „Zadbaj o siebie z OSE: odzyskaj kontrolę nad czasem ekranowym". Z kolei w tekście „Niebieski Poniedziałek – zadbajmy o zdrowie psychiczne dzieci" przypominamy o wsparciu w przypadku wystąpienia sytuacji kryzysowej. Polecamy też nasze publikacje dostępne na portalu OSE IT Szkoła: poradnik „Offline znaczy zdrowiej. O cyfrowej higienie dla rodziców i wychowawców" i zbiór felietonów „O cyfrowej higienie". Sięgnijcie też po materiały edukacyjne opracowane w ramach kampanii edukacyjnej „FOMOwscy i JOMOwscy".

Źródła:

„Fonoholizm, czyli uzależnienie od telefonu”, (b.r.), artykuł w serwisie gov.pl.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

F

G

Gaming

Gaming to, najprościej rzecz ujmując, granie w gry komputerowe, mobilne, konsolowe, choć terminem tym określa się też profesjonalne rozgrywki e-sportowe. Gaming to nie tylko sposób na nudę i spędzanie wolnego czasu, ale też rozrywka, która może przerodzić się w prawdziwą pasję – wiedzą o tym szczególnie młodzi amatorzy nowych technologii.

Gry komputerowe – strategiczne, fabularne, przygodowe, zręcznościowe, sportowe, symulacyjne, logiczne czy edukacyjne – niejednokrotnie wspomagają rozwój dziecka. Gra odpowiednio dobrana do wieku i możliwości uczy praktycznych umiejętności i działania w grupie, rozwija zainteresowania, wzmacnia kompetencje społeczne, a nawet pomaga zawierać przyjaźnie.

Wasze dziecko lubi grać w gry? Przede wszystkim to Wy, jako rodzice, powinniście dokonywać świadomych wyborów. Popularne nie zawsze oznacza odpowiednie dla dziecka. Sprawdzajcie, czy gra nie zawiera szkodliwych treści ani nie promuje agresywnych zachowań. Pomocna będzie klasyfikacja PEGI (ang. *Pan-European Game Information*), która składa się z dwóch elementów. Pierwszy to oznaczenia wiekowe – określają, czy zawartość konkretnej gry nie wpłynie negatywnie na dziecko w danym wieku. Drugi to deskryptory treści – wskazują typ treści występujących w grze, np. przemoc, wulgaryzmy czy elementy hazardu.

Zawartość gier to jedna ważna kwestia, druga dotyczy czasu spędzanego przed urządzeniem ekranowym. W grach łatwo się zatracić – na naszą niekorzyść działają mechanizmy stosowane przez producentów, które potrafią skutecznie utrzymać użytkowników przy ekranie. Tymczasem długi czas przed ekranem sprzyja rozwojowi nadwagi, może przyczyniać się do wad postawy, a także powodować szereg dolegliwości somatycznych, takich jak bóle i zawroty głowy, zmęczenie wzroku czy niewyraźne widzenie.

To jednak nie wszystko. Gaming może prowadzić do nadużywania nowych technologii, a nawet uzależnienia od gier komputerowych. Światowa Organizacja Zdrowia (WHO) szczególne zagrożenie dostrzega w uzależnieniu od gier online (gaming disorder). Z tego też powodu zostało ono wpisane na listę Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych (ICD-11). Jakie sygnały powinny nas zaniepokoić?

- Pasja dziecka zaczyna nabierać obsesyjnego charakteru. Myśli tylko o grze, ciągle poszukuje informacji na jej temat lub jest ona stałym elementem rozmów i opowieści.
- Dziecko organizuje swój świat wokół grania, rezygnując z dotychczasowych zainteresowań. Zaniedbuje obowiązki i wycofuje się z relacji z rówieśnikami, którzy nie grają.
- Niemożność grania powoduje skrajne stany emocjonalne, duże wahania nastroju, zachowania agresywne. Sam proces grania również eskaluje emocje.
- Dziecko potrzebuje coraz więcej czasu przed ekranem, aby uspokoić się i rozładować napięcie, uwolnić się od lęku lub poczucia winy.
- Dziecko zapomina o posiłkach, zaniedbuje sen, zgłasza różne dolegliwości bólowe (bóle głowy, oczu, szyi, nadgarstka, pleców itp.). Podejmuje próby ograniczania czasu przed ekranem, ale nie przynosi to pożądanego rezultatu. Granie prowadzi więc do napięć oraz eskalacji konfliktów w domu i szkole.
- Inwestuje w granie więcej środków, niż posiada, co może prowadzić do problemów finansowych, a nawet kradzieży (Witkowska, 2023).

Jak przeciwdziałać negatywnym skutkom gamingu? Przede wszystkim poznajcie zainteresowania swojego dziecka, wspólnie postawcie na zasady i kształtowanie prawidłowych nawyków cyfrowych. Pamiętajcie też, że ważnym elementem każdej rozmowy o obecności dziecka w cyfrowym świecie powinno być bezpieczeństwo. Jeśli dziecko gra trybie multiplayer, czyli podczas

rozgrywki spotyka się online ze znajomymi lub nieznajomymi, uczulajcie, że nie wszyscy w sieci mają dobre zamiary. Uczcie zasad ograniczonego zaufania podczas zawierania znajomości w internecie oraz nieujawniania prywatnych informacji na swój temat. Rozgrywki online, wymiana wirtualnych dóbr, pobieranie niezaufanych aplikacji – wszystko to zwiększa ryzyko zetknięcia się z cyberoszustwami.

Więcej informacji o pozytywnych i negatywnych skutkach gamingu znajdziecie w aktualności na stronie ose.gov.pl: „Cyfrowe gry a rozwój dziecka" oraz w wywiadzie „5 pytań o... gaming". Skorzystajcie też z kursu „Bezpiecznie w grach cyfrowych" dostępnego na platformie bezpieczniwsieci.edu.pl oraz ze zbioru felietonów „O grach cyfrowych" – na OSE IT Szkole.

Źródło:

Witkowska M., (2023), „Nastolatki i gry cyfrowe. Poradnik dla rodziców", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Generator hasła

Jeszcze do niedawna częstą praktyką tworzenia silnych i bezpiecznych haseł było stosowanie ciągu znaków niezwiązanych ze sobą znaczeniowo, ale na pierwszy rzut oka tworzących niemożliwy do złamania szyfr. Na takie hasło składały się małe i duże litery, a także cyfry oraz znaki specjalne, np. mx6t6Y8IsKWaYoo. Generatory hasła służą właśnie do tworzenia losowych kombinacji różnych znaków, co ma nam dać silne zabezpieczenie. I choć wiele portali stosuje jeszcze takie wymagania przy tworzeniu zabezpieczeń, to rekomendacje CERT Polska w tym zakresie zwracają uwagę przede wszystkim na długość hasła.

Czy zatem popularne generatory hasła przejdą do lamusa? Zanim to nastąpi, podpowiadamy, jak samodzielnie tworzyć silne i bezpieczne hasła:

- Używajcie długich haseł składających się z min. 14 znaków. Korzystajcie ze sprytnie zmienionych fraz – łatwych do zapamiętania dla Was, ale trudnych do złamania dla przestępców. Siłę hasła wzmocnią też obcojęzyczne wtręty (np. DwaBialeLatajace-SophisticatedKroliki).
- Sprawdźcie listę najpopularniejszych haseł opublikowaną przez CERT Polska i wystrzegajcie się podanych tam oczywistych kombinacji!
- Pamiętajcie też o unikalnych hasła do wszystkich swoich kont. W ten sposób ochronicie się np. przed atakiem typu credential stuffing, który polega na tym, że wykorzystując raz zdobyte dane logowania, oszuści próbują dostać się do wielu różnych portali, licząc na to, że wykradzione hasło będzie pasować do więcej niż jednego konta.

Bezpieczeństwo w sieci można wzmocnić, stosując się do kolejnych zaleceń:

- Wszędzie, gdzie to możliwe, wykorzystujcie uwierzytelnianie dwuskładniowe lub wieloskładnikowe, czyli oprócz hasła logujcie się dodatkowymi składnikami, np. kodem otrzymanym SMS-em, odciskiem palca czy kluczem U2F.
- Sprawdzajcie, czy Wasze hasła nie wyciekły, np. na stronie bezpiecznedane.gov.pl. Jeśli tak się stało, bezzwłocznie zmieńcie dotychczasowe hasła do logowania, w tym hasła pokrewne, które łatwo zgadnąć.
- Używajcie menedżerów haseł, dzięki którym nie będziecie musieli pamiętać wszystkich swoich zabezpieczeń.

Więcej o zasadach tworzenia silnych haseł przeczytacie na stronie CERT Polska w poradniku „Kompleksowo o hasłach", a także w naszych aktualnościach na ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: wyciek danych", „Bezpieczni w sieci z OSE: bezpieczny login i hasło".

Geolokalizacja

Czy wiecie, że wiele platform i aplikacji zbiera dane na temat Waszej aktualnej lokalizacji? Geolokalizacja to nic innego, jak określanie położenia geograficznego urządzenia podłączonego do sieci. W ustaleniu miejsca Waszego pobytu pomaga wiele narzędzi, choć nie zawsze zdajecie sobie sprawę z tego, że akurat w danym momencie jesteście „namierzani".

Położenie określane jest na podstawie włączonej funkcji udostępniania lokalizacji i adresu IP. Dzięki temu po wpisaniu w wyszukiwarkę zapytania o wyznaczenie trasy lub wskazanie interesującego Was obiektu otrzymacie precyzyjną informację, gdzie znajduje się najbliższa kawiarnia lub kino, a nawet jaka jest pogoda w danym miejscu!

Warto pamiętać, by nie wpaść w pułapkę zbyt łatwej dostępności serwisów społecznościowych, gier mobilnych czy aplikacji do informacji o Waszej lokalizacji. Zanim zainstalujecie takie narzędzie na smartfonie, dokładnie przeczytajcie regulamin i politykę prywatności. Sprawdźcie, na co wyrażacie zgodę. Zastanówcie się, czy uzasadnione jest żądanie dostępu do aparatu, zdjęć, filmów, kontaktów, wiadomości, kamery lub właśnie geolokalizacji. Ulubiona gra lub apka może zbierać i przekazywać zbyt wiele wiadomości o Was, co ma wpływ na Wasze bezpieczeństwo.

A może sami zostawiacie w internecie cyfrowe ślady, korzystając z funkcji tagowania lokalizacji? Jeśli oznaczacie miejsca, które odwiedzacie, Wasza prywatność w sieci i bezpieczeństwo również mogą być zagrożone. Informowanie innych o swoich podróżach, odwiedzanych miejscach, wydarzeniach, w których bierzecie udział, sprawia, że Wasza aktywność online podlega większemu monitorowaniu. Wiele aplikacji zbiera takie dane, analizuje, a następnie wykorzystuje np. do celów marketingowych czy precyzyjnego określenia Waszych preferencji. Tagowanie lokalizacji to też informacja dla cyberprzestępców, którzy mogą wykorzystać zdobytą o Was wiedzę do szpiegowania, zaplanowania ataku typu spear phishing (ukierunkowanego ataku na konkretną osobę lub firmę), kradzieży tożsamości czy nękania w sieci. Z kolei dla przestępców spoza cyfrowego świata, np. złodziei, wiedza o tym, gdzie i kiedy dokładnie się znajdujecie, stwarza okazję do kradzieży czy innej formy przestępczości.

Zanim włączycie funkcję geolokalizacji w telefonie i oznaczycie w sieci miejsce swojego pobytu, pomyślcie o prywatności online. Warto strzec poufnych informacji i danych – szczególnie w internecie. W wirtualnej przestrzeni to, co prywatne, bardzo szybko może stać się publiczne i trafić w niepowołane ręce.

Więcej informacji o ochronie prywatności w sieci oraz zasadach korzystania z aplikacji przeczytacie na ose.gov.pl w aktualnościach „Bezpieczni w sieci z OSE: aplikacje mobilne" i „Zadbaj o siebie z OSE: prywatność w mediach społecznościowych". Z kolei informacje o materiałach edukacyjnych na temat rozważnego dzielenia się informacjami w sieci znajdziecie w artykułach na OSE IT Szkole: „Lekcja o cyberbezpieczeństwie: prywatność online", „Lekcja o cyberbezpieczeństwie: prywatność online cz. 2".

Gray hat

Kim jest osoba w szarym kapeluszu? Takim mianem określa się członka społeczności hakerskiej, czyli kogoś, kto odznacza się dużymi umiejętnościami informatycznymi. Gray hats działają jednak na krawędzi prawa, choć w przeciwieństwie do black hats (czarnych kapeluszy) – w dobrej wierze. Włamują się do systemów komputerowych lub sieci, by zlokalizować luki i błędy, a następnie pozyskane informacje zgłaszają zainteresowanym stronom. Dzięki temu możliwe jest zlikwidowanie potencjalnego zagrożenia.

W tym miejscu warto podkreślić, że haker to nie to, co zapewne macie na myśli – czyli złodziej, oszust. W powszechnej opinii utarło się, że haker to cyberprzestępca, który wykorzystuje podatności bezpieczeństwa i malware (złośliwe oprogramowanie), by przeprowadzić atak. I choć jest to osoba wykazująca się bardzo dużymi umiejętnościami informatycznymi, dobrze znająca języki programowania i systemy operacyjne, przed którą internet nie ma żadnych tajemnic, nie oznacza to, że działa niezgodnie z prawem. Jeśli chcecie być precyzyjni, powinniście odróżnić hakera od crackera (black hat), który swoje umiejętności wykorzystuje do działań przestępczych.

Poza szarym i czarnym oczywiście jest jeszcze biały. White hats (białe kapelusze) to prawdziwi cyfrowi dżentelmeni. Zastanawiacie się pewnie, co ich odróżnia od gray hats? Białe kapelusze również tropią podatności oprogramowania na ataki i błędy w aplikacjach, ale robią to zgodnie z prawem – często na zlecenie administratorów danego systemu. Potencjalne luki zgłaszają właśnie administratorom, producentom oprogramowania czy zespołom reagowania na incydenty bezpieczeństwa – CSIRT oraz CERT. Ważna jest dla nich satysfakcja z możliwości uczestniczenia w procesie usuwania błędów, które mogą zagrażać bezpieczeństwu użytkowników.

G

H

Haktywista

Jeśli powiemy, że grupa Anonymous jest przykładem haktywistów, chyba nie będziecie mieli wątpliwości, co oznacza to pojęcie, które powstało z połączenia dwóch angielskich słów: *hacking* – hakowanie i *activism* – aktywizm.

Haktywiści, używając komputerów, sieci i swoich umiejętności, działają poza prawem, ale zawsze kieruje nimi chęć promocji swojej ideologii. Walka o wolność obywateli, prawdę, dostęp do informacji, sprzeciw wobec niesprawiedliwości, dyskryminacji, złych decyzji rządzących, ale także realizacja interesów jednej ze stron konfliktu lub destabilizacja sytuacji w gronie nieprzyjaciół: to motywacje anonimowych specjalistów od łamania wszelkich zabezpieczeń. Atak na rządowe strony czy upublicznianie tajnych dokumentów – dla nich to nic trudnego. Haktywista to gray hat (szary kapelusz), czyli osoba, która potrafi działać w dobrej wierze, choć niekoniecznie zgodnie z obowiązującym prawem.

H

Warto pamiętać, że haktywizm, mimo że utożsamiany jest z wyższymi pobudkami, wiąże się z wieloma cyberzagrożeniami. Oto niektóre z nich:

- Wyciek danych – haktywiści często uzyskują dostęp do baz danych zawierających poufne informacje, takie jak dane osobowe, numery kart kredytowych, adresy e-mail czy hasła.
- Ataki typu DDoS – polegają na sparaliżowaniu i blokowaniu dostępu do usług online.
- Dezinformacja – haktywiści mogą rozpowszechniać fałszywe informacje lub manipulować upublicznionymi materiałami.
- Naruszenie prywatności – dostęp do prywatnych danych użytkowników czy wrażliwych informacji (wyników badań) wiąże się z naruszeniem prawa do prywatności.
- Ransomware – wykorzystanie oprogramowania do zaszyfrowania danych na komputerze ofiary, tak by nie miała do nich dostępu, prowadzi do szantażu, jeśli żądania haktywistów nie zostaną spełnione.
- Atak na infrastrukturę krytyczną kraju – np. energetyczną, wywołuje chaos i niepokój społeczny. W skrajnych przypadkach może być odebrany jako forma cyberterroryzmu, jeśli zagraża bezpieczeństwu narodowemu.

Koszty działalności haktywistów ponoszone przez państwa, firmy czy organizacje są ogromne. Ataki narażają na straty finansowe i wizerunkowe. Częste incydenty związane z cyberbezpieczeństwem prowadzą też do spadku zaufania społeczeństwa do nowych technologii.

Happy slapping

Zapewne wielu z Was natknęło się w sieci na filmik, na którym przypadkowa ofiara została znienacka zaatakowana: okradziona czy pobita, a całe zajście nagrano, najczęściej smartfonem. Rozśmieszyć odbiorców i oczywiście zwiększyć statystyki „kliknięć” – taki cel mają twórcy „zabawnej przemocy”. Happy slapping nie ma jednak nic wspólnego z komedią.

Ofiarami happy slappingu bywają zarówno osoby przypadkowe, jak i znajome, np. z tej samej szkoły. W wyniku takiego zdarzenia cierpią podwójnie: pobicie i inne akty agresji zostawiają fizyczne rany, do tego dochodzi cyberprzemoc (zwana też cyberbullingiem), która również zostawia ślady, choć niewidoczne dla sprawcy.

Powinniśmy stanowczo przeciwstawiać się każdej formie agresji w sieci, bo wyrządzone krzywdy często trudno odwrócić. Nagrania typu happy slapping bardzo szybko rozprzestrzeniają się w sieci, a skutki przemocy w internecie mogą być długofalowe i wiązać się z poważnymi konsekwencja-

mi. Ofiara cyberprzemocy może przeżywać poniżenie i upokorzenie, lęk, rozpacz, smutek, poczucie osamotnienia, bezradność, co w efekcie może prowadzić nawet do zaburzeń depresyjnych czy myśli samobójczych.

Badania NASK „Nastolatki" pokazują, że cyberprzemoc na dobre zagościła w sieci. Różnych form agresji online (wyzywania, ośmieszania, poniżania i straszenia) doświadczył co trzeci nastolatek. Warto przy tym wiedzieć, że młodzi ludzie bardzo rzadko proszą dorosłych – rodziców i nauczycieli – o pomoc, gdy padną ofiarą cyberprzemocy. Te same badania pokazują, że aż 47% badanych zadeklarowało, że w ogóle nie podjęło żadnych działań i nikomu nie powiedziało o swoim problemie (Ładna i in., 2025). Tymczasem pozbawione pomocy dziecko często nie jest w stanie samo stawić czoła trudnej sytuacji online.

Co zrobić, jeśli Wasze dziecko doświadcza przemocy online? Przede wszystkim okażcie mu wsparcie, spróbujcie wyjaśnić i zrozumieć zaistniałą sytuację. Wspólnie zabezpieczcie też dowody cyberprzemocy, zapiszcie lub wydrukujcie: e-maile, SMS-y, MMS-y, wiadomości w komunikatorach, wpisy na stronach internetowych, komentarze do wpisów lub do zdjęć w mediach społecznościowych, na blogach itp. Zebranie dowodów ułatwi dostawcy usługi odnalezienie sprawcy, usunięcie szkodliwych treści z serwisu, ale też będzie stanowiło materiał, z którym powinny się zapoznać wszystkie osoby zaangażowane w sprawę.

Pamiętajcie – cyberprzemoc jest karalna! Wszelkie przypadki cyberbullyingu, będące naruszeniem prawa (uporczywe nękanie, kradzież tożsamości, groźby karalne, publikowanie nielegalnych treści itp.), powinny być zgłaszane na policję.

Chcecie wiedzieć, jak chronić dziecko przed cyberprzemocą oraz w jaki sposób reagować, gdy padnie ofiarą ataku w sieci? Sięgnijcie do materiałów zamieszczonych na stronie OSE IT Szkoła: kursy e-learningowe (w tym kurs dla młodszych dzieci „Owce w sieci – Zabawa w śnieżki", który przybliża problem happy slappingu), animacje, poradniki, scenariusze lekcji, plakaty, infografiki. Skorzystajcie też ze zbioru felietonów „O cyberprzemocy i hajcie w sieci". Ponadto zachęcamy do lektury naszych aktualności na ose.gov.pl: „Bezpieczni w sieci z OSE: cyberbullying" oraz „Temat lekcji: przemoc w sieci".

Źródła:

Borkowska A., (2023), „Cyberprzemoc. Włącz blokadę na nękanie. Poradnik dla rodziców", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Hardening

Jeśli jesteście użytkownikami sieci i urządzeń cyfrowych, dobrze wiecie, że dbanie o cyberbezpieczeństwo to jedno z ważniejszych zadań. Wiedzą to też specjaliści zajmujący się zarządzaniem bezpieczeństwem IT (od ang. *Information Technology* – technologia informacyjna), którzy codziennie starają się wzmacniać odporność na ataki i minimalizować podatności. Jednym z ich działań jest hardening. Pojęcie to dosłownie oznacza „utwardzanie". Jest to proces zabezpieczania systemów komputerowych, sieci, urządzeń lub oprogramowania przed atakami, włamaniami lub nieautoryzowanym dostępem. „Utwardzać" można też bazy danych, usługi, aplikacje czy stacje robocze przeznaczone do wykonywania zaawansowanych zadań.

Hardening wymaga odpowiedniego przygotowania, a przede wszystkim dokładnej analizy ryzyka związanego z bezpieczeństwem cyfrowych rozwiązań. Przed „utwardzaniem" należy wskazać systemy najbardziej narażone na włamania, kluczowe, a także określić, które z nich, w sytuacji utraty integralności i dostępności, wiązałyby się z największymi stratami. W odpowiedzi na te zagadnienia pomocny może być np. przeprowadzony wcześniej audyt, a także testy penetracyjne, które ocenią stan bezpieczeństwa danego systemu.

Jakie działania może obejmować hardening? Oto kilka z nich, które mogą przydać się również każdemu użytkownikowi urządzeń cyfrowych:

- **Aktualizowanie oprogramowania** – regularna aktualizacja oprogramowania to podstawa cyberbezpieczeństwa. Nowe wersje programów czy aplikacji zwykle naprawiają większość błędów, zawierają nowe funkcjonalności, wpływają również na wygodę użytkowania sprzętów.
- **Wyłączenie nieużywanych usług** – usunięcie lub dezaktywacja niepotrzebnych usług lub funkcji zmniejsza ryzyko potencjalnych cyberataków.
- **Odinstalowanie niepotrzebnych programów** – szczególnie takich, które nie są już wspierane przez producenta. Jeśli użytkownik nie otrzymuje niezbędnych aktualizacji zabezpieczeń, narażony jest na ataki.
- **Konfiguracja firewall** – czyli urządzenia lub oprogramowania zabezpieczającego sieć, które filtruje zarówno dane sieciowe przychodzące, jak i wychodzące z urządzeń cyfrowych, udaremniając nieautoryzowany dostęp do naszych zasobów. Ustawienie odpowiednich reguł zapory sieciowej pomaga kontrolować ruch sieciowy i blokować nieuprawnione działania.
- **Zarządzanie uprawnieniami użytkowników** – działanie to polega na przyznaniu użytkownikom dostępu tylko do tych zasobów, które są niezbędne do wykonywania powierzonych im zadań.
- **Szyfrowanie danych** – oprogramowanie szyfrujące pomaga chronić dane zarówno podczas przesyłania, jak i przechowywania. Dzięki niemu uniemożliwiamy osobom niepowołanym dostęp do naszych dokumentów i danych.
- **Monitorowanie systemu** – regularny monitoring i audyt pozwala na szybkie wykrycie podejrzanych aktywności, a także na podjęcie odpowiednich kroków w przypadku naruszenia bezpieczeństwa.

Źródło:

Krauzowicz M., (b.r.), „Hardening od podstaw, czyli jak ze swojej organizacji zrobić twierdzę nie do zdobycia?”, artykuł w serwisie integritypartners.pl.

Hasło

To najprostsze i najbardziej popularne zabezpieczenie, które chroni Wasz sprzęt przed atakiem cyberprzestępców. Silne, bezpieczne hasło to strażnik cyfrowych danych przechowywanych w różnych miejscach. Dostęp do portalu społecznościowego, bankowości elektronicznej czy skrzynki e-mail powinien być chroniony odpowiednim zabezpieczeniem. Czyli jakim?

Podstawą bezpieczeństwa jest długie, nieoczywiste hasło, unikalne we wszystkich miejscach w sieci, gdzie zakładacie konta. Niestety, w praktyce okazuje się, że często tworzymy krótkie, przewidywalne zabezpieczenia, które można złamać w kilka sekund.

Zespół ekspertów z CERT Polska po przenalizowaniu haseł, które wyciekły, stwierdził, że ponad połowa z nich była złożona maksymalnie z ośmiu znaków. Ponadto do tworzenia haseł używano głównie imion lub popularnych zwrotów typu „misiek” czy prostych schematów klawiatury komputera, np. „123qwe” (CERT Polska, 2022).

Stosowanie oczywistych haseł może sprawić, że padniecie ofiarą ataku słownikowego (ang. *dictionary attack*), a w przypadku wycieku danych – przestępcy przeprowadzą skuteczny atak typu credential stuffing, uzyskując dostęp do różnych Waszych kont zabezpieczonych tym samym hasłem.

Jak zatem stworzyć silne hasło? CERT Polska radzi:

- Używajcie długich fraz składających się z co najmniej 14 znaków (najlepiej będące zdaniem złożonym z min. pięciu słów). Unikajcie oczywistych kombinacji liter i cyfr, nie wykorzystujcie kojarzących się z Wami danych (np. daty urodzenia) ani potocznych zwrotów itd. Nie korzystajcie z tego samego hasła w wielu serwisach!
- Tworząc hasło, korzystajcie z długich, sprytnie zmienionych fraz, które będą łatwe do zapamiętania dla Was, ale trudne do złamania dla przestępców (np. Wlazł**Kostek**NaMostekI**Stuka**). Siłę hasła wzmocnią też obcojęzyczne wtręty (np. DwaBialeLatajace**Sophisticated**Kroliki).
- Sprawdźcie listę najpopularniejszych haseł opublikowaną przez CERT Polska i wystrzegajcie się podanych tam przykładów!
- Używajcie menedżerów haseł, dzięki którym nie będziecie musieli pamiętać wszystkich swoich zabezpieczeń.
- Wszędzie, gdzie to możliwe, stosujcie uwierzytelnianie dwuskładniowe lub wieloskładnikowe, czyli oprócz hasła logujcie się dodatkowymi składnikami, np. kodem otrzymanym SMS-em, odciskiem palca czy kluczem U2F.
- Często sprawdzajcie, czy Wasze hasła nie wyciekły, np. na stronie bezpiecznedane.gov.pl lub haveibeenpwned.com. Jeśli tak się stało, użyjcie oprogramowania antywirusowego, żeby sprawdzić bezpieczeństwo swojego komputera. Następnie bezzwłocznie zmieńcie dotychczasowy login i hasło, w tym również wszystkie hasła pokrewne, które łatwo zgadnąć.

Więcej o zasadach tworzenia silnych haseł i ochrony przed atakami przeczytacie na stronie CERT Polska w poradniku „Kompleksowo o hasłach", a także w naszych aktualnościach dostępnych na ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: bezpieczny login i hasło", „Bezpieczni w sieci z OSE: ataki słownikowe".

Źródło:

„Co wycieki danych mówią o hasłach", (2022), artykuł na stronie cert.pl.

Hazard w internecie

Zapewne hazard kojarzy się Wam głównie z kasynem, ruletką, kartami i… grą na pieniądze. Powszechny dostęp do sieci sprawił, że rozrywkę z elementami hazardowymi mamy dziś na wyciągnięcie ręki i nie musimy nawet wychodzić z domu, by sprawdzić, czy Fortuna nam sprzyja. Niestety, niewinna zabawa może stanowić duże ryzyko dla młodych użytkowników. Jakie mogą być konsekwencje wpadnięcia w sidła hazardu? Wyczerpanie fizyczne, emocjonalne, a nawet kryzys psychiczny.

Jak pokazują badania, młodzi mają częsty kontakt z hazardem w sieci. Z danych przygotowanych przez Gemius wynika, że w okresie od października do listopada 2022 r. młodzież korzystała z wielu stron, w tym odwiedzała witryny, które wprowadzają odbiorców w świat hazardu, np. dotyczące zakładów bukmacherskich. Ponad 800 tys. młodych internautów weszło na stronę STS.pl, a niespełna pół miliona na stronę Betclic.pl (Lange, 2023).

Hazard w sieci ma jednak niejedno oblicze. Stykają się z nim już najmłodsi pasjonaci gier komputerowych – nie typu typu free to play (dostępnych do pobrania za darmo), ale też wysokobudżetowych produkcji triple-A (AAA), w które „zaszywane" są elementy hazardowe. Przykładem rozwiązań bazujących na mechanizmach hazardowych mogą być lootboxy (skrzynki z łupem), czyli artefakty oferujące losową zawartość, która może zwiększyć szansę na lepszy wynik czy uzyskanie unikatowych przedmiotów. Na zakupie jednej skrzynki zazwyczaj się nie kończy (otwieranie lootboxów wywołuje dreszczyk emocji), a mikropłatności szybko potrafią wymknąć się graczowi spod kontroli.

Warto pamiętać, że hazard w internecie nie zawsze wiąże się z wydawaniem realnych pieniędzy. „Środkiem płatności" mogą być też punkty lub wewnętrzne waluty używane np. w grach. Częste granie w gry wykorzystujące elementy hazardowe kształtuje charakterystyczne postawy i przekonania. Dzieci zaczynają postrzegać hazard jako opłacalną zabawę, inwestycję, która kiedyś się zwróci. Chętniej też sięgają po tego typu rozrywkę w dorosłym życiu.

Takie postawy zwiększają ryzyko uzależnienia od hazardu, które znajduje się w grupie e-uzależnień behawioralnych (czynnościowych). Jakie sygnały powinny zaniepokoić rodziców? Wczesne znaki ostrzegawcze to ogólna zmiana zachowania – większa niż zwykle tajemniczość, ukrywanie swojej aktywności w sieci, kłamstwa, brak lub nagły przypływ gotówki. Z czasem dziecko oddala się od rodziny, przyjaciół, znajomych, zaniedbuje codzienne obowiązki. Bywa rozdrażnione czy reaguje agresją, zwłaszcza na próby ograniczenia korzystania z urządzeń ekranowych (por. Wojewódzka, b.r.).

W sytuacji podejrzenia o uzależnienie od hazardu konieczna jest opieka specjalisty – najlepiej terapeuty uzależnień. Gdzie uzyskać pomoc? Zerknijcie do hasła helpline – znajdziecie tam numery telefonów, pod którymi otrzymacie wsparcie. Ponadto odwiedźcie portal uzaleznieniabehawioralne.pl i skorzystajcie z wyszukiwarki poradni online oraz ośrodków terapeutycznych dostępnych na terenie całej Polski.

Jak grać bezpiecznie? Odwiedźcie portal OSE IT Szkoła, znajdziecie tam poradnik dla rodziców „Nastolatki i gry cyfrowe", zbiór felietonów „O grach cyfrowych" oraz aktualności „Letnia Akademia OSE 2022: hazard online", „Temat lekcji: gry cyfrowe". Polecamy też wykład Marty Witkowskiej wygłoszony podczas Kongresu OSE 2024 „Niepokojące, nieodpowiednie, krzywdzące. Dzieci i szkodliwe treści w internecie" dostępny na YouTubie OSE.

Źródła:

„Jak pomóc dziecku wciągniętemu w hazard? Rozmowa z ekspertem", (b.r.), wywiad z Barbarą Wojewódzką na portalu uzaleznieniabehawioralne.pl.

Lange R. (red.), (2023), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Hejt

Określenie hejt (od ang. *hate* – nienawidzić) na stałe weszło do naszego słownika. Oznacza obrażanie, poniżanie, wyśmiewanie innych w sieci. Negatywne, agresywne komentarze znajdziecie na forach, w mediach społecznościowych czy internetowych dyskusjach. Hejt jest jedną z form cyberprzemocy a obiektem ataku może stać się każdy.

Badania wskazują, że młodzież styka się z cyberprzemocą i hejtem. Z raportu NASK „Nastolatki" wynika, że różnych form agresji online (wyzywania, ośmieszania, poniżania i straszenia) doświadczył co trzeci nastolatek (Ładna i in., 2025). Ale cyberprzemoc to nie tylko agresja słowna (hejt, mowa nienawiści). Może ona przybierać różne formy: wykluczania z grona znajomych, szantażu, podszywania się pod daną osobę, publikowania w sieci upokarzających materiałów – filmów lub zdjęć – czy kradzieży tożsamości.

Dzieci mogą być nie tylko ofiarami, ale też sprawcami agresji online. Internetowa przemoc bardzo często dotyczy rówieśników. Sprawcami są zwykle znajomi z klasy lub szkoły. Poczucie anonimowości w sieci sprawia, że hejter – kierowany zazdrością lub chęcią odreagowania własnych niepowodzeń – bez większej refleksji stosuje mowę nienawiści. Sprawca przemocy nie widzi skutków swoich działań i krzywdy, którą wyrządza ofierze. Ta też często nie może zapobiec atakom w sieci, bo krzywdzące materiały (zdjęcia, filmiki, komentarze) bardzo szybko się rozprzestrzeniają i nie tak łatwo giną z cyfrowego świata.

Tymczasem dręczenie sprawia, że osoba napiętnowana w internecie mierzy się z wieloma problemami. Długotrwałe doświadczanie cyberprzemocy wpływa na sposób myślenia o sobie i innych, na relacje z otoczeniem. Ofiary ataków częściej niż ich rówieśnicy doświadczają problemów w kontaktach z innymi ludźmi, mają zaniżone poczucie własnej wartości. Ponadto zaczynają

mieć kłopoty z nauką oraz mierzą się z problemami psychologicznymi i zdrowotnymi, takimi jak bóle głowy, brzucha, problemy ze snem itp. W skrajnych przypadkach mają myśli i próby samobójcze (Borkowska, 2023).

Niestety, badania NASK „Nastolatki" pokazują, że dziecko doświadczające cyberataków niepokojąco często pozostaje z tym problemem samo – 47% badanych nikomu nie mówi, że padło ofiarą cyberagresji. Nawet rodzice rzadko mają świadomość, że ich dziecku dzieje się krzywda w internecie.

Dręczenie w sieci może dotknąć każdego, stąd tak ważna jest profilaktyka. Po pierwsze należy tłumaczyć dzieciom, czym tak naprawdę jest cyberprzemoc. 17% badanych nastolatków nie jest bowiem w stanie określić, czy sytuacje, które obserwuje lub których doświadcza w internecie, są formą przemocy (Ładna i in., 2025). Po drugie trzeba uczyć, jak przeciwstawiać się aktom internetowej agresji i co robić, by wspierać jej ofiary.

Chcecie wiedzieć, jak reagować na hejt? Skorzystajcie z naszych materiałów edukacyjnych na temat przemocy w sieci dostępnych na platformie OSE IT Szkoła: kursów e-learningowych, animacji, poradników, np. „Cyberprzemoc. Włącz blokadę na nękanie", zbioru felietonów „O cyberprzemocy i hejcie w sieci", scenariuszy lekcji (w szczególności „Nie wywołuj hejtu z lasu. Czerwony Kapturek i cyberprzemoc"), plakatów, infografik. Ponadto przeczytajcie nasze aktualności: „Bezpieczni w sieci z OSE: cyberbullying" – na stronie ose.gov.pl oraz „Temat lekcji: przemoc w sieci" – na OSE IT Szkole.

Źródła:

Borkowska A., (2023), „Cyberprzemoc w szkole. Poradnik dla nauczycieli", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Helpline

To inaczej linia pomocowa, czyli numer telefonu, pod którym możecie uzyskać poradę specjalisty, emocjonalne wsparcie w trudnej sytuacji lub po prostu zostać wysłuchani. Osoby w kryzysie anonimowo mogą zgłaszać się do różnych służb oraz instytucji oferujących pomoc.

Pamiętajcie, że na zdrowie psychiczne dorosłych, dzieci i młodzieży ma wpływ wiele czynników, w tym problemowe użytkowanie internetu (PUI) i nowych technologii. Urządzenia cyfrowe podłączone do sieci oferują nam wiele możliwości, ale też mogą stać się źródłem kłopotów. Przed ekranem urządzenia potrafimy spędzać każdego dnia kilka, a nawet kilkanaście godzin – jeśli weźmiemy pod uwagę pracę i naukę. Złe cyfrowe nawyki mogą wpędzić nas w pułapkę stresu cyfrowego, przeciążenia informacją, FOMO (ang. *Fear of Missing Out*, lęku przed odłączeniem), a nawet – w skrajnych przypadkach – w sidła e-uzależnienia od hazardu online, gier cyfrowych czy mediów społecznościowych.

Cyfrowy świat wiąże się też z cyberzagrożeniami – w tym z cyberprzemocą, hejtem, mową nienawiści. Nie należy lekceważyć żadnych przejawów agresji w sieci, bo jej ofiary niejednokrotnie przeżywają trudne emocje: poniżenie i upokorzenie, lęk, rozpacz, smutek, poczucie osamotnienia, bezradność, a nawet mogą mieć zaburzenia depresyjne czy myśli samobójcze.

Pamiętajcie, nie jesteście sami! Skorzystacie z helpline i skontaktujcie się ze specjalistami, jeśli czujecie, że jakaś sytuacja Was przerasta albo ktoś z Waszych bliskich nie radzi sobie z problemami. Podpowiadamy, gdzie możecie uzyskać rzetelną pomoc:

- 116 111 (116111.pl) – Bezpłatny i anonimowy telefon zaufania dla dzieci
- 116 123 – Bezpłatny kryzysowy telefon zaufania dla dorosłych

- 800 100 100 (800100100.pl) – Bezpłatny i anonimowy telefon zaufania dla rodziców i nauczycieli
- 800 70 2222 (centrumwsparcia.pl) – Centrum wsparcia dla osób w stanie kryzysu psychicznego
- 800 12 12 12 (brpd.gov.pl, e-mail: rpd@brpd.gov.pl) – Telefon zaufania Rzecznika Praw Dziecka

Higiena cyfrowa

Internet i urządzenia cyfrowe towarzyszą nam na co dzień. Dziś trudno wyobrazić sobie naukę, pracę, rozrywkę, komunikację, załatwianie wielu spraw bez dostępu do sieci. Życie ułatwiają nam szczególnie urządzenia mobilne, dzięki którym możemy być „always on" – zawsze podłączeni, zawsze na bieżąco, bez względu na to, gdzie się znajdujemy.

Nowe technologie zawładnęły sercami i umysłami nie tylko dorosłych, ale też dzieci. Potwierdzają to badania. Z raportu NASK „Nastolatki" wynika, że młodzi spędzają w internecie średnio 4 godziny i 59 minut w dni powszednie oraz 5 godzin i 16 minut w weekendy (Ładna i in., 2025). Niestety cyfrowa nadaktywność wpływa negatywnie na nasze – oraz młodych – zdrowie i funkcjonowanie. Ból głowy, szyi, zmęczenie, problemy ze snem – to tylko niektóre fizyczne objawy nadużywania urządzeń. Brak kontroli nad czasem spędzanym online nie pozostaje też obojętny dla zdrowia psychicznego. Szczególnie młodzi mierzą się z takimi problemami, jak: stres cyfrowy, przeciążenie informacją, FOMO (ang. *Fear of Missing Out*), czyli lęk przed odłączeniem, PUI – problemowe używanie internetu, a nawet e-uzależnienia. Lista skutków zbytniego przywiązania do internetu i urządzeń jest długa.

Jak wyjść z błędnego koła nadużywania nowych technologii? Ważne jest zachowanie równowagi między światem online i offline, czyli zadbanie o cyfrową higienę.

Zacznijmy od wyjaśnienia, czym jest cyfrowa higiena. „(…) można patrzeć na nią w różnych kontekstach, uwzględniając czas ekranowy (ang. *screen time*) i/lub cyberbezpieczeństwo, i/lub wszelkie praktyki pozwalające zachować zdrową równowagę między aktywnościami online i offline" (Gańko, 2024).

Od czego więc zacząć dbanie o cyfrową higienę? Na początek sprawdźcie, czy rzeczywiście macie problem z nadużywaniem smartfona, komputera, serwisów społecznościowych czy gier. Określcie, co sprawia, że tak wiele czasu spędzacie z urządzeniem w ręce – być może w taki sposób radzicie sobie z nudą lub tylko w sieci potraficie dobrze się bawić. Powodów może być wiele. Po diagnozie możecie działać. Ale pamiętajcie – radykalne odłączenie od internetu rzadko kiedy przyniesie pożądany efekt. Jeśli na co dzień nie potraficie odłożyć smartfona nawet na chwilę, spędzacie godziny zanurzeni w grze, trudno Wam będzie z tego zrezygnować bez przygotowania. Najlepiej stosować metodę małych kroków, przyzwyczajając się stopniowo do bycia offline.

W budowaniu zdrowych nawyków cyfrowych próbujcie różnych rozwiązań: starannie planujcie czas poza siecią, postawcie na ciekawe aktywności, które wiążą się z odpoczynkiem od cyfrowego przemęczenia. Organizujcie rodzinne wyzwania – offline challenge, wyznaczajcie w domu strefy bez urządzeń, odkładajcie telefony przed snem i w czasie posiłku, nie sięgajcie po smartfona zaraz po przebudzeniu. W budowaniu zdrowych nawyków starajcie się działać zespołowo: z przyjaciółmi, rodzicami, rodzeństwem – w grupie raźniej! Nie zapominajcie też o modelowaniu zdrowych nawyków cyfrowych u swoich dzieci – już od najmłodszych lat. We wspólnym ustalaniu zasad korzystania z sieci pomoże Wam nasza bezpłatna aplikacja mOchrona.

Więcej informacji na temat cyfrowej higieny i praktyczne porady znajdziecie w naszych aktualnościach: „Zadbaj o siebie z OSE: problemowe używanie internetu", „Cyfrowa higiena i bezpieczeństwo w sieci z OSE", „5 pytań o… równowagę cyfrową" dostępnych na stronie ose.gov.pl. Skorzystajcie też z bezpłatnych materiałów zamieszczonych na platformie OSE IT Szkoła. Polecamy szczególnie: poradniki – „Mniej znaczy więcej – o multiscreeningu i wielozadaniowości", „Offline znaczy zdrowiej. O cyfrowej higienie dla rodziców i wychowawców", „FOMO i problemowe

używanie internetu”, zbiór felietonów „O cyfrowej higienie”, kurs e-learningowy „Zrozumieć FOMO” oraz scenariusze zajęć profilaktycznych. Scenariusze i kursy o tej tematyce znajdziecie także na naszej platformie Bezpieczni w sieci.

Źródła:

Gańko K., (2024), „Offline czyli zdrowiej. O cyfrowej higienie dla rodziców i wychowawców”, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy”, Warszawa: Państwowy Instytut Badawczy NASK.

Hotline

H

Na pewno każdy z Was potrzebował kiedyś uzyskać informację w sprawie danego produktu, usługi czy wydarzenia albo zgłosić jakiś incydent. W takich sytuacjach z pomocą przychodzi „gorąca linia”, czyli infolinia znana jako hotline.

Tak działa np. przynależny do Stowarzyszenia INHOPE (*The Association of Internet Hotline Providers*) Dyżurnet.pl. To zespół ekspertów NASK, który przyjmuje zgłoszenia nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Na każde zgłoszenie dotyczące twardej pornografii, rasizmu, ksenofobii lub innych nielegalnych treści, eksperci NASK reagują natychmiast. Współpracują z policją i krajowymi zespołami zrzeszonymi wokół INHOPE, aby skutecznie eliminować zagrożenia.

Specjaliści z Dyżurnet.pl podejmują również działania wobec innych szkodliwych treści, z którymi stykają się dzieci w internecie. W takich przypadkach najczęściej podejmują kontakt z administratorem serwisu społecznościowego i dostawcami usług internetowych, aby usunąć niebezpieczne treści lub ograniczyć do nich dostęp.

Każdy zgłoszony incydent jest analizowany przez zespół Dyżurnet.pl, który dba o to, by internet był bezpieczniejszym miejscem dla młodych użytkowników. Jak zgłosić szkodliwe i nielegalne treści? Można to zrobić za pomocą formularza na stronie dyzurnet.pl, pisząc na adres e-mailowy (dyzurnet@dyzurnet.pl), dzwoniąc na infolinię: 801 615 005 lub korzystając z usługi „Bezpiecznie w sieci” w aplikacji mObywatel.

W ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) również działa Centrum Kontaktu, które obsługuje szkoły podłączone do szybkiego i bezpiecznego internetu OSE. Nasi specjaliści odpowiadają na wszystkie pytania dyrektorów szkół i Technicznych Reprezentantów Szkół (TRS). Wystarczy zadzwonić na infolinię OSE: +48 22 182 55 55 czynną od poniedziałku do piątku w godzinach 7:30–16:00.

Zgłoszenia przyjmujemy także mailowo (wsparcietechniczne_ose@nask.pl) oraz przez portal Moje OSE i formularz dostępny na ose.gov.pl w zakładce Kontakt.

I

Incydent bezpieczeństwa

Fałszywe strony logowania do bankowości internetowej lub mediów społecznościowych, szkodliwe treści, ataki komputerowe czy podejrzane wiadomości SMS lub e-mail – te i inne niebezpieczne działania mogą doprowadzić do incydentu bezpieczeństwa komputerowego. To sytuacja, w której korzystając z internetu, możecie być narażeni na niebezpieczeństwo.

W sieci codziennie możemy stać się ofiarą różnych prób cyberataków, dlatego warto na bieżąco śledzić informacje na temat metod stosowanych przez oszustów (a tych ciągle przybywa!) oraz pamiętać o zgłaszaniu incydentów bezpieczeństwa. Jak to zrobić?

Z pomocą przychodzi CERT Polska, czyli zespół reagowania na incydenty. Aby zgłosić niebezpieczne zdarzenie, wypełnijcie formularz dostępny na stronie incydent.cert.pl lub wyślijcie e-mail na adres: cert@cert.pl.

W przypadku potencjalnie niebezpiecznej wiadomości SMS – możecie ją też przekazać do CERT Polska pod numer 8080. Co ważne, od 2024 r. za złośliwe uznawane są także wiadomości niezawierające linku, ale wpisujące się w znane schematy oszustw, co wynika z ustawowej definicji smishingu.

Zgłoszenia dotyczące nielegalnych treści w internecie (szczególnie materiały przedstawiające seksualne wykorzystywanie dziecka, twardą pornografię czy rasizm i ksenofobię) powinniście przesyłać do zespołu Dyżurnet.pl. W tym celu skorzystajcie z formularza na stronie dyzurnet.pl, wyślijcie e-mail na adres dyzurnet@dyzurnet.pl lub zadzwońcie na infolinię: 801 615 005.

W „Raporcie rocznym 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu" czytamy, że w porównaniu z 2023 r. liczba zgłoszeń incydentów bezpieczeństwa zwiększyła się o 62%, natomiast liczba zarejestrowanych incydentów – o 29%. Ten wzrost świadczy nie tylko o wzmożonej aktywności cyberprzestępców, ale również o większej świadomości internautów dotyczącej bezpieczeństwa w sieci. Ich reakcje przekładają się na budowanie większej odporności na zagrożenia płynące z cyfrowego świata.

Wszelkie incydenty bezpieczeństwa należy zgłaszać jak najszybciej! Dzięki temu inni użytkownicy internetu będą mogli uchronić się przed zagrożeniami czyhającymi w sieci.

Więcej o reagowaniu na zagrożenia w sieci przeczytacie w naszej aktualności na ose.gov.pl: „Europejski Miesiąc Cyberbezpieczeństwa z OSE: naucz się reagować na incydenty bezpieczeństwa".

Źródło:

CERT Polska, (2025), „Raport roczny 2024 z działalności CERT Polska", (2025), Warszawa: Państwowy Instytut Badawczy NASK.

Influencerzy

W internecie każdy z nas może być nie tylko odbiorcą, ale i twórcą treści. Bywa też, że działania podejmowane w mediach społecznościowych stają się sposobem na życie. Z pewnością zetknęliście się w sieci z filmikami, vlogami, transmisjami, w których występują influencerzy – osoby znane i popularne w social mediach, gromadzące wokół siebie wierną grupę odbiorców. Internetowe „gwiazdy" wykorzystują swoją pozycję i rozpoznawalność: zachęcają swoich obserwatorów do zakupów produktów czy usług, promują określone postawy, pokazują swoje sposoby na życie. Słowem: mają wpływ (od ang. *influence*) na ludzi, którzy śledzą ich poczynania online.

Influencerzy zajmują się różnymi tematami – m.in. prowadzą streamy z gier, pokazują haule zakupowe, recenzje różnych produktów, relacje z wyjazdów i życia codziennego, karuzele edukacyjne, tutoriale, prowadzą live'y z widzami. Wielokrotnie współpracują też z różnymi firmami i markami, które oczekują od nich promocji swoich artykułów czy usług.

Trzeba wiedzieć, że wpływ influencerów na odbiorców nie musi być dobry. Niezaprzeczalnie osoby popularne w sieci są społecznie odpowiedzialne, poruszają ważne tematy, np. zachęcają do głosowania, życia w stylu less waste czy promują zdrowe odżywianie. Istnieje jednak też druga, ciemniejsza strona medalu. Influencerzy nierzadko pokazują też piękne, pełne wrażeń, luksusowe życie – wykreowane na potrzeby publikacji w social mediach. W wielu odbiorcach, zwłaszcza tych młodszych, może to wywoływać frustrację, zaniżać samoocenę, zachęcać do nieustannych porównań. Bezrefleksyjne obserwowanie influencerów może też nakręcać spiralę konsumpcji, budzić nierealne pragnienia posiadania przedmiotów polecanych przez internetowych ulubieńców. Osoby, które zyskały popularność online, promując szkodliwy lub nierealny styl życia, można nazwać wręcz patoinfluencerami.

Jakie postawy i zachowania influencerów powinny Was skłonić do kliknięcia przycisku „Przestań obserwować" (Dębski, 2024)?

- Promowanie ryzykownych zachowań, takich jak nadmierne spożywanie alkoholu czy niebezpieczne wyzwania (challenge'e).
- Publikowanie kontrowersyjnych treści, które mają wywołać silne emocje.
- Ignorowanie konsekwencji swoich działań w przestrzeni publicznej.
- Wyrażanie dyskryminujących, obraźliwych opinii.
- Promowanie fałszywego obrazu życia.
- Nadmierne promowanie produktów i usług.
- Granie na emocjach odbiorców.
- Angażowanie się w publiczne spory i konflikty.
- Nadmierne dzielenie się w sieci szczegółami ze swojego prywatnego życia.
- Świadome ignorowanie norm i zasad społecznych.

Czy na tym kończą się negatywne wpływy internetowych celebrytów? Niestety nie. Okazuje się, że niektórzy z nich przemieniają się w domorosłych doradców finansowych i podpowiadają, jak zarządzać pieniędzmi. Tacy finfluencerzy (od ang. *finance* „finanse" i *influence* „wpływ") często nie mają doświadczenia w inwestowaniu i pomnażaniu gotówki!

To bardzo ważne – interesujcie się tym, kogo Wasze dzieci i uczniowie obserwują w sieci, a także sami zastanawiajcie się, jaki wpływ mają na Was osoby, które śledzicie w internecie. W większości przypadków tylko jedno kliknięcie odetnie Was od negatywnych bodźców!

Źródło:

Dębski M., (2024), „10 tricków patoinfluencera", grafika dostępna na stronie Fundacja Dbam o Mój Zasięg na Facebooku.

Infostealer

Jak już pewnie wiecie, nasze dane – różnego rodzaju – to łakomy kąsek dla cyberprzestępców. Dlatego stale wymyślają oni nowe sposoby, aby je pozyskać i wykorzystać, oczywiście działając na szkodę użytkowników sieci. W jaki sposób dokonują kradzieży cennych informacji? Oszuści stworzyli m.in. złośliwe oprogramowanie: infostealer. Jak sama nazwa wskazuje, info (informacje) stealer (złodziej) – to złodziej informacji.

Za pomocą tego oprogramowania przestępcy mogą pozyskać Wasze dane uwierzytelniające do bankowości elektronicznej, ale też innych serwisów, zapamiętane w menedżerze haseł i zapisane na dysku. Mogą również przejąć pliki cookies i sesje logowania. Wykradziony zestaw danych umożliwia oszustom dostęp do Waszych oszczędności, także do skrzynek e-mailowych

czy kont w mediach społecznościowych, które posłużą im do dalszej dystrybucji złośliwego oprogramowania. Ponadto niektóre typy infostealera potrafią przechwytywać ruch na klawiaturze, co również ułatwia przestępcom kradzież cennych danych.

W jaki sposób pobieramy infostealera? Jak zwykle naszym wrogiem jest działanie pochopne, bez namysłu i zachowania podstawowych zasad cyberbezpieczeństwa. Przestępcy, aby nas zwieść, wykorzystują znane metody rozpowszechniania złośliwego oprogramowania, np. poprzez malspam, czyli złośliwy spam. W tym przypadku wykorzystują phishing – aby wzbudzić zaufanie, podszywają się pod znane instytucje czy używają przejętych kont pocztowych. W specjalnie przygotowanych wiadomościach nierzadko kryje się niebezpieczny załącznik. Pobranie jego zawartości może się skończyć infekcją urządzenia. Na infostealery powinni też uważać amatorzy gier online. Niebezpieczne oprogramowanie kryje się np. w crackach do gier, które mają pomagać w łamaniu technicznych zabezpieczeń, a w efekcie umożliwiać korzystanie z gry bez licencji. Odwiedzanie stron z nielegalnym oprogramowaniem również może się skończyć pobraniem infostealera.

Aby zapobiec infekcji infostealerem, należy zachować ostrożność i rozwagę. Przede wszystkim dokładnie sprawdzajcie, kto jest nadawcą wiadomości. Jeśli jakiś e-mail wzbudza Wasze podejrzenia, nie klikajcie w linki, nie otwierajcie przesłanych załączników. Pobierajcie oprogramowanie tylko z legalnych źródeł. Korzystajcie z dobrych programów antywirusowych i pamiętajcie o regularnych aktualizacjach!

Natknęliście się na podejrzaną stronę? Koniecznie zgłoście incydent do CERT Polska – możecie to zrobić za pośrednictwem formularza internetowego na stronie incydent.cert.pl.

Internet

Rok 1991 zapisał się szczególnie w historii internetu w Polsce. To właśnie wtedy podłączono nasz kraj do sieci, a Państwowy Instytut Badawczy NASK miał w tym swój znaczący udział. Z możliwości internetu korzystamy dziś każdego dnia, ale czy wiemy, czym właściwie jest?

To ogólnoświatowa sieć komputerowa, która jest zbiorem wielu mniejszych sieci. W skład internetu wchodzą: serwery, routery, komputery użytkowników. Dzięki podłączeniu do sieci możecie – niezależnie od kraju i strefy czasowej – wymieniać się informacjami, komunikować, edukować na odległość czy korzystać z różnych e-usług. Wygodne, prawda?

Komputer podłączony do sieci to wspaniałe narzędzie, pod warunkiem, że korzystamy z niego mądrze i z zachowaniem podstawowych zasad bezpieczeństwa. Niestety, na użytkowników urządzeń cyfrowych czyha wiele niebezpieczeństw. Kampanie phishingowe, fałszywe sklepy, przestępstwa finansowe, malware (złośliwe oprogramowanie)... Co możecie zrobić, żeby ustrzec się przed tymi i innymi zagrożeniami?

Uniwersalna rada: jako użytkownicy internetu kierujcie się zasadą ograniczonego zaufania. Ignorujcie podejrzane wiadomości, uważajcie na osoby nowo poznane w sieci – szczególnie na te, które proszą o Wasze poufne dane lub pieniądze. Na co jeszcze warto zwrócić uwagę, by korzystanie z internetu nie stało się źródłem kłopotów?

- Dbajcie o regularne aktualizacje systemu operacyjnego swoich urządzeń i oprogramowania. Ponadto wszelkie aplikacje i oprogramowanie pobierajcie tylko z zaufanych źródeł – sklepów z apkami (Google Play czy App Store) lub ze stron producenta.
- Korzystajcie ze sprawdzonego programu antywirusowego – nie zapominajcie, że on też wymaga bieżącej aktualizacji!
- Ustawiajcie silne hasła – różne do wielu portali. Silne hasło składa się z min. 14 znaków. Szczegółowe wskazówki znajdziecie w poradniku CERT Polska „Kompleksowo o hasłach”.
- Postawcie na dodatkowe zabezpieczenie swoich kont – uwierzytelnianie dwuskładnikowe (wtedy podczas logowania oprócz hasła będziecie wpisywać drugi składnik, np. kod ze specjalnej aplikacji) lub na zabezpieczenia biometryczne (np. odcisk palca).

- Uważajcie na akcje phishingowe, czyli wszelkie próby wyłudzenia danych czy działania zmierzające do zainfekowania Waszego sprzętu szkodliwym oprogramowaniem.
- Regularnie róbcie backup Waszych dokumentów i danych, które będziecie mogli odzyskać w razie awarii sprzętu, wycieku danych czy cyberataku.
- Zadbajcie o swoją prywatność w sieci. Korzystajcie z ustawień prywatności, np. w mediach społecznościowych. Z rozwagą publikujcie online informacje o sobie. Nigdy nie wrzucajcie do internetu zdjęć dowodów tożsamości lub kart płatniczych (nawet ich fragmentów), także biletów lotniczych czy na koncert – one też zawierają istotne dane. Instalując aplikacje na smartfonie, zawsze czytajcie politykę prywatności, aby przypadkiem nie przekazać dostępu do zbyt wielu danych (np. listy kontaktów, zdjęć czy lokalizacji).
- Uważajcie na szkodliwe treści, w tym na dezinformację. Fałszywe wiadomości udostępniane online mogą skutkować chaosem informacyjnym i utrudniać proces dochodzenia do prawdy.
- Zgłaszajcie incydenty bezpieczeństwa. Jeśli przypadkiem zostaniecie przeniesieni na fałszywą stronę (np. banku), zgłoście to do CERT Polska. Wystarczy wypełnić formularz dostępny na stronie incydent.cert.pl lub napisać mailowo na adres cert@cert.pl. Możecie też przesłać wiadomość SMS na bezpłatny numer 8080, używając funkcji „przekaż" albo „udostępnij".
- Stale zdobywajcie wiedzę na temat cyberzagrożeń! Cyberprzestępcy wciąż wymyślają nowe metody ataków. Śledźcie na bieżąco informacje na stronach prowadzonych w ramach NASK: nask.pl, cert.pl, ose.gov.pl i itszkola.ose.gov.pl. Korzystajcie z naszych bezpłatnych materiałów dotyczących cyberbezpieczeństwa: poradników, raportów, broszur, kursów e-learningowych, które pomogą Wam lepiej zadbać o swoje bezpieczeństwo online.

Bądźcie bezpieczni w sieci!

Zobaczcie kurs e-learningowy „Techniki internetu" i dowiedzcie się więcej o internecie oraz możliwościach, jakie otwiera przed użytkownikami nowych technologii. Materiał znajdziecie na platformie OSE IT Szkoła.

Internet rzeczy (ang. *Internet of Things*, IoT)

Wiecie, że już dziś inteligentne domy umożliwiają zdalne sterowanie oświetleniem, ogrzewaniem, klimatyzacją i sprzętami takimi jak odkurzacze, pralki czy lodówki? Internet rzeczy (ang. *Internet of Things*, IoT) to sieć fizycznych urządzeń połączonych online, które gromadzą, przetwarzają i wymieniają dane. Mogą to być sprzęty domowe, pojazdy, maszyny przemysłowe, czujniki w rolnictwie czy urządzenia medyczne. Kluczowym elementem jest zdolność tych obiektów do komunikacji bez udziału człowieka. Dzięki temu systemy stają się coraz bardziej autonomiczne, a procesy – zautomatyzowane.

Zalety wykorzystania internetu rzeczy są niezaprzeczalne. W prywatnych domach technologia ta pozwala na oszczędność energii (np. poprzez inteligentne termostaty), zwiększa komfort (np. oświetlenie reagujące na ruch, lodówki samodzielnie zamawiające dostawę brakujących produktów) oraz poprawia bezpieczeństwo (np. kamery monitoringu dostępne z poziomu telefonu). W przemyśle IoT umożliwia monitorowanie stanu maszyn w czasie rzeczywistym, co pozwala zapobiegać awariom i optymalizować procesy produkcyjne. Z kolei w sektorze medycznym urządzenia IoT wspierają diagnostykę i opiekę nad pacjentami – od zdalnego monitorowania parametrów życiowych po przypomnienia o przyjmowaniu leków. W rolnictwie natomiast czujniki badają jakość gleby i warunki atmosferyczne, co przekłada się na wydajniejsze zarządzanie uprawami.

Musicie mieć świadomość, że każdy ze sprzętów internetu rzeczy, choć funkcjonalny, może być potencjalnym celem ataku. Z perspektywy cyberbezpieczeństwa IoT to jeden z ekosystemów najbardziej podatnych na incydenty. Wynika to z kilku powodów:

1. **Brak standardów bezpieczeństwa** – wielu producentów wypuszcza na rynek urządzenia z podstawowymi zabezpieczeniami (lub nie zabezpiecza ich wcale). Domyślne loginy i hasła (np. „admin" / „admin") wciąż są powszechne.
2. **Złożoność sieci** – im więcej sprzętów, tym więcej możliwości przeprowadzenia ataku. Cyberprzestępcy mogą wykorzystać jedno słabo zabezpieczone urządzenie jako „punkt wejścia" do całej sieci. Uwaga – najczęstszym punktem styku między światem zewnętrznym a domową siecią IoT jest router!
3. **Brak aktualizacji** – niektóre urządzenia nie mają wbudowanej funkcji automatycznej aktualizacji oprogramowania. To oznacza, że znane luki bezpieczeństwa mogą pozostawać niezałatane przez długi czas.
4. **Niska świadomość użytkowników** – wielu konsumentów nie zdaje sobie sprawy z zagrożeń, jakie niesie za sobą brak odpowiedniego zabezpieczenia inteligentnych sprzętów.

Czy trzeba bać się zagrożeń płynących z korzystania z urządzeń internetu rzeczy? Na pewno należy zrobić wszystko, by zadbać o swoje bezpieczeństwo. Oto kilka prostych, ale skutecznych zasad, których warto przestrzegać:

1. **Kupujcie świadomie** – wybierajcie sprzęt renomowanych producentów, sprawdzajcie ich reputację pod kątem bezpieczeństwa.
2. **Czytajcie instrukcje obsługi urządzeń**, zwłaszcza w zakresie bezpieczeństwa korzystania z danego sprzętu.
3. **Zmieniajcie domyślne dane logowania** – hasła, loginy administracyjne – i ustawiajcie własne zabezpieczenia, w tym uwierzytelnianie dwuskładnikowe lub wieloskładnikowe.
4. **Oddzielajcie sieć IoT od głównej sieci domowej** – zabezpieczajcie komputery, telefony i dane przed dostępem z zainfekowanego urządzenia.
5. **Regularnie aktualizujcie oprogramowanie**, co pozwoli szybko ujawnić ewentualne luki bezpieczeństwa i załatać je.
6. **Korzystajcie z monitoringu ruchu sieciowego**, czyli aplikacji i urządzeń wykrywających podejrzaną aktywność. Może to zapobiec poważnym problemom!

Wyzwaniem jest dbałość nie tylko o bezpieczeństwo technologiczne, ale też informacje na nasz temat, które gromadzą urządzenia IoT. Inteligentny odkurzacz może zbierać dane o układzie mieszkania, a inteligentny zamek do drzwi – o naszych zwyczajach. Dlatego warto dokładnie przeanalizować: jakie dane są gromadzone, gdzie i jak długo są przechowywane, komu mogą być udostępniane (np. partnerom biznesowym producenta) oraz czy można ograniczyć zakres zbieranych informacji. Zanim podłączycie kolejne urządzenie do domowej sieci, zadajcie sobie pytanie: czy zrobiłem/zrobiłam wszystko, by zabezpieczyć siebie i swoją rodzinę? W erze inteligentnych sprzętów mądrość i ostrożność użytkownika są bowiem równie ważne jak innowacyjność inżyniera.

Źródło:

„Bezpieczni w sieci z OSE: internet rzeczy (IoT)", (2025), artykuł na stronie ose.gov.pl.

IP

Adres IP (ang. *IP address*) to unikatowy numer identyfikacyjny nadawany urządzeniom podłączonym do sieci (np. komputerom, tabletom). Jego rolę można porównać do tej, którą pełni adres na kopercie lub paczce wysyłanej tradycyjną drogą pocztową – umożliwia identyfikację i lokalizację urządzeń oraz komunikację i wymianę danych.

W wersji czwartej adres IP składa się z czterech liczb dziesiętnych oddzielanych kropkami (np. 192.168.1.1). Dwie pierwsze oznaczają numer sieci, natomiast kolejne – numer komputera w tej sieci. Ponieważ w takiej postaci można zaadresować wyłącznie ok. czterech miliardów urządzeń, już w 1998 r. wprowadzono wersję szóstą protokołu IP (IPv6), gdzie adres jest znacznie dłuższy i ma aż osiem pól, z których każde zawiera cztery liczby szesnastkowe (od 0 do F). Ze względu na jego długość często jest zapisywany w postaci skróconej, z pominiętymi grupami zer.

Każdy Wasz sprzęt posiada unikalne IP, które może być przydzielone na stałe (adres statyczny) lub na określony czas (adres dynamiczny).

Więcej wiadomości na temat adresu IP znajdziecie na stronie ose.gov.pl w webinarze „Bezpieczni w sieci z OSE – Internet bez tajemnic".

J

Jailbreak

Czy „ucieczka z więzienia” może mieć coś wspólnego z cyberbezpieczeństwem, a dokładnie – bezpieczeństwem urządzenia mobilnego? Okazuje się, że więcej niż można by się spodziewać! Jailbreak (z ang. *jail* – więzienie i *break* – złamać, ale też przerwa, luka) to bowiem usuwanie narzuconych przez producenta ograniczeń na urządzenia z danym systemem operacyjnym. Brzmi skomplikowanie, prawda? Chodzi tu o ustawienie urządzenia w trybie, który pozwala na instalację rozszerzeń do oprogramowania, modyfikowanie poszczególnych funkcjonalności, elementów wyglądu, a także instalację nowych aplikacji niedostępnych dla danego systemu operacyjnego.

Niektórzy użytkownicy widzą zalety takiego działania. Trzeba jednak pamiętać, że każda ingerencja w system operacyjny wiąże się z wieloma zagrożeniami, przede wszystkim brakiem oficjalnych aktualizacji oprogramowania. Jailbreak wykorzystuje luki i może sprawić, że system Waszego urządzenia stanie się niestabilny, co zdecydowanie zwiększa ryzyko awarii i błędów w zakresie cyberbezpieczeństwa.

Jailbreaki wykorzystywane są obecnie także do… oszukiwania sztucznej inteligencji (ang. *artificial intelligence*, AI). W ostatnich latach w sieci pojawiły się gotowe instrukcje pozwalające obejść zabezpieczenia chatbotów AI. Ich twórcy wykorzystują fakt, że modele językowe dążą do realizacji celu użytkownika, nawet kosztem zasad bezpieczeństwa.

Zjawisko to zostało szczegółowo opisane przez naukowców z Uniwersytetu Ben Guriona w Beer Szewie. Pod kierunkiem prof. Liora Rokacha i dr. Michaela Fire’a opracowano tzw. uniwersalny jailbreak, który był w stanie przełamać zabezpieczenia wszystkich testowanych modeli AI. Po „odblokowaniu” chatboty udzielały odpowiedzi na pytania dotyczące włamań komputerowych, wytwarzania narkotyków czy prania pieniędzy.

W internecie pojawiły się nawet specjalne wersje dużych modeli językowych (ang. *Large Language Model*) określane mianem dark LLM – pozbawione etycznych filtrów, a niekiedy celowo przystosowane do działań przestępczych. Ich użytkownicy mogą w kilka minut wygenerować szczegółowe instrukcje dotyczące phishingu, podszywania się pod instytucje finansowe czy manipulacji opinią publiczną.

Źródło:

„Sekrety sztucznej inteligencji: chatboty na usługach cyberprzestępców”, (2025), artykuł na stronie ose.gov.pl.

Jamming

Czy zastanawialiście się kiedyś, na czym polega łączność bezprzewodowa? Telefony komórkowe, routery Wi-Fi, nadajniki GPS, ale też radia, piloty zdalnego sterowania czy kontrolery dronów wysyłają i odbierają sygnały radiowe na różnych częstotliwościach (aby sobie wzajemnie „nie przeszkadzać”). Istnieją rozwiązania, które umożliwiają zagłuszanie tych sygnałów, a więc blokują komunikację urządzeń między nadajnikami/odbiornikami. To jamming (z ang. zagłuszanie).

Atak polega na zakłóceniu lub uniemożliwieniu odbioru transmisji. Używa się go do zablokowania pracy urządzeń sterowanych falami radiowymi, jak również do zahamowania przepływu informacji przekazywanych z wykorzystaniem tych fal. Zagłuszający emituje sygnały radiowe na tej samej częstotliwości i przy użyciu tej samej modulacji, co fala pierwotna. Najczęstszymi „zakłócaczami” są szum, pulsowanie dźwięku, muzyka lub inny program radiowy.

Obecnie coraz częściej zdarza nam się słyszeć o GPS jamming, czyli celowym zakłócaniu sygnałów systemu nawigacji satelitarnej GPS poprzez emitowanie silnych fal radiowych na tych samych częstotliwościach, które wykorzystują satelity GPS. Okazuje się, że nawet stosunkowo

niewielkie urządzenie nadawcze może skutecznie przesłonić lub zniekształcić sygnał pochodzący z satelitów. Efektem są: utrata precyzyjnej pozycji, znaczące błędy nawigacyjne lub całkowity brak możliwości określenia położenia przez odbiornik. Zasięg zagłuszacza zależy od jego mocy, anteny, warunków propagacji i otoczenia. W praktyce zwykłe przenośne jammery wpływają na odbiorniki w promieniu od kilku do kilkudziesięciu metrów. Silniejsze instalacje mogą oddziaływać na większą odległość, zwłaszcza w terenie otwartym. Odbiorniki mobilne, samochodowe i telefony są szczególnie wrażliwe na zagłuszanie ze względu na słaby poziom sygnału satelitarnego. Warto wiedzieć, że zagłuszanie GPS to realne zagrożenie o licznych konsekwencjach – od lokalnych utrudnień po poważne skutki dla bezpieczeństwa publicznego i działalności gospodarczej.

Co ciekawe, historia jammingu sięga już lat 20. XX w., kiedy to w Berlinie zagłuszano transmisje radiofoniczne w Radiu Komintern. Do kolejnych takich prób dochodziło podczas II wojny światowej i zimnej wojny.

Źródło:

„Czym jest GPS Jamming?”, (2025), artykuł na stronie instytutcyber.pl.

JavaScript injection

J

JavaScript jest jedną z najpopularniejszych i najczęściej wykorzystywanych technologii tworzenia stron i aplikacji internetowych. Nadaje im interaktywności i umożliwia m.in. dynamiczne modyfikowanie zawartości czy tworzenie prostych funkcji, takich jak slidery, karuzele czy galerie zdjęć. Jak widać, JavaScript można wykorzystać do dobrych celów, jednak – niestety – także do szkodliwych działań. Jedynym z nich jest JavaScript injection. Jak działa?

To forma ataku na witrynę internetową, która polega na ulokowaniu (ang. *injection* – wstrzyknięciu) w jej treści kodu JavaScript uruchamianego po stronie użytkownika. Atakujący stronę oszust zyskuje dzięki temu wiele możliwości – jest w stanie modyfikować projekt witryny, uzyskiwać z niej informacje i manipulować parametrami (z wykorzystaniem plików cookie). Do opisu tej klasy ataków wykorzystuje się też termin cross-site scripting.

Efektem „wstrzyknięcia” kodu JavaScript może być np. wyciek poufnych informacji, istotna zmiana parametrów lub włamanie do kont użytkowników.

JOMO

Wielu z nas dotyka FOMO (ang. *Fear of Missing Out*), czyli wszechogarniający lęk przed odłączeniem, wypadnięciem z obiegu, strach przed tym, że coś może nas ominąć w sieci. Na drugim biegunie stoi JOMO (ang. *Joy of Missing Out*) – radość ze świadomego odłączenia się od internetu, ignorowania stale napływających komunikatów czy rezygnacji z ciągłego śledzenia znajomych online. JOMO pozwala cieszyć się z czasu spędzanego offline oraz nabrać dystansu do aktywności w sieci.

Jak jednak zmienić swoje cyfrowe nawyki i nauczyć się częściej odkładać smartfon na bok? Na początek przyda się na pewno metoda małych kroków. Znajdźcie ciekawą i atrakcyjną aktywność offline. Może to być nowe hobby lub coś, co już kiedyś sprawiało Wam przyjemność, np. jazda na rowerze, czytanie książek, puzzle czy podróże. Warto też nauczyć się spędzać przerwy (w pracy czy nauce) na aktywnościach innych niż przeglądanie stron internetowych oraz odciąć się od rozpraszaczy – wyłączyć dźwięki powiadomień, a nawet zainstalować specjalną aplikację, która poprzez małe nagrody zachęca do odkładania smartfona na bok.

Koniecznie spróbujcie też podjąć wyzwanie offline challenge – przeżyjcie świadomie 48 godzin bez internetu. Trudne? Pewnie tak, ale gwarantujemy, że te dwa dni bez dostępu do sieci nauczą Was o sobie czegoś nowego!

Dlaczego warto cieszyć się z odłączenia? Korzyści płynące z JOMO obejmują poprawę samopoczucia, poprawę koncentracji oraz lepsze wykorzystanie czasu. Osoby praktykujące JOMO rzadziej doświadczają chronicznego stresu wynikającego z porównywania życia z wykreowanymi obrazami

w mediach społecznościowych. Poza tym uwaga nie jest stale rozpraszana, co sprzyja efektywności w pracy i głębszym relacjom z bliskimi. JOMO może też przyczynić się do świadomego gospodarowania energią emocjonalną: zamiast rozpraszać się wieloma równoległymi aktywnościami, wybieramy te, które dają realną satysfakcję. Coraz częściej psychologowie i eksperci wskazują JOMO i monotasking (zajmowanie się jedną czynnością naraz) jako antidotum na stres cyfrowy i przeciążenie informacją. Umiejętność „bycia offline" staje się kompetencją XXI w. – potrzebną nie tylko dla zdrowia psychicznego, lecz także dla zachowania koncentracji, kreatywności i autentycznych relacji. JOMO przypomina, że prawdziwy luksus to czas, w którym można naprawdę odpocząć.

Chcecie dowiedzieć się więcej o FOMO, JOMO i offline challenge? Sięgnijcie do naszych poradników „FOMO i problemowe używanie internetu", „FOMO i nadużywanie nowych technologii", „Mniej znaczy więcej – o multiscreeningu i wielozadaniowości", „Offline znaczy zdrowiej" i e-kursów z serii „FOMOwscy i JOMOwscy" dostępnych na OSE IT Szkole oraz aktualności: „Majówka – cyfrowy detoks czy balans?", „Bezpieczni w sieci z OSE na wakacje: offline challenge" i „Zadbaj o siebie z OSE: zrób coś dobrego dla swojego mózgu" na stronie ose.gov.pl.

K

Keylogger

Znacie to uczucie, kiedy ktoś stoi za Waszymi plecami i podgląda, co robicie na komputerze? Szkodliwe oprogramowanie typu keylogger działa podobnie do podglądaczy – monitoruje Waszą aktywność na urządzeniu. Pojęcie to powstało z połączenia dwóch angielskich słów: key – klawisz oraz logger – rejestrator i oznacza oprogramowanie szpiegujące (spyware).

Jak dokładnie działa keylogger? Śledzi ruch ofiary na klawiaturze i przekazuje dane osobom trzecim. Choć to niejedyne zagrożenie – może też przechwytywać zrzuty ekranu, dźwięk z mikrofonu, a także rejestrować ruch kursora myszki. Tym sposobem w niepowołane ręce wpadają poufne informacje: dane logowania do bankowości elektronicznej, poczty e-mail czy serwisów społecznościowych. Warto mieć na uwadze, że keylogger może zainfekować nie tylko komputer, ale też smartfon z systemem Android czy iOS.

Do infekcji może dojść poprzez otwarcie pliku z malware (złośliwym oprogramowaniem) lub w wyniku działania przestępców, którzy wykorzystują wszelkie luki w zabezpieczeniach, by przeprowadzić atak. Spowolnione działanie sprzętu, zawieszanie się komputera czy pojawienie się na dysku folderu ze zrzutami ekranu, którego sami nie stworzyliście – te sygnały powinny Was zaniepokoić!

Aby uchronić się przed zainfekowaniem, pamiętajcie o podstawowych zasadach cyberbezpieczeństwa:

K

- Dbajcie o regularne aktualizacje – także przeglądarki internetowej i oprogramowania antywirusowego;
- Podczas logowania stosujcie uwierzytelnianie dwuskładnikowe lub wieloskładnikowe, czyli oprócz hasła logujcie się dodatkowymi składnikami, np. kodem otrzymanym SMS-em, odciskiem palca czy kluczem U2F;
- Uważajcie na phishing i wszelkie próby przekierowania Was na strony z niebezpiecznym oprogramowaniem;
- Weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości;
- Nie pobierajcie darmowych programów z nieautoryzowanych źródeł.

Klucz U2F

Większość z nas spędza w sieci dużo czasu i niestety nie zawsze pamiętamy o właściwej ochronie swoich danych dostępowych do różnego rodzaju kont: pocztowych, bankowości internetowej i innych. Często silne hasło może nie być wystarczające – potrzebne jest jeszcze logowanie dwuetapowe, czyli wprowadzenie drugiej warstwy uwierzytelniającej. Takim drugim składnikiem może być np. kod z SMS-a lub specjalnej aplikacji w telefonie, odcisk palca czy klucz U2F (ang. *Universal 2nd Factor*).

To niewielkie urządzenie – rozmiarem i wyglądem przypominające pendrive lub mały brelok – gwarantuje bezpieczeństwo podczas logowania do wspomnianych wyżej kont i innych usług online. Jego działanie jest bardzo proste: po wpisaniu loginu i hasła wystarczy zweryfikować stronę i potwierdzić logowanie za pomocą klucza, który należy umieścić w porcie USB lub przybliżyć do urządzenia (łącząc się poprzez NFC, ang. *Near Field Communication* – komunikacja bliskiego zasięgu). Mówiąc najprościej, klucz U2F potwierdzi Waszą tożsamość, a także sprawdzi, czy strona, na której się znajdujecie, jest tą, na którą chcecie się zalogować. Jeśli znajdziecie się na fałszywej stronie, natychmiast otrzymacie powiadomienie.

Fizyczny klucz sprzętowy, podobnie jak inne dodatkowe składniki uwierzytelniania dwuetapowego, spełnia bardzo ważną funkcję: uniemożliwia logowanie do serwisów i kont, nawet jeśli oszust

uzyska dostęp do Waszego loginu i hasła. Z klucza U2F możecie korzystać w wielu różnych serwisach, aplikacjach czy platformach. Ich jedyną wadą jest konieczność posiadania urządzenia w momencie logowania, tak więc, jeśli zdecydujecie się na takie zabezpieczenie swoich kont, powinniście nosić klucz U2F zawsze przy sobie.

Kompetencje cyfrowe

W obecnych czasach wiele mówi się o tym, że kompetencje cyfrowe (ang. *digital competences*) należą do jednych z najważniejszych umiejętności współczesnego człowieka. Czym dokładnie są?

Według Ministerstwa Cyfryzacji (2020) kompetencje cyfrowe to „harmonijna kompozycja wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym, tj. społeczeństwie wykorzystującym w życiu codziennym i pracy technologie cyfrowe".

Na kompetencje cyfrowe składają się:

- **kompetencje informatyczne** – m.in. umiejętność posługiwania się komputerem i innymi urządzeniami elektronicznymi, bezpieczne korzystanie z internetu, aplikacji i oprogramowania, znajomość nowych inteligentnych technologii cyfrowych;
- **kompetencje informacyjno-komunikacyjne** – umiejętność wyszukiwania, rozumienia, selekcji i krytycznej oceny informacji, umiejętność komunikowania się na odległość za pomocą technologii cyfrowych;
- **kompetencje funkcjonalne** – realne wykorzystanie wyżej wymienionych kompetencji w różnych sferach codziennego życia, takich jak finanse, praca i rozwój zawodowy, utrzymywanie relacji, zdrowie, hobby, itd., zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych (Ministerstwo Cyfryzacji, 2020).

Jak widać, kompetencje cyfrowe zakładają nie tylko naukę korzystania z urządzeń, ale też odpowiedzialne korzystanie z nowych technologii i bezpieczne poruszanie się w internecie. Dzięki rozwiniętym kompetencjom cyfrowym łatwiej nam funkcjonować we współczesnym świecie. Praca, nauka, utrzymywanie znajomości, sprawy urzędowe, zakupy, rozrywka – to tylko wybrane dziedziny, które w coraz szerszym zakresie przenoszą się do sieci.

Zwykliśmy (my, dorośli) mawiać, że najmłodsze pokolenia, jako że nie znają już życia bez internetu, poruszają się w sieci instynktownie i mają niejako wpojone kompetencje cyfrowe. Ale czy na pewno? Raport z najnowszej edycji badania „Nastolatki" prowadzonego przez NASK wskazuje niepokojące dane dotyczące (nie)bezpiecznego korzystania z internetu przez młodych. Trudno im ocenić, czy treści, jakie napotykają online, są bezpieczne i prawdziwe (Ładna i in., 2025).

Warto zwrócić uwagę także na inne badania, które dotyczą funkcjonowania nastolatków w sieci – ySKILLS (Pyżalski, Walter, Iwanicka, Bartkowiak, 2022). Znajdziemy tam m.in. dane na temat umiejętności cyfrowych polskich nastolatków w czterech wymiarach (umiejętności technologiczne i operacyjne, w zakresie poszukiwania informacji i nawigacji, komunikacji i interakcji, tworzenia oraz produkcji treści). Okazuje się, że umiejętności komunikacyjne i interakcyjne są u młodych respondentów na zdecydowanie wyższym poziomie niż umiejętności w zakresie tworzenia treści oraz wyszukiwania informacji. Jaki z tego wniosek? Nie możemy sądzić, że młodym internautom nie są potrzebne lekcje dotyczące mądrego korzystania z internetu i omawiające zagrożenia obecne w wirtualnej przestrzeni.

Chcecie sprawdzić, na jakim poziomie są Wasze kompetencje cyfrowe? Wypełnijcie test dostępny na stronie europa.eu/europass/pl. Wyniki mogą Was zaskoczyć!

Źródła:

„Kompetencje cyfrowe", (2020), artykuł na stronie gov.pl.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy", Warszawa: Państwowy Instytut Badawczy NASK.

Pyżalski J., Walter N., Iwanicka A., Bartkowiak K., (2023), „Wyniki badań ySKILLS. Druga fala (2022) Polska", KU Leuven, Leuven: ySKILLS.

Komunikacja bliskiego zasięgu (ang. *Near Field Communication*, NFC)

Zapewne nie raz widzieliście w sklepach osoby płacące telefonem lub zegarkiem (smartwatchem) i zastanawialiście się, jak to działa. A może sami też już korzystacie z tej funkcji? NFC (ang. *Near Field Communication*), bo to o nim mowa, to telefoniczny moduł służący do bezprzewodowej wymiany plików między urządzeniami. Najczęściej wykorzystywany jest do płatności zbliżeniowych, ale nie tylko – za pośrednictwem tej technologii można wymieniać też np. dane.

Jak to działa? NFC – podobnie jak Bluetooth – bazuje na komunikacji krótkiego zasięgu pomiędzy urządzeniami. Umożliwiają to wykorzystywane w tej technologii fale radiowe pozwalające na łączenie sprzętów w czasie poniżej jednej sekundy. Jednak w przeciwieństwie do Bluetooth NFC nie wymaga ręcznego parowania urządzeń, gdyż połączenie nawiązywane jest automatycznie – w chwili, gdy inny sprzęt znajdzie się w odpowiedniej odległości. Komunikować się ze sobą w ten sposób mogą nie tylko smartfony, ale też np. smartfony z terminalami płatniczymi.

Obecnie większość nowoczesnych telefonów (zarówno z systemem operacyjnym Android, jak i iOS), jest wyposażona w moduł NFC – wystarczy jedynie odpowiednio go skonfigurować i połączyć z aplikacją bankową. Oznacza to, że tylko kilka prostych kroków dzieli Was od bezpiecznych i wygodnych płatności mobilnych. Gdy będziecie chcieli zapłacić za zakupy, wystarczy, że zbliżycie smartfon do czytnika kart płatniczych. Nie musicie już zabierać z sobą na zakupy karty płatniczej ani gotówki!

K

Jeśli obawiacie się, że podczas takich transakcji zostaną wykradzione Wasze dane, uspokajamy – z dużym prawdopodobieństwem nic takiego się nie wydarzy. Takie ryzyko eliminuje naprawdę niewielki zasięg działania NFC: to tylko maksymalnie 20 cm. Dodatkowo parowanie wystąpi dopiero po odblokowaniu urządzenia, dlatego w zasadzie niemożliwe są nieautoryzowane połączenia NFC.

Zastosowania komunikacji bliskiego zasięgu nie kończą się tylko na płatnościach. Dzięki tej technologii możecie np. logować się do komputera poprzez stuknięcie telefonem lub odblokowywać w ten sam sposób drzwi samochodu.

Komunikatory internetowe

Zapewne korzystacie z nich bardzo chętnie! Nic dziwnego – narzędzia te łączą w sobie wiele niezbędnych funkcji. Dzięki nim możecie wysyłać wiadomości, prowadzić rozmowy – a nawet wideoczaty – przesyłać zdjęcia, filmiki, linki... A przede wszystkim być w stałym kontakcie z bliskimi i znajomymi.

Rosnąca popularność komunikatorów internetowych nie umknęła też uwadze cyberprzestępców. To właśnie tą drogą często rozsyłają niebezpieczne wiadomości. Mogą one trafić także do Was: z jednej strony od osoby nieznanej, co na pewno wzbudzi Wasze podejrzenia, a z drugiej – od potencjalnego znajomego. Dlaczego potencjalnego, skoro wyraźnie widać, że akurat pisze osoba, którą macie na liście kontaktów? Może się zdarzyć, że urządzenie znajomego zostało zainfekowane malware (złośliwym oprogramowaniem) lub przypadkiem podał on swoje dane logowania oszustom. Przejęcie kontroli nad cudzym kontem oznacza więc, że nadawca komunikatu wcale nie musi być tym, za kogo się podaje. Kliknięcie w przesłany przez oszusta link lub zalogowanie się w oknie fałszywej strony, może się dla Was źle skończyć – utratą poufnych danych lub pieniędzy.

O czym warto pamiętać, korzystając z komunikatorów internetowych? Przede wszystkim bądźcie ostrożni i z rezerwą podchodźcie do wiadomości otrzymanych tą drogą. Jeśli trafi do Was łańcuszek szczęścia, budzący wątpliwość link czy prośba o dopłatę do paczki lub przesłanie kodu BLIK – nie reagujcie na takie komunikaty! Uważajcie też na nieuczciwych kupujących, którzy przeszukują portale lub media społecznościowe z ogłoszeniami i kontaktują się z potencjalną ofiarą przez czat dostępny w serwisie lub na komunikatorze. Cel zazwyczaj jest jeden – przekierować na fałszywą

stronę, wyłudzić dane logowania do bankowości internetowej, a następnie dokonać kradzieży pieniędzy. Schematy działania przestępców znajdziecie na stronie CERT Polska.

Co zrobić, gdy dostaniecie podejrzaną wiadomość od potencjalnego znajomego? Najlepiej skonsultować się telefonicznie z nadawcą i wyjaśnić wszelkie wątpliwości. Jeśli jakaś wiadomość wzbudzi Wasze podejrzenia, prześlijcie ją do CERT Polska – eksperci sprawdzą np., czy nie zawiera szkodliwych linków. Wiadomość SMS możecie „przekazać" albo „udostępnić", wysyłając ją na numer 8080. Podejrzewacie, że zostaliście przekierowani na fałszywą stronę? Taki incydent również zgłoście do CERT Polska na stronie incydent.cert.pl.

Pamiętajcie, jeśli zależy Wam na prywatności i bezpieczeństwie informacji, wybierajcie takie komunikatory, które nie gromadzą danych o użytkownikach oraz wykorzystują szyfrowanie end-to-end (inaczej E2E).

Więcej informacji znajdziecie na ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: komunikatory internetowe".

Źródło:

„Oszustwa na portalach z ogłoszeniami", (2022), artykuł w serwisie cert.pl.

Kongres OSE

Kongres OSE to jedno z najważniejszych wydarzeń w kalendarzu Ogólnopolskiej Sieci Edukacyjnej (OSE), która działa w ramach Państwowego Instytutu Badawczego NASK. W konferencjach OSE (organizowanych od 2019 r., z przerwą w 2020 r. w związku z pandemią COVID-19 oraz lockdownem) uczestniczą przedstawiciele środowiska szkolnego – nauczyciele, dyrektorzy szkół, psycholodzy i pedagodzy szkolni, także pracownicy administracji szkolnej, przedstawiciele kuratoriów oświaty – oraz inne osoby zainteresowane tematyką bezpieczeństwa uczniów w sieci.

Na Kongresach OSE nie brakuje też wykładowców prestiżowych uczelni, cenionych ekspertów oraz praktyków, którzy podczas wystąpień i debat dzielą się wiedzą na temat zagadnień dotyczących aktualnych cyberzagrożeń, nowych zjawisk online oraz kształtowania pozytywnych nawyków korzystania z urządzeń cyfrowych. Jakie tematy poruszano dotąd na konferencjach OSE?

Pierwszy Kongres OSE 2019 „Świat możliwości" poświęcony był bezpieczeństwu w sieci oraz konieczności podnoszenia kompetencji cyfrowych uczniów i nauczycieli. Ponadto uczestnicy wydarzenia wzięli udział w warsztatach. Podczas praktycznych sesji poruszano tematy z obszaru: Ekosystemu OSE, cyfrowych możliwości w edukacji, zagrożeń w sieci oraz nauki myślenia programistycznego od najmłodszych lat.

Podczas Kongresu OSE 2021 dyrektorzy, nauczyciele oraz Techniczni Reprezentanci Szkół wysłuchali debaty i wystąpień dotyczących m.in. tego, jak pandemia wpłynęła na nasze bezpieczeństwo cyfrowe i obecność w sieci. Eksperci szukali odpowiedzi na pytania: Czego pandemia nauczyła nas o nowych technologiach w edukacji? Czy umiemy zadbać o bezpieczeństwo cyfrowe swoje i uczniów? Kim są nastolatki z pokolenia Z?

W 2022 r. głównym tematem wydarzenia OSE była szeroko pojęta edukacja medialna. Eksperci podjęli próbę odpowiedzi na następujące pytania: Czy nastolatki potrafią bronić się przed dezinformacją w sieci, fake newsami i teoriami spiskowymi? Jakie umiejętności cyfrowe ma polska młodzież? Jak media społecznościowe i kultura influencerów wpływają na młodych odbiorców? Czy urządzenia cyfrowe mogą służyć edukacji ekologicznej?

Z kolei podczas Kongresu OSE 2023 zaproszeni goście przybliżyli szereg niebezpieczeństw, z jakimi młodzi mogą spotkać się online. Kontakt ze szkodliwymi treściami, doświadczanie agresji i przemocy w sieci, glamouryzacja ryzykownych zachowań w internecie, e-uzależnienia, multiscreening i wielozadaniowość – to niektóre z nich. Podczas debaty omówiono też ważne dane pochodzące z raportu NASK „Nastolatki 3.0", wskazując, jak współczesna młodzież korzysta z internetu, co robi w sieci, z jakimi zagrożeniami się spotyka.

Kongres OSE 2024 dotyczył ochrony dzieci i młodzieży przed szkodliwymi treściami w sieci. Uczestnicy konferencji usłyszeli, z jakimi niebezpiecznymi materiałami stykają się dziś dzieci online, kim są patoinfluencerzy i dlaczego młodzi się na nich wzorują. Poznali też założenia ustawy o ochronie małoletnich przed treściami szkodliwymi w internecie, a także rozwiązania zagraniczne w tym zakresie.

Natomiast temat przewodni Kongresu OSE 2025 to „Szacunek i odporność społeczna – edukacja wobec hejtu, AI i wyzwań przyszłości". Dyskutowano o tym, w jaki sposób szkoła może reagować na nowe zjawiska, oraz jakie kompetencje są dziś kluczowe dla uczniów.

Kongresy OSE odbywają się hybrydowo – stacjonarnie i online. Dzięki czemu w ważnych i inspirujących prelekcjach oraz dyskusjach zaproszonych ekspertów do tej pory wzięło udział tysiące uczestników z całej Polski! Wystąpienia kongresowe dostępne są na profilach mediów społecznościowych programu OSE (na Facebooku i YouTubie), a także na stronie kongres.ose.gov.pl.

Kradzież danych

Z internetu i urządzeń cyfrowych korzystamy chętnie i często. W związku z tym cyberprzestępcy mają też więcej okazji do ataku i kradzieży naszych danych. Zależy im na różnych informacjach na nasz temat, a w szczególności na:

- danych osobowych – imionach, nazwiskach, numerach PESEL, adresach zamieszkania, numerach telefonów, danych logowania, danych lokalizacyjnych i innych informacjach, dzięki którym bez problemu można nas zweryfikować;
- danych finansowych – numerach kart kredytowych i numerach CVV, numerach kont, informacjach o pożyczkach czy ubezpieczeniach;
- danych uwierzytelniających – loginach i hasłach do bankowości elektronicznej, poczty e-mail, sklepów online, portali społecznościowych.

Ten katalog jest dużo szerszy – zawiera np. dane biometryczne czy tajemnice handlowe. Jeśli przestępcy wejdą w posiadanie tak ważnych informacji, możecie stracić nie tylko poczucie bezpieczeństwa, ale też swoje oszczędności. Wyciek danych wiąże się również z utratą zaufania do firm czy instytucji, które naraziły użytkowników na straty.

W jaki sposób poufne informacje mogą wpaść w niepowołane ręce? Cyberprzestępcy stosują różne metody, by je zdobyć. Rozsyłają e-maile i SMS-y (phishing), albo dzwonią, podszywając się pod znane instytucje: urzędy, banki, firmy kurierskie. Grożą np. utratą dostępu do internetowych usług, wymuszając na odbiorcy określone działanie – zazwyczaj nalegają na wpisane loginu i hasła w panelu logowania fałszywej strony. W ten sposób uzyskują np. dostęp do naszych kont w bankowości internetowej. Cyberprzestępcy często też wysyłają szkodliwe linki i załączniki, by infekować komputer ofiary malware (złośliwym oprogramowaniem), a następie przejąć kontrolę nad cyfrowymi zasobami.

Do kradzieży ważnych informacji może dojść zupełnie przypadkiem – w wyniku ludzkiego błędu, nieuwagi – lub przez celowe działania cyberprzestępców, np. rozbudowywanie szkodliwego oprogramowania typu ransomware o funkcje pozwalające na kradzież danych z zainfekowanych urządzeń.

Kradzież danych – mimo że wirtualna – może mieć bardzo realne skutki. Jak zatem chronić się przed utratą cennych informacji?

- Udostępniajcie w sieci jak najmniej informacji o sobie, np. podczas zakładania konta w sklepie internetowym czy w serwisie społecznościowym.
- Postawcie na silne hasła, składające się z min. z 14 znaków, najlepiej będących kilkuwyrazową frazą łatwą do zapamiętania dla Was i trudną do odgadnięcia dla oszustów. Nie korzystajcie z tego samego hasła w wielu serwisach! Ustawcie też

uwierzytelnianie dwuskładnikowe lub wieloskładnikowe. Niezbędne informacje znajdziecie w poradniku CERT Polska „Kompleksowo o hasłach".

- Korzystajcie z separacji tożsamości. Nie używajcie służbowego adresu e-mail do celów prywatnych, stwórzcie osobną skrzynkę pocztową do spraw urzędowych i zakupów online. Takie odrębne konta ograniczą szkody, które może wyrządzić potencjalny wyciek.
- Sprawdzajcie, czy Wasze dane nie wyciekły, logując się na stronie bezpiecznedane.gov.pl. Ponadto śledźcie komunikaty administratorów danych, którzy mają obowiązek informować klientów o wyciekach. Zaglądajcie też na Facebooka CERT Polska, gdzie znajdziecie aktualne informacje o cyberzagrożeniach.
- Zastrzeżcie swój numer PESEL – możecie to zrobić w aplikacji mObywatel. Dzięki temu w przypadku wycieku danych osobowych czy logowania do bankowości internetowej przestępcy nie zaciągną w Waszym imieniu zobowiązań finansowych.

Jeśli zauważyliście podejrzane domeny internetowe służące do wyłudzeń danych i środków finansowych, koniecznie zgłoście to do CERT Polska, wypełniając formularz na stronie incydent.cert.pl. A może przyszedł do Was dziwny SMS, np. informujący o konieczności dopłaty do paczki? Prześlijcie tę wiadomość na numer 8080, używając funkcji „przekaż" lub „udostępnij". Każde zgłoszenie może pomóc innym ustrzec się przed kradzieżą danych!

Chcecie wiedzieć, jak nie dać się oszukać? Przeczytajcie nasze aktualności na ose.gov.pl: „Bezpieczni w sieci z OSE: phishing", „Uwaga, złodziej!", „Bezpieczni w sieci z OSE: wyciek danych".

Kradzież tożsamości

K

Wyobraźcie sobie, że dostajecie wezwanie do zapłaty za niezamawiane usługi, towary lub, co gorsza, monit o zaległych ratach kredytu, o którym nie mieliście pojęcia. Może się tak stać, jeśli Wasze dane osobowe – PESEL lub seria i numer dowodu osobistego – wpadną w ręce cyberprzestępców.

Do kradzieży tożsamości dochodzi w momencie, gdy ktoś bezprawnie wejdzie w posiadanie naszych danych osobowych i wbrew naszej woli, ale działając rzekomo w naszym imieniu, wykorzysta je w nieuprawniony sposób – w celu popełnienia przestępstwa.

W jaki sposób złodziej zdobywa cenne informacje? Może zainfekować Wasz komputer malware (złośliwym oprogramowaniem) lub przesłać e-mail z próbą wyłudzenia poufnych informacji. Pamiętajcie, że oszuści niejednokrotnie też bacznie obserwują aktywność internautów w sieci. Źródłem cyberataku może być np. widoczny na opublikowanym przez Was zdjęciu dokument tożsamości czy fragment numeru karty kredytowej.

W dobie rozwoju sztucznej inteligencji OSINT (z ang. *open-source intelligence*), biały wywiad – czyli wyszukiwanie, gromadzenie i analizowanie informacji z różnych, ogólnodostępnych źródeł na temat firm, organizacji, osób – staje się o wiele mniej kosztowny dla oszustów, przez co bardziej powszechny. Warto więc szczególnie zadbać o swoją prywatność w sieci.

Oto podstawowe zasady ochrony danych w internecie:

- **Stosujcie silne hasła** – składające się z min. 14 znaków, różne do wielu portali. Wszędzie, gdzie to możliwe, ustawcie uwierzytelnianie dwuskładnikowe lub wieloskładnikowe.
- **Strzeżcie poufnych informacji** – nie udostępniajcie w sieci prywatnych danych typu numer telefonu, adres pobytu, e-mail.
- **Chrońcie się przed kradzieżą** – dbajcie o aktualizację oprogramowania, aplikacji, zainstalujcie program antywirusowy od renomowanego dostawcy. Pamiętajcie o wylogowaniu się z urządzenia, blokadzie telefonu, jeśli go nie używacie.
- **Uważajcie na phishing** – weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości.

- **Zapoznajcie się z polityką prywatności** – za każdym razem, gdy zaczynacie korzystać z nowego portalu lub aplikacji. Niektóre narzędzia wymagają dostępu do zbyt wielu danych, np. listy kontaktów.
- **Pomyślcie, zanim coś opublikujecie** – nie wszystkie informacje o Was powinny znaleźć się w sieci. Wiele udostępnionych danych wpłynie na Wasz cyfrowy ślad.

Jeśli padliście ofiarą kradzieży tożsamości, niezwłocznie powiadomcie o tym fakcie policję. Koniecznie poinformujcie też bank o podejrzanych transakcjach czy ewentualnych wnioskach kredytowych złożonych w Waszym imieniu. Ponadto szybko unieważnijcie swój dowód – kradzież tożsamości możecie zgłosić online lub w urzędzie – ściągawkę, jak to zrobić, znajdziecie w artykule „Zgłoś nieuprawnione wykorzystanie swoich danych osobowych (kradzież tożsamości) – unieważnij dowód" na stronie gov.pl.

Zawczasu zastrzeżcie też swój numer PESEL – można to zrobić w aplikacji mObywatel. W ten sposób w przypadku wycieku danych osobowych czy logowania do bankowości internetowej przestępcy nie zaciągną w Waszym imieniu zobowiązań finansowych.

Dowiedzcie się więcej o przeciwdziałaniu kradzieży tożsamości z biuletynu „OUCH! – Kradzież tożsamości – ochroń się przed nią".

Źródło:

„Na czym polega kradzież tożsamości?", (2024), artykuł na stronie wojtanis.com.pl.

K

Kradzież własności intelektualnej

W internecie można znaleźć praktycznie wszystko: zdjęcia, filmy, artykuły, opracowania naukowe, książki, pliki muzyczne, zdigitalizowane dzieła sztuki, programy komputerowe, aplikacje, gry… Możliwość korzystania z bogactwa różnych materiałów, sprawia, że często zapominamy o ważnym fakcie: zostały one przez kogoś wytworzone podczas kreatywnej, twórczej pracy, a więc stanowią czyjąś własność intelektualną. Ta natomiast podlega prawu autorskiemu. Oznacza to, że każdemu twórcy dzieła przysługuje prawo do wynagrodzenia i decydowania, w jaki sposób jego prace będą wykorzystywane.

Niestety, w sieci często dochodzi do naruszenia prawa autorskiego – najczęściej podczas plagiatu, kopiowania, pobierania z sieci utworów i rozpowszechniania ich bez wiedzy twórcy czy używania znaku towarowego bez zgody właściciela. Kradzież własności intelektualnej to bezprawne wykorzystanie zasobów, które są chronione prawem. Takie działanie jest nielegalne i podlega karze!

Nieznajomość prawa nie zwalnia od odpowiedzialności. Jeśli więc jesteście użytkownikami internetu, pamiętajcie o kwestiach związanych z ochroną własności intelektualnej.

- Udostępnianie lub rozpowszechnianie w sieci utworu bez zgody jego twórcy jest niezgodne z prawem. Na takie działania musicie uzyskać pozwolenie właściciela autorskich praw majątkowych. Jeśli już potrzebujecie jakichś materiałów z sieci, np. obrazków, wybierajcie te, które są udostępniane na licencji Creative Commons.
- Warto wiedzieć, że zamieszczanie linków prowadzących do innych treści online nie jest traktowane jako ich publiczne udostępnienie pod warunkiem, że po kliknięciu w link użytkownik zostanie przeniesiony na stronę, gdzie pierwotnie znajduje się treść, do której się odwołujecie.
- Ochronie prawnej podlegają także znaki towarowe, czyli np. logotypy. Prowadząc sklep internetowy, lepiej jest stosować wersję słowną marki produktu, bo na wykorzystanie znaku też musicie mieć zgodę! Pamiętajcie również o tworzeniu własnych opisów produktów i zdjęć. Korzystanie z materiałów producenta bez jego pozwolenia jest naruszeniem prawa własności intelektualnej.

- W mediach społecznościowych nie możecie korzystać z cudzych materiałów. Jeśli „szerujecie" post innej osoby lub firmy, musi być jasność, kto jest jego autorem. Z rozwagą dzielcie się cudzymi treściami! Odsyłanie do nielegalnie udostępnionych przez kogoś materiałów sprawia, że Wy też możecie działać niezgodnie z prawem autorskim.
- Planujecie założyć swoją stronę internetową? Pamiętajcie o kilku kwestiach. Jeśli zlecicie stworzenie strony projektantowi, zadbajcie w umowie o zapis przeniesienia na Was autorskich praw majątkowych do strony internetowej – do warstwy graficznej oraz kodu źródłowego. Nie zwlekajcie z rejestracją swojej domeny! Uważajcie na cybersquatting – ktoś wcześniej może wykupić domenę, która dla Was będzie ważna, i próbować Wam ją sprzedać za dużo większe pieniądze niż ją nabył.
- Sami jesteście twórcami? Zamieszczając swój utwór w sieci, określcie warunki jego wykorzystania. Jeśli nie pozwolicie na przetwarzanie czy dalsze przekazywanie Waszego dzieła, zgodzicie się tym samym na korzystanie z niego tylko na użytek prywatny. W praktyce oznacza to, że inni będą mogli się nim dzielić np. z członkami rodziny, ale bez czerpania żadnych zysków z tego tytułu.

Więcej o naruszeniu prawa autorskiego znajdziecie w bezpłatnych kursach dostępnych na platformie OSE IT Szkoła: „Własność intelektualna" oraz „Prawo autorskie – najważniejsze definicje".

Źródło:

„Jak chronić własność intelektualną firmy w internecie", (2021), artykuł w portalu Biznes.gov.pl.

Kryptowaluty

K

Zapewne nieraz słyszeliście o nowoczesnym systemie płatności, jakim są kryptowaluty. To wirtualne pieniądze, które istnieją tylko w postaci cyfrowej. Najbardziej znaną kryptowalutą jest bitcoin, ale istnieje wiele innych, takich jak ethereum, litecoin czy ripple.

Kryptowaluty działają na zasadzie rozproszonej sieci komputerów, które przechowują informacje o transakcjach w formie bloków połączonych w łańcuch (ang. *blockchain*). Każdy blok zawiera szczegóły dotyczące transakcji, a cała sieć jest zabezpieczona zaawansowanymi algorytmami kryptograficznymi. Dzięki temu transakcje są trudne do podrobienia, a jednocześnie anonimowe. Można powiedzieć, że blockchain to rozproszona księga, w której każda transakcja jest zapisywana w sposób transparentny i niemodyfikowalny, co utrudnia manipulacje danymi.

Aby kupić kryptowaluty, potrzebujecie portfela kryptowalutowego, który może być aplikacją, stroną internetową lub specjalnym urządzeniem. Portfel ten służy do przechowywania Waszych środków (zimny – niepodłączony do internetu, gorący – stale dostępny online). Kryptowaluty można kupić na giełdach, takich jak Binance, Coinbase czy Kraken, ale też w specjalnym kantorze, bitomacie lub od innej osoby. Przed zakupem warto zrozumieć ryzyko związane z inwestowaniem w kryptowaluty, ponieważ ich wartość może być bardzo zmienna. Należy przygotować się na duże wahania wartości i inwestować tylko te środki, które jesteście gotowi stracić.

Choć póki co nie zapłacicie kryptowalutami w osiedlowym sklepie, warto wiedzieć, że takie płatności przejmuje coraz więcej firm, można nimi zapłacić za produkty i usługi online, a nawet w niektórych sklepach stacjonarnych. Kryptowaluty są szczególnie popularne w branży technologicznej oraz wśród firm oferujących usługi cyfrowe.

Co wspólnego mają kryptowaluty i cyberbezpieczeństwo? Okazuje się, że całkiem sporo. Oto kilka informacji związanych z ochroną wirtualnych środków:

- Giełdy kryptowalutowe, gdzie użytkownicy przechowują swoje środki, są często celem przestępców. W przeszłości dochodziło do licznych włamań, w wyniku których użytkownicy tracili swoje kryptowaluty. Dlatego tak ważne jest przechowywanie środków w prywatnych portfelach, zwłaszcza sprzętowych, które trudniej zaatakować.

- Użytkownicy kryptowalut często stają się celem ataków phishingowych, gdzie przestępcy próbują wyłudzić dane logowania lub klucze prywatne, podszywając się pod zaufane instytucje lub osoby. Pierwszą linią obrony jest ostrożność i zasada ograniczonego zaufania.
- Anonimowość kryptowalut może być wykorzystywana przez cyberprzestępców do przeprowadzania nielegalnych działań, takich jak ataki z wykorzystaniem ransomware (oprogramowanie wymuszające okup). Przestępcy żądają zapłaty w kryptowalutach, aby utrudnić ich namierzenie.
- Niektóre kryptowaluty kładą szczególny nacisk na prywatność użytkowników, oferując anonimowe transakcje. Choć zwiększa to prywatność, może także utrudniać ściganie przestępstw, takich jak pranie pieniędzy czy handel nielegalnymi towarami.
- Wraz z rozwojem kryptowalut powstają także nowe technologie i narzędzia mające na celu zwiększenie bezpieczeństwa, takie jak bardziej zaawansowane algorytmy szyfrowania, lepsze protokoły bezpieczeństwa na giełdach czy narzędzia do monitorowania podejrzanych transakcji.

Źródła:

„Co to jest kryptowaluta?”, (b.r.), artykuł w serwisie coinbase.com.

„Co to jest kryptowaluta i jak funkcjonuje?”, (2021), artykuł w serwisie skrill.com.

„Jak i gdzie kupić bitcoin?”, (b.r.), artykuł w serwisie odkryjbitcoin.pl.

K

L

LAN (Local Area Network)

Być może nie zawsze zdajemy sobie z tego sprawę, ale LAN towarzyszy nam na co dzień. Wiecie, czym jest? To lokalna sieć komputerowa – rodzaj połączenia, które umożliwia współpracę komputerów i urządzeń peryferyjnych (np. drukarek czy tablic multimedialnych) na danym obszarze, np. w obrębie przedsiębiorstwa czy szkoły. Sieci o większym zasięgu noszą nazwę WAN (ang. *Wide Area Network*, rozległa sieć komputerowa).

Dobrym przykładem sieci LAN są chociażby sieci szkolne budowane w ramach Ogólnopolskiej Sieci Edukacyjnej. Taki typ połączenia stosują także bezprzewodowe drukarki, smartfony, laptopy czy inne urządzenia korzystające z jednej sieci. Można mówić o trzech typach sieci LAN: bezprzewodowej (WLAN), przewodowej i wirtualnej (VLAN). Najpopularniejszymi technologiami używanymi do budowy sieci LAN są Ethernet oraz Wi-Fi.

Szczegółowe informacje o typach sieci oraz sposobach dbania o ich bezpieczeństwo znajdziecie w webinarze „Bezpieczni w sieci z OSE – Internet bez tajemnic", w którym wzięli udział nasi eksperci techniczni. Zapraszamy do oglądania!

Lateral reading

Jak unikać dezinformacji? Którym wiadomościom znalezionym w sieci można ufać, a którym nie? Takie i podobne pytania zadają sobie wszyscy użytkownicy internetu. Żyjemy bowiem w rzeczywistości przepełnionej doniesieniami docierającymi do nas w każdej chwili, za pośrednictwem różnych mediów. Stykamy się niestety coraz częściej z fałszywymi, zmanipulowanymi treściami, które bardzo skutecznie udają te godne zaufania. Warto więc rozwijać umiejętność odróżniania prawdy od nieprawdy w sieci oraz weryfikowania źródeł. Z pomocą przychodzi lateral reading – jedna z metod świadomego korzystania z informacji.

L

Lateral reading – z ang. „czytanie boczne" lub „czytanie w poziomie" – pozwala sprawdzić, z jakim źródłem informacji mamy do czynienia. Korzystając z tej techniki, zwracamy uwagę nie tylko na to, co widać tylko na pierwszy rzut oka (tzw. czytanie w pionie), ale też na to, co można wyczytać niejako pomiędzy wierszami. Skupiamy się więc nie tylko na treściach newsów i ogólnie całej witryny, ale też wszelkich innych informacjach na temat tej strony.

Co daje nam taka wiedza? Możemy dzięki temu ocenić wiarygodność witryny i stwierdzić, czy jest wartościowym źródłem informacji. Nie zawsze łatwo jest znaleźć takie dane, ale musicie pamiętać, że w tym przypadku brak odpowiedzi również jest odpowiedzią!

Jeśli chcecie „czytać bocznie", zwracajcie uwagę na:

- **Tematykę strony.** Czy informacje na stronie nie są zmanipulowane? Czy nie wpisują się w teorie spiskowe? Czy artykuły na ten temat można znaleźć też w innych serwisach?
- **Informacje na temat właściciela strony** (np. w zakładce „O nas"). Kim jest? W jaki sposób finansuje swoją działalność?
- **Możliwość kontaktu z właścicielem strony.** Czy w zakładce „Kontakt" znajduje się formularz lub dane takie jak adres e-mail? Czy właściciel strony reaguje na próby kontaktu?
- **Bezpieczeństwo strony.** Czy strona korzysta z certyfikatu SSL?
- **Autora treści.** Czy można zidentyfikować autora danej informacji? Co wiadomo na temat tej osoby? Czy autor jest ekspertem w danej dziedzinie, czy wypowiadał się na ten temat już wcześniej? Czy publikował swoje teksty również w innych serwisach?
- **Źródła**. Do jakich źródeł odnosi się autor tekstu? Czy są to wiarygodne badania lub dane?

- **Zdjęcia i inne materiały dodatkowe**. Skąd pochodzą wykorzystane w artykule zdjęcia? Czy nie były używane wcześniej?
- **Język**. Czy artykuł jest napisany emocjonalnym językiem, ma clickbaitowy tytuł? Czy publikacja opisuje różne punkty widzenia, czy skupia się na jednym aspekcie zagadnienia?
- **Adres strony**. Czy w adresie nie występują literówki? Czy po wejściu na stronę nie wyświetla się informacja o potencjalnym zagrożeniu? Czy witryna nie znajduje się na liście ostrzeżeń przed niebezpiecznymi stronami prowadzonej przez CERT Polska?
- **Wygląd strony**. Czy na stronie pojawiają się nieuporządkowane elementy, zdjęcia niepasujące do treści? Czy strona jest estetyczna?

Jak widać, żeby dojść do prawdy, nierzadko trzeba przejść naprawdę długą drogę! Weryfikacja informacji – zwłaszcza tych, które budzą w nas duże emocje – powinna wejść nam w nawyk. W ten sposób będziemy w stanie ustrzec się przed dezinformacją i szkodliwym wpływem zmanipulowanych doniesień. Pamiętajcie, że nie potrzebujecie do tego drogich, skomplikowanych narzędzi – wystarczy umiejętność wyszukiwania obrazem i… bystre oko. Jeśli macie wątpliwości co do znalezionej informacji, skorzystajcie z serwisów fact-checkingowych, które pomogą Wam się upewnić, czy warto ufać temu „wyjątkowemu newsowi".

Więcej o dezinformacji, jej metodach i sposobach rozpoznawania fałszywych treści dowiecie się z bezpłatnego kursu dla nauczycieli „(Dez)informacja, czyli w co wierzyć w internecie" dostępnego na platformie e-learningowej OSE IT Szkoła. Zajrzyjcie też do aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: dezinformacja w mediach społecznościowych" i „Jak nie wpaść w pułapkę fake newsów?".

Źródło:

Tomaszewska I., (2023), „Czy strona jest wiarygodna – jak to sprawdzić samodzielnie?", artykuł w serwisie demagog.org.

Likejacking

W świecie mediów społecznościowych często wiele zależy od „polubień" (ang. *like*). Lubimy zdjęcia i posty naszych znajomych, zostawiamy „lajki" też na fanpage'ach celebrytów, instytucji i miejsc. Wydawałoby się, że to po prostu miły gest, oznaka sympatii albo wyraz uznania. Okazuje się, że nie zawsze…

Bywa, że „polubienia" wykorzystywane są przez cyberoszustów, którzy chcą zwiększyć oglądalność wybranych profili, aby otrzymywać korzyści z umieszczonych tam reklam. Próbują w tym celu zainteresować jak największą liczbę internautów szokującą wiadomością lub bardzo atrakcyjnym materiałem. Ci, którzy połkną haczyk, zostają przekierowani na stronę, gdzie rzekomo znajdą szczegółowe informacje. Zobaczą jednak nie zawartość, której się spodziewają, ale spreparowaną stronę z niewidoczną ramką, aktywującą się razem z kliknięciem. Efektem jest zmiana ustawień konta użytkownika.

Co się stanie, gdy nieopatrznie klikniecie w jakikolwiek przycisk lub obrazek na tej stronie? Wasz profil w mediach społecznościowych zostanie zainfekowany. Konto może stać się widoczne dla wszystkich (a więc dojdzie do zmiany ustawień prywatności), na tablicy pojawi się post o tym, że lubicie fałszywą stronę, a do Waszych znajomych trafi spam. Co więcej – pechowe kliknięcie może uruchomić instalację aplikacji, która będzie próbować wyłudzać pieniądze, dane osobowe i inne poufne informacje, pobierać szkodliwe oprogramowanie i wciąż rozprzestrzeniać się wśród osób z Waszej listy znajomych.

Co zrobić, by nie paść ofiarą tego oszustwa, zwanego likejackingiem? Przede wszystkim nie możecie bezrefleksyjnie klikać we wszystkie linki, nawet jeśli pozornie wydają się ciekawe albo polecą je Wam znajomi. Uważajcie też na wszystkie sensacyjne informacje, które widzicie w swoich mediach społecznościowych. Czujność przede wszystkim!

Link

W świecie internetu pewnie nikomu nie trzeba przedstawiać linków – odnośników, dzięki którym, po kliknięciu, w ułamku sekundy przenosimy się pod dany adres w sieci. Linki, czyli inaczej mówiąc: hiperłącza, wykorzystują protokoły http lub https (w zależności od tego, czy strony są szyfrowane). Te internetowe odsyłacze albo występują w postaci adresu strony, albo mogą być ukryte pod innym tekstem (ang. *anchor text*).

Korzystanie z linków znacząco przyspiesza wymianę informacji, ułatwia dostęp do treści online i umożliwia błyskawiczne przekazywanie danych. Jednak to, co stanowi o ich wygodzie, może być również źródłem zagrożeń. Nie wszystkie linki są bezpieczne – część z nich może prowadzić do stron wyłudzających dane (phishingowych), malware (złośliwego oprogramowania) czy fałszywych paneli logowania do banku, poczty lub mediów społecznościowych.

Cyberprzestępcy często wykorzystują zaufanie użytkowników, podszywając się pod znane firmy, instytucje publiczne czy sklepy internetowe. Niebezpieczny link może pojawić się w wiadomości e-mail, SMS-ie, komunikatorze, a nawet w mediach społecznościowych. Wystarczy jedno nieuważne kliknięcie, aby przekazać przestępcom swoje dane logowania, numery kart płatniczych lub umożliwić im przejęcie urządzenia.

Warto pamiętać o kilku zasadach bezpiecznego korzystania z linków:

- Zawsze sprawdzajcie adres URL – zwracajcie uwagę na literówki, nietypowe znaki lub dziwne domeny (np. zamiast „.pl" może pojawić się „.com" lub „.xyz").
- Nie klikajcie w linki z nieznanych źródeł, zwłaszcza jeśli wiadomość wymusza na Was natychmiastowe działanie („Twoja paczka została zatrzymana", „Twoje konto zostanie zablokowane").
- Używajcie podglądu linku – najeżdżajcie kursorem na odnośnik, aby zobaczyć, dokąd faktycznie prowadzi.
- Korzystajcie z aktualnego oprogramowania antywirusowego oraz rozszerzeń przeglądarki, które ostrzegają przed podejrzanymi stronami.

Jeśli link, który otrzymacie, prowadzi do lub strony, gdzie macie podać dane logowania – nie klikajcie, nie podawajcie haseł ani innych informacji. Lepiej samodzielnie wejść na stronę instytucji, wpisując jej adres w przeglądarce. Ostrożność to najskuteczniejsza forma obrony przed oszustwem!

Lista ostrzeżeń przed niebezpiecznymi stronami

Linki prowadzące do niebezpiecznych stron mogą do Was trafić różnymi kanałami: przez SMS, e-mail lub media społecznościowe. Akcje phishingowe, które mają skłonić ofiary do szybkiego i nieprzemyślanego działania, a w konsekwencji do wyłudzenia danych osobowych oraz uwierzytelniających do kont bankowych czy serwisów społecznościowych, to wciąż częste zagrożenie, z jakim możemy spotkać się w sieci. Dlatego CERT Polska od marca 2020 r. prowadzi listę ostrzeżeń przed niebezpiecznymi stronami. Eksperci 24 godziny na dobę, 7 dni w tygodniu, analizują zgłaszane podejrzane strony, a te szkodliwe zapisują na liście.

Korzystają z niej m.in. operatorzy telekomunikacyjni, firmy, organizacje i wszyscy administratorzy sieci, dla których ważne jest bezpieczeństwo ich użytkowników. Dzięki liście ostrzeżeń dostęp do złośliwych stron może być blokowany automatycznie, czyli podczas próby skorzystania ze szkodliwej witryny dostaniecie komunikat „Uwaga, ta strona stanowi zagrożenie". Tylko w 2022 r., dzięki liście ostrzeżeń, zablokowanych zostało blisko 21 milionów prób wejścia na strony, które łudząco przypominają popularne portale.

Niebezpieczne strony pojawiają się jak grzyby po deszczu. Często wykorzystywane są przez cyberprzestępców tylko przez chwilę, następnie są porzucane lub usuwane. W to miejsce tworzone są nowe niebezpieczne adresy.

Bądźcie więc czujni! Uważajcie na podejrzane panele logowania i potencjalnie fałszywe domeny – zwracajcie uwagę na szczegóły, takie jak: błędne adresy (regulamin-wirtualnapolska.com, 24platnosci.online) czy literówki w adresie (inP0ST.pl). Jeśli dostaniecie wiadomość, w której pod presją czasu macie podjąć jakieś działanie, np. kliknąć w załączony link, by dokonać szybkiej dopłaty za paczkę, nie reagujcie! To może być próba cyberataku.

Jakaś strona wzbudza Wasze podejrzenia? Koniecznie zgłoście incydent do CERT Polska za pośrednictwem formularza dostępnego na stronie incydent.cert.pl. Niepokojące SMS-y, zawierające potencjalnie groźne linki, przesyłajcie na numer 8080, korzystając z funkcji „przekaż" albo „udostępnij".

Login

Gdy zakładacie internetowe konta – np. w mediach społecznościowych czy sklepach internetowych – pierwszą informacją, jaką musicie podać, jest Wasz login. To swoisty identyfikator użytkownika sieci lub systemu komputerowego. Swoją nazwę możecie wymyślić sami (np. dodając cyfry czy znaki do Waszego imienia lub pseudonimu), często jest nią np. adres e-mail lub jego początkowa część.

Login będziecie wpisywać za każdym razem podczas logowania do danego systemu, razem z hasłem. Sam kształt loginu nie wpływa na nasze bezpieczeństwo w sieci, warto jednak pamiętać, by nie zapisywać nigdzie loginów ani nie przekazywać ich nikomu. Znając login, cyberoszuści mogą spróbować włamać się do naszych kont, korzystając z funkcji „nie pamiętam hasła".

Warto stosować kilka prostych zasad:

- Używajcie unikalnych loginów do najważniejszych usług – utrudni to przestępcom powiązanie kont w różnych serwisach.
- Nie udostępniajcie loginu innym osobom, nawet znajomym – w przypadku wycieku danych trudno potem ustalić, kto faktycznie z nich korzystał.
- Tam, gdzie to możliwe, korzystajcie z uwierzytelniania dwuskładnikowego, dzięki temu nawet w przypadku poznania loginu i hasła przez osobę niepowołaną, dostęp do konta pozostanie zablokowany.

A skoro jesteśmy już przy hasłach, warto przypomnieć sobie zasady tworzenia silnych zabezpieczeń. Sięgnijcie do aktualności „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe" na ose.gov.pl i rekomendacji CERT Polska w zakresie tworzenia haseł na stronie cert.pl.

Lootbox

Kto z nas nie męczył się długo z przejściem trudnego poziomu w grze i nie marzył o wsparciu wirtualnych mocy? Można próbować do skutku, można też skorzystać ze sprytnie podsuwanych ułatwień, np. dodatkowych skrzynek, zawierających losowo dobrane przedmioty czy inne pomoce ułatwiające rozgrywkę. To lootboxy (ang. *loot* – łup i *box* – skrzynka). Takie bonusy można kupić za monety zgromadzone w grze lub za realne pieniądze – za pomocą mikropłatności lub na specjalnych platformach dla graczy. Gracz nigdy nie wie, co znajdzie w środku, a oczekiwanie na losowy wynik wyzwala emocje podobne do tych, które towarzyszą grom hazardowym. Właśnie ta niepewność sprawia, że wielu użytkowników kupuje kolejne skrzynki, licząc na trafienie wyjątkowej nagrody.

Lootboxy sprawiają, że gra staje się bardziej angażująca, a co za tym idzie: uzależniająca. Okazuje się bowiem, że działają tu te same mechanizmy co w przypadku gier kasynowych. Choć mikropłatności wydają się pozornie niegroźne, niska z początku kwota zachęca do kupowania kolejnych skrzynek z bonusami. W efekcie może się nawet okazać, że za dodatkowe pomoce zapłacimy więcej niż za nową grę…

Aby uniknąć pułapki niekontrolowanych wydatków, warto zachować świadomość i umiar. Dobrym rozwiązaniem jest ustawienie limitu płatności w grach lub całkowite wyłączenie mikropłatności. Pamiętajcie: nawet jeśli wirtualna skrzynka może przynieść satysfakcję, prawdziwą nagrodą powinna być przyjemność z samej gry, a nie przypadkowy łup.

Więcej informacji o lootboxach oraz jasnych i ciemnych stronach gier komputerowych znajdziecie m.in. w poradniku dla rodziców „Nastolatki i gry cyfrowe", publikacji „O grach cyfrowych" oraz w aktualnościach „Grać czy nie grać? Oto jest pytanie" i „Gra pod choinkę? Poradnik świętego Mikołaja" dostępnych na platformie OSE IT Szkoła.

M

Malware (złośliwe oprogramowanie)

To hasło z pewnością nie powinno kojarzyć się Wam pozytywnie – malware to złośliwe oprogramowanie, mogące przysporzyć nie lada kłopotów. Termin pochodzi od angielskich słów malicious (złośliwy) oraz software (oprogramowanie) i oznacza programy komputerowe, których celem jest wykonywanie szkodliwych działań, np. przejęcie kontroli nad urządzeniem ofiary czy kradzież danych, haseł bądź plików. Kiedyś pod hasłem „malware" kryły się wirusy i trojany, dziś głównie ransomware (oprogramowanie szyfrujące dane i wyłudzające okup), spyware (oprogramowanie monitorujące naszą aktywność, np. to, co wpisujemy na klawiaturze – tzw. keylogger), wszelkiego rodzaju stealery (oprogramowanie, które wykrada dane z dysku) czy też adware (oprogramowanie zalewające użytkownika zainfekowanego systemu reklamami). Czasami złośliwe oprogramowanie działa w tle i dołącza zainfekowany system do tzw. botnetu – sieci urządzeń, z której przeprowadza się ataki typu DDoS, o czym prawowity właściciel często nie ma pojęcia.

Złośliwe oprogramowanie może zaatakować niemal każde Wasze urządzenie – smartfony, komputery, kamery, a nawet inteligentne urządzenia domowe, takie jak wideodomofony, sprzęt RTV – telewizory, a nawet AGD – lodówki, pralki. Niestety, im więcej sprzętów ofiary uda się cyberprzestępcom zainfekować, tym bardziej odczuje ona negatywne konsekwencje ich działania.

Aby chronić się przed malware, powinniście pamiętać o kilku ważnych zasadach:

- Zadbajcie o swój sprzęt – korzystajcie ze sprawdzonego programu antywirusowego oraz pamiętajcie o aktualizacjach używanego oprogramowania, systemu operacyjnego, przeglądarek internetowych i aplikacji.
- Nie instalujcie i nie pobierajcie programów niewiadomego pochodzenia, wybierajcie jedynie te ze sprawdzonych i znanych źródeł.
- Uważajcie na phishing. Weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości.
- Uważajcie na strony, które odwiedzacie. Korzystajcie z tych znanych i zaufanych. Zawsze weryfikujcie też, czy witryna, na której się znajdujecie, jest na pewno prawdziwa. Jeśli strona wydaje się Wam podejrzana lub ostrzega o niej Wasze oprogramowanie, skopiujcie jej adres i wyślijcie do zespołu CERT Polska – w ten sposób możecie ochronić siebie i innych.
- Stwórzcie kopie zapasowe plików, zdjęć i ważnych dokumentów. Jeśli zetkniecie się ze złośliwym oprogramowaniem lub Wasz sprzęt ulegnie zniszczeniu albo kradzieży – backup pomoże w odzyskaniu danych.

Więcej informacji na temat ochrony przed malware znajdziecie w aktualności na ose.gov.pl „Bezpieczni w sieci z OSE: malware" oraz w biuletynie „OUCH! – Ochrona przed złośliwym oprogramowaniem".

Man-in-the-middle (MITM)

Czy wiecie, że właśnie w tej chwili możecie być śledzeni i podglądani? Jest to możliwe za sprawą ataku sieciowego typu man-in-the-middle (MITM), który polega na przejęciu przez przestępcę danych przesyłanych pomiędzy dwiema stronami.

W tym wariancie cyberzagrożenia potrzebne są więc trzy ogniwa biorące udział w komunikacji: nadawca informacji (Wy), ich odbiorca (np. bank) i tytułowy man-in-the-middle, czyli człowiek pośrodku (cyberprzestępca). To właśnie on „podsłuchuje" oraz przechwytuje cenne informacje lub podszywa się pod jednego z rozmówców i tak manewruje komunikacją, by wejść w posiadanie poufnych danych.

Jak dokładnie działa man-in-the-middle? Manipuluje istniejącymi sieciami lub tworzy nowe złośliwe sieci, następnie przechwytuje ruch i zbiera informacje, które go interesują. Do ataku MITM może dojść na kilka sposobów:

- Wrogi punkt dostępowy – punkt dostępu (access point) ma zapewniać użytkownikom dostęp do sieci. Jednak przestępcy często instalują wrogi punkt dostępowy jako zaufaną sieć, by przekierować ofiarę do kontrolowanego przez nich miejsca, a następnie skłonić ją np. do pobrania szkodliwego oprogramowania.
- Fałszowanie DNS (czyli protokołu, który tłumaczy wpisywane w przeglądarce adresy na zrozumiałe dla komputerów dane liczbowe) – w ten sposób cyberprzestępca może zmienić adres strony.
- Fałszowanie ARP – atak polega na podszywaniu się pod inne urządzenie w sieci poprzez manipulację tablicą ARP (Address Resolution Protocol – to protokół używany w sieciach komputerowych do mapowania, czyli przyporządkowywania jednych zasobów danego systemu do drugich). Łączy się w ten sposób adres MAC atakującego (czyli unikalny identyfikator nadawany każdemu sprzętowi sieciowemu) z adresem IP ofiary. Przestępca może wykorzystać tę technikę, aby „podsłuchiwać" poufne informacje, np. pozyskać numery kart kredytowych.
- Atak typu sniffing – polega na monitorowaniu ruchu sieciowego i przechwytywaniu danych wysyłanych przez użytkownika. W ręce przestępcy mogą więc wpaść wiadomości mailowe, hasła czy ustawienia routera.

Jak widać, atak typu man-in-the-middle ma wiele odsłon. Jest trudny do wykrycia i oczywiście przynosi wiele szkód. Warto więc wzmocnić swoją czujność. Bacznie śledźcie adresy stron – pamiętajcie, że jedna zmieniona literka w nazwie świadczy już o próbie oszustwa. Nie ignorujcie też alertów informujących o błędnym certyfikacie. Ponadto zwracajcie uwagę na nagłe wyłączenia sieci – to też może być objaw ataku.

Warto wiedzieć, że przed atakami MITM chroni nas szyfrowanie i HTTPS, które są obecnie bardzo powszechnie stosowane. Eksperci twierdzą, że niedługo przeglądarki nie będą w ogóle pozwalać na odwiedzanie nieszyfrowanych stron.

Maskarada

Termin maskarada kojarzy się najczęściej z zabawą, której uczestnicy występują w przebraniach i maskach. Od dziś hasło to możecie też wiązać z jednej strony z cyberatakiem, podczas którego przestępcy podszywają się pod uprawnionego użytkownika albo urządzenie, wykorzystują pozyskane wcześniej identyfikatory – certyfikaty czy hasła – i uzyskują nieautoryzowany dostęp do sieci, systemu lub wrażliwych danych. Z drugiej strony termin maskarada łączony jest ze zjawiskiem cyberprzemocy.

Do maskarady, a ściślej mówiąc ataków maskujących czy ataków maskarady, dochodzi najczęściej podczas kampanii phinshingowych. Są one przygotowywane tak, by wszystko wyglądało wiarygodnie i nie wzbudzało żadnych podejrzeń. Przestępcy próbują podszywać się pod znane instytucje i firmy czy po prostu naszych znajomych, wysyłają specjalnie przygotowane wiadomości, by skłonić ofiarę do określonego działania: kliknięcia w link, podania swoich danych uwierzytelniających w fałszywym panelu logowania czy pobrania zainfekowanego załącznika. Postępowanie zgodnie z instrukcją oszustów zazwyczaj kończy się utratą pieniędzy lub wyłudzeniem cennych danych.

Warto wiedzieć, że odmianą phishingu jest spoofing, który polega na podszywaniu się pod konkretną osobę, podmiot (np. instytucję, firmę) lub serwer w celu pozyskania istotnych informacji czy wyłudzenia pieniędzy. Wyróżniamy np. spoofing telefoniczny – to rodzaj ataku, który skupia się na użytkowniku – oraz spoofing IP wymierzony w sieć, aby otrzymać do niej dostęp, i spoofing DNS, który umożliwia przekierowanie ruchu na inny adres IP, czyli prowadzi użytkownika na niebezpieczną stronę.

Eksperci zajmujący się badaniem zjawiska cyberprzemocy posługują się też terminem maskarady, opisując proceder polegający na zamieszczaniu materiałów kompromitujących osobę, pod którą podszywa się agresor. W tym przypadku maskarada polega na „tworzeniu fałszywego profilu w mediach społecznościowych lub uzyskaniu do niego dostępu bez świadomości ofiary. W ten sposób sprawca, podszywając się pod ofiarę, tworzy fałszywe wpisy lub zamieszcza kompromitujące zdjęcia, powodując szkody wizerunkowe ofiary oraz komplikacje w relacjach interpersonalnych" (Siemieniecka, Skibińska, Majewska, 2020).

Jak uchronić się przed maskaradą? Przede wszystkim nie dajcie się zwieść niebezpiecznym kampaniom phishingowym. Zachowajcie spokój i nie działajcie pochopnie, szczególnie jeśli ktoś nakłania Was do szybkich, nieprzemyślanych reakcji i straszy, że jeśli czegoś nie zrobicie, wydarzy się coś złego albo stracicie niepowtarzalną okazję. Pamiętajcie, że phishing to wciąż najpopularniejsza forma oszustwa. Z danych zamieszczonych w „Rocznym raporcie z działalności CERT Polska za 2024 r." wynika, że w 2024 r. zespół działający w NASK zarejestrował 97 995 oszustw komputerowych, z czego 40 120 incydentów dotyczyło phishingu (CERT Polska, 2025)! Dbajcie też o swoje bezpieczeństwo w internecie: z rozwagą dzielcie się informacjami o sobie w mediach społecznościowych, chrońcie swoją prywatność w sieci, stosujcie silne hasła, a najlepiej uwierzytelnianie dwuskładnikowe lub wieloskładnikowe.

Źródła:

CERT Polska, (2025), „Raport roczny 2024 z działalności CERT Polska", Warszawa: Państwowy Instytut Badawczy NASK.

Siemieniecka D., Skibińska M., Majewska K., (2020), „Cyberagresja – zjawisko, skutki, zapobieganie", Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

Media społecznościowe

M

Kto z Was nie korzysta z mediów społecznościowych? W końcu to właśnie one są dla wielu internautów główną aktywnością online. Dzięki nim nawiązujemy i podtrzymujemy relacje, docieramy do informacji, dzielimy się swoimi opiniami lub wydarzeniami z życia.

Media społecznościowe (ang. *social media*) to środki przekazu wykorzystujące technologie internetowe i mobilne, które pozwalają na komunikację na dowolną skalę. W odróżnieniu od tradycyjnych mediów (np. telewizji czy radia) social media nie tylko umożliwiają odbiór wiadomości, ale też dwukierunkową komunikację, np. w komentarzach. Dzięki nim nie musimy więc być już tylko biernymi odbiorcami, ale możemy też reagować na to, co publikują inni, oraz sami tworzyć przekazy.

Istnieje wiele rodzajów mediów społecznościowych i, jak łatwo się domyślić, ciągle ich przybywa. Pamiętajcie jednak, że choć bardzo przyjemnie spędza się z nimi czas, to ich nadmierne użytkowanie może wiązać się z zagrożeniami, takimi jak: FOMO i nadużywanie nowych technologii, dezinformacja, cyberprzemoc, przejęcie profilu czy kradzież tożsamości.

Co zrobić, by przyjemne chwile w sieci nie zamieniły się w przykre doświadczenie? Warto trzymać się kilku uniwersalnych zasad cyberbezpieczeństwa. Ich przestrzeganie to podstawa – niezależnie od tego, czy korzystacie z social mediów, czy logujecie się do banku lub skrzynki e-mailowej.

Po pierwsze używajcie silnych haseł, które zminimalizują ryzyko włamania. Wszędzie, gdzie się da, stosujcie też uwierzytelnianie dwuskładnikowe, czyli oprócz hasła logujcie się do witryny dodatkowym składnikiem, np. kodem otrzymanym SMS-em.

Po drugie zachowajcie ostrożność i krytyczny stosunek do treści publikowanych w sieci. Uważajcie szczególnie na akcje phishingowe, czyli wszelkie próby wyłudzenia Waszych danych czy działania zmierzające do zainfekowania Waszego sprzętu malware (złośliwym oprogramowaniem). Oszuści również w mediach społecznościowych podszywają się pod inne osoby lub firmy, wysyłają wiadomości i nakłaniają odbiorcę, by ten pod presją czasu np. kliknął w przesłany link. Postępowanie ofiary zgodnie z otrzymaną instrukcją zazwyczaj kończy się utratą pieniędzy

lub przejęciem konta w mediach społecznościowych, które posłuży do dalszych działań przestępczych.

I wreszcie po trzecie – pamiętajcie o regularnych aktualizacjach: oprogramowania, programów antywirusowych oraz aplikacji mediów społecznościowych (oczywiście pobranych tylko z oficjalnych sklepów). Błędy i luki w zabezpieczeniach oznaczają otwarcie drzwi cyberprzestępcom. Najnowsze wersje oprogramowania gwarantują natomiast większą odporność na ataki.

A teraz kilka rad dotyczących bezpiecznego korzystania z mediów społecznościowych:

- **Chrońcie swoją prywatność**. Stosujcie ustawienia prywatności i uważajcie na to, co udostępniacie w mediach społecznościowych, ile szczegółów ze swojego życia zdradzacie.
- **Sprawdzajcie (nie)znajomych**. Nie przyjmujcie zaproszeń od nieznanych osób. Jeśli ktoś dołączy do grona Waszych znajomych, będzie miał wgląd w publikowane przez Was treści. Ponadto pamiętajcie, że oszuści tworzą fikcyjne konta do przeprowadzania ataków. Jeśli zaakceptujecie przypadkowe zaproszenie, uwiarygodnicie fałszywy profil.
- **Dbajcie o swój wizerunek online**. Pomyślcie dwa razy, zanim opublikujecie jakiś materiał. Zastanówcie się, jak wpłynie on na Waszą reputację – teraz i za kilka lat. Reagujcie, gdy ktoś bez Waszej zgody udostępnił w internecie materiał z Waszym wizerunkiem.
- **Nie zdradzajcie swojej lokalizacji**. Nie oznaczajcie za każdym razem miejsc, w których przebywacie. Wyłączcie funkcję geolokalizacji w smartfonie. Wiadomości o Waszym wyjeździe czy aktualnych planach mogą wykorzystać przestępcy.
- **Nie wierzcie we wszystko**. Media społecznościowe to też źródło dezinformacji. Fałszywe newsy wyrabiają błędne przekonania, manipulują, sieją zamęt. Sprawdźcie wiarygodność informacji, zanim przekażecie ją dalej. Nie wdawajcie się w dyskusje, które promują nieprawdziwe, często szkodliwe tezy – Wasz komentarz niepotrzebnie wzmocni dany przekaz.

Jak bezpiecznie korzystać z mediów społecznościowych? Odpowiedzi znajdziecie w materiałach zamieszczonych na platformie OSE IT Szkoła, m.in. plakacie „Media społecznościowe a dobrostan psychiczny”. Przeczytajcie też aktualności dostępne na ose.gov.pl: „Bezpieczne media społecznościowe”, „Bezpieczni w sieci z OSE: trolling w mediach społecznościowych”, „Zadbaj o siebie z OSE: media społecznościowe” oraz ulotkę CERT Polska „Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych”.

Menedżery haseł

Bezpieczne i unikalne hasła są ważne – to już na pewno wiecie – ale co zrobić, by spamiętać je wszystkie? Hasło do poczty, mediów społecznościowych, bankowości internetowej czy gier online: sami przyznajcie, że jest tego wiele. Pomocą w zapamiętaniu Waszych szyfrów mogą być właśnie menedżery haseł.

Na jakiej zasadzie działają? Takie aplikacje mają za zadanie przechowywać hasła w szyfrowanej bazie, dzięki czemu są one bezpieczne, a Wy nie musicie pamiętać ich wszystkich – wystarczy znać tylko jedno hasło, które umożliwia logowanie się do menedżera. Programy tego typu oferują również pomoc w wygenerowaniu silnego hasła, a często umożliwiają też jego automatyczne wpisanie. Warto wiedzieć, że menedżery haseł mogą być wbudowane w przeglądarkę lub działać w chmurze.

Jeśli jednak zechcecie samodzielnie stworzyć hasło, pamiętajcie, że powinno się ono składać z min. 14 znaków. CERT Polska podpowiada, że podczas wymyślania zabezpieczenia warto wykorzystywać łatwe do zapamiętania, jednak sprytnie zmienione frazy, takie jak np. WlazłKotekNaMostekIStuka. Kolejnym dobrym pomysłem jest używanie słów w kilku językach, jak np. DwaBialeLatajaceSophisticatedKroliki. Unikajcie natomiast haseł pozornie silnych, takich jak Galwaniczny123$ czy admin.1. W przypadku wycieku danych przestępca łatwo stworzy listę

podobnych haseł, co zwiększy jego szasnę na skuteczny atak na usługi bądź serwisy, z których korzystacie.

Hasła bronią dostępu do wielu ważnych informacji, dlatego warto stosować najsilniejsze z możliwych sposoby zabezpieczeń, w tym również uwierzytelnianie dwuskładnikowe lub uwierzytelnianie wieloskładnikowe. Nie zapomnijcie też strzec swoich haseł jak oka w głowie: z nikim się nimi nie dzielcie – ani z najbliższymi, ani z osobami, które kontaktują się w imieniu zaufanych instytucji. Nikt, przedstawiciel banku czy firmy, nigdy nie powinien prosić Was o podanie danych uwierzytelniających (loginów i haseł)!

Więcej informacji znajdziecie w biuletynie „OUCH! – Menedżer haseł" dostępnym na stronie CERT Polska. Zapoznajcie się też z poradnikiem CERT Polska „Kompleksowo o hasłach" oraz aktualnością „Silne hasło to podstawa!" – znajdziecie ją na platformie OSE IT Szkoła.

Mikropłatności

Jako użytkownicy aplikacji mobilnych lub gier nie raz zetknęliście się z mikropłatnościami, czyli niewielkimi transakcjami, które w szybki sposób pozwalają opłacić nowe ułatwienie rozgrywki, wyłączyć reklamy lub dodać kolejną funkcjonalność do oprogramowania. Według Koalicji na Rzecz Obrotu Bezgotówkowego mikropłatności to transakcje do maksymalnie 20 zł. To nie majątek, czy jest więc się czym martwić?

Mikropłatności z założenia mają pozwolić nam dokonywać szybkich transakcji – obecnie zwłaszcza bezgotówkowych. Najczęściej korzystamy z nich za pośrednictwem Google Pay i Apple Pay, zdarza się też, że podajemy dane karty płatniczej, która jest automatycznie obciążana na daną kwotę. Inna opcja to transakcje za pomocą bramek płatniczych lub BLIK. Cały proces jest szybki i intuicyjny, a wszystko po to, byśmy już po kilku kliknięciach mogli cieszyć się zakupionym dodatkiem.

Warto zauważyć, że mikropłatności dotyczą głównie produktów cyfrowych: wspomnianych już dodatków w grach i nowych funkcjonalności aplikacji, ale też np. dostępu do muzyki czy innych treści w internecie. Dzięki tym szybkim transakcjom możemy wypożyczyć film spoza standardowej oferty ulubionej platformy streamingowej, kupić e-booka udostępnianego przez internetowego twórcę, wesprzeć zbiórkę charytatywną online czy kupić bilet na komunikację miejską w przeznaczonej do tego aplikacji. Mikropłatności mają obecnie wiele zastosowań i wszystko wskazuje na to, że na dobre zadomowiły się w naszej codzienności.

Jeśli dokonujecie niewielkich transakcji w aplikacjach i grach, zapewne nawet nie zauważacie zbytnich ubytków na koncie. To może być pułapka: drobne, ale częste mikropłatności w finalnym rozrachunku mogą złożyć się w całkiem pokaźną kwotę! Na co jeszcze warto uważać?

- Dokonując mikropłatności, upewniajcie się, czy transakcja jest jednorazowa (czyli czy określone sumy nie będą pobierane z Waszego konta cyklicznie, w ramach subskrypcji).
- Korzystajcie tylko z bezpiecznych metod płatności – wybierajcie te, w których nie musicie podawać wrażliwych danych. Nie klikajcie w linki przesyłane mailem lub SMS-em.
- Podczas zakupów upewniajcie się, że zapoznaliście się ze wszystkimi warunkami transakcji.
- Mikropłatności mogą prowadzić do uzależnienia i stanowić ryzyko dla graczy, którzy tracą kontrolę nad zakupami. Nabywane przez nich loot boxy i inne dodatki uatrakcyjniają rozgrywkę i sprawiają przyjemność, a że są dostępne na wyciągnięcie ręki, łatwo się w nich zatracić. Kontrolujcie zwłaszcza zakupy dokonywane przez młodych graczy!

mOchrona

Coraz młodsi użytkownicy korzystają z internetu, gdzie mogą być narażeni na wiele cyberzagrożeń, m.in. zetknięcie ze szkodliwymi treściami czy nadużywanie nowych technologii. mOchrona to bezpłatna aplikacja kontroli rodzicielskiej stworzona w ramach Ogólnopolskiej Sieci Edukacyjnej

(OSE). Pomaga rodzicom w zapewnianiu dzieciom bezpieczeństwa w sieci oraz diagnozowaniu potencjalnych problemów i zagrożeń, a co za tym idzie – szybszym reagowaniu na pojawiające się niebezpieczeństwa.

Aplikacja działa poprzez połączenie (sparowanie) urządzeń rodzica i dziecka, dzięki czemu ułatwia stałą opiekę nad najmłodszymi użytkownikami sieci. mOchrona wspiera ustalanie reguł dotyczących korzystania z urządzeń cyfrowych. Umożliwia wprowadzenie ustawień, które pomogą zminimalizować ryzyko kontaktu ze szkodliwymi treściami w internecie – rodzic może na sprzęcie dziecka m.in. blokować wybrane kategorie stron i aplikacji czy weryfikować czas, jaki spędza ono online. mOchrona umożliwia ponadto kontakt pomiędzy dzieckiem a rodzicem – na kilka sposobów. Zawiera funkcjonalność pozwalającą na wysyłanie próśb o dostęp do określonych treści (rodzic może je zaakceptować lub odrzucić), komunikator tekstowy oraz przycisk S.O.S. – dostępny na urządzeniu dziecka.

Apka jest łatwa w obsłudze i zapewnia rodzicom dostęp do stale aktualizowanych treści edukacyjnych, dotyczących zasad bezpiecznego korzystania przez dzieci z internetu. Można pobrać ją z oficjalnych sklepów z aplikacjami na urządzenia mobilne lub skorzystać z wersji przeglądarkowej dla systemu Windows.

Więcej informacji na temat aplikacji znajdziecie na stronie: ose.gov.pl/mochrona.

Mowa nienawiści

W dobie internetu słowa rozchodzą się szybciej niż kiedykolwiek wcześniej. Jeden komentarz, jeden post, jedno udostępnienie potrafią dotrzeć do tysięcy osób w kilka sekund. Niestety, równie szybko rozprzestrzenia się także zjawisko, które potrafi zostawić głębokie rany – mowa nienawiści (ang. *hate speech*).

To wszelkie wypowiedzi, które poniżają, obrażają lub wzywają do przemocy wobec innych osób lub grup – „z powodu ich przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu ich bezwyznaniowości" (art. 257 Kodeksu karnego). Warto mieć świadomość, że mowa nienawiści to nie tylko obelgi, ale też drwiny, stereotypy, wykluczające komentarze lub memy, które pozornie są żartem, a w rzeczywistości krzywdzą.

Wielu sprawców mowy nienawiści nie zdaje sobie sprawy, że ich słowa mogą wyrządzić realną szkodę. Psychologowie alarmują: hejt, wyśmiewanie i nienawistne komentarze prowadzą do poczucia zagrożenia, izolacji, depresji, a w skrajnych przypadkach – nawet do prób samobójczych. Warto pamiętać, że w sieci i nie tylko wolność słowa kończy się tam, gdzie zaczyna się krzywda drugiego człowieka. Kodeks karny (m.in. art.119, 256, 257) przewiduje kary za nawoływanie do przemocy, znieważanie czy publiczne poniżanie grup społecznych.

Czy możemy przeciwdziałać mowie nienawiści? Tak – możemy na nią reagować oraz uczyć tego swoje dzieci i uczniów. Oto podstawowe zasady:

- **Nie udostępniajcie** treści, które poniżają lub ośmieszają innych.
- **Zgłaszajcie** obraźliwe komentarze i profile w mediach społecznościowych.
- **Reagujcie**, gdy widzicie hejt – nawet jedno słowo wsparcia potrafi wiele zmienić.
- **Rozmawiajcie** z młodymi użytkownikami sieci o odpowiedzialności za słowa.

Każdy z nas tworzy przestrzeń, w której żyjemy – również tę cyfrową. Możemy używać słów jak tarczy albo pocisków: wybór należy do nas.

O mowie nienawiści przeczytacie więcej w zbiorze felietonów „O cyberprzemocy i hejcie w sieci" dostępnym na platformie OSE IT Szkoła.

Multitasking (wielozadaniowość)

Multitasking towarzyszy nam od zawsze. To nic innego jak wykonywanie kilku czynności jednocześnie. Pewnie nie raz w tym samym czasie oglądaliście telewizję, prasowaliście i rozmawialiście z bliskimi, czyli byliście wielozadaniowi. Rozwój technologii cyfrowych sprawił jednak, że dodatkowo staliśmy się wielozadaniowi medialnie, a przy okazji wpadliśmy w pułapkę multiscreeningu. Myślicie, że to Was nie dotyczy? Jeśli oglądacie film, a w tym samym czasie scrollujecie media społecznościowe, robicie zakupy online i odpisujecie na e-maile – to oznacza, że praktykujecie cyfrowy multitasking.

Multiscreening (*multi* – wielo-, *screen* – ekran) to rodzaj wielozadaniowości medialnej (ang. *media multitasking*). Czym dokładnie charakteryzują się te dwa zjawiska?

Wielozadaniowość medialna to jednoczesne:

- używanie dwóch lub więcej mediów elektronicznych (np. oglądanie telewizji i korzystanie z internetu w telefonie);
- wykonywanie wielu czynności na jednym urządzeniu (np. jednoczesne korzystanie z laptopa do oglądania filmów i robienia zakupów online czy korzystanie z komputera z otwartymi wieloma kartami przeglądarki);
- korzystanie z mediów podczas wykonywania niezwiązanych z nimi czynności (np. wysyłanie wiadomości tekstowych podczas nauki) (Borkowska, 2024).

Multiscreening z kolei definiuje się jako korzystanie z kombinacji wielu ekranów równocześnie do wykonywania zadań lub czynności powiązanych ze sobą bądź nie (Borkowska, 2024).

Wielozadaniowość medialna jest atrakcyjna pod wieloma względami – szczególnie dla młodych użytkowników sieci. Możliwość korzystania z wielu ekranów to źródło dodatkowej stymulacji, a im większa przyjemność, tym większy wyrzut dopaminy, czyli neuroprzekaźnika odpowiedzialnego za motywowanie nas do działania. Łatwo jednak wpaść w pułapkę pętli dopaminowej – z czasem układ nagrody będzie potrzebował zwiększonej liczby silnych bodźców, czyli w tym przypadku więcej treści płynących do nas z ekranów w tym samym czasie. Przebodźcowanie nadmiarem informacji wiąże się również z uwolnieniem hormonów stresu, a przewlekły stres powoduje wyczerpanie ciała i umysłu, w tym problemy ze snem.

Dlaczego jeszcze młodzi wpadają w pułapkę media multitaskingu? Przeglądanie internetu i odpowiadanie na wiadomości podczas przerwy reklamowej czy w oczekiwaniu na załadowanie gry to sposób na uniknięcie nudy. Ponadto multiscreening pozwala śledzić informacje w sieci i być na bieżąco. Multitasking daje też złudne uczucie produktywności. Wykonywanie wielu zadań w tym samym czasie wcale nie pomaga, wręcz przeciwnie – obniża koncentrację i negatywnie wpływa na pamięć roboczą, która jest odpowiedzialna za zapamiętywanie i przyswajanie informacji.

Świadomość zagrożeń związanych z multitaskingiem sprawiła, że powstał nowy trend – monotasking, czyli poświęcanie swojej uwagi tylko jednemu zadaniu. To trudne, ale osiągalne. Można spróbować w wyznaczonym wcześniej czasie być „tu i teraz", czyli skupiać się na danej czynności – bez rozpraszaczy, jakimi są urządzenia cyfrowe.

Źródło:

Borkowska A., (2024), „Mniej znaczy więcej – o multiscreeningu i wielozadaniowości", Warszawa: Państwowy Instytut Badawczy NASK.

N

Nadużywanie nowych technologii

Może dotknąć każdego – zarówno dorosłych, jak i dzieci – ale badacze wskazują, że nadużywanie nowych technologii najczęściej dotyczy nastolatków. Dane NASK z raportu „Nastolatki" pokazują, jak ważne miejsce w życiu młodych ludzi zajmują urządzenia cyfrowe i internet.

- Młodzież spędza w sieci 5 godzin dziennie bez jednej minuty w dni powszednie, a w weekendy 5 godzin i 16 minut.
- Niemal co trzeci nastolatek (31%) ma trudność z rozstaniem się ze swoim smartfonem, a 5 na 100 (5%) – ma z tym duży problem.
- Nastolatki posiadają średnio sześć kont w mediach społecznościowych i poświęcają na korzystanie z nich 3 godziny i 23 minuty każdego dnia.
- Około jedna trzecia (31%) uczniów i uczennic przyznała, że z powodu aktywności związanej z platformami społecznościowymi często zaniedbuje swoje zobowiązania szkolne. W odniesieniu do obowiązków domowych analogicznych odpowiedzi udzieliło 25% uczestników badania (Ładna i in., 2025).

Zbyt intensywne korzystanie z internetu i urządzeń cyfrowych może prowadzić do wielu problemów ze zdrowiem. Ból głowy, szyi, nadgarstków – to niektóre fizyczne objawy nadużywania nowych technologii. Utrata kontroli nad czasem spędzanym przed ekranem, wynikające z niej zmęczenie i problemy ze snem, wpływają też na zdrowie psychiczne. Zarówno młodzi, jak i starsi mierzą się ze stresem cyfrowym, przeciążeniem informacją, problemowym używaniem internetu (PUI) czy FOMO (ang. *Fear of Missing Out*), czyli lękiem przed odłączeniem.

Ponadto nadmierne zaangażowanie w świat online i coraz większa zależność od nowych technologii może powodować nadużywanie telefonu (fonoholizm), a także zwiększa ryzyko e-uzależnienia – od gier czy hazardu w internecie.

Wraz z rozwojem nowych technologii staliśmy się dodatkowo multiscreenersami: robimy zakupy online, jednocześnie oglądając serial, albo odpisujemy na maile i w tym samym czasie zerkamy na telefon… Multitasking wcale nie działa na nas dobrze – obniża naszą koncentrację i negatywnie wpływa na pamięć roboczą, która jest odpowiedzialna za zapamiętywanie i przyswajanie nowych informacji.

Zaniedbywanie przez dziecko nauki, przyjaciół spoza sieci, codziennych obowiązków, a także sięganie po urządzenie nawet w nocy, kosztem snu, smutek, rozdrażnienie, gdy w zasięgu ręki nie ma smartfona – te symptomy powinny Was zaniepokoić. Co robić, aby internet i smartfon nie stały się problemem? Warto postawić na edukację i kształtowanie zdrowych nawyków cyfrowych. Na początek zachęcamy do odkładania telefonu na czas posiłków, wyłączania powiadomień i nieużywania urządzenia godzinę przed snem. Sposobem na spędzenie czasu bez dostępu do sieci może być też offline challenge – wyzwanie polegające na odłączeniu się od internetu na 48 godzin.

Z pomocą rodzicom w dbaniu o higienę cyfrową przychodzi bezpłatna aplikacja Ogólnopolskiej Sieci Edukacyjnej mOchrona. Ułatwia ona opiekę nad młodszymi dziećmi, które już korzystają z internetu.

A co, gdy na profilaktykę jest już za późno? Jeśli używanie smartfona, komputera staje się dla dziecka przymusem, działajcie! Szczera rozmowa i wspólne ustalenie zasad korzystania z sieci to pierwszy krok do zmian. Pamiętajcie, że częstym powodem nadużywania internetu jest nuda, dlatego należy postawić na ciekawe i angażujące dziecko aktywności offline.

Więcej informacji i praktycznych porad znajdziecie w publikacjach dostępnych na OSE IT Szkole: „FOMO i nadużywanie nowych technologii. Poradnik dla rodziców" i „FOMO i problemowe używanie internetu. Poradnik dla nauczycieli" oraz kursie e-learningowym „Zrozumieć FOMO". Polecamy też nasze publikacje dotyczące higieny cyfrowej: poradnik „Offline znaczy zdrowiej. O cyfrowej higienie dla rodziców i wychowawców" i zbiór felietonów „O cyfrowej higienie". Sięgnijcie również po inne materiały opracowane w ramach kampanii edukacyjnej „FOMOwscy i JOMOwscy".

Naruszenia prawa autorskiego

Twórcy, a więc autorowi dzieła – czy to muzycznego, literackiego, plastycznego, naukowego czy fotograficznego – przysługuje prawo do wynagrodzenia i decydowania, w jaki sposób jego prace będą wykorzystywane. Niestety, w sieci bardzo często dochodzi do łamania praw autorskich. Dzieje się tak np. w przypadku, gdy ktoś pobiera z internetu utwory (najczęściej pliki muzyczne, filmy, aplikacje, zdjęcia, gry) i bez zgody je rozpowszechnia. Takie działanie jest karalne!

Pamiętajcie też, że udostępnianie treści z internetu bez podania ich autora, źródła czy odnośnika do oryginalnego dzieła (łącza) również wiąże się z naruszeniem prawa autorskiego. Podobnie jest ze zdjęciami – jeśli już potrzebujecie obrazków z sieci, koniecznie wybierajcie te, które są udostępnione na licencji Creative Commons (CC).

Z licencją Creative Commons wiąże się system oznaczeń, dzięki któremu wiemy, jak korzystać z różnych utworów zgodnie z zasadami prawa autorskiego:

- CC BY: można używać materiału pod warunkiem, że podamy autora (atrybucja);
- CC BY-SA: można korzystać z materiału, pod warunkiem atrybucji i udostępnienia na tej samej licencji;
- CC BY-NC: materiału można używać wyłącznie niekomercyjnie, przy zachowaniu atrybucji;
- CC BY-ND: można używać materiału bez modyfikacji, z atrybucją.

Czy wiecie, gdzie znajdują się otwarte zasoby, które można swobodnie wykorzystywać, np. do celów edukacyjnych lub komercyjnych? W poszukiwaniu darmowych zdjęć, dzieł literackich, plików wideo i audio oraz innych materiałów odwiedzajcie domeny publiczne – dostępne utwory można kopiować i dowolnie modyfikować. Otwarte zasoby tworzą treści publikowane na otwartych licencjach, np. dzieła dodane automatycznie – 70 lat po śmierci autora lub w sytuacji, gdy autor rezygnuje z ochrony swojego utworu i zezwala na jego dowolne wykorzystanie (takie treści oznaczone są symbolem CC0 – Creative Commons Zero).

Z kolei w otwartych zasobach edukacyjnych (OZE) znajdziecie bezpłatne materiały (często na licencjach CC), stworzone głównie z myślą o wykorzystaniu do celów edukacyjnych. OZE obejmują: podręczniki, poradniki, ćwiczenia, e-kursy, filmy, wykłady, testy, programy nauczania i inne materiały. Mogą z nich korzystać (także je modyfikować i udostępniać) nauczyciele, uczniowie i inne osoby zainteresowane edukacją. Przykładami otwartych zasobów edukacyjnych są takie platformy, jak: Khan Academy, Polska Biblioteka Internetowa, Polska Platforma Otwartych Zasobów Edukacyjnych czy Wikimedia Commons, a także np. treści na bezpłatnych platformach e-learningowych: OSE IT Szkoła czy Bezpieczni w sieci.

W sieci mamy wręcz nieograniczony dostęp do różnych utworów, co nie znaczy, że możemy je kopiować i korzystać z nich bez żadnych ograniczeń. Pamiętajcie, że w przypadku wytworów sztucznej inteligencji (ang. *artificial intelligence*, AI) również mają zastosowanie ogólne zasady dotyczące ochrony praw autorskich i własności intelektualnej. To oznacza, że kopiowanie i wklejanie przez kogoś treści generowanych przez sztuczną inteligencję bez podania źródła może skutkować naruszeniem praw autorskich, o ile dana treść jest oryginalna i podlega ochronie.

W przypadku publikacji treści audio, wideo lub obrazów wygenerowanych przy użyciu AI, przypominających istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe (deepfake), należy wskazać, że zostały one sztucznie wygenerowane lub zmanipulowane (przerobione).

Nieznajomość prawa nie zwalnia z obowiązku jego przestrzegania! Konsekwencje naruszenia prawa autorskiego mogą być bardzo dotkliwe. Za złamanie przepisów grożą kary finansowe, odpowiedzialność cywilna, a nawet karna (głównie za nielegalną dystrybucję na dużą skalę).

Więcej o zasadach prawa autorskiego w Polsce przeczytacie w ustawie o prawie autorskim i prawach pokrewnych z dn. 4 lutego 1994 r., a także w przepisach unijnych, np. dyrektywie Parlamentu 2019/790 w sprawie prawa autorskiego na jednolitym rynku cyfrowym, która wprowadza m.in. przepisy dotyczące dozwolonego użytku edukacyjnego i licencji na treści cyfrowe. Obowiązki dotyczące oznaczania deepfake'ów określa rozporządzenie 2024/1689 (tzw. akt w sprawie sztucznej inteligencji).

Materiały dotyczące naruszeń prawa autorskiego znajdziecie również na naszej platformie e-learningowej OSE IT Szkoła. Zachęcamy do skorzystania z kursów: „Własność intelektualna" oraz „Prawo autorskie – najważniejsze definicje", które w przystępny sposób przybliżają wiedzę na temat prawa autorskiego.

Źródła:

„Jak zgodnie z prawem korzystać z materiałów dostępnych w internecie?", (2024), artykuł na stronie kompetencjecyfrowe.gov.pl.

Zradzińska A., (2024), „AI, boty, awatary i szkodliwe treści", wideo na platformie YouTube.

Naruszenia prywatności

Każdy z nas ma prawo do prywatności – również w internecie – a szczególnie do ochrony danych osobowych, takich jak: imię i nazwisko, data urodzenia, adres e-mail, numer PESEL, czy wrażliwych, osobistych informacji, np. wyników badań.

Naruszenie prywatności odnosi się do nieuprawnionego dostępu, zbierania, używania lub ujawniania informacji osobistych bez posiadania właściwej podstawy prawnej dla przetwarzania danych osoby, której dane dotyczą (Dzieciuchowicz, 2024). To też sytuacje, w których ktoś wykorzystuje cudzy wizerunek lub dane osobowe w celu wyrządzenia krzywdy osobistej bądź majątkowej. Przykładem takiego działania jest kradzież tożsamości, czyli np. przejęcie konta społecznościowego i podszywanie się pod jego właściciela. Uwaga: to przestępstwo!

Naruszenia prywatności w przestrzeni cyfrowej mogą przybierać również inne formy, takie jak:

- **Nieautoryzowany dostęp do danych** – obejmuje przypadki kradzieży lub nielegalnego pozyskania poufnych informacji, np. numerów kart płatniczych czy dotyczących szczegółów kont bankowych.
- **Inwigilacja** – śledzenie działań danej osoby, np. za pomocą oprogramowania szpiegującego.
- **Złamanie tajemnicy korespondencji** – obejmuje nieuprawnione otwieranie, czytanie lub przekazywanie prywatnych wiadomości e-mail bez zgody ich adresata.
- **Cyberstalking** – uporczywe nękanie ofiary poprzez przesyłanie niechcianych materiałów i informacji, cyberataki czy inne działania zakłócające poczucie bezpieczeństwa użytkownika. Może skutkować karą pozbawienia wolności (Dzieciuchowicz, 2024).

Niestety, sieć nie sprzyja ochronie prywatności, szczególnie że sami często udostępniamy online więcej informacji o sobie, niż jest to konieczne. Nasze dane to też częsty cel cyberataków. Przestępcy wykorzystują malware (złośliwe oprogramowanie), by zainfekować cudzy sprzęt i wykraść cenne informacje. Ponadto stosują phishing, wyłudzając w ten sposób wartościowe dane (hasła logowania do serwisów społecznościowych czy bankowości elektronicznej).

Jak uchronić się przed naruszeniem prywatności? Przede wszystkim sami chrońcie swoją prywatność w sieci! Jeśli rejestrujecie się na nowej platformie lub w aplikacji, czytajcie politykę prywatności. Być może korzystanie z tych narzędzi będzie wymagać od Was zgody na udostępnie-

nie zbyt wielu danych. Ponadto nie klikajcie w podejrzane linki, stosujcie silne i bezpieczne hasła, zmieńcie opcje prywatności w ustawieniach przeglądarki lub włączcie tryb incognito. Ograniczajcie też cyfrowy ślad. Pamiętacie, że cyberprzestępcy zdobywają wiedzę o Was, przeszukując różne platformy i serwisy – publikujcie więc w sieci jak najmniej informacji o sobie!

O naruszeniach prywatności przeczytacie na ose.gov.pl w aktualnościach: „Bezpieczni w sieci z OSE: ochrona danych osobowych" oraz „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci". Sięgnijcie też po materiały dostępne na platformie OSE IT Szkoła: np. e-kurs dla dzieci „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu". Pierwszy moduł „Pokaż siebie!" podejmuje właśnie temat ochrony prywatności online. Kursy z zakresu prywatności online (dla nauczycieli i uczniów klas 7–8 szkół podstawowych oraz ponadpodstawowych) znajdziecie też na platformie bezpieczniwsieci.edu.pl.

Źródło:

Dzieciuchowicz N., (2024), „Naruszenie prywatności – co oznacza, jakie może mieć skutki i kto ponosi odpowiedzialność", artykuł na stronie lexdigital.pl.

NASK

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) działa od 1991 r., a naszą misją jest cyfryzacja kraju oraz zapewnienie bezpieczeństwa w cyberprzestrzeni. Instytut prowadzi działalność:

- naukową – specjalizujemy się w cyberbezpieczeństwie, sztucznej inteligencji oraz obliczeniach chmurowych;
- badawczą – analizujemy m.in., jak zmienia się społeczeństwo pod wpływem nowych technologii, a wyniki naszych prac udostępniamy np. w formie raportów (Thinkstat NASK);
- edukacyjną – realizujemy projekty edukacyjne (platforma e-learningowa OSE IT Szkoła oraz bezpieczniwsieci.edu.pl, projekty: Cyberprofilaktyka NASK, Safer Internet, ESA – Edukacyjna Sieć Antysmogowa), przekazując dzieciom i młodzieży wiedzę na temat zagrożeń w internecie. Promujemy też koncepcję społeczeństwa informacyjnego otwartego na nowe technologie.

Ponadto, zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa, NASK pełni obowiązki jednego z Zespołów Reagowania na Incydenty Komputerowe – CSIRT (incydenty bezpieczeństwa i potencjalnie nielegalne treści można zgłaszać do CERT Polska i zespołu Dyżurnet.pl).

Wspieramy też instytucje publiczne, realizując strategiczne projekty. W ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) zapewniamy szkołom dostęp do bezpiecznego internetu; dla administracji państwowej tworzymy EZD RP – System Elektronicznego Zarządzania Dokumentami oraz rozwijamy polski model językowy PLLuM; prowadzimy również Rejestr Domeny .pl.

Warto pamiętać, że to NASK w 1991 r. podłączył Polskę do internetu. Od tego czasu współtworzymy nowoczesną cyberprzestrzeń i dbamy o bezpieczeństwo wszystkich użytkowników sieci: dzięki własnym produktom chronimy firmy przed cyberzagrożeniami, walczymy z dezinformacją, usuwamy strony z nielegalnymi treściami i ostrzegamy przed oszustwami internetowymi.

Dowiedzcie się więcej o NASK-PIB – wejdźcie na stronę nask.pl.

„Nastolatki" (raport)

Od 2014 r. NASK prowadzi cykliczne, ogólnopolskie badanie uczniów „Nastolatki", którego celem jest diagnoza zachowań polskich nastolatków w internecie. Od 2018 r. badaniem objęliśmy także rodziców, co umożliwia konfrontację opinii i wyobrażeń młodych z obserwacjami dorosłych. Regularność podejmowanych działań pozwala na uchwycenie dynamiki zmian związanych z aktywnością nastolatków online.

Każda kolejna edycja raportu pomaga dostrzegać trwałe trendy, ale też gwałtowne zmiany związane z cyfrową transformacją. Tym samym wyznacza ramy dalszej dyskusji publicznej na temat cyfrowej codzienności młodych ludzi oraz sposobów wspierania ich rozwoju w świecie dynamicznych zmian.

Do tej pory opublikowaliśmy sześć raportów, a ostatnie badanie zrealizowaliśmy w 2024 r. W kwestionariuszu znalazły się pytania dotyczące m.in.: czasu spędzanego w sieci, sposobu użytkowania internetu – w tym mediów społecznościowych, świadomości zagrożeń, korzystania z internetu w szkole, kontroli rodzicielskiej, doświadczenia cyberprzemocy czy sposobów reagowania na niebezpieczne sytuacje w sieci. W edycji 2024 raportu po raz pierwszy spytaliśmy też uczniów, jak korzystają ze sztucznej inteligencji i co czują, myślą oraz czego oczekują od tej technologii. Ponadto poruszyliśmy problem deepfake'ów – fałszywych treści generowanych cyfrowo.

Raport „Nastolatki" to lektura obowiązkowa dla rodziców, nauczycieli, specjalistów i wszystkich osób, które chcą realnie wspierać dzieci w ich wędrówkach po cyfrowym świecie.

Poznajcie interesujące wnioski płynące z raportu „Nastolatki" – znajdziecie go na stronie nask.pl.

Netykieta

Czy wiecie, że dobre maniery obwiązują także w internecie? Netykieta (ang. *netiquette*, od net – „sieć" i *etiquette* – „etykieta") to zbiór zasad dotyczących pozytywnych zachowań w sieci, a te wpływają też na nasze bezpieczeństwo.

Kodeks online – choć niespisany i nie zatwierdzony odgórnie – odnosi się do ogólnie przyjętych norm w relacjach międzyludzkich i obejmuje wszystkich użytkowników wirtualnego świata. Złamanie dobrych obyczajów może wiązać się ze zgłoszeniem sprawy do administratora serwisu, a w konsekwencji – usunięciem członka z danej grupy, np. forum dyskusyjnego.

O jakich zasadach netykiety powinniście pamiętać?

- **Okażcie innym użytkownikom szacunek** – nie bądźcie hejterami lub trollami! Kierujcie się empatią i tolerancją – szczególnie dla odmiennych poglądów.
- **Przestrzegajcie regulaminu danego serwisu** – nie zaśmiecajcie wirtualnej przestrzeni spamem, nie naruszajcie prawa autorskiego.
- **Nie rozpowszechniajcie fałszywych informacji** – szokujące, niepotwierdzone treści nie tylko szerzą dezinformację, ale też sieją zamęt i negatywnie wpływają na innych użytkowników sieci.
- **Piszcie klarownie i poprawnie** – zachowujcie jasność przekazu, pamiętajcie też o ortografii i interpunkcji, ponadto nie używajcie wulgaryzmów i nie przesadzajcie z emotikonami.
- **Nie krzyczcie w internecie** – wyłączcie CAPS LOCK i nie używajcie w nadmiarze wykrzykników, które sygnalizują poniesiony ton.
- **Reagujcie na niebezpieczne i szkodliwe treści online** – zgłaszajcie je do odpowiednich instytucji, np. do CERT Polska lub zespołu Dyżurnet.pl.

Przestrzeganie zasad netykiety na pewno sprawi, że cyfrowy świat będzie przyjaźniejszy i bezpieczniejszy dla jego wszystkich użytkowników.

Więcej informacji na temat netykiety znajdziecie na stronie ose.gov.pl w artykule „Netykieta, czyli jak zostać mistrzem słowa w internecie". Jeśli natomiast chcecie nauczyć dziecko dobrych zachowań w internecie, zachęcamy do skorzystania z naszych kursów e-learningowych na OSE IT Szkole: „Krasnoludki 2.0 – Mech w potrzebie" i „Relacje w środowisku medialnym".

Nieautoryzowany dostęp

Najprościej mówiąc, nieautoryzowany dostęp to sytuacja, w której osoba, program lub urządzenie uzyskuje dostęp do systemu komputerowego, sieci, aplikacji, danych lub innych zasobów bez odpowiednich uprawnień lub zgody właściciela. Taki dostęp może mieć miejsce w wyniku działania oszustów, złośliwego oprogramowania (malware), a także błędów w konfiguracji zabezpieczeń lub niedbalstwa użytkowników.

Kiedy możecie się spotkać z nieautoryzowanym dostępem? Przytaczamy najczęstsze przykłady:

- **Włamanie do systemu komputerowego**. Oszust przełamuje zabezpieczenia, aby uzyskać dostęp do systemu, np. w celu kradzieży danych lub zainstalowania malware.
- **Phishing**. Ofiara zostaje podstępem nakłoniona do podania swoich danych logowania na fałszywej stronie internetowej, co umożliwia przestępcy zalogowanie się na jej konto.
- **Uzyskanie dostępu do konta**. Oszust zdobywa nielegalnie hasło do konta użytkownika (np. poczty elektronicznej) i korzysta z niego bez wiedzy właściciela.
- **Złośliwe oprogramowanie**. Na komputerze ofiary (bez jej wiedzy!) zostaje zainstalowany program, który umożliwia atakującym przejęcie kontroli nad urządzeniem.

Nieautoryzowany dostęp jest poważnym zagrożeniem dla bezpieczeństwa Waszych danych, prywatności oraz integralności systemów informatycznych. Może prowadzić do kradzieży tożsamości, strat finansowych, zniszczenia danych czy też szantażu. Na szczęście nie jesteście bezradni wobec tego zagrożenia. Pamiętajcie o kilku kluczowych wskazówkach:

- Twórzcie silne, unikalne hasła. Używajcie co najmniej 14-znakowych fraz, które będą łatwe do zapamiętania dla Was, ale trudne do złamania przez przestępców. Wystrzegajcie się oczywistych kombinacji cyfr i znaków! Stosujcie różne hasła do różnych kont i wspomagajcie się menedżerami haseł – dzięki temu Wasze szyfry będą zawsze bezpieczne.
- Wszędzie tam, gdzie to możliwe, używajcie uwierzytelniania dwuskładnikowego lub wieloskładnikowego. Wówczas podczas logowania będziecie podawać nie tylko hasło, ale też dodatkowy element znany tylko Wam (np. tymczasowy kod ze specjalnej aplikacji).
- Regularnie aktualizujcie system operacyjny oraz aplikacje i inne programy, z których korzystacie. Zabezpieczycie się w ten sposób przed znanymi lukami w zabezpieczeniach, które mogą być wykorzystywane przez oszustów.
- Zadbajcie też o fizyczne zabezpieczenia Waszych urządzeń: ustawcie blokady ekranu, hasła do odblokowania sprzętu po wybudzeniu, a także upewniajcie się, czy nikt nie podgląda Waszych działań na ekranie, gdy się logujecie.
- Ustawcie powiadomienia o nietypowej aktywności na swoim koncie bankowym i reagujcie, gdy tylko zaważycie nietypowe przelewy.
- Uważajcie na wiadomości e-mail, SMS-y czy telefony, które mogą próbować wyłudzić Wasze dane logowania. Nigdy nie klikajcie w podejrzane linki i nie otwierajcie załączników od nieznanych nadawców.
- Nie podawajcie nikomu poufnych informacji, takich jak dane do logowania. Ważne pliki udostępniajcie tylko tym, którzy faktycznie powinni mieć do nich dostęp.

Pamiętajcie, że Wasze bezpieczeństwo w sieci zaczyna się od Was samych – regularne aktualizacje, silne hasła oraz ostrożność w kontaktach online to kluczowe elementy ochrony.

Niebezpieczne kontakty

Kontakty online mają wiele zalet – cenią je szczególnie osoby, dla których komunikacja przez internet bywa łatwiejsza od tej prowadzonej w realnym świecie, lub te poszukujące drugiej połówki online. Warto jednak pamiętać, że niektóre znajomości bywają bardzo niebezpieczne.

W dobie komunikatorów internetowych, czatów, mediów społecznościowych, portali randkowych ławo poznać w sieci bratnią duszę, ale też paść ofiarą np. romance scam, czyli „romantycznego oszustwa". Złamane serce i puste konto – tak kończy się miłość, jeśli trafimy na oszusta.

Choć z osobą o nieuczciwych intencjach może się w sieci zetknąć każdy, to skutki takiego kontaktu szczególnie dotkliwie odczują dzieci. Miły znajomy z internetu może się okazać niebezpiecznym przestępcą!

Na jakie zagrożenia narażeni są młodzi użytkownicy sieci podczas zawierania znajomości online? Jednym z nich jest child grooming, czyli uwodzenie nieletnich w internecie. To przestępstwo wiąże się też z nakłonieniem ofiary do produkcji intymnych materiałów (self generated content), a także z szantażem (sextortion), który sprawia, że generowane są kolejne zdjęcia lub filmy. Pamiętajcie, że relacja groomingowa bardzo często prowadzi do wykorzystania dziecka w świecie realnym!

Wbrew pozorom kontakt młodych ludzi twarzą w twarz z nieznajomymi osobami dorosłymi poznanymi w internecie to dość powszechne zjawisko. Według raportu NASK „Nastolatki" na taki krok zdecydował się co dziewiąty badany (11%), a jeśli już doszło do spotkania – co czwarty zachował tę informację tylko dla siebie (Ładna i in., 2025).

Warto podjąć kroki zmierzające do ochrony dzieci i młodzieży przed nawiązywaniem niebezpiecznych kontaktów online. Postawcie na rozmowę i edukację w zakresie cyberzagrożeń. Budujcie relacje z dzieckiem oparte na zaufaniu. Wspierająca postawa rodziców i opiekunów sprawi, że chętniej zwróci się ono do Was po pomoc w przypadku doświadczenia trudnej sytuacji w internecie.

Pamiętajcie, jeśli Wasze dziecko padło ofiarą przestępstwa – uwodzenia w sieci, ujawnienia wiadomości sekstingowych lub szantażu w oparciu o intymne materiały – natychmiast zgłoście sprawę policji. Wcześniej zabezpieczcie jednak dowody przestępstwa – skopiujcie, zróbcie zrzuty ekranu, wydrukujcie: zapisy chatu, przesłane zdjęcia itp. Jeśli macie taką możliwość, jak najszybciej usuńcie kompromitujące treści z sieci – pomogą Wam w tym specjaliści z działającego w NASK zespołu Dyżurnet.pl.

W kryzysie warto skorzystać z pomocy specjalisty. Wsparcie znajdziecie też po drugiej stronie słuchawki telefonu – w liniach pomocowych hepline. Zadzwońcie np. pod numer 116 111 (116111.pl) – Bezpłatny i anonimowy telefon zaufania dla dzieci czy 116 123 – Bezpłatny kryzysowy telefon zaufania dla dorosłych. W trudnych chwilach możecie liczyć na profesjonalną poradę, szczerą rozmowę o przeżywanych emocjach lub po prostu zostać wysłuchani – bez oceniania, z pełnym zrozumieniem.

Jak bezpiecznie nawiązywać i podtrzymywać relacje w sieci? Wskazówek szukajcie w naszych aktualnościach na ose.gov.pl: „Złote zasady internetowych znajomości", „Bezpieczni w sieci z OSE: wakacyjne przyjaźnie – uwaga na niebezpieczne kontakty!". O zagrożeniach związanych internetowymi znajomościami przeczytacie też w aktualnościach: „Uwaga na romance scam!", „Walentynki online? Sexting – niebezpieczny trend", „Wirtualna miłość – realne zagrożenie", „Bezpieczni w sieci z OSE na wakacje: catfishing i letnie kontakty online". Polecamy również poradniki przygotowane przez ekspertów NASK: „Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online" i „Internetowe love II – randkowanie, AI i cyberbezpieczeństwo".

Źródło:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Nielegalne treści

To szczególny rodzaj szkodliwych treści, które mogą wywołać negatywne emocje u odbiorcy i destrukcyjnie wpływać na rozwój dzieci i młodzieży. Nielegalne treści ponadto naruszają przepisy polskiego prawa (najczęściej przepisy Kodeksu karnego), a ich rozpowszechnianie jest karalne!

Do nielegalnych treści zaliczamy materiały przedstawiające m.in.: seksualne wykorzystywanie dziecka, związane z uwodzeniem dziecka przez internet (child grooming), propagujące rasizm i ksenofobię czy mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym.

Eksperci przestrzegają: sporadyczny kontakt z niebezpiecznymi treściami wpływa na emocje i samopoczucie dziecka. Natomiast regularne oglądanie szkodliwych materiałów oddziałuje na postrzeganie świata, wzmacnia skłonność do podejmowania ryzykownych działań, w tym niezgodnych z normami społecznymi, znieczula na losy ofiar przemocy, utrwala negatywne stereotypy i fałszywe poglądy na sferę seksualności, a nawet może zachwiać osobowością młodych ludzi!

Jeśli zetkniecie się w sieci z nielegalnymi treściami – reagujcie! O takiej sytuacji należy poinformować policję, a także działający w NASK zespół Dyżurnet.pl. Możecie to zrobić za pomocą formularza na stronie dyzurnet.pl, wysyłając wiadomość e-mail na adres: dyzurnet@dyzurnet.pl lub dzwoniąc pod numer 801 615 005.

Warto też postawić na działania profilaktyczne. Na początek rozmowa i edukacja na temat treści, które naruszają bezpieczeństwo użytkowników sieci. A co zrobić, gdy dziecko wpadnie w spiralę oglądania nielegalnych materiałów? Pamiętajcie, że niektóre z nich mogą bardzo ciekawić dzieci, wywoływać ekscytację, dlatego nie oceniajcie, nie krytykujcie, ale wysłuchajcie i okażcie wsparcie. Starajcie się zrozumieć, dlaczego dziecko się nimi interesuje. Wyjaśniajcie mu też różnicę między prezentowanymi treściami a tym, jak wygląda prawdziwe życie.

Więcej informacji o nielegalnych treściach znajdziecie na platformie OSE IT Szkoła w naszym poradnikach: dla nauczycieli „Szkodliwe treści w internecie” oraz rodziców „Szkodliwe treści w internecie. Nie akceptuję, reaguję!”. Zajrzyjcie też do aktualności „Cyberbezpieczna biblioteczka: szkodliwe treści” oraz „Niebezpieczne zjawiska w internecie: szkodliwe treści” – polecamy w nich różne materiały (webinary, broszury, e-kursy, scenariusze lekcji, inne artykuły) na temat tego niebezpiecznego zjawiska.

N

Nomofobia

Nomofobia (z ang. *no mobile phone phobia*) oznacza paniczny strach przed brakiem dostępu do telefonu podłączonego do internetu. I choć tego terminu nie znajdziemy w Międzynarodowej Klasyfikacjach Chorób i Problemów Zdrowotnych, w powszechnej świadomości funkcjonuje on jako „specyficzna fobia”, rodzaj zaburzenia lękowego.

Z nomofobią wiązane są sytuacje, w których osoba może reagować atakiem paniki na samą myśl, że może zgubić lub uszkodzić telefon. Osoby dotknięte tym zjawiskiem mogą też odczuwać zawroty głowy, nudności czy ból w klatce piersiowej. Frustracja pojawia się również w momencie utraty urządzenie z zasięgu wzroku, gdy bateria jest niemal wyczerpana lub telefon nie ma połączenia z siecią. Próby ograniczenia dostępu do urządzenia, brak możliwości przeglądania mediów społecznościowych i reagowania na każde powiadomienie mogą powodować nerwowość, poirytowanie, agresję.

Czy nomofobia to realne zagrożenie? Z raportu NASK „Nastolatki” wynika, że smartfon to najważniejsze urządzenie w życiu online młodych ludzi – korzysta z niego aż 93% badanych. Ponadto co trzeci nastolatek (31%) deklaruje, że ma trudność z rozstaniem się ze swoim ulubionym urządzeniem, a 5 na 100 respondentów (5%) – ma z tym duży problem. Jednocześnie ponad połowa młodych ludzi zauważa potrzebę ograniczenia korzystania z telefonu (55%) oraz przyznaje, że używa go dłużej, niż planowała (52%). Co więcej – co czwarty nastolatek odczuwa fizyczne i emocjonalne skutki nadmiernego używania smartfona (Ładna i in., 2025).

Nomofobia łączy się z innymi zjawiskami: fonoholizmem – poważnym nadużywaniem telefonu i FOMO (ang. *Fear of Missing Out*) – lękiem przed odłączeniem. Osoby cierpiące z powodu no-

mofobii niejednokrotnie potrzebują pomocy specjalisty. Warto jednak zawczasu podjąć działania profilaktyczne, by smartfon nie stał się w przyszłości źródłem problemów.

Najważniejsza jest szczera rozmowa i uświadomienie problemu. Następnie warto zadbać o wprowadzenie zasad higieny cyfrowej – w tym przypadku warto eksperymentować i szukać rozwiązań, które wspierają równowagę online–offilne. Planujcie świadomie czas z dala od ekranów, wybierajcie aktywności, które pozwalają odpocząć od cyfrowego zgiełku oraz odzyskać wewnętrzny spokój. Zachęcajcie też bliskich do wspólnych wyzwań offline – wyznaczajcie w domu strefy wolne od urządzeń, odkładajcie telefony przed snem i podczas posiłków, a poranki zaczynajcie od chwili dla siebie, a nie od ekranu. Małe zmiany mogą przynieść wielkie efekty – wystarczy tylko podjąć świadomą decyzję.

Co zrobić, by nowe technologie były wsparciem w rozwoju młodych użytkowników? Zachęcamy do lektury aktualności „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa" dostępnej na ose.gov.pl.

Źródła:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK [online, dostęp dn. 14.10.2025].

„Uzależnienie od telefonu i nomofobia – przyczyny, objawy, leczenie", (b.r), artykuł na stronie emc-sa.pl [online, dostęp dn. 14.10.2025].

Nudging

Zdarzyło się Wam zajrzeć do internetu tylko na chwilę, żeby coś sprawdzić, a okazało się, że zostaliście w sieci dłużej, niż zamierzaliście, bo zaczęliście oglądać obrazki z kategorii „najśmieszniejsze zwierzęta"? Jeśli coś Was przyciąga do cyfrowego świata i nie potraficie się tej sile oprzeć, to może być nudging (ang. „impuls", „szturchnięcie", „trącenie łokciem"), czyli stwarzanie takich okoliczności, które zachęcają do częstszego i dłuższego korzystania z urządzeń.

Twórcy cyfrowych usług wiedzą, jak zatrzymać Was przed ekranem urządzenia. Mają na to kilka sposobów:

- **Częste powiadomienia typu „push"** – nieodebrane połączenia, przychodzące SMS-y, e-maile, wiadomości w komunikatorach, powiadomienia o komentarzach, reakcjach czy transmisjach w mediach społecznościowych – o zdarzeniach tego typu dowiadujecie się natychmiast dzięki ikonom pojawiającym się na ekranie urządzenia. To one „popychają" Was (z ang. *push* – „pchać") do działania, czyli zachęcają do częstego sięgania po smartfon.
- **Feed bez końca** – platformy streamingowe czy społecznościowe są tworzone tak, by wpisy, posty i filmiki nie miały końca. W ten sposób możecie godzinami przeglądać zamieszczane w nich materiały.
- **Kuszące clickbaity** – również skutecznie utrzymują Waszą uwagę. To chwytliwe hasła lub sensacyjne tytuły, które zachęcają do kliknięcia w dany materiał. Najczęściej ma on niewiele wspólnego z krzykliwym nagłówkiem.
- **Ciąg dalszy nastąpi…** – influencerzy i twórcy seriali, chętnie dzielą swoje filmiki na części. Kontynuują historię w kolejnych odcinkach, co ma Was zachęcić do pozostania z nimi na dłużej.
- **Cliffhangers** (z ang. „zawieszenie na krawędzi klifu") – to kolejny zabieg, który wykorzystują twórcy usług cyfrowych. Polega on na budowaniu napięcia i ucięciu akcji w najciekawszym momencie, by widz ponownie zasiadł przed ekranem i zobaczył, co wydarzy się dalej. Ten chwyt stosują z powodzeniem platformy streamingowe. W kulminacyjnym momencie odcinek serialu się kończy, ale zaraz – dzięki autoodtwarzaniu – możecie oglądać następny.
- **Personalizacja treści** – za sprawą tego działania zawsze traficie online na treści, które Was zainteresują. Preferencje internautów zapisywane są np. w plikach cookies. O Waszą

wzmożoną aktywność w sieci dbają też algorytmy wykorzystujące sztuczną inteligencję, dzięki którym w internecie zawsze znajdziecie coś, na czym skupicie swoją uwagę.

Jak widać, nudging potrafi skutecznie zatrzymać użytkownika przed ekranem urządzenia. Warto też pamiętać, że wszystkie bodźce, które docierają do nas z cyfrowego świata, uwalniają dopaminę, czyli neuroprzekaźnik odpowiedzialny za odczuwanie przyjemności oraz wzmacnianie motywacji do działania. To dlatego tak chętnie sięgamy po smartfon i korzystamy z niego przez długi czas. Łatwo jednak wpaść w pułapkę pętli dopaminowej – z czasem układ nagrody będzie potrzebował zwiększonej liczby silnych bodźców, czyli w tym przypadku treści płynących z ekranów.

Na tym jednak nie koniec. Nudging ma jeszcze ciemniejszą stronę – to tzw. dark patterns, czyli wzorce, które celowo wprowadzają użytkowników w błąd. Są zaprojektowane tak, by utrudniać rezygnację z subskrypcji, nakłaniać do niechcianych zakupów albo wymuszać na nas np. akceptację regulaminów. Do takich praktyk należą m.in.:

- **drip pricing** (z ang. „wycena kropelkowa") – ujawnianie dodatkowych kosztów lub opłat dopiero na ostatnim etapie zakupów;
- **zmuszanie do subskrypcji** – użytkownicy są manipulowani, by nieświadomie zgodzili się na subskrypcję, która jest trudna do odwołania (wypisanie się z newslettera wymaga kilku kroków lub kontaktu telefonicznego);
- **zmanipulowane przyciski** – np. „Odrzuć" jest szary i ledwo widoczny, a „Akceptuj" świeci się na zielono;
- **fake countdowns** (ang. „sztuczne liczniki") – liczniki obrazujące upływ czasu do końca promocji mają wywoływać presję zakupu;
- **ranking popularności** – komunikaty w stylu „ten produkt kupiło już 300 osób", „50 osób interesuje się tym terminem" itd.;
- **reklamy typu bait and switch** (z ang. „przynęta i zamiana") – użytkownicy są kuszeni atrakcyjnymi ofertami, które nie są dostępne, a te, z których można skorzystać, są zdecydowanie mniej opłacalne;
- **misdirection** (z ang. „wprowadzenie w błąd") – zastosowanie elementów, które odwracają uwagę użytkownika i utrudniają porównanie ofert, np. wyróżnianie kolorystyczne lub graficzne jednej opcji, podczas gdy inna, potencjalne lepsza, jest mniej widoczna;
- **brak możliwości odmowy udzielenia zgody na profilowanie**;
- **wyświetlenie komunikatów, które mają zachęcać do nabywania kolejnych produktów, zanim zostanie zakończona procedura aktualnych zakupów**.

Więcej informacji na temat nudgingu znajdziecie w poradniku „Mniej znaczy więcej. O multi-screeningu i wielozadaniowości" oraz aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE": online'owy nudging" i „Letnia Akademia Cyfrowej Higieny: o nudgingu i cyfrowych sztuczkach".

O

Ochrona urządzeń mobilnych

Urządzenia mobilne – smartfony, laptopy, tablety – to nieodłączni towarzysze naszej codzienności. Zapewne i dla Was stały się one minicentrami zarządzania Waszymi aktywnościami w sieci. Czy na pewno wiecie, jak z nich bezpiecznie korzystać?

Zacznijcie od blokady ekranu nieużywanego urządzenia, tak aby za każdym razem, gdy weźmiecie telefon do ręki, trzeba było wpisać PIN, narysować wzór, użyć odcisku palca lub innego zabezpieczenia biometrycznego. Wybierając hasło, unikajcie przewidywalnych kombinacji (np. 1234, 1111, 1010) oraz kojarzących się z Wami ciągów cyfr (np. daty urodzin).

Pamiętajcie, że blokada ekranu nie chroni w pełni przed niepowołanym dostępem do danych zgromadzonych na smartfonie czy tablecie. Dobrym rozwiązaniem jest więc szyfrowanie urządzeń mobilnych (dostępne w ustawieniach) i włączenie opcji umożliwiającej zdalne zarządzanie sprzętem w przypadku jego utraty (np. kradzieży). Gdy zaszyfrujecie swój telefon, złodziej nie będzie mógł dostać się do pamięci urządzenia, Wasze dane będą zatem bezpieczne. Z kolei zdalnie zarządzając swoim urządzeniem, możecie nie tylko zablokować do niego dostęp czy wyczyścić całą pamięć, ale też namierzyć jego lokalizację.

Na bezpieczeństwo Waszych mobilnych sprzętów wpływa także przestrzeganie prostych zasad, które w połączeniu z Waszymi świadomymi działaniami zdecydowanie utrudnia cyberprzestępcom dostęp do urządzeń.

1. Korzystajcie z aktualnych wersji systemu operacyjnego i aplikacji. Włączcie więc na swoich urządzeniach automatyczne aktualizacje, które łatają zauważone przez producentów luki w oprogramowaniu i zmniejszają podatność telefonów czy tabletów na cyberataki.
2. Pobierajcie oprogramowanie tylko z zaufanych źródeł sklepów z apkami (Google Play dla urządzeń z systemem Android, App Store – z systemem iOS) lub ze stron producenta.
3. Ograniczcie uprawnienia aplikacji, zwłaszcza te dotyczące dostępu do listy kontaktów czy danych dotyczących lokalizacji. Nie wszystkie apki wykorzystują takie informacje (bo np. nie potrzebują zdjęć z galerii do prawidłowego funkcjonowania). Sprawdzajcie opisy apek w sklepach – tam znajdziecie wszystkie informacje o tym, jakie Wasze dane i w jaki sposób będzie wykorzystywała dana aplikacja. Często dostęp do np. lokalizacji czy zdjęć można limitować, tj. udostępniać lokalizację tylko raz albo tylko podczas korzystania z aplikacji. Uważajcie na aplikacje, do których nie można mieć pełnego zaufania!
4. Upewnijcie się, że poufne powiadomienia, np. kody weryfikacyjne, nie pojawiają się na ekranie zablokowanego sprzętu.
5. We wszystkich serwisach i aplikacjach wymagających zalogowania ustawiajcie unikalne, łatwe do zapamiętania, ale trudne do złamania hasło. Najlepiej, jeśli składa się ono z co najmniej 14 znaków i jest zmodyfikowaną, kilkuwyrazową frazą. Korzystajcie też z menedżerów haseł, które pomogą je zapamiętać, a także z uwierzytelniania dwuskładnikowego, które zdecydowanie pozytywnie wpłynie na Wasze cyfrowe bezpieczeństwo.

Więcej porad znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: aplikacje mobilne”, „Bezpieczni w sieci z OSE: bezpieczne logowanie”, „Dzień Bezpiecznego Komputera: zadbaj o swój sprzęt”, „Bezpieczni w sieci z OSE: bezpieczeństwo urządzeń mobilnych”.

Odporność cyfrowa (digital resilence)

Do prawidłowego funkcjonowania organizmu człowieka niezbędna jest odporność immunologiczna, która polega na zdolności do ochrony przed wirusami i innymi patogenami. Podobnymi cechami muszą wykazywać się też systemy informatyczne, tak jak my podatne na różne zagrożenia.

O

Odporność cyfrowa definiowana jest jako zdolność do szybkiego powrotu do stanu pierwotnego, także jako wytrzymałość. W praktyce oznacza to zdolność organizacji do utrzymywania, dostosowywania i odtwarzania operacji w obliczu cyfrowych zagrożeń, zakłóceń lub awarii (Sikora, 2024).

W zakres odporności cyfrowej wchodzi wiele działań, takich jak dbałość o odpowiednie środki cyberbezpieczeństwa, ochrona danych wrażliwych, planowanie schematów działań w przypadku różnego rodzaju ataków. Wszystko to ma zapewnić, że wykorzystywane w danej organizacji zasoby cyfrowe pozostaną bezpieczne i odporne na wszelkie formy zagrożeń z cyberprzestrzeni.

Choć odporność cyfrowa w dużej mierze dotyczy organizacji, trudno nie zauważyć podobieństw do działań, które w swoim interesie powinien podejmować każdy internauta. Odporność cyfrowa to przede wszystkim świadomość istnienia cyberzagrożeń i sposobów radzenia sobie z nimi. To też wszelkie działania, które mają chronić ważne dane. W naszym przypadku będą to z jednej strony kopie zapasowe, a z drugiej – reguły bezpieczeństwa, o których nie powinniśmy zapominać na co dzień. Silne hasła i inne zabezpieczenia, ochrona swojej tożsamości w internecie, zasada ograniczonego zaufania: wszystko to sprawia, że stajemy się mnie podatni na cyfrowe zagrożenia.

Zachęcamy – zbudujcie własną długoterminową strategię ochrony przed internetowymi niebezpieczeństwami, wdrażajcie ją w swoich domach, zachęcajcie do takich działań znajomych i bliskich. Razem możecie zrobić bardzo wiele dla swojego bezpieczeństwa w sieci!

Źródło:

„Lektura obowiązkowa: cyfrowa odporność”, (2020), artykuł w serwisie vertiv.com.

Offline challenge

Zastanawialiście się kiedyś, ile razy w ciągu doby sięgacie po swój smartfon? Telefon towarzyszy nam w zasadzie wszędzie: podczas posiłków, w podróży, spotkań ze znajomymi. Zostawiamy lajki, scrollujemy media społecznościowe, wpadamy w pułapkę automatycznego odtwarzania filmików na YouTubie czy TikToku. Internet wciąga – to niezaprzeczalny fakt. Ale czy to znaczy, że nie mamy wpływu na nasze cyfrowe nawyki? Wręcz przeciwnie!

Warto zatrzymać się na chwilę i sprawdzić, jak dużo czasu spędzamy w sieci i na czym polegają nasze aktywności online. Z pomocą przychodzi akcja #offlinechallenge polegająca na odłączeniu się od internetu na 48 godzin. Czy dwie doby bez dostępu do sieci to dużo? I tak, i nie. W tym czasie na pewno nie zmienicie diametralnie swojego życia i przyzwyczajeń, nie będzie to detoks, który zakończycie odmienieni. Jednak 48 godzin offline na pewno pozwoli dokładniej przyjrzeć się temu, jak funkcjonujecie, gdy nie rozpraszają Was powiadomienia, gdy w różnych sytuacjach musicie sobie radzić bez kilku kliknięć na ekranie smartfona.

Aby podjąć to wyzwanie, wystarczą jedynie trzy kroki:

1. **Ustalcie, kiedy dokładnie odłączycie się od sieci.** Uprzedźcie znajomych o tym zamiarze i dokładnie zaplanujcie swoje aktywności podczas cyfrowego detoksu. Wyjście do kina, na basen, do parku z książką, udział w koncercie – każdy pomysł jest dobry!

2. **Przyjrzyjcie się sobie.** Pozwólcie sobie na wszystkie uczucia, które wywoła w Was odłączenie od sieci – złość, frustrację, może nawet lęk i smutek. Obserwujcie, jak radzicie sobie w różnych sytuacjach, np. gdy nie możecie za pomocą kilku kliknięć sprawdzić prognozy pogody, rozkładu jazdy autobusów czy zapłacić zbliżeniowo.

3. **Wyciągnijcie wnioski.** Zastanówcie się, co dały Wam dwa dni bez smartfona. Może znaleźliście więcej czasu na spotkania ze znajomymi czy swoje hobby, może lepiej spaliście, a może w pewnym momencie musieliście się poddać? Najcenniejsze w #offlinechallenge są właśnie przemyślenia – to one pomagają budować nowe, zdrowsze nawyki cyfrowe!

Trzymamy kciuki, by to nietypowe wyzwanie stało się początkiem większych zmian, które wprowadzicie w swoim codziennym życiu. Spróbujcie i sami się przekonajcie – warto!

Szczegółowe informacje o wyzwaniu znajdziecie na stronie offlinechallenge.pl, a wskazówki dotyczące budowania zdrowych nawyków cyfrowych – w naszych aktualnościach na stronach ose.gov.pl i OSE IT Szkoła: „Bezpieczni w sieci z OSE na wakacje: offline challenge", „Zadbaj o siebie z OSE: Dzień bez Komputera".

Ogólnopolska Sieć Edukacyjna (OSE)

Trudno mówić o bezpieczeństwie w sieci bez przypomnienia, czym jest… Ogólnopolska Sieć Edukacyjna!

OSE to program publicznej sieci telekomunikacyjnej, dający szkołom w całej Polsce możliwość podłączenia szybkiego, bezpiecznego i bezpłatnego internetu. Realizujemy go my, czyli NASK Państwowy Instytut Badawczy, pod nadzorem Ministerstwa Cyfryzacji. W ramach programu OSE prowadzimy także działania edukacyjno-informacyjne, promujące zasady bezpiecznego korzystania z technologii cyfrowych. Ogólnopolska Sieć Edukacyjna jest bowiem odpowiedzią na wyzwania współczesnej edukacji – kształtującej kompetencje cyfrowe i otwartej na nowoczesne technologie.

W ramach OSE razem z internetem dostarczamy profesjonalne usługi bezpieczeństwa: „Bezpieczny internet OSE", „Bezpieczeństwo użytkownika OSE", „Ochrona przed szkodliwym oprogramowaniem". Nasze usługi strzegą bezpieczeństwa szkolnych sieci, chronią przed różnego rodzaju niebezpieczeństwami online i atakami sieciowymi, a także monitorują, wykrywają i blokują zagrożenia związane ze złośliwym oprogramowaniem (malware) oraz nielegalnymi, szkodliwymi treściami. Codziennie dbamy o to, aby korzystający z internetu OSE byli bezpieczni online!

Usługi bezpieczeństwa to jednak nie wszystko. Sercem naszego programu są działania edukacyjne, które wspierają uczniów w bezpiecznym korzystaniu z sieci. Podpowiadamy nauczycielom, dyrektorom szkół i rodzicom, jak być przewodnikami dzieci w cyfrowym świecie. Z pomocą przychodzą nasi eksperci i tworzone przez nich materiały edukacyjne: poradniki, scenariusze zajęć i kursy e-learningowe, dotyczące m.in. rozważnych zachowań w sieci czy zagrożeń, z którymi mogą zetknąć się online dzieci i młodzież. Nasze treści edukacyjne znajdziecie na bezpłatnej platformie e-learningowej OSE IT Szkoła, która powstała z myślą o dostarczeniu nauczycielom i uczniom wartościowych kursów w wielu kategoriach, takich jak cyberbezpieczeństwo, sztuczna inteligencja czy programowanie. Zapoznajcie się z całą ofertą edukacyjną OSE już dziś!

W ramach projektu OSEhero wspólnie tworzymy też grupę zaangażowanych nauczycieli, którzy we współpracy z ekspertami OSE przekazują wiedzę o bezpieczeństwie w internecie uczniom, pedagogom oraz rodzicom. Wiemy, że bezpieczeństwo cyfrowe to nasza wspólna sprawa i każdy może sprawić, by internet stał się dla dzieci i młodzieży bezpieczną przystanią.

Oprogramowanie antywirusowe

Często naszym pierwszym skojarzeniem z cyberbezpieczeństwem jest program antywirusowy. Co to takiego? Główną funkcją antywirusa – zawartą już w nazwie – jest skanowanie, wykrywanie, rozpoznawanie oraz usuwanie malware (złośliwego oprogramowania) z komputera lub innego urządzenia, na którym zostało zainstalowane. Można powiedzieć, że program antywirusowy to swego rodzaju szczepionka: jeśli na bieżąco go aktualizujemy, ryzyko cyfrowej infekcji się zmniejsza.

Zapewnianie bezpiecznego przeglądania zasobów internetu polega na skanowaniu dostępnych na urządzeniu obiektów i porównywaniu z dostępną bazą, czyli sygnaturami wirusów. Odbywa się na dwa sposoby: poprzez skanowanie ręczne, gdy sami uruchamiamy program antywirusowy, lub w trakcie automatycznego poszukiwania intruzów na naszym urządzeniu.

Jeśli antywirus wykryje złośliwe oprogramowanie, natychmiast zareaguje i zaproponuje potrzebne działanie – usunięcie, zablokowanie lub przeniesienie zainfekowanego pliku do kwarantanny. Współczesne programy antywirusowe oferują znacznie więcej niż tylko ochronę przed wirusami. Wiele z nich posiada funkcje zabezpieczające przeglądanie stron internetowych, chroniące dane logowania, hasła czy transakcje online. Warto jednak pamiętać, że nawet najlepszy antywirus nie

zastąpi rozsądnego zachowania w sieci. Regularne aktualizacje, ostrożność przy pobieraniu plików i unikanie podejrzanych stron to wciąż najskuteczniejsze sposoby, by uniknąć cyfrowej infekcji.

Jak ważne jest regularne aktualizowanie oprogramowania, w tym antywirusa? Dowiecie się tego z naszych aktualności na stronie ose.gov.pl: „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!" i „Czas na wiosenne – cyfrowe – porządki!".

Oprogramowanie reklamowe (adware)

Pewnie nie raz podczas przeglądania internetu zdarzyło Wam się spotkać natarczywe reklamy, występujące przede wszystkim w formie bannerów lub wyskakujących okienek typu pop-up, zachęcających np. do zakupu „cudownej kuracji odchudzającej" czy ostrzegających o wirusach. Odpowiada za nie adware – niechciane oprogramowanie, które podszywa się pod pozornie bezpieczne aplikacje, aby skłonić użytkowników do zainstalowania ich na swoich urządzeniach (telefonach, komputerach, tabletach). Bywa, że adware występują w pakiecie z innym bezpłatnym oprogramowaniem jako potencjalnie niechciane programy (PUP, ang. *potentially unwanted program*).

Adware zarabia dla swojego twórcy, wyświetlając reklamy – najczęściej w interfejsie programu, który zainstalowaliśmy, albo w wyskakujących okienkach podczas przeglądania internetu. Może też przekierowywać ruch na wybrane strony, generując zysk z odwiedzin. Reklamy bywają uciążliwe, ale jeszcze groźniejsze jest to, że niekiedy prowadzą do fałszywych witryn, z których można pobrać złośliwe oprogramowanie czy dać się oszukać. Zdarza się też, że łączą się z programami programami czy umożliwiającymi włamania do systemów informatycznych (root-kit). Dodatkowo adware potrafi zbierać dane o naszej aktywności – jakie strony odwiedzamy, gdzie się logujemy, w jakiej lokalizacji jesteśmy – i wykorzystywać te informacje do podsuwania nam spersonalizowanych reklam albo przekazywać je innym podmiotom.

Takiej infekcji nie da się przegapić. Jeśli reklamy pojawiają się w miejscach, w których nie powinny, przeglądarka działa niezwykle wolno albo zawiesza się, nagle zmieniła się Wasza strona startowa lub domyślna wyszukiwarka, a na komputerze lub telefonie instalują się nieznane aplikacje – możecie być pewni, że macie do czynienia z adware. Gdy tylko zauważycie podejrzane objawy, przeskanujcie sprzęt za pomocą antywirusa i odinstalujcie aplikacje, które podejrzewacie o to, że są powiązane z programem typu adware.

Jak chronić się przed oprogramowaniem reklamowym? Niezmiernie ważne jest przestrzeganie podstawowych zasad bezpieczeństwa w sieci:

- Przede wszystkim, chcąc pobrać jakąś aplikację czy program, korzystajcie tylko z wiarygodnych źródeł. Zastanówcie się dwa razy, czy faktycznie potrzebujecie nowego oprogramowania, zanim je pobierzecie!
- Korzystajcie też z aktualnego oprogramowania antywirusowego. Wiele z nich automatycznie wykrywa i usuwa adware.
- Regularnie aktualizujcie oprogramowanie i system operacyjny, z którego korzystacie. Usuniecie w ten sposób podatności bezpieczeństwa, które ułatwiają adware wślizgiwanie się na Wasze urządzenia.
- Weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości.

Co ważne, nie każda aplikacja z reklamami to adware. Wiele legalnych programów (np. darmowe gry) wyświetla reklamy, ale robi to w sposób jawny i kontrolowany. Różnica polega na tym, że w przypadku adware reklamy są nachalne, pojawiają się w nieoczekiwanych miejscach, a sama aplikacja często ukrywa swoje intencje.

Na koniec ciekawostka: adware pojawiło się w połowie lat 90. i przez kilka lat było traktowane niemal jak normalny model biznesowy. W szczytowym momencie, w latach 2005–2008, rynek adware kwitł, dopóki nie zaczęto nakładać wysokich kar na firmy za agresywne i wprowadzające w błąd praktyki.

Źródło:

„Czym jest adware?", (b.r.), artykuł na stronie malwarebytes.com.

Oprogramowanie szpiegujące (spyware)

W internecie nic nie ginie i nie do końca możemy pozostać anonimowi – to prawda stara jak (przynajmniej ten cyfrowy) świat. Niestety zdarza się, że nasze poczynania w sieci są bacznie śledzone, a dzieje się to za pomocą złośliwego oprogramowania szpiegującego spyware (do ang. *spy* – szpieg, *software* – oprogramowanie). Oprogramowanie to zaraża komputer, telefon lub inne urządzenia, aby gromadzić nasze dane oraz ważne informacje, np. o sposobach korzystania z internetu czy naszej lokalizacji.

Złośliwe działania tych programów obejmują też przechwytywanie naciśnięć klawiszy na klawiaturze urządzenia (keylogger), zrzutów ekranu, poświadczeń uwierzytelniających (loginów i haseł), danych z formularzy internetowych i innych poufnych informacji, w tym numerów kart kredytowych. Ponadto spyware może przyznawać aplikacjom dostęp do mikrofonu i kamery naszego urządzenia.

Oprogramowanie szpiegujące rozprzestrzenia się najczęściej dzięki nieświadomości użytkownika. Uważajcie więc na pozornie przydatne narzędzia czy aplikacje, darmowe oprogramowanie pobierane z niezaufanych źródeł, a nade wszystko – na linki i załączniki w podejrzanych e-mailach. Zdarza się też, że spyware kryje się pod odpowiednio przygotowaną reklamą opłaconą przez cyberprzestępców.

Zła wiadomość jest taka, że programy szpiegujące są wyjątkowo podstępne: zwykle instalują się na urządzeniach bez naszej wiedzy, a następnie działają w tle, zbierając informacje i wywołując szkody. Działają po cichu, ale ich obecność zdradza kilka symptomów zainfekowania sprzętu złośliwym oprogramowaniem.

Jednym z niepokojących sygnałów może być spowolnione działanie urządzenia – system zaczyna reagować z opóźnieniem, aplikacje się zawieszają, a bateria rozładowuje się szybciej niż zwykle. Często można też zauważyć niechciane reklamy, nietypowe przekierowania w przeglądarce lub pojawienie się aplikacji, których wcześniej nie instalowaliśmy. Jeśli dostrzeżecie nieznane procesy działające w tle – co sygnalizuje zwiększone zużycie danych – to też znak, że należy podjąć działania naprawcze.

W usunięciu intruza pomogą sprawdzone programy antywirusowe. Czasem niezbędne może się okazać przywrócenie urządzenia do ustawień fabrycznych. W tym przypadku przyda się Wam backup sprzed infekcji, czyli kopia zapasowa danych.

Jak nie wpuścić szpiega do systemu operacyjnego? Nadrzędne jest zachowanie zasady ograniczonego zaufania – nie otwierajcie wiadomości od nieznanych nadawców, nie klikajcie w reklamy, weryfikujcie linki otrzymane z nieznanych źródeł, zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości. Zaopatrzcie się też w program antywirusowy, który zapewnia ochronę w czasie rzeczywistym i blokuje potencjalnego szpiega, zanim ten zdąży uruchomić się na komputerze. Ponadto dbajcie o regularne aktualizacje systemu operacyjnego i programów na Waszym urządzeniu – luki w zabezpieczeniach to furtka dla spyware.

Źródło:

„Co to jest spyware? Jak się chronić i usunąć oprogramowanie szpiegujące?", (2025), artykuł na stronie cyberacademy.com.pl.

Oprogramowanie szyfrujące

Silne hasła, uwierzytelnianie dwuskładnikowe i wieloskładnikowe, zabezpieczenia biometryczne – kolejne sposoby ochrony naszych kont i cennych informacji pojawiają się wraz z nowymi działaniami cyberprzestępców. Do niemałego arsenału środków bezpieczeństwa warto dołączyć też oprogramowanie szyfrujące, które uniemożliwia osobom niepowołanym dostęp do naszych plików lub danych.

Prywatne materiały, tajne projekty, wrażliwe dane: wszystkie tego typu pliki warto zamykać w symbolicznym sejfie zabezpieczonym dobrze strzeżonym kluczem. Oprogramowanie szyfrujące jest przydatne zwłaszcza teraz – w czasach, gdy bardzo chętnie korzystamy z usług chmurowych umożliwiających przechowywanie informacji na wirtualnych serwerach. Warto wiedzieć, że szyfrowanie zapobiega kradzieży danych w przypadku wycieku.

Jak działa oprogramowanie szyfrujące? Po zainstalowaniu odpowiedniego programu nasze pliki są przetwarzane przez algorytm szyfrowania, który następnie konwertuje je i sprawia, że są nieczytelne. Gdy zamierzony odbiorca (my lub ktoś, komu udostępniamy dany dokument) uzyskuje dostęp do pliku, zawarte w nim informacje tłumaczone są na powrót do swojej pierwotnej postaci. Aby odszyfrować wiadomość, należy użyć klucza deszyfrującego.

O szyfrowaniu powinniście pamiętać nie tylko przechowując poufne dokumenty, ale też wysyłając je za pośrednictwem poczty elektronicznej! To samo dotyczy szyfrowania end-to-end stosowanego w komunikatorach. Dzięki niemu do wymienianych wiadomości mają dostęp wyłącznie nadawca i odbiorca, a nie osoby trzecie, np. dostawca platformy.

Korzyści ze stosowania szyfrowania są wielowymiarowe: chroni prywatność, minimalizuje ryzyko kradzieży tożsamości, zabezpiecza tajne projekty firmowe oraz wspiera zgodność z regulacjami prawnymi dotyczącymi ochrony danych, takimi jak RODO (Ogólne rozporządzenie o ochronie danych). Dla firm i instytucji szyfrowanie jest wręcz niezbędnym elementem strategii bezpieczeństwa, natomiast dla użytkowników indywidualnych – prostym sposobem na ochronę życia cyfrowego.

Dodatkowo oprogramowanie szyfrujące pozwala wprowadzać różne poziomy ochrony: od standardowego szyfrowania folderów po pełne szyfrowanie dysku, dzięki czemu wszystkie dane zapisane na urządzeniu są automatycznie zabezpieczone. W połączeniu z innymi narzędziami, jak menedżery haseł czy VPN (ang. *Virtual Private Network*) tworzy kompleksową barierę ochronną, która znacznie utrudnia dostęp nieuprawnionym osobom.

Pamiętajcie: szyfrowanie to nie tylko technologia dla specjalistów – to praktyczna i dostępna metoda ochrony danych, która powinna stać się standardem w codziennym korzystaniu z komputerów, smartfonów i usług online. Dzięki niemu możecie korzystać z cyfrowego świata z większym spokojem, wiedząc, że Wasze pliki pozostają bezpieczne nawet w obliczu zagrożeń.

Oszustwa internetowe

Zapewne nie raz spotkaliście się z ostrzeżeniami przed oszustwami w internecie, może nawet śledzicie ostrzeżenia publikowane przez CERT Polska. To dobrze! Warto trzymać rękę na pulsie, bo wraz z szerokim dostępem do internetu pojawiają się kolejne sposoby oszukiwania ofiar w sieci.

Mamy tutaj na myśli różnego rodzaju ataki przeprowadzane online – bezpośrednio w internecie lub przy użyciu oprogramowania z dostępem do sieci. Mają one wspólny mianownik, mianowicie przestępcy wykorzystują niewiedzę, nieświadomość, a nawet samotność i naiwność użytkowników, by okraść ich lub zdobyć cenne informacje. Na co powinniście uważać?

- **Fałszywe inwestycje**. Przestępcy podszywają się pod znane instytucje, np. banki, i próbują nakłonić ofiary do zainwestowania dużych sum, które w założeniu mają zwrócić się z nawiązką. Takie oferty możemy znaleźć w wyszukiwarkach, w mediach społecznościowych, mogą do nas trafić także w wiadomościach e-mail (uwaga, to phishing!). Oszuści chcą nakłonić nas do kliknięcia w link prowadzący do strony, gdzie konieczne jest podanie

danych osobowych, lub do pobrania oprogramowania umożliwiającego zdalny dostęp do komputera. Obydwie drogi prowadzą do jednego celu: uzyskania naszych danych osobowych, danych logowania oraz kradzieży środków z konta.

- **Fałszywe reklamy** w wyszukiwarce. Nierzadko zdarza się, że kampanie phishingowe docierają do nas w formie reklam w wyszukiwarkach. Takie fałszywe strony są pozycjonowane na pierwszych miejscach w wynikach wyszukiwania, dlatego łatwo do nich dotrzeć i złapać się na haczyk przestępców. Sprawy nie ułatwia też fakt, że do złudzenia przypominają te oryginalne – witryny banków, sklepów, producentów oprogramowania. Dlatego zanim klikniecie w pierwszy wynik wyszukiwania, upewnijcie się, czy jest to strona, którą faktycznie chcecie odwiedzić. Jak to zrobić? Sprawdźcie, czy w adresie nie ma np. literówki, zastanówcie się, czy żaden element witryny nie wzbudza Waszego niepokoju.

- **Fałszywe sklepy internetowe i aukcje**. „Okazja – wyprzedaż na cały asortyment", „Tylko dziś: minus 90% na wszystko!": takie hasła w sklepach internetowych nie wróżą niczego dobrego. Choć zakupy online są o wiele wygodniejsze i szybsze niż tradycyjne, warto pamiętać o tym, że również w sieci możemy paść ofiarą złodziei. Nie dajcie się skusić wyjątkowym ofertom i zawsze przed dodaniem rzeczy do koszyka dokładnie przyjrzyjcie się stronie sklepu. Nie znaleźliście regulaminu i danych kontaktowych? Brakuje informacji o różnych metodach płatności i sposobach zwrotu? Uważajcie! Jeśli Wasz niepokój potwierdzą też negatywne opinie innych klientów – koniecznie poszukajcie innego sklepu. Zasadzki mogą czekać na Was też w serwisach aukcyjnych i zakupowych. Wystrzegajcie się sprzedających, którzy chcą kontaktować się z Wami poza oficjalną platformą. Nie przesyłajcie im kodów BLIK, nie przelewajcie pieniędzy bezpośrednio na ich konta, nie klikajcie w linki, które Wam przesyłają.

- **Fałszywe nagrody**. Lubimy dostawać dobre wiadomości – to naturalne. Jednak nie wszystkimi powinniśmy tak samo się cieszyć. Z dużą dozą niepewności podchodźcie do e-maili informujących o atrakcyjnych nagrodach w konkursach, w których nie braliście udziału. Wiadomość o dużym spadku po nieznanym krewnym? Informacja o intratnej ofercie pracy? Jeśli cokolwiek w treści e-maila wyda Wam się „zbyt piękne, by mogło być prawdziwe", raczej właśnie takie jest. Co jeszcze może świadczyć o zasadzce? Konieczność dopłaty „za dostawę" nagrody lub uczestnictwa w spotkaniu promocyjnym. Zwróćcie też uwagę na niepokojące zachowania „organizatora" konkursu: wysyłanie niespersonalizowanych e-maili z błędami językowymi czy próby wyłudzenia Waszych danych osobowych.

- **Fałszywe oferty matrymonialne**. W mediach społecznościowych oraz w aplikacjach randkowych oprócz szczęścia w życiu osobistym możecie spotkać też oszustów matrymonialnych. Wykorzystując Waszą samotność i – niestety – dobre cechy charakteru, będą próbowali wyłudzić od Was pieniądze. W jaki sposób? Być może opowiedzą Wam wzruszającą historię, może będą chcieli pożyczyć od Was środki na leczenie. Wszelkimi sposobami postarają się wzbudzić Wasze współczucie, a potem bezlitośnie wykorzystają Wasze zaufanie. Zawsze, gdy poznajecie kogoś nowego w internecie, stosujcie wobec niego zasadę ograniczonego zaufania. Nie wysyłajcie pieniędzy znajomym z sieci. Uważajcie też na relacje, które trwają długo, ale nigdy nie dochodzi do spotkania „na żywo".

Źródło:

„Europejski Miesiąc Cyberbezpieczeństwa z OSE: uważaj na różne typy oszustw w internecie", (2025), aktualność na stronie ose.gov.pl.

OUCH!

Źródeł informacji o bezpiecznym korzystaniu z internetu jest bardzo wiele. Oprócz materiałów tworzonych w ramach Ogólnopolskiej Sieci Edukacyjnej (poradników, webinarów, kursów e-learningowych czy aktualności) należy wspomnieć jeszcze o co najmniej jednym – serii biuletynów OUCH!. Dlaczego warto po nie sięgać?

OUCH! to zestawy porad w zakresie cyberbezpieczeństwa, wydawane w 22 językach na całym świecie. Polska wersja ukazuje się co miesiąc od kwietnia 2011 r. w ramach współpracy CERT Polska i SANS Institute. Każdy z biuletynów przybliża wybrane zagadnienie z obszaru bezpieczeństwa komputerowego. Co ważne – nie brakuje tutaj listy wskazówek, jak chronić się przed zagrożeniami w internecie.

Szukacie porad dotyczących bezpieczeństwa w sieci? Sięgnijcie np. do biuletynów OUCH! dotyczących oszustw w serwisach społecznościowych, wykrywania deepfake, kariery w cyberbezpieczeństwie i ataków w wiadomościach tekstowych. Wszystkie archiwalne wydania znajdziecie na stronie CERT Polska, koniecznie do nich zaglądajcie!

Oversharing

Zdjęcie śniadania, selfie w windzie i podczas treningu, fotka ze śpiącym kotem czy dzieckiem umorusanym marchewkową zupką. Wszyscy to znamy – dzielenie się w sieci szczegółami ze swojego życia to już codzienność. Chętnie dokumentujemy swoje dni i jeszcze chętniej pokazujemy prywatne pamiątki światu. Jednak czy zawsze słusznie…?

Zjawisko oversharingu (ang. *over* – ponad i *sharing* – udostępnianie), czyli nadmierna wylewność online, jednym może przysporzyć internetowych fanów, a drugim – kłopotów. Gdy zamieszczamy w mediach społecznościowych wiele swoich zdjęć i postów z informacjami o tym, gdzie teraz jesteśmy czy co robimy, narażamy się na niebezpieczeństwo związane np. z kradzieżą (złodziej będzie przecież doskonale wiedział, że skoro właśnie opalamy się nad morzem, to nasz dom stoi pusty). A gdy na udostępnionym w sieci zdjęciu znajdzie się fragment dokumentu tożsamości czy numer PESEL, ułatwiamy cyberprzestępcom np. zaciągnięcie kredytu na nasze konto.

Dorosłych oversharing naraża często na śmieszność i zniecierpliwienie znajomych, którzy oglądają np. dziesiątki zdjęć zwierząt domowych w różnych pozach. Co jednak ze zdjęciami dzieci udostępnianymi przez rodziców? Warto pamiętać, że nadmierne publikowanie w sieci zdjęć najmłodszych (sharenting) również może nieść za sobą spore ryzyko. Przestępcy, obserwując kolejne dodawane posty, uzyskują o Waszym dziecku wiele ważnych informacji – w którym przedszkolu spędza czas do południa, jaka jest jego ulubiona maskotka i jakie bajki najbardziej lubi oglądać. Czy takie dane nie wystarczą, żeby wzbudzić zaufanie dziecka i przy nadarzającej się okazji spróbować je wykorzystać…?

Uważajcie na to, co udostępniacie w sieci. Jak zwykle kluczowy jest umiar i zdrowy rozsądek. Co to oznacza? Mamy dla Was kilka wskazówek:

- Przede wszystkim: zwróćcie uwagę na ustawienia prywatności. Jeśli publikujecie w mediach społecznościowych osobiste informacje, choćby zdjęcia z wakacji – ograniczcie ich widoczność tylko do grona znajomych. W przeciwnym razie każdy będzie mógł je zobaczyć.
- Zastanówcie się dwa razy. Zadajcie sobie pytania: Czy na pewno chcę opublikować to zdjęcie? Czy chciałoby tego moje dziecko, które jest na nim obecne? Czy mam potrzebę podzielenia się z innymi tym materiałem? A jeśli tak – to z czego ona wynika? Pamiętajcie – mniej znaczy więcej. Z pewnością docenią to również Wasi znajomi. Fajnie wiedzieć, co u kogoś słychać, ale nadmiar tej wiedzy potrafi zmęczyć.
- Uważajcie na dane wrażliwe. Zdarzają się sytuacje, w których ktoś wrzuca do sieci zdjęcie czy film, na którym widać np. numer jego karty kredytowej czy dowodu. Najczęściej oczywiście dzieje się to zupełnie przypadkowo, ale konsekwencje mogą być poważne.
- Rozmawiajcie na ten temat z innymi – jeśli Wasze dziecko wyjeżdża na wakacje i korzysta już z mediów społecznościowych, zwróćcie mu uwagę na potencjalne zagrożenia związane z oversharingiem. A może to ktoś dorosły z Waszego otoczenia potrzebuje takiej rozmowy i wiedzy? Nie bójcie się o tym mówić, jeśli uznacie, że przekracza granicę.

Źródło:

„Zadbaj o siebie z OSE: oversharing”, (2024), artykuł na stronie ose.gov.pl.

P

Pan European Game Information (PEGI)

Gry cyfrowe mogą być doskonałą rozrywką. Co więcej, dobrze dobrana gra będzie treningiem dla mózgu, pozwoli zdobyć liczne umiejętności i wiedzę z wielu dziedzin. Pomoże rozwijać zdolności poznawcze i kompetencje społeczne oraz kształtować kreatywność. Grając w gry, uczymy się podejmowania decyzji i rozwiązywania skomplikowanych problemów, budujemy poczucie własnej skuteczności, uczymy się, jak radzić sobie z niepowodzeniem. Nie mówiąc o ćwiczeniu spostrzegawczości, motoryki, czy powtarzaniu obcojęzycznych słówek! Wymienione korzyści są istotne zwłaszcza wtedy, gdy szukamy odpowiedniej gry dla swojego dziecka. Czym się kierować?

Istotną podpowiedzią są wskazania ogólnoeuropejskiego systemu klasyfikacji gier PEGI (Pan-European Game Information). Pamiętajcie jednak, że rating PEGI podaje jedynie informację, czy gra jest właściwa dla danego wieku, nie uwzględnia natomiast poziomu jej trudności – jako PEGI 3 może być oceniona np. trudna gra ekonomiczna, ponieważ nie zawiera treści nieodpowiednich dla dzieci.

W systemie PEGI znajdziecie dwa rodzaje informacji: oznaczenia wiekowe (w sumie pięć) oraz deskryptory treści, czyli oznaczenia zawartości gry (łącznie osiem). W wersjach pudełkowych te pierwsze znajdują się na opakowaniu gry z obu stron, natomiast drugie – z tyłu.

Oznaczenia wiekowe w systemie PEGI:

- PEGI 3: gra odpowiednia dla wszystkich grup wiekowych. Nie powinna zawierać treści, języka lub sytuacji, które mogą przestraszyć dziecko. Może występować w niej pewna ilość przemocy (w komicznym lub dziecięcym kontekście).
- PEGI 7: gra może zawierać dźwięki lub sceny mogące przerazić młodsze dzieci. Dopuszczalne są bardzo łagodne formy przemocy (niedosłowne, nieprzedstawione szczegółowo, nierealistyczne).
- PEGI 12: w takich grach może być pokazana przemoc wobec postaci fantastycznej nieco bardziej dosłownie i/lub przemoc wobec postaci o ludzkim wyglądzie. Mogą pojawić się wulgaryzmy o łagodnym charakterze lub elementy nagości. Obecne mogą być również gry hazardowe, które w rzeczywistości są rozgrywane w kasynach lub punktach gier (np. gry karciane, w które w rzeczywistości gra się na pieniądze).
- PEGI 16: sceny przemocy lub seksualne wyglądają w tych grach tak jak w rzeczywistości. Gry mogą zawierać bardziej rażące wulgaryzmy, treści o grach losowych, paleniu tytoniu, piciu alkoholu lub zażywaniu narkotyków.
- PEGI 18: gry przeznaczone wyłącznie dla dorosłych. Poziom przemocy jest daleko posunięty, gry mogą pokazywać zabijanie bez oczywistego motywu lub przemoc wobec bezbronnych postaci. Do tej kategorii zalicza się również gry gloryfikujące zażywanie narkotyków i pokazujące dosłownie sceny seksualne.

Deskryptory treści w systemie PEGI:

- Violence (Przemoc): gra zawiera sceny przemocy. Mogą być one przedstawione bez szczegółów i w nierealistyczny sposób (PEGI 7), zawierać przemoc w fantastycznym otoczeniu lub nierealistyczną przemoc wobec postaci o ludzkim wyglądzie (PEGI 12). Gry oznaczone PEGI 16 i PEGI 18 zawierają zdecydowanie bardziej realistyczne obrazy przemocy.
- Bad language (Wulgarny język): gra zawiera wulgaryzmy. W PEGI 12 mają one łagodniejszy charakter, w PEGI 16 i PEGI 18 są dosadne, odwołują się do seksu lub bluźnierstwa.
- Fear (Strach): gra zawiera obrazy lub dźwięki, które mogą przestraszyć dzieci (PEGI 7) lub budzić grozę, nie prezentuje jednak treści wskazujących na przemoc (PEGI 12).

P

- Gambling (Hazard): w grze znajdują się elementy zachęcające do gier hazardowych lub objaśniające ich zasady. Zawiera ona symulacje losowych gier hazardowych, w które w rzeczywistości można zagrać na pieniądze w kasynie lub punkcie gier (PEGI 12, PEGI 16, PEGI 18).
- Sex (Treści seksualne): gra ukazuje pozy seksualne lub zawiera odwołania do seksu (PEGI 12), występuje w niej nagość o charakterze erotycznym lub stosunek płciowy z niewidocznymi organami płciowymi (PEGI 16) czy dosłowna aktywność seksualna (PEGI 18). Sceny nagości bez kontekstu seksualnego nie wymagają specjalnego ratingu wiekowego, a deskryptor nie jest wówczas konieczny.
- Drugs (Używki): gra odnosi się do zażywania narkotyków, picia alkoholu, palenia tytoniu lub pokazuje takie czynności. Gry z tego rodzaju deskryptorem noszą zawsze znaki PEGI 16 lub PEGI 18.
- Discrimination (Dyskryminacja): gra zawiera sceny ze stereotypami (o charakterze etnicznym, religijnym, nacjonalistycznym i in.), które mogą nawoływać do nienawiści. Takie treści są zawsze opatrzone znakiem PEGI 18 (i mogą stanowić naruszenie krajowych przepisów prawa karnego).
- In-game purchases (Zakupy w grze): w 2018 r. PEGI wprowadziło oznaczenie informujące o zawartych w grze mikropłatnościach (możliwość zakupu walut premium, subskrypcji, lootboxów, poziomów bonusowych, przepustek sezonowych i innych płatnych udogodnień).

Już na samym początku przygód młodego gracza w wirtualnym świecie powinniście zadbać o szczerą rozmowę i ustalenie reguł zdrowego grania. Pozwoli to m.in. na wypracowanie egzekwowalnych w przyszłości zasad, a także ukierunkuje na tytuły dostosowane do wieku dziecka.

Źródło:

Witkowska M., (2023), „Nastolatki i gry cyfrowe”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Password spraying

Używacie przewidywalnych, łatwych do odgadnięcia haseł? Uwaga, możecie być narażeni na password spraying!

To atak polegający na wykorzystaniu przez cyberprzestępców popularnego hasła w celu uzyskania dostępu do wielu Waszych kont: e-mailowych, założonych w bankowości elektronicznej czy sklepach online. Password spraying to dość częsty sposób działania oszustów, ponieważ – niestety – wiele osób zapomina o zasadach tworzenia silnych i bezpiecznych haseł.

Słabe, nieprzemyślane zabezpieczenia to problem wielu użytkowników sieci. Zespół ekspertów z CERT Polska po przenalizowaniu haseł, które wyciekły, stwierdził, że ponad połowa z nich była złożona maksymalnie z ośmiu znaków. Ponadto do tworzenia haseł używano głównie imion lub popularnych zwrotów typu „misiek” czy prostych schematów klawiatury komputera, np. „123qwe” (CERT Polska, 2022). Łatwo się domyślić, czym grozi zastosowanie słabych haseł – i to na kilku lub wszystkich kontach. Cyberprzestępcy bez trudu mogą uzyskać do nich dostęp!

Koniecznie podejmijcie działania, które zminimalizują ryzyko ataku. Przede wszystkim zadbajcie o odpowiednie zabezpieczenie cyfrowych danych. Rekomendacje CERT Polska w zakresie tworzenia silnych haseł zawierają np. zalecenie, by szyfry miały min. 14 znaków i były łatwe do zapamiętania dla nas, ale trudne do odgadnięcia przez potencjalnych przestępców.

Zanim utworzycie swoje hasło, zapoznajcie się z listą najpopularniejszych haseł opublikowaną przez CERT Polska i wystrzegajcie się jak ognia podanych tam propozycji. A jeśli macie problem z wymyśleniem i zapamiętaniem swoich danych logowania, używajcie generatorów haseł i menedżerów haseł.

Wasze bezpieczeństwo zostanie wzmocnione także dzięki:

- Stosowaniu uwierzytelniania dwuskładnikowego (ang. *Two Factor Authenticaton*, 2FA) – dodatkowy kod przesłany SMS-em czy za pośrednictwem aplikacji lub zabezpieczenie biometryczne sprawią, że Wasze dane będą bardzo trudne do przejęcia przez cyberprzestępców.
- Częstemu sprawdzaniu, czy Wasze hasła nie wyciekły, np. na stronie bezpiecznedane.gov.pl. Jeśli tak się stanie, bezzwłocznie zmieńcie dotychczasowe dane logowania, w tym również hasła pokrewne, które łatwo zgadnąć.
- Świadomości zagrożeń takich jak phishing – warto znać sztuczki socjotechniczne stosowane przez przestępców, żeby przez nieuwagę lub pod wpływem emocji nie udostępnić innym swoich danych logowania.
- Dbaniu o bezpieczeństwo swoich urządzeń, przede wszystkim wykonywaniu aktualizacji systemu operacyjnego, oprogramowania antywirusowego czy przeglądarki internetowej. Każda aktualizacja usuwa błędy i luki w zabezpieczeniach.

Więcej praktycznych porad znajdziecie na ose.gov.pl w aktualnościach „Bezpieczni w sieci z OSE: bezpieczne logowanie" i „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe". Sprawdźcie też rekomendacje CERT Polska dotyczące tworzenia silnych i bezpiecznych haseł.

Źródło:

„Co wycieki danych mówią o hasłach", (2022), artykuł na stronie cert.pl.

Patotreści

Współczesna młodzież spędza coraz więcej czasu w internecie, który stał się nie tylko źródłem wiedzy, ale także przestrzenią do rozrywki. Niestety, z dynamicznie rozwijającą się kulturą online pojawiają się także patotreści – szokujące i często niebezpieczne materiały, które zdobywają popularność wśród młodych ludzi. Rozprzestrzeniają się poprzez platformy streamingowe i social media, pokazują kontrowersyjne i nierzadko nielegalne zachowania, którym ich autorzy nadają pozory zabawy. Dla wielu nastolatków twórcy takich materiałów stają się idolami, a ich skandaliczne postawy mogą wpływać na postrzeganie norm społecznych i moralnych.

Psychologowie wskazują na kilka kluczowych mechanizmów, które sprawiają, że patotreści stają się atrakcyjne dla młodych ludzi. Przede wszystkim młody mózg jest bardzo wrażliwy na bodźce, zwłaszcza te związane z silnymi emocjami. Patotreści często szokują, budzą kontrowersje, a to przykuwa uwagę młodzieży bardziej niż tradycyjna rozrywka. W tego typu materiałach pojawiają się elementy przekraczania granic, łamania norm społecznych, co przyciąga szczególnie nastolatków znajdujących się w okresie rozwojowym, w którym dominują naturalna impulsywność, testowanie norm, skłonność do eksperymentowania i bunt wobec zastałych autorytetów. Nie bez znaczenia jest tu także presja rówieśnicza.

Choć nie każdy młody człowiek ulegnie wpływowi patoinfluencerów, należy mieć świadomość, że kontakt z nimi może wywoływać negatywne efekty. Jednym z najbardziej niepokojących następstw jest obniżenie wrażliwości na przemoc i cierpienie innych. Młodzi ludzie regularnie oglądający patotreści mogą stopniowo tracić zdolność do empatii. Przemoc, której są świadkami, zostaje znormalizowana, a agresja i inne niebezpieczne bądź szkodliwe zachowania przestają budzić takie emocje jak wcześniej. Kolejnym poważnym skutkiem jest zmiana podejścia do relacji międzyludzkich. Patotreści często promują toksyczne wzorce, w tym poniżanie innych, namawianie do szkodliwych działań, a także pokazują treści obrazujące przemoc, obrażenia fizyczne, okrucieństwo wobec zwierząt. Relacje międzyludzkie bazujące na wzajemnym szacunku ustępują tutaj miejsca schematom opartym na wykorzystywaniu słabości innych osób. Może to prowadzić do problemów w relacjach z rówieśnikami, a także w przyszłych związkach osobistych.

Jak zatem reagować, gdy widzimy, że dziecko ogląda relacje patoinfluencerów? Jeśli doszło przypadkiem do kontaktu dziecka ze szkodliwymi materiałami i odczuwa ono dyskomfort

w związku z treściami, które zobaczyło na ekranie, powinniśmy mu pomóc poradzić sobie z silnymi emocjami. Należy otoczyć je opieką, wysłuchać, okazać wsparcie i przede wszystkim: nie oceniać. Trzeba mieć świadomość, że niektóre szkodliwe treści mogą być dla młodych internautów bardzo ciekawe i ekscytujące. Zamiast krytykować, lepiej tłumaczyć, że to, co oglądamy w internecie, często ma niewiele wspólnego z prawdziwym życiem. Jeśli wiemy, że nasze dziecko lub uczeń intencjonalnie sięga po patoreści, rozmawiajmy z nim o tym, czym naprawdę są te pseudozabawne filmiki. Budujmy świadomość wśród młodych ludzi, że tego rodzaju materiały promują przemoc i są źródłem krzywdy innych ludzi – nie tylko tych, którzy w nich występują, ale także tych, którzy je oglądają. Wyrażajmy wyraźną niezgodę na agresję i przemoc promowane w takich materiałach.

Nie wszystkie szkodliwe treści są nielegalne. Istnieją jednak materiały, takie jak obrazy przedstawiające wykorzystywanie seksualne dzieci, których wytwarzanie, przechowywanie i upowszechnianie jest karalne. Takie należy zgłaszać na policję. Można skorzystać też ze wsparcia ekspertów z zespołu Dyżurnet.pl.

Źródło:

Borkowska A., Witkowska M., Gańko K., (2025), „O cyberprzemocy i hejcie w sieci", Warszawa: Państwowy Instytut Badawczy NASK.

Pętla dopaminowa

Trudno dziś wyobrazić sobie funkcjonowanie bez internetu i urządzeń cyfrowych. Technologia pomaga nam w nauce, pracy, załatwianiu spraw urzędowych, komunikacji, jest też źródłem rozrywki. I choć po całym dniu korzystania z urządzeń cyfrowych niejednokrotnie czujemy przesyt ekranów, na koniec dnia chętnie dalej angażujemy się w świat online.

Zastanawialiście się, dlaczego tak trudno jest Wam oderwać się od przeglądania mediów społecznościowych, śledzenia komentarzy i reakcji na dany wpis? Skąd bierze się chęć korzystania bez końca z gier online czy potrzeba oglądania kolejnego odcinka serialu na platformie streamingowej? Dlaczego googlujecie informacje nawet długo po tym, jak znaleźliście odpowiedź na nurtujące Was pytanie? To w dużej mierze wina dopaminy!

Dopamina to neuroprzekaźnik, który odpowiada za odczuwanie przyjemności i wzmacnianie motywacji do sięgania po bodźce, które sprawiają, że dostaniecie oczekiwaną nagrodę, czyli poczujecie się dobrze. Na nieszczęście internet i urządzenia cyfrowe uaktywniają ośrodek nagrody w mózgu, a kiedy robicie coś, co sprawia Wam radość, wydziela się dopamina. To ona zatrzymuje Was przy urządzeniu.

Po „szot" z dopaminy możemy sięgnąć o każdej porze dnia, w dowolnym miejscu i to bez żadnego wysiłku – wystarczy włączyć urządzenie z dostępem do sieci, by zapewnić sobie dodatkową stymulację. Nasz mózg szybko zapamiętuje czynności, które są źródłem satysfakcji, a my chętnie je powtarzamy, by jeszcze raz poczuć się dobrze, czyli uwolnić kolejny wyrzut dopaminy. W ten sposób uruchamiamy pętlę dopaminową w układzie nagrody.

Z dopaminą (podobnie jak z alkoholem i narkotykami) nie ma żartów. Pod jej wpływem łatwo przebodźcować mózg, który z czasem będzie potrzebował coraz więcej stymulacji, by znów wprawić nas w dobry nastrój. Stąd pojawia się wewnętrzny przymus, by spędzać w sieci coraz więcej czasu.

Jak wyjść z błędnego koła nadużywania nowych technologii? Warto dbać o higienę cyfrową – już od najmłodszych lat. W tym przypadku sprawdzi się metoda małych kroków. Spróbujcie stopniowo wprowadzać w swoje życie – ale też w życie domowników, przyjaciół (w grupie raźniej!) – pozytywne nawyki korzystania z urządzeń. Wyznaczcie w domu strefy bez smartfona, nie korzystajcie z telefonów podczas posiłków, przed snem, stawiajcie sobie wyzwania (offline challenge – odłączcie się od sieci na 48 godzin). Planujcie też aktywności poza internetem. Starajcie się odpoczywać od urządzeń cyfrowych tak często, jak to możliwe.

Więcej porad, w jaki sposób uzyskać równowagę online–offline znajdziecie na ose.gov.pl w wywiadzie „5 pytań o… równowagę cyfrową”. Skorzystajcie też z naszych bezpłatnych kursów e-learningowych: „Zrozumieć FOMO” – kurs dla dorosłych, dostępny na naszej platformie OSE IT Szkoła oraz „Cyfrowa higiena, nadużywanie internetu oraz nowych technologii” – kurs dla nauczycieli i uczniów klas, dostępny na platformie bezpieczniwsieci.edu.pl. Ponadto polecamy nasze publikacje dotyczące higieny cyfrowej: poradnik „Offline znaczy zdrowiej. O cyfrowej higienie dla rodziców i wychowawców” i „Mniej znaczy więcej. O multiscreeningu i wielozadaniowości” oraz zbiór felietonów „O cyfrowej higienie” – do pobrania na OSE IT Szkole.

Phishing

Nazwa wydaje się Wam znajoma? I słusznie – termin phishing budzi dźwiękowe skojarzenie z angielskim słowem fishing oznaczającym łowienie ryb. Na tym jednak podobieństwo się nie kończy… Cyberprzestępcy podobnie do wędkarzy przygotowują odpowiednią przynętę, na którą usiłują złapać swoje potencjalne ofiary. Celem takich działań jest wyłudzenie poufnych danych – najczęściej logowania do serwisów społecznościowych lub bankowości elektronicznej.

Podczas ataku oszust stara się wprowadzić nas w błąd i przekonać do wykonania określonej czynności: otwarcia zainfekowanego załącznika, kliknięcia w złośliwy link, zalogowania się w oknie fałszywej strony (np. bramki do płatności elektronicznych) lub pobrania dodatkowego oprogramowania. Aby osiągnąć swój cel, próbuje skontaktować się z ofiarą, wykorzystując specjalnie przygotowane e-maile, SMS-y, wiadomości na komunikatorach i portalach społecznościowych. Do oszustwa może też dojść za pośrednictwem rozmowy telefonicznej, podczas której przestępca podszywa się pod pracowników instytucji zaufania publicznego lub innego użytkownika. Jeśli podążycie za instrukcją oszusta, szybko możecie przekonać się, że straciliście środki z konta bankowego, ważne dane lub informacje.

Jak nie połknąć haczyka? Najważniejsze są ostrożność i rozsądne podejście do otrzymywanych wiadomości. Pamiętajcie, że oszuści mogą podszywać się pod Waszych znajomych, zaufane instytucje czy firmy, z których usług korzystacie na co dzień. Waszą podejrzliwość powinna wzbudzić m.in. treść nakłaniająca do szybkiego i nieprzemyślanego działania lub udostępnienia wrażliwych danych, gdyż w przeciwnym wypadku wydarzy się coś złego (np. konto zostanie zablokowane) lub stracicie niepowtarzalną okazję.

Cyberprzestępcy wykorzystujący phishing często nie potrzebują zaawansowanej wiedzy technicznej, by przeprowadzić atak. Zamiast tego grają na emocjach, liczą na naszą nieuwagę, pośpiech lub brak wiedzy o powszechnych cyberzagrożeniach. Jak nie dać się oszukać?

- Zwracajcie uwagę, jak zaczyna się wiadomość. Jeśli nadawca zwraca się do Was ogólnie, np. „Szanowny Kliencie” lub „Witaj!”, może to być sygnał ostrzegawczy.
- Sprawdzajcie też adres e-mail nadawcy – jeśli nadawca podaje się za pracownika znanej firmy lub instytucji, ale w jego adresie widnieje ogólnodostępna domena, np. @gmail.com, @wp.pl czy @hotmail.com, zachowajcie ostrożność.
- Czerwona lampka powinna się też zapalić, gdy ktoś pyta Was o dane, do których teoretycznie powinien mieć dostęp, np. rzekomy pracownik banku dopytuje o numer konta. Pamiętajcie też, że nikt nie ma prawa żądać od Was podania poufnych informacji, takich jak numer karty płatniczej czy hasło.
- Przyjrzyjcie się uważnie treści wiadomości – błędy językowe, dziwne sformułowania czy nieudolne tłumaczenie mogą świadczyć o próbie oszustwa. Miejcie jednak na uwadze fakt, że dziś praktycznie każdy – dzięki dostępności narzędzi wykorzystujących sztuczną inteligencję – może napisać poprawną wiadomość, która nie wzbudzi większych podejrzeń.
- Niebezpieczne bywają również wiadomości, np. z prośbą o kod BLIK, które wyglądają, jakby pochodziły od znajomego. Bądźcie czujni, być może jego konto w mediach społecznościowych zostało przejęte przez przestępców. Jeśli coś nasuwa pytania lub sugeruje oszustwo – zadzwońcie i upewnijcie się, że to faktycznie znajomy próbował się z Wami skontaktować.

- Zawsze sprawdzajcie adres strony internetowej. Nawet drobna różnica – literówka, dodatkowy znak czy inna końcówka domeny – może oznaczać, że jesteście na fałszywej stronie.

Dostaliście podejrzaną wiadomość SMS lub trafiliście na stronę banku lub sklepu, która łudząco przypomina tę oryginalną? Natychmiast zgłoście to do CERT Polska! Wypełnijcie formularz internetowy dostępny na stronie cert.pl lub prześlijcie otrzymany SMS na numer 8080, używając funkcji „przekaż" albo „udostępnij". Pamiętajcie, nie musicie mieć stuprocentowej pewności, że to próba oszustwa, wystarczy, że nabierzecie podejrzeń. Wszystko sprawdzą za Was eksperci zajmujący się cyberbezpieczeństwem.

Dzięki Waszym zgłoszeniom niebezpieczne domeny zamieszczane są na liście ostrzeżeń przed niebezpiecznymi stronami, tym samym blokowana jest możliwość wejścia na stronę wykorzystywaną do wyłudzenia danych czy pieniędzy. Z kolei wszystkie podejrzane SMS-y służą do tworzenia wzorców niebezpiecznych wiadomości, które będą blokowane przez operatorów, by finalnie nie trafiały do użytkowników.

Warto reagować na wszelkie próby oszustwa – w ten sposób chronicie nie tylko siebie, ale też innych internautów!

Więcej na temat ochrony przed phishingiem dowiecie się z biuletynu „OUCH! – Powstrzymać phishing" oraz aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: phishing", „Bezpieczni w sieci z OSE: kampanie phishingowe w 2024 roku". Na młodszych uczniów czeka zaś na platformie OSE IT Szkoła kurs e-learningowy „Krasnoludki 2.0 – Phishing, czyli kłopoty to nasza specjalność".

Phubbing

Jak często prosicie dziecko lub ucznia o odłożenie telefonu i skupienie się na rozmowie czy lekcji? A może sami macie problem z rozstaniem się ze smartfonem nawet podczas rozmowy lub to właśnie Wy zostaliście zignorowani przez kogoś, kto nie może oderwać wzroku od ekranu urządzenia? Takie zachowanie to phubbing.

Termin ten powstał z połączenia angielskich słów phone (telefon) i snubbing (lekceważenie, odtrącenie). Odnosi się do sytuacji, w której ktoś jest tak skoncentrowany na swoim smartfonie, że podczas spotkania z innymi osobami po prostu je lekceważy. W takich przypadkach potrzeba korzystania ze smartfona jest niestety silniejsza od przestrzegania zasad dobrego wychowania, a czasem nawet… własnego bezpieczeństwa!

Częste spoglądanie na ekran urządzenia wiąże się z FOMO (ang. *Fear Of Missing Out*) – lękiem przed odłączeniem, wypadnięciem z obiegu, gdy akurat nie jesteśmy online. Pojawiające się poczucie niepokoju, związane z brakiem wiedzy o tym, co w danej chwili robią nasi znajomi, rodzi potrzebę ciągłego sprawdzania mediów społecznościowych i reagowania na każdy sygnał powiadomienia. To właśnie osoby z wysokim FOMO phubbują najmocniej.

FOMO dzieli już tyko krok do fonoholizmu – nałogowego korzystania z telefonu. To stan, w którym nie możemy normalnie funkcjonować bez smartfona. Urządzenie towarzyszy nam zawsze i o każdej porze dnia i nocy. Gdy znika z zasięgu wzroku, pojawia się niepokój, irytacja, a nawet atak paniki.

Aby zaradzić phubbingowi, warto wprowadzić kilka zdrowych, cyfrowych nawyków. Ważne, by stosowali się do nich wszyscy domownicy.

- **Posiłki bez smartfona.** Umówcie się, że przy stole nie używacie telefonów. Najlepiej jest zostawić urządzenie w innym pokoju. Kto sięgnie po smartfon podczas posiłku, ten zmywa!
- **Strefy offline.** Wyznaczcie w domu strefy na odkładanie i ładowanie urządzeń. Pozbądźcie się też nawyku noszenia telefonu przy sobie.
- **Zabawa bez ekranów.** Ekrany rozpraszają, dlatego podczas wspólnej rozrywki odłóżcie telefony na bok i wyciszcie powiadomienia.

- **Limity czasowe.** Ustalcie, ile czasu dziennie spędzacie przed ekranem urządzenia, i przestrzegajcie tego limitu.
- **Być tu i teraz.** Załóżcie, że wspólnie spędzany czas to okazja do rozmów, planowania rodzinnych zajęć, dzielenia się przeżyciami i emocjami – bez patrzenia w ekran smartfona.
- **Walka z nudą.** Nuda to sprzymierzeniec phubbingu. Zadbajcie więc o ciekawe i rozwijające dziecko aktywności offline. Może to być zabawa na świeżym powietrzu, wyprawa do parku, kina lub teatru.

Źródło:

„Tylko zerknę. Sprawdź, czy Twoje dziecko doświadcza phubbingu", (2021), artykuł na stronie ose.gov.pl.

Pliki cookie

„Ta strona korzysta z plików cookie, aby poprawić komfort użytkowania. Zakładamy, że nie masz nic przeciwko, ale możesz zrezygnować, jeśli chcesz" – taki lub podobny komunikat wita nas za każdym razem, gdy wchodzimy na nową (dla naszej przeglądarki) stronę internatową. Akceptujecie politykę cookie bez czytania czy zgadzacie się tylko na niezbędne „ciasteczka"? Czym w ogóle są pliki cookie?

Najprościej rzecz biorąc, cookies (HTTP cookies, pliki cookie lub w tłumaczeniu z języka angielskiego – ciasteczka) to nieduże pliki tekstowe, generowane przez serwer internetowy oraz wysyłane do używanej przeglądarki, gdzie są przechowywane i wykorzystywane podczas kolejnych sesji. W jakim celu?

- Właściciele witryn używają plików cookies w celu usprawniania działania stron internetowych.
- Ciasteczka pomagają „zapamiętywać" informacje o naszych wcześniejszych wizytach na danych stronach, by ułatwić i uprzyjemnić nam późniejsze korzystanie z portalu, e-sklepu czy forum (np. nie musimy już wybierać preferowanego języka lub innych ustawień).
- Pliki cookie mogą być wykorzystywane także do dostarczania reklam dostosowanych do naszych preferencji, zainteresowań i/lub poprzednich wyszukiwań.

To wciąż nie wszystko! Ciasteczka ułatwiają Wam także logowanie – pozwalają bowiem na zapisywanie loginów i haseł – oraz umożliwiają automatyczne uzupełnianie formularzy (zapamiętują wpisywane uprzednio adresy i inne dane kontaktowe). Dzięki plikom cookie możecie „porzucić" na chwilę koszyk z zakupami i po czasie dokończyć transakcję lub zrezygnować z niechcianych produktów. Cookies przydają się także właścicielom stron internetowych, m.in. do sprawdzenia, jak użytkownicy korzystają z serwisu (np. które strony odwiedzają, jak długo na nich pozostają).

Być może zastanawiacie się, czy ciasteczka nie zagrażają Waszemu bezpieczeństwu. Chociaż z reguły cookies są nieszkodliwe, trzeba pamiętać o tym, że od każdej reguły istnieją wyjątki. Uważajcie przede wszystkim wtedy, gdy logujecie się do banku, poczty elektronicznej czy na inne ważne konta za pomocą cudzych lub ogólnodostępnych sprzętów – oszuści mogą wykorzystać niezakończoną sesję i uzyskać dostęp do Waszych prywatnych zasobów. Aby temu zapobiec, korzystajcie z trybu incognito lub usuwajcie zapisane pliki cookies – taką opcję znajdziecie w tej samej zakładce co usuwanie historii przeglądania. Pamiętajcie też, że możecie zablokować dostęp do plików cookies stronom, które uznajecie za niezaufane.

Nie musicie z kolei martwić się tym, że Wasze pliki cookie będą wykorzystywane przez witryny, których nie odwiedzaliście – z tych danych (jedynie w celach informacyjnych, statystycznych i reklamowych) może korzystać tylko właściciel danej strony. Warto jednak wiedzieć, że choć plików cookies nie można używać np. do uruchomienia malware (złośliwego oprogramowania), to mogą je wykorzystywać programy zainstalowane na Waszych urządzeniach. Czy trzeba się zatem

bać ciasteczek? Pliki cookies same w sobie są bezpieczne, jednak dobrze traktować je jak wszystko w internecie – bez pełnego zaufania. Nie zaszkodzi od czasu do czasu usuwać je w przeglądarce na komputerze i w telefonie. Pomoże to jeszcze lepiej zadbać o Waszą prywatność w sieci. Jeśli przed wejściem na daną stronę internetową pojawi się komunikat z prośbą o akceptację plików cookies (lub polityki cookies, polityki prywatności), przeczytajcie go i zdecydujcie, czy chcecie udostępniać wszystkie opisane tam informacje. W większości przypadków obsługa ciasteczek jest konieczna, by w pełni korzystać z funkcjonalności danego konta czy witryny.

Płatności biometryczne

Często zapominamy, jak żyło nam się bez szybkich płatności. Transakcje online to nie wszystko: w wielu sklepach zapłacimy już BLIK-iem albo za pomocą urządzenia ubieralnego (ang. *wearables*), np. zegarka czy opaski płatniczej obsługujących moduł NFC (ang. *Near Field Communication*, komunikacji bliskiego zasięgu). Czy transakcje mogą być jeszcze łatwiejsze? Okazuje się, że tak!

Jedną z nowszych i prężnie rozwijających się możliwości są płatności biometryczne, które umożliwiają dokonywanie transakcji na podstawie analizy unikalnych cech użytkownika. Brzmi jak science fiction? Nic bardziej mylnego. Z ulotki „Płatności biometryczne" opracowanej przez CERT Polska dowiadujemy się, że obecnie podczas transakcji możemy korzystać z:

- urządzeń do rozpoznawania twarzy (np. technologii FaceID używanej w smartfonach);
- urządzeń do rozpoznawania głosu (dokonywanie operacji finansowych umożliwia wbudowany np. w smartfony asystent głosowy);
- skanerów linii papilarnych (dostępnych nie tylko w telefonach czy laptopach, ale też bezpośrednio na kartach płatniczych wyposażonych w czujniki do odczytywania wzorca biometrycznego palca właściciela);
- skanerów tęczówki (np. technologia PayEye);
- skanerów do mapowania żył w palcu (np. technologia Payvein).

Czy takie rozwiązania są bezpieczne? Czy nie musimy obawiać się tego, że nasze dane biometryczne są przechowywane w pamięci urządzeń lub bazach danych? Warto wiedzieć, że linie papilarne, obrazy oka czy naczyń krwionośnych są zaszyfrowane i do dostawców usług trafia jedynie liczba odzwierciedlająca daną cechę. Do weryfikacji tożsamości klienta służy więc ten zaszyfrowany numer, a nie faktyczny odcisk palca czy skan tęczówki. Można więc uznać, że płatności biometryczne – podobnie jak zabezpieczenia wykorzystujące fizyczne cechy użytkowników – są tak bezpieczne, jak powiązane z nimi bazy danych.

Korzystając z nowych form płatności – płatności internetowych lub biometrycznych – musicie pamiętać, że najważniejszą metodą ochrony jest zdrowy rozsądek. Jeżeli Waszą uwagę zwróci coś podejrzanego, nie finalizujcie transakcji. Wszystkie oszustwa zgłaszajcie do CERT Polska: za pośrednictwem formularza na stronie incydent.cert.pl, mailowo na adres incydent@cert.pl oraz SMS-em na numer 8080.

Źródło:

„Wystarczy jedno spojrzenie – płatności biometryczne", (2023), artykuł w serwisie bezpiecznymiesiac.pl.

Płatności internetowe

Pandemia COVID-19 zmieniła nasze zwyczaje zakupowe – to niezaprzeczalny fakt. Zamiast galerii handlowych coraz częściej wybieramy sklepy internetowe. Kieruje nami już nie tylko troska o bezpieczeństwo, ale też oszczędność i wygoda: korzystamy z darmowej dostawy, cieszymy się dużym wyborem produktów, łatwo porównujemy ceny i unikamy kolejek.

Kiedyś za zakupy mogliśmy płacić wyłącznie gotówką, dziś – w sklepach internetowych i nie tylko – tych możliwości mamy o wiele więcej:

- **BLIK**. To najszybszy i bardzo bezpieczny sposób na dokonanie płatności online. Wystarczy zainstalować na swoim telefonie aplikację banku, tam wygenerować 6-cyfrowy kod, wpisać go w odpowiednim miejscu podczas płatności, a następnie potwierdzić transakcję w aplikacji. Pieniądze za zakupy już po kilku chwilach trafią na konto sprzedającego!
- **Płatność kartą (debetową, kredytową)**. Wybierając tę opcję, zostaniecie poproszeni o uzupełnienie danych z karty (imię i nazwisko właściciela, numer karty, data jej ważności i kod zabezpieczający CVV/CVC). Następnym krokiem będzie autoryzacja za pomocą kodu otrzymanego SMS-em z banku lub aplikacji mobilnej. Transakcje kartą są dodatkowo zabezpieczone obciążeniem zwrotnym (chargeback).
- **Tradycyjny przelew internetowy**. Tej metody płatności zapewne nikomu nie trzeba przedstawiać – aby zapłacić za zakupy, przelewacie określoną sumę na numer konta podany przez sprzedającego. Pamiętajcie jedynie, by wybierać przelew tylko w przypadku zaufanych sklepów.
- **E-przelew (PayU, Dotpay)**. Ten wygodny typ transakcji obsługują zewnętrzni dostawcy. Korzystając z takich płatności, możemy mieć pewność, że są odpowiednio szyfrowane, a przekazywane dane – bezpieczne. Kolejną zaletą e-przelewów jest czas ich realizacji: są wykonywane natychmiastowo, także w weekendy.
- **Wirtualny portfel (PayPal)**. Aby skorzystać z takiego elektronicznego portfela, najpierw musicie zasilić go środkami. Dzięki temu podczas transakcji nie trzeba już podawać danych karty kredytowej/debetowej czy logować się do swojej bankowości elektronicznej. Ta metoda jest w pełni bezpieczna – nie musicie się obawiać ani o swoje pieniądze, ani dane osobowe.
- **Płatność odroczona** (ang. *deferred payment*). Obecnie coraz częściej możecie skorzystać także z opcji „kup teraz, zapłać później", dostępnej w wielu sklepach i serwisach aukcyjnych. Termin zapłaty za kupiony towar można przesunąć nawet o 30 dni.
- **Płatności cykliczne (rekurencyjne)**. Macie z nimi do czynienia w różnych serwisach (np. streamingowych), w których zdecydowaliście się na subskrypcję. Zakładając konto, podajecie dane karty kredytowej i zgadzacie się, że w określonym terminie (najczęściej raz w miesiącu) będzie ona obciążana kwotą abonamentu.

Płatności internetowe z zasady można uznać za bezpieczne – banki i instytucje pośredniczące w płatnościach dbają o to, by transakcje przebiegały prawidłowo i nie narażały klientów na straty. Szyfrowanie płatności, wieloetapowa weryfikacja i inne metody zabezpieczeń mimo wszystko czasami okazują się niewystarczające. Wiele zależy też od Waszej czujności. O czym powinniście pamiętać, by nie zapłacić słono za własną nieuwagę?

- Nie otwierajcie załączników z podejrzanych e-maili i nie klikajcie bezrefleksyjnie we wszystkie linki znalezione w sieci.
- Robiąc przelew, zawsze dokładnie sprawdzajcie, czy poprawnie wpisaliście dane odbiorcy.
- Zwracajcie uwagę na powiadomienia o transakcjach, które wysyłają Wam aplikacje bankowe. Zanim je potwierdzicie, upewnijcie się, że podana kwota jest poprawna.
- Aby ustrzec się przed kradzieżą środków z konta, warto ustawić limity wysokości transakcji. Dzięki temu, gdy np. utracicie swoją kartę płatniczą, oszust nie będzie w stanie szybko przejąć wszystkich Waszych pieniędzy.
- Jeśli padliście ofiarą oszusta lub transakcja nie została rozliczona prawidłowo, możecie skorzystać z obciążenia zwrotnego. Wystarczy, że złożycie reklamację w banku, który wystawił Waszą kartę – kredytową lub debetową.

Więcej o bezpiecznych zakupach przeczytacie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: BLIK i płatności internetowe”, „Jak nie kupić kota w worku, czyli bezpieczne zakupy online” i „Bezpieczni w sieci z OSE: uwaga na okazje w Black Friday”.

Podatność bezpieczeństwa

Tak jak każdy ma swoją piętę achillesową, tak i systemy informatyczne miewają słabe punkty. To podatności, czyli luki w oprogramowaniu, które pozwalają cyberprzestępcom na wykonanie działań, których nie przewidział twórca danego programu, aplikacji lub urządzenia. Wykorzystanie takiej luki może mieć poważne skutki, jak choćby wyciek danych czy uzyskanie nieautoryzowanego dostępu do systemu przez oszusta, prowadzące np. do ingerencji w kod oprogramowania.

Z podatnościami nierozłącznie wiąże się też exploit, czyli program, który wykorzystuje istniejące błędy w oprogramowaniu i umożliwia atakującemu przejęcie kontroli nad urządzeniem.

Aby zapobiegać skutkom luk bezpieczeństwa (czyli mitygować ich ryzyko), musicie przede wszystkim czuwać nad tym, by systemy operacyjne i programy na urządzeniach, z których korzystacie, były aktualne. Jeżeli dostaniecie powiadomienie o nowej wersji systemu – natychmiast wykonajcie aktualizację. Najnowsze wersje oprogramowania zwykle naprawiają błędy zauważone np. w trakcie testów penetracyjnych, a tym samym skuteczniej chronią Was przed atakami!

Warto wiedzieć, że istnieje międzynarodowy program wspierający ujawnianie luk bezpieczeństwa w oprogramowaniu komputerowym – CVE, czyli Common Vulnerabilities and Exposures. Każdy, kto znajdzie podatność bezpieczeństwa, może zgłosić ją do CNA (CVE Numbering Authority): organizacji, które nadają CVE, służące identyfikacji i katalogowaniu publicznie ujawnionych podatności. Od sierpnia 2023 r. taką funkcję pełni także CERT Polska – jako jedyna instytucja w kraju i jeden z 7 CERT-ów w Europie.

Wspomniana baza CVE jest bezpłatna i dostępna dla wszystkich. Pomaga organizacjom z całego świata w rozpoznawaniu nowych luk bezpieczeństwa i informowaniu o ich wystąpieniu. Można ją znaleźć na stronie cve.mitre.org.

Jak zgłosić podatność? Najpierw należy skontaktować się bezpośrednio z właścicielem podatnego systemu lub dostawcą oprogramowania. Jeśli to niemożliwe, lukę należy zgłosić do CERT Polska/CSIRT NASK za pomocą formularza na stronie incydent.cert.pl.

Chcecie dowiedzieć się więcej o polityce zgłaszania podatności do CERT Polska i zasadach działania programu CVE? Zajrzyjcie na stronę cert.pl/cvd.

Podatność zero-day

W każdym systemie informatycznym, np. systemie operacyjnym czy aplikacji, możemy spotkać się z podatnością, czyli luką w oprogramowaniu, pozwalającą cyberprzestępcom na wykonanie działań nieprzewidzianych przez twórcę danego urządzenia czy programu.

Poważnym rodzajem podatności są luki zero-day (luki dnia zerowego), które nie są znane ani ogółowi społeczeństwa, ani autorom danych produktów, a co za tym idzie – nie zostały publicznie ujawnione i naprawione. Luki zero-day są więc tajną bronią w rękach oszustów!

Jako że nikt nie wie o niewykrytej podatności, nie ma sposobu, by się przed nią ustrzec: oprogramowanie antywirusowe oraz inne środki bezpieczeństwa „nie wiedzą”, że mają chronić użytkowników przed nowym zagrożeniem. Oszuści odnajdują takie luki, bo studiują kody źródłowe w poszukiwaniu usterek pozostawionych przez programistów. Gdy na takie trafią – przez krótki czas (dopóki podatność nie zostanie naprawiona dzięki tzw. łatce) mogą np. w najgorszym scenariuszu szpiegować osoby korzystające z danej aplikacji, wykradać ich dane lub powodować uszkodzenia ich urządzeń.

Niestety sami nie możecie chronić się przed podatnościami, w tym lukami zero-day. Ważne jednak, byście pamiętali, że bardzo przydatne okażą się tu Wasze… systematyczność i uważność.

- Pamiętajcie o regularnym aktualizowaniu systemu operacyjnego i oprogramowania, z którego korzystacie. Nie zwlekajcie z aktualizacją, gdy otrzymacie powiadomienie, że dostępna jest nowa wersja aplikacji czy programu!
- Instalujcie na swoich urządzeniach oprogramowanie antywirusowe i upewniajcie się, że używacie zawsze jego najświeższych wersji. Choć antywirus nie chroni przed zerodayem, to w przypadku upublicznienia takiej podatności na aplikację czy system, używany przez nas program antywirusowy może szybko zaktualizować bazy danych do zwalczania tego zagrożenia.
- Regularnie twórzcie backup, czyli kopie zapasowe swoich ważnych danych, i przechowujcie je w bezpiecznym miejscu – na dysku zewnętrznym lub w chmurze.

Więcej o podatnościach przeczytacie w aktualności na stronie ose.gov.pl – „Bezpieczni w sieci z OSE: podatności i luki bezpieczeństwa".

Polskie Centrum Programu Safer Internet (PCPSI)

W NASK aktywnie działamy na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii, m.in. jesteśmy koordynatorem projektu Polskie Centrum Programu Safer Internet. PCPSI zostało powołane w 2005 r. w ramach programu Komisji Europejskiej Safer Internet, a obecnie funkcjonuje jako element programu Digital Europe. Tworzymy je razem z Fundacją Dajemy Dzieciom Siłę.

Na działania PCPSI składają się trzy projekty:

1. Saferinternet.pl: projekt, w którym zwiększamy społeczną świadomość na temat zagrożeń w cyberprzestrzeni. Publikacje powstające w ramach projektu oraz organizowane konferencje kształtują kompetencje – dzieci, rodziców i profesjonalistów – w zakresie bezpiecznego korzystania z sieci. Z naszymi działaniami docieramy zarówno do młodszych (np. Sieciaki, Necio, Plik i Folder, Digital Youth), jak i starszych użytkowników internetu (np. Dzień Bezpiecznego Internetu, Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w internecie").
2. Pomoc telefoniczna i online: realizujemy ją poprzez Telefon zaufania dla dzieci i młodzieży (116 111) oraz Telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci (800 100 100). Eksperci Fundacji Dajemy Dzieciom Siłę za ich pośrednictwem reagują w przypadkach zagrożeń związanych z korzystaniem z internetu.
3. Dyżurnet.pl: to punkt kontaktowy, który prowadzimy w NASK. Możecie do niego anonimowo zgłaszać przypadki występowania w internecie nielegalnych treści, w tym materiałów przedstawiających seksualne wykorzystanie dzieci (formularz zgłoszeniowy na stronie dyzurnet.pl, tel.: 801 615 005, e-mail: dyzurnet@dyzurnet.pl).

Więcej informacji o działaniach w ramach PCPSI znajdziecie na stronie saferinternet.pl.

Problemowe używanie internetu (PUI)

Zastanawialiście się, kiedy korzystanie z internetu i urządzeń cyfrowych Wam służy, a kiedy działa na Waszą niekorzyść? Granica jest cienka, ale są pewne symptomy świadczące o tym, że złe nawyki cyfrowe wpływają negatywnie na Wasz dobrostan psychiczny i fizyczny, a zatem możecie się mierzyć z problemowym używaniem internetu (PUI).

PUI może dotknąć każdego użytkownika sieci. Przedstawiamy sześć symptomów problemowego używania internetu, na które zwrócił uwagę badacz Mark Griffiths już w 1996 r.:

- Dominacja – korzystanie z sieci staje się priorytetem codziennego funkcjonowania.
- Zmiana nastroju – korzystanie z internetu w celu poprawy samopoczucia.

- Zwiększona tolerancja – zwiększona potrzeba korzystania z sieci.
- Zespół abstynencyjny – pojawienie się rozdrażnienia, niepokoju, poirytowania w momencie ograniczenia dostępu do internetu.
- Konflikt – między użytkownikiem a rodziną, znajomymi lub obowiązkami szkolnymi.
- Nawroty – intensywne, niekontrolowane powracanie do problemowego korzystania ze świata wirtualnego.

Jak widać, problemem jest nie tylko zbyt duża ilość czasu spędzanego w sieci, choć tego czynnika nie należy bagatelizować. Wiadomo bowiem, że im dłużej przebywamy online, tym większa podatność na szkodliwe treści, ryzyko e-uzależnienia – od gier i hazardu online, mediów społecznościowych, zakupów online, smartfona (fonoholizm), również większe prawdopodobieństwo doświadczania przemocy w sieci czy cyberataków.

Jak nie wpaść w pułapkę problemowego używania internetu? Postawcie na profilaktykę, czyli wprowadzajcie zasady higieny cyfrowej. Na początek poczytajcie o popularnych cyberzagrożeniach – wiedza na ich temat pomoże Wam uniknąć wielu niebezpiecznych sytuacji online. Popracujcie też nad swoimi cyfrowymi nawykami: nie korzystajcie ze smartfonów podczas posiłku, spotkań towarzyskich, przed snem i zaraz po przebudzeniu. Stawiajcie przed sobą wyzwania (do zabawy zaproście najbliższych i znajomych – razem raźniej!) – spróbujcie np. nie zaglądać do mediów społecznościowych jednego popołudnia (wcześniej wyłączcie wszystkie powiadomienia). A może offline challenge i próba odłączenia się od sieci na 48 godzin? Przy okazji przypomnicie sobie, co sprawia Wam radość offline. Pamiętajcie też o modelowaniu zdrowych nawyków cyfrowych u swoich dzieci – już od najmłodszych lat. We wspólnym ustalaniu zasad korzystania z sieci pomoże Wam nasza bezpłatna aplikacja mOchrona.

Więcej pomocnych informacji znajdziecie na stronie ose.gov.pl w aktualnościach: „Zadbaj o siebie z OSE: problemowe używanie internetu", „Cyfrowa higiena i bezpieczeństwo w sieci z OSE", „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa".

Źródło:

Griffiths M., (1996), „Behavioural addiction: An issue for everybody?", Journal of Workplace Learning, nr 8(3), s. 19–25, za: Makaruk K., Włodarczyk J., Skoneczna P., (2019), „Problematyczne używanie internetu przez młodzież. Raport z badań", Warszawa: Fundacja Dajemy Dzieciom Siłę.

Propaganda

P

W internecie każdego dnia spotykamy się z różnymi przekazami, które mogą mieć na celu szerzenie propagandy i wpływanie na nasze poglądy. Propaganda to bowiem zaplanowane działanie, które ma za zadanie oddziaływać na zbiorowość i jednostki, zjednywać zwolenników i sojuszników określonych idei, poglądów, działań, wpajać dane przekonania oraz wywoływać konkretne zachowania. Nie zawsze jest jawnie wroga – może przybierać formę pozornie neutralnych wiadomości, memów, filmów czy grafik. Kluczowe jest to, że propaganda nie informuje – ona przekonuje, czasem przy użyciu emocji, strachu lub uproszczeń.

Celem propagandy może być np. narzucanie odbiorcom danych poglądów lub postaw. Wykorzystywane są do tego środki perswazji intelektualnej i emocjonalnej (m.in. słowa, gesty, obrazy) oraz metody manipulacji:

- **powtarzanie komunikatu** – im częściej coś słyszymy lub widzimy, tym bardziej wierzymy, że jest prawdą;
- **odwołanie do emocji** – strach, gniew, poczucie zagrożenia lub dumy narodowej są silnymi narzędziami manipulacji;
- **uproszczenie problemu** – złożone kwestie przedstawiane są w czarno-białych barwach czy w postaci prostych dychotomii typu „my kontra oni", „dobrze – źle", „przyjaciel – wróg", „swoi – obcy";

- **stereotypy i etykietowanie** – propaganda określa grupy ludzi, instytucje lub kraje w jednoznacznie negatywny lub pozytywny sposób;
- **symbole i obrazy** – plakaty, memy, zdjęcia czy filmy, które szybko przemawiają do emocji i zapadają w pamięć.

W erze cyfrowej propaganda przeniosła się do internetu. Media społecznościowe pozwalają na szybkie i szerokie rozpowszechnianie komunikatów. Algorytmy promują treści, które wywołują silne reakcje – nawet jeśli są jednostronne lub fałszywe. Dzięki temu propaganda staje się trudniejsza do wykrycia niż dawniej, gdy jej narzędziami były plakaty lub radiowe audycje. Jedno jednak się nie zmieniło: słowa, obrazy i powtarzające się komunikaty mają ogromną moc. Mogą inspirować, ale też manipulować, dzielić lub wzbudzać strach. Świadomość istnienia propagandy i mechanizmów jej działania jest kluczem do tego, by nie stać się biernym odbiorcą manipulacji, lecz świadomym uczestnikiem życia społecznego.

O tym, jak rozpoznawać dezinformację i propagandę oraz im przeciwdziałać, dowiecie się więcej z kursu e-learningowego „(Dez)informacja, czyli w co wierzyć w internecie" dostępnego na platformie OSE IT Szkoła. Sięgnijcie też do aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: metody i techniki dezinformacji" i „Bezpieczni w sieci z OSE: dezinformacja w mediach społecznościowych".

Prywatność w sieci

Myśląc o bezpieczeństwie online, zwykle instalujemy program antywirusowy czy stosujemy silne hasła, ale czy równie często pamiętamy o ochronie prywatności? Wiemy, że prawo do prywatności to jedno z podstawowych praw każdego człowieka. Niestety, nie wszyscy pamiętają, że poufne informacje i dane powinny być szczególnie strzeżone – także w internecie. W wirtualnej przestrzeni to, co prywatne, bardzo szybko może stać się publiczne, trafić w niepowołane ręce, wpłynąć na nasz wizerunek online.

O ochronie prywatności w sieci można mówić w różnych aspektach. Warto podkreślać, że z jednej strony szczegółowe informacje o sobie udostępniamy online świadomie. Podajemy np. imię i nazwisko, wiek, miejsce zamieszkania, gdy korzystamy z portali, które wymagają od nas ujawnienia takich danych. Z drugiej strony wiele dotyczących nas szczegółów „wycieka" bez naszej świadomości. Cyfrowy ślad zostawiamy podczas przeglądania stron internetowych, robienia zakupów w e-sklepach czy instalowania aplikacji, które zbierają więcej danych, niż byśmy chcieli.

Warto pamiętać, że podczas różnych aktywności w sieci łatwo może dojść do kradzieży danych, a stąd już tylko krok od niemałych problemów. Skradzione dane mogą posłużyć m.in. do wyłudzenia pożyczki, przeprowadzenia fałszywych transakcji bankowych czy podszywania się pod Was w korespondencji.

Jak oszuści uzyskują dostęp do poufnych informacji? Może się to wydarzyć na skutek ataku phishingowego czy w wyniku wycieku danych np. z e-sklepów. Najczęściej jednak sami dajemy cyberprzestępcom dostęp do prywatnych informacji – swobodnie dzieląc się nimi m.in. w serwisach społecznościowych. Pamiętajcie więc o konieczności zadbania o swoje bezpieczeństwo i prywatność w sieci – rozważnie publikujcie wiadomości o sobie, uważnie czytajcie politykę prywatności i regulaminy serwisów, wirtualnych sklepów oraz platform, na jakich się rejestrujecie. Udostępniajcie tylko te dane, które są niezbędne do skorzystania z usługi. Stosujcie też silne i unikalne hasła, a także weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości. Warto również zastrzec swój PESEL, np. w aplikacji mObywatel.

Więcej praktycznych wskazówek, jak dbać o swoją prywatność w sieci, znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: ochrona danych osobowych", „Zadbaj o siebie z OSE: prywatność w mediach społecznościowych".

P

Przeciążenie informacją

Dziś, dzięki urządzeniom mobilnym z dostępem do internetu, możemy być stale „on": sprawdzać interesujące nas wiadomości w sieci, komunikować się, monitorować przychodzące z różnych aplikacji powiadomienia – jednym słowem być na bieżąco. Natłok docierających do nas informacji daje nam poczucie, że trzymamy rękę na pulsie wydarzeń, ale może też męczyć, powodować przeciążenie informacją, co nie służy naszemu zdrowiu.

Czym dokładnie jest przeciążenie informacyjne? Ogólnie można powiedzieć, że to „stan psychiczny, w którym nadmiar informacji utrudnia nam wykonywanie zadań" (Politechnika Warszawska, 2024). Przebodźcowanie wiadomościami płynącymi z sieci sprawia, że nie możemy się skoncentrować, odczuwamy silny stres (w tym stres cyfrowy), zmęczenie, niepokój, a nawet lęk. Cierpi też na tym nasza wydajność. Skutkiem przeciążenia informacyjnego jest również brak motywacji do działania i utrata zainteresowania codziennymi obowiązkami.

Sprawy nie ułatwia multitasking, czyli coraz częstsza skłonność do korzystania z kilku urządzeń ekranowych jednocześnie (np. smartfona, laptopa i telewizora) lub wykonywania wielu czynności na jednym urządzeniu (jednoczesne korzystanie z laptopa do oglądania filmów i robienia zakupów online).

Warto wiedzieć, że dostęp do wielu ekranów to źródło dodatkowej stymulacji i przyjemności. Te z kolei powodują większy wyrzut dopaminy, czyli neuroprzekaźnika odpowiedzialnego za motywowanie nas do działania. Łatwo jednak wpaść w pułapkę pętli dopaminowej – z czasem układ nagrody będzie potrzebował zwiększonej liczby silnych bodźców, czyli w tym przypadku więcej treści płynących do nas z ekranów w tym samym czasie. Przebodźcowanie nadmiarem informacji przyczynia się do uwolnienia hormonów stresu, co wpływa na nasze zdrowie, w tym na jakość snu (Borkowska, 2024).

Jak pokonać cyfrowy stres wynikający z przeciążenia informacyjnego czy ekspozycji na szum informacyjny? Przede wszystkim należy kształtować pozytywne wzorce korzystania z internetu i urządzeń ekranowych – już u najmłodszych. Wdrażać zasady higieny cyfrowej, które sprawią, że zachowacie tak ważny balans między czasem spędzanym online i offline. Ciągle zdobywać wiedzę na temat ochrony przed powszechnymi cyberzagrożeniami – bezpieczeństwo w sieci to ważny element dbania o cyfrowy dobrostan.

Więcej informacji o sposobach unikania przeciążenia informacyjnego znajdziecie w aktualnościach na stronie ose.gov.pl: „Zadbaj o siebie z OSE: cyfrowy stres", „Stres cyfrowy – czym jest i jak go pokonać?".

Źródła:

Borkowska A., (2024), „Mniej znaczy więcej – o multiscreeningu i wielozadaniowości", Warszawa: Państwowy Instytut Badawczy NASK.

„Jak sobie radzić z przeciążeniem informacyjnym?", (2024), artykuł w serwisie pw.edu.pl.

Q

Quishing

Wraz z usprawnianiem metod przeciwdziałania różnym atakom, cyberprzestępcy doskonalą swoje metody wyłudzania naszych danych osobowych oraz środków finansowych. Jedną z nich jest quishing. To forma phishingu, która wykorzystuje już nie linki przesyłane w e-mailach, ale odpowiednio spreparowane kody QR (ang. Quick Response, czyli szybka odpowiedź). Znacie na pewno czarno-białe kwadratowe kody graficzne, które po zeskanowaniu przenoszą na zaszyte pod nimi strony, prawda?

W przypadku quishingu po zeskanowaniu takiego kodu, rzekomo prowadzącego do e-płatności lub odbioru nagrody, pobieramy zainfekowany plik lub trafiamy na fałszywą stronę banku czy innej instytucji. Uwaga! Z takimi kodami możecie mieć do czynienia nie tylko w e-mailach czy na stronach internetowych, ale też np. na przystankach komunikacji miejskiej, w hotelach, restauracjach czy nawet na ubraniach!

Tak jak w przypadku innych internetowych oszustw, przed quishingiem ochroni nas przede wszystkim zasada ograniczonego zaufania. Gdy po zeskanowaniu kodu cokolwiek wzbudzi Wasze wątpliwości – natychmiast zamknijcie stronę! Co jeszcze możecie zrobić?

- Pod żadnym pozorem nie skanujcie kodów pochodzących z niepewnego źródła.
- Jeśli skanujecie kod z nośnika fizycznego, np. plakatu czy ulotki, upewnijcie się, że jest on oryginalny, tzn. że np. w tym miejscu nie naklejono naklejki.
- Zwracajcie uwagę na to, jaki link wyświetla się po zeskanowaniu kodu – jeśli budzi Wasze wątpliwości, wybierzcie inny sposób na dotarcie do informacji, której poszukujecie, np. wejdźcie bezpośrednio na stronę.
- Bezwzględnie unikajcie podawania swoich danych osobowych, czy danych kart płatniczych w sytuacjach, w których nie jest to konieczne (np. w ramach zachęty do wzięcia udziału w loterii).

Czy można mieć 100% pewności, że za czarno-białym kodem nie kryje się potencjalnie groźna strona? Jedyną skuteczną metodą jest po prostu… nieskanowanie kodów QR, które nawet w najmniejszym stopniu wydają nam się podejrzane.

Więcej o oszustwach z wykorzystaniem kodów QR przeczytacie na stronie cert.pl i w aktualności „Bezpieczni w sieci z OSE: kody QR” na stronie ose.gov.pl.

Q

R

Ransomware

To rodzaj złośliwego oprogramowania często wykorzystywanego przez przestępców, którego zadaniem jest zaszyfrowanie danych na komputerze ofiary, tak by nie miała do nich dostępu. Atak ma najczęściej na celu wyłudzenie pieniędzy w zamian za odblokowanie systemu – stąd nazwa ransomware, która powstała z połączenia angielskich słów ransom (okup) i software (oprogramowanie).

Coraz częściej pojawiają się przypadki, kiedy to atakujący nie tylko szyfrują dane, ale także wykradają je, by następnie szantażować ofiarę, grożąc ich ujawnieniem lub poinformowaniem innych o ataku, np. partnerów biznesowych, instytucji współpracujących czy opinii publicznej w przypadku niezapłacenia okupu.

Na tego typu niebezpieczeństwo narażone są przede wszystkim duże firmy i instytucje publiczne, które przechowują dane wrażliwe klientów lub dostarczają kluczowe usługi. Oczywiście ransomware może też przeniknąć do systemu indywidualnego użytkownika – wystarczy, że otworzycie zainfekowany załącznik w e-mailu czy zainstalujecie aplikację lub program pochodzący z nieznanego źródła.

Jak zabezpieczyć się przed atakiem? Niezawodne rady: na bieżąco aktualizujcie system operacyjny, aplikacje i oprogramowanie – w tym antywirusy. Stosujcie silne, bezpieczne hasła, a najlepiej uwierzytelnianie dwuskładnikowe. Twórzcie też kopie zapasowe (backup), co pomoże Wam odzyskać dane bez potrzeby „negocjacji" z przestępcami.

I co najważniejsze – zachowajcie czujność i podstawowe zasady cyberhigieny. Unikajcie podejrzanych stron oraz linków i załączników przesyłanych przez nieznanych nadawców. Z rezerwą podchodźcie też do otrzymywanych wiadomości, szczególnie takich, w których nakłania się Was do działania bez zastanowienia i złamania wszelkich procedur bezpieczeństwa – nie dajcie się złapać na haczyk oszustów przeprowadzających akcje phishingowe. Może Was to sporo kosztować!

Pamiętajcie, że każde niebezpieczne zdarzenie zawsze możecie zgłosić do zespołu CSIRT NASK. Wystarczy wypełnić formularz na stronie incydent.cert.pl albo wysłać e-mail: cert@cert.pl. Administratorom zasobów informatycznych polecamy stronę nomoreransom.org, która pomaga w rozpoznaniu próbek złośliwego oprogramowania i bezpłatnie udostępnia narzędzia deszyfrujące dla znanych podtypów ransomware.

Więcej praktycznych porad, jak postępować w przypadku zainfekowania sprzętu ransomware, znajdziecie na ose.gov.pl w aktualności: „Bezpieczni w sieci z OSE: ransomware". Skorzystajcie też z publikacji CERT Polska „Poradnik ransomware".

Regulamin

R

Najprościej mówiąc, regulamin to zbiór zasad opisujących sposób postępowania w danej sprawie. Z regulaminami spotkacie się praktycznie wszędzie: w bibliotece, na basenie, w pracy, szkole i… w internecie. I choć wszyscy wiemy, że takie dokumenty są, to niestety zbyt rzadko je czytamy.

Obowiązki, zakazy, nakazy, paragrafy nie zachęcają do lektury – a niesłusznie. Znajomość regulaminu bardzo pomaga – również w sieci. Warto znać reguły panujące w wirtualnym świecie i pamiętać, że internauci oprócz obowiązków mają także swoje prawa. Jakie praktyczne wiadomości znajdziecie w regulaminach online? M.in. dokładne dane firmy świadczącej usługi drogą elektroniczną, zasady bezpiecznego korzystania z danego portalu, rejestracji, składania zamówień, reklamacji, zwrotów, dodawania komentarzy, informacje o ochronie danych osobowych (RODO)…

Zanim jednak zaakceptujecie regulamin – przeczytajcie go! Dlaczego to takie ważne? Zdarza się, że czasem pochopnie zatwierdzicie coś, na co prawdopodobnie nie wyrazilibyście zgody, gdyby-

ście wiedzieli, co kryje dany zapis. W regulaminach np. gier online może być zawarta informacja o dodatkowych opłatach. A jeśli bez zastanowienia zgodzicie się na warunki korzystania z jakiejś aplikacji, Wasze dane (np. lista kontaktów) lub zdjęcia w galerii na telefonie mogą zostać przekazane innym i dowolnie wykorzystane.

Warto uczulać dzieci, by nie wyrażały zgody na coś, z czym się nie zapoznały lub czego nie rozumieją. Regulaminy często pisane są skomplikowanym językiem, dlatego młodzi internauci przed ich akceptacją powinni zwrócić się o pomoc do rodziców lub opiekunów.

Romance scam

Nawiązujecie w sieci nowe znajomości albo szukacie online drugiej połówki? Uważajcie na romance scam, czyli „romantyczne oszustwo".

W dobie dostępu do internetu nasze serce może zabić szybciej również do osoby po drugiej stronie ekranu. Komunikatory, media społecznościowe, portale randkowe stwarzają szansę na poznanie online bratniej duszy. Często historie internetowych znajomości kończą się happy endem, ale nie zawsze. Niestety cyberprzestępcy wykorzystają każdą okazję, żeby zaatakować i wyłudzić pieniądze. Co więcej – potrafią po mistrzowsku żerować na naszych emocjach, stosując ataki bazujące na różnych technikach manipulacji. Schemat działania „romantycznych oszustów" jest podobny: wzbudzają zaufanie, wyznają miłość, roztaczają wizję wspólnej przyszłości… i proszą o pomoc finansową. Gdy to się nie uda albo pieniądze ukochanej osoby po prostu się skończą, miłość pryska – podobnie jak oszust.

Przykładów romance scam jest wiele, ale popularne są przede wszystkim dwa scenariusze.

- **Oszustwo na „amerykańskiego żołnierza"**, „lekarkę na misji w kraju objętym wojną" lub inną „niezwykłą" osobę, która nagle znalazła się w bardzo trudnej sytuacji i potrzebuje pieniędzy. Najczęściej przyczyną problemów ukochanego lub ukochanej jest choroba bliskiej osoby, brak dostępu do konta, konieczność zakupu biletu powrotnego.
- **Wzbudzenie zaufania i wyłudzenie od ofiary intymnych materiałów**, np. zdjęć lub filmików o charakterze erotycznym (seksting), w przypadku romance scam często prowadzi do szantażu (sextortion) i żądania zapłaty okupu w zamian za obietnicę nieupublicznienia krępujących materiałów.

Nie wszystko złoto, co się świeci – i nie każdy w internecie może być tym, za kogo się podaje. Podszywanie się w sieci pod istniejącą lub nieistniejącą osobę w celu złowienia potencjalnej ofiary w sidła miłości ma nawet swoją nazwę: catfishing. Wiemy, że zauroczenie nowo poznaną osobą potrafi uśpić naszą czujność, ale zanim dacie się ponieść emocjom, pamiętajcie o zachowaniu podstawowych zasad bezpieczeństwa:

- **Weryfikujcie profil danej osoby w mediach społecznościowych**. Sprawdźcie, kiedy założyła swoje konto, czy ma wielu znajomych, czy fotografuje się z nimi. Skorzystajcie też z opcji wyszukiwania obrazem w sieci. Być może okaże się, że fotografia potencjalnego oszusta pochodzi np. z banku zdjęć.
- **Namawiajcie poznaną w sieci osobę na kontakt online, ale z włączoną kamerką, lub na spotkanie w „realu"**. Jeśli wystarczy jej tylko rozmowa na czacie, przez telefon albo za pośrednictwem e-maila, to znak, że może chcieć ukryć swoją prawdziwą tożsamość.
- **Nie działajcie pod presją czasu**. Uważajcie na natarczywe prośby o przesłanie swoich zdjęć lub pieniędzy osobie, której nawet nie widzieliście na oczy. Pod żadnym pozorem nie podawajcie swoich haseł, danych do logowania, numerów kart płatniczych!
- **Z rozwagą dzielcie się w sieci informacjami o sobie**. Pamiętajcie, że oszust to doskonały manipulator i z pewnością wykorzysta wszystkie pozyskane o Was wiadomości, żeby odegrać rolę idealnie dopasowanej połówki.

Więcej o zagrożeniach związanych internetowymi znajomościami przeczytacie w naszych aktualnościach na stronie ose.gov.pl: „Uwaga na romance scam!", „Walentynki online? Sexting – niebezpieczny trend", „Wirtualna miłość – realne zagrożenie". Polecamy też poradniki przygotowane przez ekspertów NASK: „Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online" i „Internetowe Love II – randkowanie, AI, cyberbebezpieczeństwo".

Rozporządzenie o ochronie danych osobowych (RODO)

Obowiązuje od 2018 r. i określa ramy prawne przetwarzania danych osobowych w Europie. Wymogi RODO (także w internecie!) musi spełniać każda organizacja, która dysponuje naszymi danymi osobowymi, czyli wszelkimi informacjami umożliwiającymi identyfikację, takimi jak: imię i nazwisko, adres zamieszkania, e-mail czy numer PESEL. Według tego rozporządzenia ochronie podlegają też dane wrażliwe, dotyczące np. zdrowia czy poglądów.

Prawo do ochrony swoich danych osobowych przysługuje wszystkim. Co to oznacza w praktyce? RODO dba, by Wasze dane nie dostawały się w niepowołane ręce i były wykorzystywane w konkretnym celu – o czym powinniście zostać poinformowani. Za każdym razem, gdy robicie zakupy przez internet, ubiegacie się o pracę i wysyłacie swoje CV lub składacie wniosek o kredyt bankowy, Wasze dane – czy to online, czy w wersji papierowej – muszą być odpowiednio chronione.

Unijne rozporządzenie mówi też, że w każdej chwili możecie skorzystać z prawa do sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia Waszych danych. Co ważne – RODO gwarantuje Wam również prawo do bycia zapomnianym. Oznacza to, że możecie zgłosić się do administratora danych (np. Google'a) z prośbą o usunięcie odnośników do stron z treściami na Wasz temat: nieaktualnymi, nieistotnymi lub takimi, które naruszają Wasz wizerunek.

Co, jeśli dojdzie do naruszenia danych? RODO nakłada też na administratora danych (osobę lub podmiot zarządzający danymi osobowymi) obowiązek zgłaszania do Urzędu Ochrony Danych Osobowych kradzieży danych osobowych, ich utraty lub nielegalnego dostępu do nich. Administrator danych musi także poinformować Was bezpośrednio o naruszeniu Waszych danych.

Więcej informacji o RODO znajdziecie w podręczniku Generalnego Inspektora Ochrony Danych Osobowych „Gotowi na RODO".

Źródło:

„Ochrona danych i prywatność w sieci", (2024), artykuł na stronie europa.eu.

Rozszerzona rzeczywistość – AR (ang. *augmented reality*)

Technologia wirtualnej rzeczywistości (VR) pomaga, dzięki specjalnym narzędziom – takim jak gogle, kontrolery czy kostiumy – zanurzyć się w wirtualnym świecie, czyli wejść z zupełnie nową przestrzeń. Ale, czy wiecie, czym jest równie popularna technologia – AR?

Rozszerzona rzeczywistość – AR (ang. *augmented reality*) również pozwala użytkownikom na interakcję z wirtualnym światem, ale na innych zasadach. Pamiętacie, jak w 2016 r. ludzie chodzili ulicami miast i za pomocą aplikacji oraz kamery w ich telefonach łapali Pokémony? Było to możliwe właśnie dzięki wykorzystaniu przez AR realnego świata i nałożeniu na niego wirtualnych obiektów.

Twórcy nowych technologii szybko dostrzegli potencjał AR, dzięki czemu dziś wykorzystywana jest ona nie tylko w rozrywce, ale też w medycynie, biznesie czy edukacji. Przykłady? AR np. aktywizuje ruchowo seniorów, wykorzystuje się ją też podczas rehabilitacji ruchowej pacjentów po udarze. Ponadto lekarze korzystają z wirtualnych modeli narządów pacjentów, poznając ich strukturę, co pomaga w diagnozowaniu i planowaniu leczenia. Rozszerzona rzeczywistość sprawdza się też np. w sytuacjach szkoleniowych. Pracownik łatwiej zdobywa nowe umiejętności, specjalistyczną wiedzę i unikalne doświadczenia przy pomocy nowych technologii. Z tego rozwiązania korzystają też architekci czy projektanci wnętrz, a także sklepy. Nie wiecie, jak będzie wyglądała nowa kanapa w Waszym salonie? Zanim złożycie zamówienie, możecie zrobić wizuali-

zację dzięki AR. Wyobraźcie sobie też lekcje, na których uczniowie przyswajają wiedzę z wykorzystaniem elementów wirtualnego świata. Podczas zajęć edukacyjnych z historii uczniowie mogą z bliska zobaczyć maszynę szyfrującą Enigmę, egipski sarkofag czy starożytne artefakty, a na lekcjach matematyki wybrać się na spacer wśród trójwymiarowych kształtów. Z AR nauka może być prawdziwą przygodą!

Warto jednak pamiętać, że korzystanie z nowych technologii wiąże się z koniecznością dbania o swoje cyberbezpieczeństwo. W kontekście AR pamiętajcie szczególnie o kilku kwestiach:

- **Ochrona prywatności w sieci**. Jeśli korzystacie z aplikacji wykorzystujących rozszerzoną rzeczywistość, za każdym razem czytajcie politykę prywatności. Technologia AR często wymaga dostępu do kamery, mikrofonu czy GPS-u. Zastanówcie się, czy chcecie dzielić się z innymi, np. swoimi danymi geolokalizacyjnymi.
- **Bezpieczeństwo danych**. Stosujcie silne hasła, a najlepiej także uwierzytelnianie dwuskładnikowe lub wieloskładnikowe, czyli oprócz hasła logujcie się do usług cyfrowych dodatkowymi składnikami, np. kodem otrzymanym SMS-em.
- **Aktualizacje**. Pamiętajcie o regularnych aktualizacjach aplikacji oraz oprogramowania, także antywirusowego. Wszelkie błędy i luki w zabezpieczeniach stwarzają okazję do ataku.
- **Higiena cyfrowa**. Zbyt częste korzystanie z technologii, w tym z rozszerzonej rzeczywistości, może zaburzać równowagę online–offline. Z rozwagą sięgajcie więc po urządzenia cyfrowe, zachowując zdrowy balans.
- **Bezpieczeństwo**. Korzystając z AR, trzymajcie się podstawowych zasad bezpieczeństwa. Nakładanie się na siebie różnych obrazów jest na tyle atrakcyjne, że możecie zapomnieć o otaczającym Was świecie. Unikajcie używania AR w potencjalnie niebezpiecznych miejscach, takich jak tory, ulica czy przejazdy kolejowe.

Źródło:

„Różnica między VR a AR", (b.r.), artykuł w serwisie 4font.pl.

Równowaga online–offline

Nietrudno zauważyć, że smartfon to nasz najwierniejszy towarzysz, a wpatrywanie się w ekrany urządzeń cyfrowych stanowi nieodłączną część naszego codziennego funkcjonowania w pracy, szkole i życiu prywatnym.

Internet i nowe technologie zawładnęły sercami i umysłami nie tylko dorosłych, ale też dzieci. Potwierdzają to badania – z raportu NASK „Nastolatki" i danych z 2024 r. wynika, że młodzi w dni powszednie spędzają online średnio 5 godzin dziennie (bez jednej minuty), a w weekendy 5 godzin i 16 minut. To bardzo dużo, choć mniej niż rekordowy wynik z 2022 r. (5 godz. 36 min w dni powszednie oraz 6 godzin i 16 minut w weekendy).

Twórcy nowych technologii wiedzą, jak przyciągnąć uwagę użytkowników. Ciągłe powiadomienia, możliwość scrollowania bez końca, sensacyjne nagłówki artykułów, spersonalizowane treści, które precyzyjnie trafiają do nas po naszych cyfrowych śladach… To wszystko sprawia, że trudno jest oderwać się od ekranu.

Niestety, ciągłe przebywanie w wirtualnym świecie nie służy zdrowiu dziecka, szczególnie jeśli zauważycie, że trudno jest mu funkcjonować bez stałego kontaktu z urządzeniem. Nadużywanie sieci może prowadzić do FOMO (ang. *Fear of Missing Out*), czyli lęku przed odłączeniem, czy fonoholizmu, czyli nałogowego korzystania z urządzenia mobilnego.

Przymus bycia na bieżąco z newsami, e-mailami, komentarzami i informacjami publikowanymi w mediach społecznościowych, reagowanie na dźwięk każdego powiadomienia – to elementy, które skutecznie odciągają od codziennych obowiązków, dekoncentrują, zaburzają sen i potrzebę

dbania o dobre samopoczucie. Stąd tak ważne jest zachowanie równowagi online–offline. Jak to zrobić?

Na początek sprawdźcie, czy problem nadużywania smartfona, komputera, serwisów społecznościowych czy gier dotyka Was samych albo Waszego dziecka. Określcie, co sprawia, że tak wiele czasu spędzacie z urządzeniem w ręce – być może w taki sposób radzicie sobie z nudą lub tylko w sieci potraficie się dobrze bawić. Powodów może być wiele. Po diagnozie możecie działać. Ale pamiętajcie: radykalne odłączenie internetu rzadko kiedy przyniesie pożądany efekt. Najlepiej stosować metodę małych kroków, przyzwyczajając się stopniowo do bycia offline.

Próbujcie różnych rozwiązań:

- Monitorujcie czas przed ekranem i ustalcie limity dla konkretnych apek.
- Starannie planujcie czas poza siecią, postawcie na ciekawe aktywności, które pomogą Wam pokonać cyfrowe przemęczenie.
- Organizujcie rodzinne wyzwania (offline challenge), które ułatwią wdrażanie nowych cyfrowych nawyków. W tym czasie np. nie korzystajcie z ekranów przynajmniej godzinę przed snem, zaraz po przebudzeniu, podczas posiłków czy rodzinnych spotkań, ponadto wyznaczcie w domu strefy bez urządzeń i miejsca, gdzie z nich korzystacie. W budowaniu zdrowych nawyków starajcie się działać zespołowo: z przyjaciółmi, rodzicami, rodzeństwem – w grupie raźniej!
- Wyłączcie zbędne powiadomienia typu push, aby uniknąć ciągłego, niekontrolowanego sięgania po urządzenie.
- Ustawcie tryb monochromatyczny w telefonie – to sprawi, że ekran nie będzie tak bardzo przyciągał Waszej uwagi.
- Unikajcie multitaskingu i multiscreeningu – wykonywanie kilku rzeczy naraz, w tym korzystanie z wielu mediów w tym samym czasie (np. internetu i telewizora), sprawia, że jesteście przeciążeni i zmęczeni, w efekcie tracicie uwagę i koncentrację. Jeśli coś robicie, pamiętajcie, by usunąć telefon z zasięgu wzroku oraz zadbać o regenerujące przerwy – oczywiście bez ekranów!

Więcej ciekawych porad znajdziecie na ose.gov.pl w artykułach: „Zadbaj o siebie z OSE: odzyskaj kontrolę nad czasem ekranowym” i „Zadbaj o siebie z OSE: cyfrowy detoks”. Zachęcamy też do skorzystania z naszego bezpłatnego kursu e-learningowego dla dorosłych „Zrozumieć FOMO” oraz innych materiałów dostępnych na platformie OSE IT Szkoła: poradników „Offline znaczy zdrowiej. O cyfrowej higienie dla rodziców i wychowawców” i „Mniej znaczy więcej. O multiscreeningu i wielozadaniowości”, zbioru felietonów „O cyfrowej higienie”. Koniecznie sięgnijcie także po materiały (kursy, scenariusze lekcji, komiksy) na temat sposobów zachowania równowagi online–offline, opracowane w ramach kampanii edukacyjnej „FOMOwscy i JOMOwscy”.

Źródło:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

S

Scam

Internetowi oszuści stają się coraz bardziej przebiegli. Zdarza się, że skutecznie działają na naszą wyobraźnię, oferując wartościową nagrodę lub wysokie zarobki, chcąc skłonić nas do powierzenia im swoich danych osobowych, a nawet środków finansowych. Takie formy oszustwa nazywamy scamem. Najczęstszą formą scamu jest masowa korespondencja elektroniczna (spam), jednak cyberprzestępcy grają na naszych emocjach również podczas kontaktów telefonicznych. Ofiara jest przekonana, że odbiera telefon od policjanta, urzędnika czy też pracownika banku, dlatego bez oporów wykonuje wszelkie polecenia, np. podaje swoje dane osobowe lub dane do logowania.

Scamerzy korzystają też z formularzy i fałszywych stron internetowych do złudzenia przypominających prawdziwe witryny banku czy urzędu. Bywa, że wysyłają e-maile, w których nakłaniają do kliknięcia linków prowadzących do takich stron.

Oferty produktów w niskich cenach, nagrody bez udziału w konkursach, obietnica spadku po dalekim krewnym – to tylko niektóre przykłady scamu. Jak się przed nim chronić? Przede wszystkim zachowujcie czujność i zdrowy rozsądek. Weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą wasze wątpliwości. Weryfikuj każdą ofertę, każdą wiadomość czy telefon – zwłaszcza jeśli dotyczy Waszych danych osobowych lub finansowych. Pamiętajcie też o zasadzie ograniczonego zaufania: w sieci nie wszystko, co wygląda wiarygodnie, jest prawdziwe. Warto też korzystać z narzędzi bezpieczeństwa, takich jak oprogramowanie antywirusowe, aktualizacje systemu i uwierzytelnianie dwuskładnikowe, które dodatkowo zabezpieczają konta przed nieuprawnionym dostępem.

Seksting

Zapewne zdajecie sobie sprawę, że w ostatnich latach, w związku z ułatwionym dostępem do internetu i urządzeń cyfrowych, problem wytwarzania i udostępniania przez uczniów intymnych materiałów staje się coraz powszechniejszy. Jednym z nasilających się zagrożeń jest seksting – ryzykowne zachowanie polegające na przesyłaniu innym osobom intymnych wiadomości tekstowych i erotycznych plików multimedialnych.

Na początku seksting dotyczył przede wszystkim tych, którzy pozostawali w związkach lub w bliskiej relacji. Wraz z rozwojem nowoczesnych technologii zaczął przyjmować nieco inną formę. Nie są to już tylko wiadomości tekstowe, ale przede wszystkim zdjęcia czy filmy, które przedstawiają ich twórców w intymnej, erotycznej sytuacji.

Seksting dla wielu młodych ludzi jest formą flirtu lub żartu. Z jednej strony pozwala na wyrażenie zainteresowania drugą osobą, bywa też sposobem na przeżywanie pierwszych doświadczeń i fascynacji seksualnych, a z drugiej – może prowadzić do niebezpiecznych sytuacji oraz utraty kontroli nad własnym wizerunkiem online.Zdarza się, że dzieci i nastolatki, których intymne fotografie lub filmy zostały udostępnione, doświadczają przemocy zarówno online, jak i w świecie realnym, np. ze strony rówieśników. Ofiarom sekstingu mogą towarzyszyć trudne emocje związane ze wstydem, lękiem, ośmieszeniem. Ostatnie edycje badania „Nastolatki" wskazują, że ok. 30% uczniów starszych klas szkoły podstawowej i szkoły ponadpodstawowej otrzymało od kogoś nagie lub półnagie zdjęcie (2022 r. – 30%, 2024 r. – 28%; por. Lange, 2023; Ładna i in., 2025).

S

W niektórych przypadkach seksting może nosić znamiona przestępstwa związanego z produkcją materiałów pornograficznych z udziałem osoby niepełnoletniej (art. 202 § 3 Kodeksu karnego). Warto wiedzieć, że polskie prawo chroni osoby poniżej 18. roku życia przed produkowaniem lub utrwalaniem treści pornograficznych z ich udziałem. Zabrania też rozpowszechniania, utrwalania, sprowadzania, przechowywania, posiadania czy nawet uzyskiwania dostępu do takich materiałów.

Młodzi ludzie, działając pod wpływem emocji, nie zawsze zdają sobie sprawę z tego, jak łatwo stracić kontrolę nad udostępnionymi w sieci materiałami. Skutki nieprzemyślanych działań mogą

być bardzo dotkliwe, dlatego warto zawczasu podjąć kroki, które zmniejszają ryzyko zaangażowania dzieci w szkodliwe dla nich zachowania.

1. **Wiedza i rozmowa.** Zanim zdecydujecie się na rozmowę z dzieckiem na temat bezpieczeństwa w internecie, warto najpierw zdobyć wiedzę na temat powszechnych cyberzagrożeń. W tym celu można skorzystać z zasobów (poradników, infografik, scenariuszy lekcji) dostępnych na platformie OSE IT Szkoła.
2. **Zaufanie i szacunek.** Budujcie relację opartą na wzajemnym szacunku oraz zaufaniu. Wspierająca postawa rodziców i opiekunów sprawi, że dziecko chętniej będzie się zwracać po pomoc w przypadku doświadczenia trudnych sytuacji w sieci.
3. **Ku przestrodze.** Podczas rozmowy z nastolatkiem na temat skutków sekstingu warto sięgnąć po przykłady z otoczenia lub mediów, dzięki którym łatwiej zrozumie on konsekwencje niebezpiecznych zachowań w sieci.
4. **Internet nie zapomina!** To stwierdzenie powinno zapaść w pamięć młodym użytkownikom internetu. Przypominajcie im, że intymne materiały może zobaczyć nie tylko sympatia, ale też rodzina, znajomi, nauczyciele, a w przyszłości współpracownicy czy pracodawcy. Pokazujcie, jak dbać o własny wizerunek online.
5. **Utrata kontroli nad materiałami, które udostępniamy.** Pamiętajcie, że nasze materiały mogą być łatwo pobrane i umieszczone na stronach, na których nie chcielibyśmy, aby się znalazły. Mogą zostać opatrzone nieprzyjemnymi komentarzami, użyte jako memy itp.
6. **Stawianie granic.** Rozmawiajcie na temat budowania związku opartego na szacunku i zdrowych relacjach. Uczcie dziecko radzenia sobie z presją, stawiania granic oraz prawa do odmowy. Zwracajcie też uwagę na prywatność w sieci i przypominajcie o ograniczonym zaufaniu do osób, które znamy tylko z internetu.

Jeśli Wasze dziecko padło ofiarą sekstingu, przeprowadźcie szczerą rozmowę, otoczcie je opieką oraz wesprzyjcie w rozwiązaniu problemu. Ponadto skontaktujcie się z administratorami serwisów, na których pojawiły się wstydliwe treści, oraz zabezpieczcie dowody nadużycia (zdjęcia, filmy, korespondencję).

Więcej na temat sextingu dowiecie się z poradnika dla nauczycieli „Sexting i nagie zdjęcia w sieci". Zachęcamy także do zapoznania się z infografikami, scenariuszem zajęć „Decyzja" dostępnymi na platformie OSE IT Szkoła oraz aktualnościami: „Temat lekcji: sexting" i „Zadbaj o siebie z OSE: seksting" na stronie ose.gov.pl.

Źródła:

Lange R. (red.), (2023), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), , Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy", Państwowy Instytut Badawczy NASK.

„Walentynki online? Sexting – niebezpieczny trend", (2024), artykuł na stronie ose.gov.pl.

S

Self generated sexual content

Wiele treści w internecie może budzić nasz niepokój – łatwo natknąć się na szkodliwe czy wręcz nielegalne materiały. Należą do nich zdjęcia czy filmy prezentujące dziecko w seksualnym kontekście lub przedstawiające wykorzystywanie seksualne nieletnich (odpowiednio CSEM – ang. *child exploitation materials* i CSAM – ang. *child sexual abuse materials*).

Trzeba w tym miejscu wspomnieć też o *self generated sexual content* (z ang. seksualne treści wytwarzane samodzielnie), czyli zdjęciach, filmach czy pokazach (np. udostępnianych w serwisach

streamingowych) o charakterze erotycznym lub pornograficznym, wykonywanych samodzielnie, choć nie zawsze dobrowolnie, przez osoby poniżej 18. roku życia. Takie materiały są szczególnym rodzajem szkodliwych treści – to treści nielegalne.

Self generated sexual content prezentują dziecko np. częściowo rozebrane, w bieliźnie lub nago, przyjmujące erotyczne pozy, czasami podejmujące różne czynności seksualne czy też naśladujące je. Dlaczego dzieci i nastolatki wytwarzają takie materiały? Może to być m.in. skutek uwodzenia dziecka przez internet (child grooming) czy szantażu na tle seksualnym (sextortion). Bywa też, że materiały sekstingowe przesyłane sobie nawzajem przez nastolatki jako „dowód miłości" lub element flirtu z różnych powodów zostają upublicznione.

Polskie prawo chroni osoby nieletnie przed produkowaniem lub utrwalaniem treści pornograficznych z ich udziałem. Zabrania także rozpowszechniania, utrwalania, poberania, przechowywania, posiadania i uzyskiwania dostępu do takich materiałów.

Jeżeli natkniecie się w sieci na materiały self generated sexual content lub będą one dotyczyły Waszego dziecka albo ucznia – niezwłocznie reagujcie! Poinformujcie o tym fakcie działający w NASK zespół Dyżurnet.pl, czyli punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Możecie to zrobić: wypełniając formularz, wysyłając e-mail na adres dyzurnet@dyzurnet.pl lub dzwoniąc pod numer 801 615 005. O takim zdarzeniu powinniście też natychmiast poinformować policję i zabezpieczyć wszystkie materiały.

Separacja tożsamości

Jeśli separacja nie kojarzy Wam się zbyt dobrze, zachęcamy: spróbujcie separacji tożsamości. Na pewno poczujecie się bezpieczniej w internecie. O co chodzi?

Separacja tożsamości może mieć dwa wymiary. Po pierwsze, polega na rozłączeniu swoich służbowych i prywatnych aktywności online. To kluczowe, bo zawsze przy jakimś wycieku, udanej infekcji czy phishingu narażamy tylko część swoich danych. Po drugie, warto pamiętać – o dzieleniu swojej wirtualnej przestrzeni, np. poprzez tworzenie osobnej skrzynki mailowej do spraw urzędowych czy kont w sklepach internetowych. Wszystko to ma na celu ochronę naszych danych osobowych. Co bardzo istotne, takie odrębne konta ograniczają szkody, które może wyrządzić potencjalny wyciek danych!

Zacznijmy od podstaw. Musicie wiedzieć, że korzystanie z prywatnego konta pocztowego do załatwiania spraw służbowych niesie za sobą wiele niebezpieczeństw. Równie ryzykowne jest używanie firmowego adresu np. do zakładania kont w mediach społecznościowych czy innych usługach niezwiązanych z pracą. Podejmując takie działania, narażacie się nie tylko na zachwianie równowagi między życiem zawodowym a prywatnym, ale też stajecie się łatwiejszym łupem dla internetowych oszustów.

W internecie wszyscy możemy paść ofiarą oszustów, dlatego dobrze jest zabezpieczać się zawczasu przed możliwymi atakami. Jednym ze sposobów, oprócz rozłączenia służbowej i prywatnej poczty elektronicznej, będzie też założenie kilku osobnych skrzynek przeznaczonych do różnych celów. Jeśli z jednego adresu będziecie wysyłać prywatne maile, z drugiego skorzystacie podczas rejestracji kont w różnych usługach, a trzeci przyda się do załatwiania spraw urzędowych, pokrzyżujecie złodziejom szyki. Nawet gdy zyskają dostęp do jednego z Waszych kont, nie przejmą jednocześnie pozostałych!

Szczegółowych informacji szukajcie w naszych aktualnościach: „Bezpieczni w sieci z OSE: poczta e-mail", „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci", „Bezpieczni w sieci z OSE: BLIK i płatności internetowe".

Sextortion

Z sekstingiem wiąże się inne niebezpieczne zjawisko – sextortion, czyli pozyskanie od ofiary materiałów o charakterze seksualnym i późniejsze wymuszenie okupu (pieniędzy albo kolejnych

treści pod groźbą ich opublikowania lub dalszego rozpowszechniania). Ofiarą takiego szantażu może paść każdy – dzieci, młodzież i dorośli, bez względu na płeć czy miejsce zamieszkania.

Sprawcy sextortion próbują coraz nowszych i skuteczniejszych metod pozyskania zdjęć lub filmów od potencjalnej ofiary. Szukają osób, które łatwo zmanipulować, które chętnie nawiązują kontakty z nieznajomymi i są gotowe do dzielenia się treściami o charakterze seksualnym. Zdarza się też, że sextortion jest jedną z konsekwencji sekstingu.

Pamiętajcie: sextortion to nie tylko zagrożenie internetowe, ale przede wszystkim przestępstwo, które należy zgłosić (art. 190 oraz 191a Kodeksu karnego) na policję. Porozmawiajcie też z nastolatkiem o włączeniu ustawień prywatności, tak aby jego profil był niedostępny dla osób spoza grona jego najbliższych znajomych. Treści nielegalne i szkodliwe, zwłaszcza związane z seksualnym wykorzystywaniem dzieci, warto zgłosić do działającego w NASK Zespołu Dyżurnet.pl.

Specjalistyczną pomoc psychologiczną i informacje dotyczące bezpieczeństwa dziecka w internecie można uzyskać, dzwoniąc pod poniższe numery telefoniczne:

- 116 111 (116111.pl) – Bezpłatny i anonimowy telefon zaufania dla dzieci
- 116 123 – Bezpłatny kryzysowy telefon zaufania dla dorosłych
- 800 100 100 (800100100.pl) – Bezpłatny i anonimowy telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci
- 800 70 222 (centrumwsparcia.pl) – Centrum wsparcia dla osób w stanie kryzysu psychicznego
- 800 12 12 12 (brpd.gov.pl, e-mail: rpd@brpd.gov.pl) – Telefon zaufania Rzecznika Praw Dziecka

Sharenting

Dokumentowanie życia dziecka w internecie stało się co najmniej powszechnym zjawiskiem, o ile nie normą społeczną wśród współczesnych rodziców. Z sharentingiem (od ang. *share* – dzielić się oraz *parenting* – rodzicielstwo) mamy do czynienia na portalach społecznościowych, blogach, forach dyskusyjnych, czyli wszędzie tam, gdzie szczegółowe informacje, zdjęcia i filmy z życia dzieci znajdą szerokie grono odbiorców. Jednak czy mamy świadomość, że fotka naszego dziecka niespodziewanie może obiec internet, stać się memem, trafić w niepowołane ręce lub przyczynić się do cyberprzemocy?

Liczba materiałów zamieszczanych przez rodziców w sieci przyprawia o zawrót głowy. Wielu z nich dokumentuje każdy moment codziennego życia swoich pociech (publikują nawet zdjęcia USG nienarodzonych jeszcze dzieci), a często także śmieszne lub wzruszające scenki z ich udziałem. Zdarza się, że takie treści zdradzają więcej niż powinny: opiekunowie opatrują je komentarzami zawierającymi wiele szczegółów z życia dziecka, np. imię, wiek, datę urodzin, nazwę szkoły lub przedszkola, do którego chodzi. Takie informacje, mimo że podane w dobrej wierze, mogą realnie zagrozić bezpieczeństwu dziecka!

Jak bezpiecznie dzielić się zdjęciami swoich dzieci w internecie? Przede wszystkim róbcie to z głową – pamiętajcie, że mniej znaczy więcej i że Wasze działania dzisiaj kształtują wizerunek dziecka w przyszłości, także ten online. Zanim wrzucicie coś do sieci, zastanówcie się, czy materiał może narazić dziecko na śmieszność, upokorzenie bądź krytykę, czy nie prezentuje intymnych treści. Ograniczajcie widoczność zdjęć czy filmików i przede wszystkim – pytajcie dziecko o zgodę przed ich publikacją!

Więcej porad dotyczących udostępniania zdjęć swoich dzieci online znajdziecie w naszym poradniku dla rodziców „Sharenting i wizerunek dziecka w sieci" i kursie e-learningowym „Sharenting. Czy warto mieć rodzinny album w sieci?" na platformie OSE IT Szkoła, webinarze eksperckim „Rodzinny album z wakacji, czyli czego o dzieciach nie powinien wiedzieć internet" oraz w aktualnościach

„Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!", „Bezpieczni w sieci z OSE na wakacje: Sharenting i wizerunek dziecka w sieci", „Zadbaj o siebie z OSE: oversharing" na stronie ose.gov.pl.

Skimming

Wypłacając gotówkę w bankomacie, zwłaszcza położonym na uboczu lub w obcym miejscu, musimy mieć oczy i uszy szeroko otwarte – w przeciwnym razie możemy paść ofiarą przestępstwa zwanego skimmingiem. Jest to oszustwo polegające na kopiowaniu przez złodzieja zawartości paska magnetycznego lub chipa z karty płatniczej, prowadzące do obciążenia rachunku bankowego okradanej osoby.

Sprawcy przy pomocy tzw. skimmera – specjalnego urządzenia kopiującego umieszczanego w bankomacie – przechwytują informacje zawarte na karcie. Towarzysząca urządzeniu kopiującemu mikrokamera lub specjalna nakładka na klawiaturę pozwalają ponadto rejestrować wpisywany przez użytkownika PIN.

Jak się ustrzec przed utratą gotówki? Korzystajcie z bankomatów położonych w uczęszczanych i dobrze oświetlonych miejscach, rezygnujcie z wypłat, gdy cokolwiek wzbudzi Wasze podejrzenia. Jak oka w głowie strzeżcie też swojej karty i numeru PIN – nie przekazujcie karty innym osobom i nie zapisujcie numeru PIN na karteczce noszonej w portfelu ani na samej karcie płatniczej.

Więcej o skimmingu dowiecie się z aktualności „Skimming, czyli co się może kryć w bankomacie" na ose.gov.pl.

Smombie

Smartfonowy zombie, czyli smombie („smartfon" + „zombie"), zapewne nie raz był Waszym towarzyszem podróży, mogliście go spotkać też w kinie, teatrze czy nawet na pasach. To osoba, która godzinami wpatruje się w ekran swojego urządzenia, nie zauważa innych ludzi i rzeczy dookoła siebie. Nierzadko swoim zachowaniem stwarza realne zagrożenie, np. nie zwracając uwagi na przejeżdżające pojazdy.

Dla smombie przymus sięgnięcia po telefon jest silniejszy od czegokolwiek innego. Tak, ten stan jest jednym ze skutków FOMO, czyli lęku przed odłączeniem od sieci. W ten sposób objawiają się zaburzenie równowagi online–offline i konieczne jest wtedy pilne zadbanie o cyfrową higienę. Jak wrócić do realnego świata? Małymi krokami.

1. **Alternatywa dla urządzeń cyfrowych.** Poszukajcie zajęć, które mogą być odskocznią od urządzeń cyfrowych. Na pewno sprawdzi się rodzinna runda gier planszowych, wspólne gotowanie czy po prostu czas spędzony z dobrą książką.
2. **Strefy offline.** Wspólnie z domownikami wyznaczcie strefy na odkładanie i ładowanie urządzeń.
3. **Zajęcia bez smartfona.** Umówcie się, że nie korzystacie z telefonu, gdy z kimś rozmawiacie, spożywacie posiłek czy podczas wspólnej rozrywki. Starajcie się też ograniczyć kontakt z ekranem urządzenia przed snem.
4. **Kontrola czasu z urządzeniem.** Ustalcie wspólnie z dzieckiem, ile czasu dziennie może poświęcić na używanie smartfona. W egzekwowaniu tego postanowienia pomocne mogą być aplikacje kontroli rodzicielskiej.
5. **Podejmijcie wyzwanie.** Spróbujcie spędzić rodzinny weekend bez telefonów. W tym czasie zaplanujcie ciekawe aktywności offline: wspólne wyjście do kina, teatru, muzeum, spacer lub zabawę na świeżym powietrzu.

Zanim zabierzecie się za wprowadzanie zmian, szczególnie u najmłodszych, pamiętajcie, że jesteście dla dzieci najlepszym przykładem. Zastanówcie się, czy sami nie poświęcacie smartfonowi zbyt wiele uwagi. Każdego dnia pokazujcie, jak zadbać o jakość wolnego czasu oraz jak mądrze i odpowiedzialnie korzystać ze zdobyczy techniki.

Jeśli chcecie dowiedzieć się więcej na temat smombie, zajrzyjcie na ose.gov.pl do naszej aktualności „Smombie są wśród nas”.

Snubbing w mediach społecznościowych

Czy wiecie, czym jest phubbing? Termin ten powstał z połączenia dwóch angielskich wyrazów: phone – „telefon” i snubbing – „lekceważenie”, „odtrącenie” oraz definiuje sytuację, w której ktoś bez przerwy wpatruje się w ekran swojego smartfona, traktując innych jak powietrze – nawet najbliższych.

Lekceważenie w kontekście używania narzędzi cyfrowych może też dotyczyć użytkowników mediów społecznościowych. Badacze zwracają uwagę na zjawisko snubbingu, dostrzegając skutki celowego odtrącenia w social mediach. Jak czują się osoby snubbowane – pomijane, ignorowane przez społeczność zgromadzoną w sieci? I co zrobić, by komunikacja za pośrednictwem portali społecznościowych nie wpływała na poczucie własnej wartości?

Z mediów społecznościowych korzysta niemal 28 mln Polaków w różnym wieku: od 7 do 75 lat (Gemius, 2023). Można więc powiedzieć, że statystycznie większość z nas posiada konto w przynajmniej w jednym portalu społecznościowym. W social mediach toczy się duża część naszego życia. To tu poszukujemy informacji i inspiracji do działania, podtrzymujemy kontakty, budujemy relacje, spędzamy czas na rozrywce. Choć portale społecznościowe odgrywają ważną rolę w naszym życiu, mogą być też pułapką. Oszustwa, zaburzenie równowagi online–offline, przymus kreowania idealnego wizerunku – to tylko niektóre problemy dotykające użytkowników popularnych platform.

Internet, a więc i social media, to też narzędzia, za pośrednictwem których ich użytkownicy doświadczają cyberprzemocy. Może ona przybierać różne formy, m.in.: agresji słownej, upubliczniania cudzych upokarzających, często przerobionych zdjęć i filmów, podszywania się pod kogoś w celu zamieszczania w jego imieniu obraźliwych postów i zdjęć na profilach innych użytkowników, szantażu, wykluczania z grona „znajomych” w internecie, ale też celowego ignorowania czyjejś działalności w sieci (Borkowska, 2023).

Snubbing jest subtelniejszą formą cyberprzemocy. Może się ona przejawiać w takich działaniach, jak:

- świadome ignorowanie wiadomości od kogoś w komunikatorach, mimo że odbiorca jest aktywny w mediach społecznościowych;
- systematyczne pomijanie postów, zdjęć i innych treści publikowanych przez konkretną osobę, poprzez brak reakcji, takich jak polubienia, komentarze czy udostępnienia, co może być odebrane jako lekceważenie innego użytkownika;
- celowe unikanie kontaktu z daną osobą i zaniedbywanie relacji w social mediach, co z kolei może być sygnałem ochłodzenia więzi, braku wzajemnego zainteresowania, a nawet zakończenia znajomości.

Snubbing na pewno może prowadzić do nieporozumień lub napięć w relacjach międzyludzkich. Co jeszcze przeżywają osoby lekceważone, odtrącone przez innych w mediach społecznościowych? Badanie opublikowane w czasopiśmie „Social Influence” pokazuje, że internauci, którzy nie otrzymali żadnej reakcji na swoje posty i publikowane materiały mieli poczucie wykluczenia i braku przynależności do danej grupy. Zanik interakcji między internautami sprawił też, że ignorowane osoby miały niskie poczucie własnej wartości, a nawet odczuwały brak sensu istnienia (CBS News, 2014).

Warto uodparniać szczególnie dzieci na snubbing w mediach społecznościowych. Jak to zrobić?

- **Pamiętajcie o edukacji medialnej**. Wyjaśnijcie dziecku, że snubbing może wynikać z różnych okoliczności, często od nas niezależnych. Wytłumaczcie, że nie wszystkie działania w social mediach odzwierciedlają rzeczywiste intencje użytkowników sieci.

Wszelkie niedomówienia warto wyjaśnić w rozmowie z drugą osobą – najlepiej twarzą w twarz.

- **Pomagajcie dziecku budować silne poczucie własnej wartości**. Przypominajcie mu, że w mediach społecznościowych kreowany jest świat, który może mieć mało wspólnego z tym, co dzieje się po drugiej stronie ekranu. Podkreślajcie, że nasza wartość nie zależy od liczby polubień czy komentarzy!
- **Rozmawiajcie z dzieckiem o emocjach – także tych trudnych**. Uczcie, że każdy z nas może doświadczyć odrzucenia i to normalne, że możemy się z tym czuć źle.
- **Wspierajcie dziecko w budowaniu zdrowych relacji poza siecią**. Dbajcie też o jego pasje i rozrywkę offline. Pokażcie młodym użytkownikom internetu, że świat poza mediami społecznościowymi jest o wiele bardziej atrakcyjny.
- **Okazujcie dziecku wsparcie** – powtarzajcie mu, że zawsze może się zwrócić do Was o pomoc.

Źródła:

„Social Media 2023”, (2023), Warszawa: Gemius, Polskie Badania Internetu, IAB Polska.

Borkowska A., (2023), „Cyberprzemoc – włącz blokadę na nękanie. Poradnik dla rodziców”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

„People snubbed on Facebook feel less meaningful existence study finds”, (2014), artykuł w serwisie cbsnews.com.

Social media sabbatical

Social media sabbatical oznacza świadomą, zaplanowaną, dłuższą przerwę od portali społecznościowych. To sposób na odzyskanie równowagi między czasem spędzanym w sieci i poza nim. Dlaczego to takie ważne?

Media społecznościowe zapewniają rozrywkę, umożliwiają podtrzymywanie kontaktów, dla wielu są też źródłem najświeższych informacji i odskocznią od codziennych obowiązków. To ważny element wirtualnego, a jednocześnie bardzo realnego życia – szczególnie dla młodych użytkowników sieci.

Badania potwierdzają, że ich aktywności online najczęściej dotyczą właśnie social mediów. Z raportu NASK „Nastolatki” wynika, że młodzież powszechnie korzysta m.in. z komunikatorów internetowych i serwisów społecznościowych – tylko 3% respondentów wskazało, że nie ma żadnego konta na takich platformach. Nastolatki spędzają w mediach społecznościowych średnio 3 godziny i 23 minuty w ciągu dnia. W jakim celu? Głównie słuchają muzyki, kontaktują się z innymi, grają w gry czy zaglądają do social mediów dla zabicia czasu (Ładna i in., 2025).

Zbytnie zaangażowanie w cyfrowy świat niesie jednak za sobą konsekwencje. Łatwo stracić kontrolę nad czasem spędzanym przed ekranem, a co za tym idzie – narazić się na skutki nadużywania nowych technologii, w tym mediów społecznościowych. Co nam grozi? Stres cyfrowy związany z nadmiarem internetu i bodźców, FOMO (ang. *Fear of Missing Out*), czyli lęk przed odłączeniem, a nawet e-uzależnienie. Jest na to rada – czasem warto po prostu pozostać offline chwilę dłużej i skupić się na aktywnościach poza siecią. Jak to zrobić?

Można spróbować social media sabbatical i zrobić sobie wakacje od mediów społecznościowych, by odzyskać równowagę online–offline. Zanim jednak postanowicie odłączyć się do sieci, należy się do tego dobrze przygotować. Ustalcie datę i poinformujcie znajomych o zniknięciu z internetu. Dokładnie zaplanujcie też czas offline – zróbcie coś, o czym dawno myśleliście, ale nie mieliście na to czasu. Ciekawy kurs, sport lub czytanie zaległych książek – brzmi świetnie, prawda? Podczas odłączenia od social mediów przyglądajcie się sobie. Być może odkryjecie, że odcięcie od wirtualnego świata przyniosło same dobre doświadczenia. Albo wręcz przeciwnie – bez mediów społecznościowych czuliście przygnębienie, lęk, irytację.

Po powrocie do popularnych serwisów społecznościowych starajcie się kontrolować czas spędzany w sieci. Uważajcie też, by stale napływające z internetu informacje, posty, komentarze znajomych i powiadomienia z komunikatorów nie pochłonęły Was zbyt mocno.

Więcej przydatnych informacji znajdziecie w aktualności „Letnia Akademia Cyfrowej Higieny: czas na social media sabbatical" dostępnej na stronie OSE IT Szkoła.

Socjotechnika

Myśląc o cyberprzestępcach czy oszustach internetowych, najczęściej wiążemy ich z zaawansowanymi narzędziami czy nowoczesnymi technologiami, które pomagają im wykradać nasze dane czy pieniądze. Warto jednak wiedzieć, że zamiast kosztownych środków najczęściej wykorzystują nasze… emocje.

U podstaw wielu działań cyberprzestępców leży socjotechnika, czyli różne sposoby wywierania wpływu, np. przy użyciu perswazji, manipulacji, zastraszania, szantażu. Okazuje się bowiem, że najłatwiejszą metodą kradzieży informacji czy zainfekowania urządzenia malware (złośliwym oprogramowaniem) jest nakłonienie nas do udostępnienia swoich danych, kliknięcia w link niewiadomego pochodzenia czy ściągnięcia np. niebezpiecznej aplikacji.

Najpopularniejszą i niezwykle skuteczną formą ataku z wykorzystaniem socjotechniki jest phishing. Na czym polega? Oszust próbuje podszywać się pod znaną osobę, markę lub instytucję, starając się namówić do wykonania określonej czynności – kliknięcia w link, pobrania załącznika czy aplikacji, dokonania pozornie drobnej wpłaty czy podania swoich danych logowania. Wysyła w tym celu ponaglające maile, SMS-y z prośbą o dopłatę do paczki, możecie spotkać się też z sytuacjami, w których rzekomy pracownik banku telefonicznie informuje nas o dużym ruchu na koncie lub prosi o potwierdzenie tożsamości. Cyberprzestępcy liczą na to, że zareagujecie w pośpiechu, nie przyglądając się treści wiadomości i nie próbując jej zweryfikować. Gdy wykonacie żądanie oszusta, możecie spodziewać się dotkliwych konsekwencji: być może przechwyci on i wykorzysta Wasze dane osobowe, loginy i hasła, włamie się na konto bankowe lub skłoni Was do zainstalowania złośliwego oprogramowania na smartfonie czy laptopie.

Cyberataki z wykorzystaniem socjotechniki są poważnym zagrożeniem bezpieczeństwa w internecie, dlatego warto wiedzieć, jak się przed nimi chronić. Co najważniejsze: włączyć myślenie i zachowywać zimną krew. W każdej sytuacji, która wydaje się podejrzana, warto też zweryfikować rozmówcę lub nadawcę wiadomości, a przede wszystkim – nie reagować na jego ponaglenia.

Aby zmusić ofiary do osiągnięcia swoich celów, oszuści próbują wzbudzać w nich cały wachlarz emocji – od strachu i onieśmielenia, aż po ciekawość i podekscytowanie. Na każdą propozycję, która jest zbyt piękna, by mogła być prawdziwa, zawsze starajcie się więc spoglądać możliwie chłodno. Uważajcie na groźby, próby wyłudzenia poufnych informacji i podejrzane wiadomości rzekomo pochodzące od znajomych.

Koniecznie przesyłajcie podejrzane wiadomości SMS na numer 8080, używając funkcji „przekaż" albo „udostępnij". Inne próby wyłudzenia danych zgłaszajcie za pośrednictwem formularza internetowego dostępnego na stronie incydent.cert.pl.

Więcej o atakach socjotechnicznych i phishingu znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: internetowi oszuści i socjotechnika", „Bezpieczni w sieci z OSE: phishing" i „Europejski Miesiąc Cyberbezpieczeństwa z OSE: phishing".

S

Spam

Najprościej mówiąc, spam to niechciane wiadomości przesyłane drogą e-mailową, SMS-ową lub za pośrednictwem serwisów społecznościowych. Termin pochodzi od… mielonki (oszukanego, mało wartościowego mięsa), co raczej nie budzi dobrych skojarzeń.

Czym charakteryzuje się spam? Wysyłany jest do wielu nadawców, przez co nie jest spersonalizowany. Zazwyczaj zawiera informacje marketingowe, ale też propagandowe. Spam to również

narzędzie popularne wśród cyberprzestępców! Za jego pomocą oszuści stosują np. phishing, czyli wysyłają wiadomości, które zawierają m.in. zainfekowane załączniki lub linki kierujące do niebezpiecznych witryn internetowych. Celem ataku jest wyłudzenie poufnych danych – loginów i haseł do bankowości internetowej lub serwisów społecznościowych – a nawet zainfekowanie urządzenia ofiary malware (złośliwym oprogramowaniem) i przejęcie nad nim kontroli.

Specjalnie przygotowany spam potrafi wyglądać bardzo wiarygodnie, ponieważ oszuści często podszywają się pod znane firmy i instytucje. Spreparowana wiadomość ma skłonić ofiarę do działania – nagminne jest straszenie, że wydarzy się coś złego, jeśli nie podąży za otrzymaną instrukcją. Niestety, spełnienie próśb nadawcy kończy się źle dla odbiorcy – najczęściej utratą środków na koncie.

Sposób na niechciane wiadomości?

- Korzystajcie ze skrzynek pocztowych wyposażonych w filtr antyspamowy.
- Stosujcie separację tożsamości – podczas rejestracji na portale czy do sklepów internetowych korzystajcie z adresu e-mail stworzonego specjalnie do tego celu.
- Przed podaniem gdziekolwiek swojego adresu zapoznajcie się z polityką prywatności, aby przypadkiem nie wyrazić zgody na wykorzystanie swoich danych do innych celów niż tylko możliwość korzystania z zasobów danej strony, aplikacji czy usługi cyfrowej.
- Na bieżąco usuwajcie wiadomości, które zaśmiecają Waszą skrzynkę.

I pamiętajcie – podejrzane e-maile lub SMS-y możecie zgłaszać do CERT Polska. Wystarczy, że otrzymaną na telefon wiadomość wyślecie na numer 8080, używając funkcji „przekaż" albo „udostępnij". Natomiast informację o stronach internetowych służących do wyłudzania danych osobowych i uwierzytelniających możecie przesłać za pomocą formularza na stronie incydent.cert.pl.

Spoofing

To rodzaj popularnego oszustwa polegający na podszywaniu się pod konkretną osobę lub podmiot (np. instytucję, firmę) w celu pozyskania istotnych informacji lub wyłudzenia pieniędzy. Termin powstał od ang. słowa *spoof* – przedrzeźnianie, naśladowanie – i odnosi się do różnych typów ataków. Wyróżniamy np. spoofing telefoniczny, e-mail, IP i DNS.

W ostatnim czasie popularną formą oszustwa stał się spoofing telefoniczny. Przestępcy podszywają się pod wybrany numer telefonu i dzwonią do ofiary, podając się np. za pracownika banku, przedstawiciela znanej instytucji czy osobę publiczną. Żądają przykładowo zainstalowania wskazanej aplikacji, która ma nas rzekomo uchronić przed utratą pieniędzy. Bezrefleksyjne spełnienie prośby to prosty krok do przekazania cyberprzestępcom zdalnego dostępu do urządzenia użytkownika, a co za tym idzie – utraty danych lub środków na koncie. Ofiary spoofingu często myślą, że atakujący miał dostęp do ich urządzenia czy numeru telefonu. Warto wiedzieć, że połączenia te są wykonywane przez specjalne bramki, które umożliwiają wyświetlenie odbierającemu dowolnego numeru dzwoniącego.

Spoofing e-mail również nie traci na popularności. Waszą czujność powinna wzbudzić każda podejrzana wiadomość, w której nadawca – na pierwszy rzut oka wiarygodny – prosi o podanie poufnych danych czy loginów i haseł do bankowości internetowej. Najtrudniej jest rozpoznać spoofing IP lub DNS. Metoda ta polega na przekierowaniu internauty na fałszywą stronę, która do złudzenia przypomina tę oryginalną. Nietrudno się domyślić, że korzystanie z platformy przygotowanej przez przestępców naraża ofiarę na poważne straty.

Jak chronić się przed spoofingiem? Włączcie zasadę ograniczonego zaufania. Nie odpowiadajcie na żadne próby wyłudzenia poufnych informacji, sprawdzajcie dokładnie, czy na pewno logujecie się w oknie prawdziwej strony, omijajcie szerokim łukiem te platformy, które po prostu wydają się Wam dziwne. Podejrzane witryny zgłaszajcie do CERT Polska za pośrednictwem formularza na

stronie incydent.cert.pl. A jeśli macie podejrzenie, że doszło do kontaktu telefonicznego z potencjalnym oszustem, rozłączcie się i sprawdźcie (np. dzwoniąc do banku), czy taka rozmowa w ogóle powinna mieć miejsce.

Więcej informacji o spoofingu telefonicznym znajdziecie na ose.gov.pl w aktualności „Uwaga na spoofing!".

Źródło:

„Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?", (2022), artykuł na stronie gov.pl.

Spray & pray

Zapewne wielokrotnie słyszeliście przestrogi dotyczące podejrzanych wiadomości e-mail zawierających np. linki prowadzące do fałszywych stron lub załączniki, które po kliknięciu instalują na Waszych urządzeniach szkodliwe oprogramowanie. Korzystając z poczty elektronicznej, musicie być czujni i pamiętać, że to Wy jesteście swoją pierwszą linią obrony. Pamiętajcie: o wiele łatwiej jest bowiem wysłać złośliwą wiadomość niż łamać Wasze hasła i inne zabezpieczenia!

Jedną z technik stosowanych przez oszustów jest metoda spray & pray (od ang. *spray* – rozpylać i *pray* – modlić się). Polega ona na wysyłaniu dużej liczby maili lub SMS-ów, np. z informacją o wygranej w konkursie lub konieczności opłacenia zaległych rachunków, do setek odbiorców naraz. Złodzieje mają nadzieję, że ktoś popełni błąd i padnie ofiarą oszustwa, np. poda swoje dane do logowania lub inne cenne informacje. W tym przypadku liczy się więc efekt skali: im więcej wiadomości zostanie wysłanych, tym statystycznie więcej osób – przez nieuwagę, z ciekawości, ze strachu, w pośpiechu itd. – kliknie w link lub pobierze zainfekowany załącznik.

Ta metoda jest wykorzystywana często w atakach phishingowych, w których oszuści podszywają się pod znane osoby lub instytucje, próbując wyłudzić od nas poufne informacje, a nawet pieniądze.

O czym powinniście pamiętać, gdy do Waszej skrzynki trafi nieoczekiwany mail lub gdy znajdziecie podejrzaną wiadomość na komunikatorze?

- Sprawdźcie, czy adres mailowy nadawcy jest poprawny, czy wiadomość nie zawiera literówek i nie wygląda na słabo przetłumaczoną.
- Nie odpowiadajcie na takie wiadomości – wtedy oszuści upewnią się, że Was adres jest aktywny i mogą wykorzystywać go do innych ataków socjotechnicznych.
- Nie otwierajcie linków i nie pobierajcie załączników przesłanych w wiadomościach od nieznanych nadawców, nie logujcie się na stronach, które wydają Wam się sfałszowane.
- Nie reagujcie na próby szantażu i prośby o natychmiastowe działanie, nawet gdy przestępca straszy, że wydarzy się coś złego, jeśli natychmiast nie zrobicie tego, czego żąda.
- Nie podawajcie nikomu danych wrażliwych, np. numeru karty płatniczej czy hasła do konta lub danych uwierzytelniających potrzebnych do zalogowania się do serwisu.

Nie możecie zapominać także o podstawowych zasadach bezpiecznego korzystania z internetu: nie odkładajcie w nieskończoność aktualizacji, instalujcie oprogramowanie antywirusowe, dbajcie o silne hasła i korzystajcie z menedżerów haseł, ustawiajcie uwierzytelnianie dwuskładnikowe i wieloskładnikowe. Nie zaszkodzi też separacja tożsamości, czyli używanie osobnych adresów e-mail do różnych aktywności w sieci. Stosujcie zasadę ograniczonego zaufania, podając innym swój adres mailowy, a także co jakiś czas sprawdzajcie, czy Wasze adresy i dane logowania nie wyciekły (np. na stronie bezpiecznedane.gov.pl).

Jeśli w swojej skrzynce znajdziecie podejrzany e-mail, zgłoście to do CSIRT NASK za pośrednictwem strony incydent.cert.pl lub na adres cert@cert.pl. SMS-y możecie przesyłać bezpośrednio na numer 8080.

Więcej informacji o bezpiecznym korzystaniu z poczty elektronicznej znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: poczta e-mail" oraz „Bezpieczni w sieci z OSE: phishing".

Stalking

Stalking oznacza uporczywe nękanie, prześladowanie drugiej osoby, co powoduje u ofiary napięcie, stres, strach i poczucie utraty bezpieczeństwa. Działania stalkera mogą doprowadzić do dużych strat emocjonalnych, a nawet materialnych, gdy osoba pokrzywdzona będzie zmuszona np. do ciągłej zmiany numeru telefonu lub rezygnacji z pracy. Stalking – tak jak większość działań przemocowych – przeniósł się też do sieci.

Cyberstalking jest formą nękania drugiej osoby w internecie i może przybierać różne formy: od wielokrotnego przesyłania niechcianych wiadomości i materiałów, przez podszywanie się pod daną osobę, rozsyłanie wiadomości w jej imieniu, aż po śledzenie aktywności ofiary online i kradzież tożsamości. Nękanie drugiej osoby w sieci to rodzaj cyberprzemocy, która też może się przejawiać na wiele sposobów, np. wykluczaniem z grona znajomych, szantażem czy publikowaniem w sieci upokarzających materiałów – filmów lub zdjęć.

Na nękanie w sieci narażeni są wszyscy użytkownicy – w tym dzieci i młodzież. Badania NASK „Nastolatki" pokazują, że różnych form agresji online (wyzywania, ośmieszania, poniżania i straszenia) doświadczył co trzeci nastolatek. Co ważne – ze swoimi problemami dzieci często pozostają same. Aż 47% badanych zadeklarowało, że w ogóle nie podjęło żadnych działań i nikomu nie powiedziało o doświadczeniu przemocy w sieci (Ładna i in., 2025). Tymczasem dziecko pozbawione pomocy często nie jest w stanie samo stawić czoła trudnej sytuacji online.

Co grozi dziecku doświadczającemu cyberprzemocy? Ofiary prześladowania w sieci:

- mogą czuć się osaczone, osamotnione i bezsilne;
- mierzą się z poniżeniem, upokorzeniem, lękiem, rozpaczą, smutkiem;
- niekiedy mogą wstydzić się i mieć poczucie winy, że nie potrafiły same sobie poradzić z agresją;
- częściej niż ich rówieśnicy doświadczają problemów w kontaktach z innymi ludźmi;
- mają zaniżone poczucie własnej wartości;
- zaczynają mieć kłopoty z nauką;
- mierzą się z problemami psychologicznymi, a także zdrowotnymi, takimi jak bóle głowy, brzucha, problemy ze snem itp.;
- w skrajnych przypadkach mają myśli i próby samobójcze (Borkowska, 2023).

Zarówno stalking, jak i cyberstalking jest przestępstwem i podlega karze pozbawienia wolności – wszelkie przejawy uporczywego nękania zgłaszajcie na policję! Ściganie stalkera odbywa się na wniosek pokrzywdzonego, a w momencie złożenia wniosku, postępowanie karne toczy się urzędu.

Źródła:

Borkowska A., (2023), „Cyberprzemoc w szkole. Poradnik dla nauczycieli", Warszawa: Państwowy Instytut Badawczy NASK.

„Czym jest stalking?", (2021), artykuł na stronie mazowiecka.policja.gov.pl.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Stealware

Zapewne wiecie, że istnieje wiele szkodliwych programów, które potrafią działać niepostrzeżenie, a jednocześnie wyrządzać duże szkody. Jednym z nich jest oprogramowanie szpiegujące stealware (od ang. *stealing software*), które zbiera informacje o użytkowniku, by następnie przekazać pozyskane dane osobom trzecim.

Oprogramowanie tego typu oczywiście instalowane jest bez wiedzy ofiary. Przedostaje się do systemu w formie plików wykonywalnych oraz dzięki wykorzystaniu luk czy błędów w przeglądarkach internetowych. Stealware potrafi np. śledzić aktywność użytkownika na platformach z płatnością elektroniczną, by w odpowiednim momencie podmienić numer konta, przez co jego środki trafią do zupełnie innego odbiorcy niż zamierzał.

Jak chronić się przed stealware?

- Nie pobierajcie na swoje urządzenia nieautoryzowanych programów, aplikacji, gier czy „przydatnych" darmowych narzędzi. To główne źródła złośliwego oprogramowania!
- Nie zwlekajcie z aktualizacją – systemu, programów, antywirusów, przeglądarki internetowej. Wszelkie luki w oprogramowaniu otwierają furtkę cyberprzestępcom.
- Uważajcie na phishing – weryfikujcie linki otrzymane z nieznanych źródeł przed kliknięciem i zwracajcie szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych – nie uruchamiajcie ich, jeśli budzą Wasze wątpliwości. Nie wpisujcie danych uwierzytelniających (loginów i haseł) w oknach stron, które wzbudzają Wasz niepokój (mogą być fałszywe!).
- Bądźcie czujni! – kierujcie się zasadą ograniczonego zaufania. Z ostrożnością podchodźcie do przychodzących wiadomości, zasobów w sieci, osób podających się za pracowników firm czy innych instytucji, którzy np. nakłaniają Was do złamania podstawowych zasad cyberbezpieczeństwa.

Źródło:

„Ochrona przed oprogramowaniem szpiegującym", (2024), artykuł w serwisie kompetencjecyfrowe.gov.pl.

Stres cyfrowy

Spędzamy ze smartfonami, laptopami, tabletami kilka, a nawet kilkanaście godzin dziennie. Praca, nauka, kontakty z bliskimi, rozrywka, inne ważne sprawy – magnesów, które przyciągają nas przed ekrany jest naprawdę wiele. Otoczeni urządzeniami cyfrowymi często nie zauważamy momentu, w którym zamiast nam pomagać, zaczynają szkodzić.

Gdy przestajemy sobie radzić z ilością docierających do nas informacji, a nasz system nerwowy zaczyna być przeciążony, tracimy koncentrację i zdolność do skupienia się na wykonywanej czynności. Ten stan podwyższonego napięcia wywołany nadmiarem technologii i bodźców nazywamy stresem cyfrowym. Potęguje go konieczność reagowania na wszelkie powiadomienia i inne informacje, które ciągłym strumieniem płyną do nas z naszych urządzeń.

Konsekwencje stresu cyfrowego mogą być bardzo dotkliwe: to nie tylko dyskomfort, ale także brak motywacji, utrata zainteresowania codziennymi sprawami, trudności w radzeniu sobie z obowiązkami szkolnymi, zawodowymi czy rodzinnymi, a nawet – problemy ze zdrowiem i pamięcią.

Na szczęście stresu cyfrowego można uniknąć, ale też pokonać go, jeśli już się pojawi. Jak to zrobić? Jednym ze sposobów jest świadome, czasowe odcinanie się od technologii, czyli tzw. cyfrowy detoks. Niezbędne okazuje się też wypracowanie nowych, zdrowszych cyfrowych nawyków. Nie warto z tym zwlekać! Najlepszym sposobem będzie tutaj ustalenie – wspólnie z domownikami – zasad dotyczących korzystania z internetu i smartfonów. Powinny one dotyczyć limitu czasu

spędzanego przed ekranem oraz sytuacji, w których nie używacie smartfonów (np. podczas posiłków, godzinę przed snem). Dobrze jest wprowadzić takie zasady jak najwcześniej – a zwłaszcza w momencie, gdy wręczacie dziecku jego pierwsze urządzenie z dostępem do internetu.

Dodatkowym wsparciem dla rodziców w ustalaniu reguł dotyczących korzystania z urządzeń cyfrowych przez dzieci może być aplikacja mOchrona. To darmowe narzędzie umożliwia ograniczanie dostępu do wybranych kategorii stron i aplikacji, a także – wgląd w raporty z aktywności dziecka na jego smartfonie, tablecie czy komputerze. Dzięki temu jako rodzice możecie nie tylko ograniczać ryzyko kontaktu ze szkodliwymi treściam i w sieci, ale również reagować, gdy z raportów dowiecie się, np. że dziecko korzysta z internetu w sposób niezgodny z ustalonymi wspólnie zasadami.

Pamiętajcie: dbanie o właściwy balans pomiędzy aktywnościami w sieci i poza nią oraz przestrzeganie zasad higieny cyfrowej to bardzo ważne elementy naszego dobrostanu!

O stresie cyfrowym i równowadze online–offline przeczytacie więcej w aktualnościach na stronie ose.gov.pl: „Stres cyfrowy – czym jest i jak go pokonać?", „Zadbaj o siebie z OSE: cyfrowy stres", „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa", a także w poradniku „Mniej znaczy więcej. O multiscreeningu i wielozadaniowości" dostępnym na platformie OSE IT Szkoła.

Szkodliwe treści

W internecie znajdziemy z jednej strony pozytywne i inspirujące materiały, a z drugiej – takie, które mogą zaniepokoić, budzić złość, szokować. Szkodliwe treści wpływają negatywnie szczególnie na młodych internautów. Zaliczamy do nich m.in. materiały przedstawiające przemoc, pokazujące zachowania niebezpieczne dla zdrowia i życia (samookaleczenia, restrykcyjne diety, zażywanie szkodliwych substancji, samobójstwa, ryzykowne wyzwania), pornografię, treści szerzące mowę nienawiści, fałszywe informacje czy patostreamy, czyli relacje online na żywo prezentujące zachowania określane i postrzegane jako patologiczne.

O ile sporadyczny kontakt dziecka z nieodpowiednimi materiałami może oddziaływać na jego samopoczucie, o tyle ich regularne oglądanie ma już destrukcyjny wpływ na rozwój, psychikę, postrzeganie świata. Szkodliwe treści narażają też młodych internautów na niebezpieczeństwa. Pod ich wpływem młodzi ludzie podejmują wiele ryzykownych zachowań. Biorą udział w internetowych wyzwaniach – challenge'ach, spotykają się „w realu" z osobami poznanymi w sieci, grają w gry zawierające elementy hazardowe bądź brutalne treści czy dzielą się z innymi swoimi intymnymi materiałami (seksting).

Jak zapobiegać kontaktowi ze szkodliwymi treściami? Na pewno nie jesteście w stanie kontrolować każdego kroku dziecka w sieci, szczególnie jeśli już samodzielnie korzysta z internetu. Postawcie więc na profilaktykę: odpowiednie zabezpieczenie urządzenia dziecka, aby minimalizować kontakt z nieodpowiednimi treściami, oraz naukę właściwego reagowania na niebezpieczne sytuacje w sieci.

W domu towarzyszcie dziecku w wirtualnym świecie, interesujcie się tym, co ogląda, jakie strony odwiedza. Wspólnie ustalcie też zasady korzystania z internetu. W przypadku starszych dzieci podstawą jest rozmowa i edukacja na temat cyberzagrożeń, u młodszych sprawdzi się np. aplikacja ochrony rodzicielskiej – mOchrona. Pamiętajcie też o wyborze odpowiednich dla wieku dziecka gier komputerowych – kierujcie się przy tym ogólnoeuropejskim systemem klasyfikowania gier (PEGI), który określa, jaka rozrywka będzie dla niego bezpieczna. W szkole rozmawiajcie o bezpieczeństwie w sieci już z najmłodszymi, uczcie krytycznego podchodzenia do informacji znalezionych online, promujcie pozytywne treści.

Jeśli doszło do kontaktu dziecka ze szkodliwymi materiałami – reagujcie, zarówno w domu, jak i w szkole. Otoczcie dziecko opieką, wysłuchajcie, okażcie wsparcie. Na wiele tego rodzaju materiałów dzieci trafiają przypadkiem, wcale ich nie szukając, co może być źródłem niechcianych emocji. Niektóre szkodliwe treści mogą jednak bardzo ciekawić dzieci, wywoływać ekscytację (np. kontakt z pornografią czy patostreamami) – nie oceniajcie, tylko starajcie się zrozumieć,

dlaczego dziecko się nimi interesuje, wyjaśniajcie też różnicę między prezentowanymi materiałami a tym, jak wygląda prawdziwe życie. Z pomocą zawsze przyjdą specjaliści – korzystajcie z telefonów zaufania (helpline). Pamiętajcie też, że szkodliwe treści nie zawsze naruszają prawo, ale są wyjątki. Rozpowszechnianie materiałów m.in. związanych z seksualnym wykorzystywaniem dzieci jest karalne! Takie przypadki bezwzględnie zgłaszajcie na policję, możecie również skorzystać z pomocy zespołu Dyżurnet.pl.

Chcecie uzyskać więcej informacji na temat tego zagrożenia? Skorzystajcie z naszych materiałów dostępnych na platformie OSE IT Szkoła. Nauczycielom polecamy poradnik: „Szkodliwe treści w internecie", scenariusz zajęć „Ryzykowne zachowania w internecie: szkodliwe treści" oraz webinar „Szkodliwe treści w internecie. Profilaktyka i reagowanie". Rodzicom natomiast – poradnik „Szkodliwe treści w internecie. Nie akceptuję, reaguję!". Zajrzyjcie też do aktualności „Cyberbezpieczna biblioteczka: szkodliwe treści", w której piszemy o innych materiałach edukacyjnych związanych z niebezpiecznymi treściami.

Źródło:

„Kongres OSE 2024: szkodliwe treści w internecie", (2025), artykuł na stronie ose.gov.pl.

Sztuczna inteligencja

Sztuczna inteligencja (ang. *artificial intelligence*, AI) dosłownie nas otacza i mamy z nią do czynienia częściej, niż mogłoby się wydawać. Inteligentne domy, zabawki, wirtualni asystenci, a nawet algorytmy wyszukiwarek to tylko niektóre z jej zdobyczy. Czym dokładnie jest?

Według jednych termin ten obejmuje jedynie zagadnienia związane ze sztucznymi formami życia, które mogą przewyższać ludzką inteligencję. Inni zaś twierdzą, że sztuczną inteligencją można nazwać każdą technologię przetwarzania danych. Nie istnieje jedna przyjęta definicja!

Sztuczna inteligencja:

- To dziedzina wiedzy obejmująca logikę rozmytą, obliczenia ewolucyjne, sieci neuronowe, sztuczne życie i robotykę.
- To dział informatyki zajmujący się tworzeniem modeli zachowań inteligentnych i programów komputerowych symulujących te zachowania.
- To dział informatyki zajmujący się rozwiązywaniem problemów, których nie da się rozwiązać za pomocą łatwego algorytmu.
- To konstruowanie maszyn, których działania są podobne do przejawów ludzkiej inteligencji.

Co bardzo istotne, sztuczna inteligencja wykorzystuje matematykę oraz logikę do symulowania rozumowania, którego ludzie używają do uczenia się na podstawie nowych informacji i podejmowania decyzji. AI prognozuje lub podejmuje decyzje w oparciu o wzorce, a następnie sama się doskonali, aby zwiększyć swoją wydajność i dokładność (Świerczek, 2024).

Skupmy się jednak na sztucznej inteligencji, która znajduje swoje zastosowanie w cyberbezpieczeństwie (lub jest wykorzystywana przez oszustów, by wprowadzić nas w błąd albo potencjalnie wykradać nasze dane). Jako że dzięki AI możliwe jest przetwarzanie dużych zbiorów informacji w krótkim czasie, tę technologię wykorzystuje się do wykrywania zagrożeń oraz automatyzacji procesów obronnych. To nie wszystko: sztuczna inteligencja umożliwia także (np. na podstawie biometrii behawioralnej) identyfikowanie potencjalnych niebezpieczeństw w sieci i reagowanie na nie w czasie rzeczywistym. Można więc powiedzieć, że na wielu polach AI jest i będzie naszym sprzymierzeńcem.

Nie można zapominać jednak o drugiej stronie medalu. Musimy liczyć się m.in. z zagrożeniami w zakresie generatywnych modeli sztucznej inteligencji, czyli – w skrócie – modeli algorytmicznych szkolonych do tworzenia nowych danych, takich jak teksty, obrazy i dźwięki (Stanecki, 2023). Wielu z Was zetknęło się z takimi modelami, np. korzystając z popularnych chatbotów AI. Choć

tacy „asystenci" mogą usprawniać pracę i optymalizować wykonywanie różnych zadań, korzystanie z nich niesie za sobą także potencjalne niebezpieczeństwa związane np. z ochroną prywatności. Dane na nasz temat zamieszczane w internecie mogą być wykorzystywane przez AI bez naszej zgody, co więcej – mogą posłużyć do tworzenia nowych obrazów, tak jak w przypadku deepfake. Generatywne modele sztucznej inteligencji są w stanie wytwarzać treści, które do złudzenia przypominają rzeczywiste, np. głosy, zdjęcia czy materiały wideo. SI może zatem posłużyć do szerzenia dezinformacji i celowego wprowadzania użytkowników internetu w błąd.

Naukowcy są pewni, że w przyszłości sztuczna inteligencja zmieni wiele aspektów naszego życia i gospodarki. Czy wygra z ludzką, czy chatboty zastąpią człowieka? Czy mamy się czego obawiać? Jedno jest pewne: jako zwykli użytkownicy internetu i narzędzi bazujących na AI, musimy zwracać szczególną uwagę na bezpieczeństwo naszych danych i nie ufać wszystkiemu, co widzimy w sieci.

Chcecie dowiedzieć się więcej na temat początków sztucznej inteligencji i jej zastosowań, testu Turinga, uczenia maszynowego i sieci neuronowych? Zajrzyjcie na OSE IT Szkołę – czeka tam na Was 27 bezpłatnych kursów, zebranych w kategorii Sztuczna inteligencja. Gwarantujemy, że nasze materiały wprowadzą Was w pasjonujący świat SI i rozbudzą Waszą ciekawość!

Źródła:

Stanecki J., (2023), „Zagrożenia związane z Chat GPT o innymi AI", artykuł w serwisie gdpr.pl.

Świerczek S., (2024), „Sztuczna inteligencja (AI) w cyberbezpieczeństwie", artykuł w serwisie netcomplex.pl.

Szyfrowanie end-to-end

Cyberprzestępcy nie śpią, dlatego my także musimy trzymać rękę na pulsie i coraz lepiej zabezpieczać nasze konta i cenne informacje. Ważną bronią może się okazać oprogramowanie szyfrujące, które uniemożliwia osobom niepowołanym dostęp do prywatnych plików lub danych.

O szyfrowaniu powinniśmy pamiętać nie tylko przechowując poufne dokumenty, ale też wysyłając je za pośrednictwem poczty elektronicznej. To samo dotyczy szyfrowania end-to-end (ang. *End-to-End-Encryption*, E2E) stosowanego obecnie w różnych aplikacjach, m.in. komunikatorach internetowych.

Na czym polega szyfrowanie „od końca do końca"? Dzięki niemu do wymienianych wiadomości mają dostęp wyłącznie prawdziwi nadawca i odbiorca, a nie osoby trzecie, np. dostawcy platformy, usług telekomunikacyjnych czy internetu. To nie wszystko – szyfrowanie end-to-end nie tylko zapobiega odczytywaniu przesyłanych danych, ale też ich potajemnej modyfikacji. Najprościej rzecz ujmując, gdy korzystacie z takiego zabezpieczenia, nie pozwalacie nikomu niepowołanemu na odszyfrowanie wymienianych wiadomości lub kluczy kryptograficznych potrzebnych do ich odszyfrowania.

Warto wiedzieć, że w wielu systemach przesyłania wiadomości, w tym w poczcie elektronicznej i wielu komunikatorach internetowych, wiadomości przechodzą przez pośredników i są przez nich przechowywane, a zatem dostępne np. dla usługodawcy. Choć takie rozwiązanie ma pewne zalety, przykładowo pozwala przeszukiwać archiwum konwersacji po konkretnych słowach, wiąże się jednak z zagrożeniami dla prywatności i poufności danych.

Czy zatem przesyłanie prywatnych zdjęć albo innych wrażliwych informacji jest w ogóle bezpieczne? Kiedy chcecie komunikować się z innymi w internecie, musicie zwracać uwagę na to, jakie opcje zabezpieczeń oferują aplikacje i programy, z których korzystacie. Wiele z nich, np. popularne komunikatory, umożliwia włączenie szyfrowania end-to-end lub domyślnie je stosuje. Sprawdźcie koniecznie (w ustawieniach aplikacji), czy bezpiecznie przesyłacie swoje wiadomości!

Uważajcie też na kopie zapasowe swoich czatów, które nierzadko są naszym swoistym pamiętnikiem – z przyjaciółmi i rodziną wymieniamy się przecież zdjęciami, filmikami i innymi treściami.

Gdy robicie backup, np. by móc przenieść zapisane rozmowy na nowe urządzenie, pamiętajcie, by zaszyfrować również te kopie. Bez tego będą one widoczne w usługach chmurowych.

Wasze aplikacje mają możliwość ustawienia „znikających wiadomości” po odczytaniu ich przez odbiorcę? Włączcie je! To dodatkowe zabezpieczenie Waszych internetowych rozmów.

Więcej informacji o tym, jak chronić swoje dane w internecie, znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: szyfrowanie end-to-end”, „Bezpieczni w sieci z OSE: komunikatory internetowe”, „Bezpieczni w sieci z OSE: poczta e-mail”, „Bezpieczni w sieci z OSE: ochrona danych osobowych”, „Bezpieczni w sieci z OSE: bezpieczne logowanie” i „Bezpieczni w sieci z OSE: przechowywanie danych w chmurze”.

T

Techniczny Reprezentant Szkoły (TRS)

To osoba upoważniona przez dyrektora szkoły do kontaktów z Operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE) w sprawach technicznych. Do jego zadań należy administracja szkolną siecią LAN oraz zarządzanie urządzeniami sieciowymi, takimi jak przełączniki (switch) i punkty dostępowe (access point). TRS odpowiada również za instalację certyfikatów w szkole oraz współpracę przy dostosowywaniu infrastruktury szkolnej do wymogów sieci OSE.

Do obowiązków technicznego reprezentanta należy także konfigurowanie szkolnych urządzeń, dołączanie nowych elementów do infrastruktury OSE i kontrola poprawności ich działania. Dba on o zapewnienie bezprzerwowego zasilania urządzeń sieciowych oraz utrzymanie ich w stanie pełnej sprawności. W swojej pracy współpracuje z Centrum Kontaktu OSE, przekazując zgłoszenia, informacje zwrotne oraz komunikaty o braku dostępności urządzeń, np. w przypadku awarii zasilania. Informuje również o planowanych pracach remontowych, konserwacyjnych i modernizacyjnych w szkole, a także przekazuje inne niezbędne dane dotyczące usług sieciowych, które są wykorzystywane w placówce, by zapewnić ciągłość i prawidłowość ich działania.

Narzędziem pracy TRS-a jest Moje OSE – portal, za pomocą którego może on w łatwy sposób zaktualizować swoje dane, odnaleźć niezbędne dokumenty, zarządzać usługami czy zgłosić problem techniczny z działaniem sieci. Zgłoszeń mogą dokonywać także za pośrednictwem infolinii (tel.: +48 22 182 55 55, e-mail: wsparcietechniczne_ose@nask.pl).

Teorie spiskowe

„Ziemia jest płaska", „Finlandia nie istnieje", „Michael Jackson żyje"... Zapewne wszyscy słyszeliście tego rodzaju rewelacje. To teorie spiskowe – przekonania, według których za określonymi wydarzeniami, zjawiskami czy decyzjami stoją ukryte grupy lub organizacje działające w tajemnicy, mające rzekomo dążyć do osiągnięcia własnych celów kosztem reszty społeczeństwa. Zazwyczaj zakładają one, że oficjalne wyjaśnienia są fałszywe, a prawda została celowo ukryta.

Źródła teorii spiskowych są różnorodne. Wiele z nich pojawia się w momentach niepewności, kryzysów i społecznego lęku, gdy ludzie szukają prostych odpowiedzi na trudne pytania. Internet i media społecznościowe przyspieszyły ich rozprzestrzenianie, ponieważ umożliwiają szybkie udostępnianie treści bez weryfikacji źródeł. Dodatkowo działają tu mechanizmy psychologiczne: ludzki mózg ma tendencję do szukania wzorców i przyczyn nawet tam, gdzie ich nie ma, co sprawia, że narracje spiskowe wydają się logiczne i uporządkowane.

Wiarę w teorie spiskowe wzmacniają także czynniki społeczne i emocjonalne. Osoby, które czują się marginalizowane, nieufne wobec władzy lub instytucji, są bardziej podatne na przekonania spiskowe. W świecie pełnym informacji teorie tego typu mogą też dawać poczucie wyjątkowości i przynależności do „grupy wtajemniczonych", którzy „znają prawdę".

Teorie spiskowe mogą dotyczyć niemal wszystkiego – od wydarzeń historycznych, takich jak lądowanie na Księżycu, po zdrowie publiczne, szczepienia czy rozwój technologii. Choć część z nich wydaje się nieszkodliwa, inne prowadzą do realnych zagrożeń, np. szerzenia dezinformacji, podważania zaufania do nauki i instytucji publicznych czy wzrostu agresji wobec określonych grup społecznych.

Jak się przed nimi bronić? Przede wszystkim warto sprawdzać źródła informacji, analizować, kto jest ich autorem i jakie ma motywacje. Pomocne jest też porównywanie treści z wiarygodnymi mediami i publikacjami naukowymi. Kluczowa jest edukacja medialna i krytyczne myślenie – umiejętność zadawania pytań, weryfikowania faktów i dostrzegania manipulacji. Dobrym nawykiem jest również unikanie emocjonalnego reagowania na sensacyjne wiadomości oraz świadomość, że nie każda niewyjaśniona sprawa musi mieć ukryty spisek w tle.

Więcej informacji znajdziecie w kursie e-learningowym „Dezinformacja, czyli w co (nie) wierzyć w internecie” i aktualności „Temat lekcji: manipulacje w sieci i teorie spiskowe” na platformie OSE IT Szkoła.

Troll parenting

Rodzice często dzielą się w internecie zdjęciami swoich dzieci – to fakt. Nierzadko to śmieszne materiały zarejestrowane podczas codziennych momentów. Jednak czy zawsze, zanim mama i tata klikną „opublikuj”, zastanawiają się, czy zdjęcie lub filmik nie są śmieszne tylko dla nich…?

Troll parenting, bo o nim mowa, polega na udostępnianiu online treści, które przedstawiają dziecko w sytuacjach ośmieszających lub zawstydzających, często bez jego zgody. Mogą to być filmiki pokazujące płaczącego, przestraszonego malucha czy zdjęcia z komentarzami mającymi rozbawić dorosłych widzów. Dla rodziców to „niewinny żart”, dla odbiorców – rozrywka. Dla dziecka jednak takie materiały mogą być źródłem wstydu i upokorzenia.

Psychologowie zwracają uwagę, że dzieci nie mają jeszcze narzędzi, by rozumieć kontekst internetowego żartu. Nagranie, które dla dorosłych jest zabawne, dla kilkulatka może być bolesnym doświadczeniem, które utrwali się w pamięci. Co więcej, raz wrzucone do sieci, takie treści mogą krążyć tam latami: pojawiać się w memach, filmach z przeróbkami, a nawet powracać w okresie dojrzewania, gdy wrażliwość i potrzeba akceptacji są u dzieci szczególnie silne.

Troll parenting to jedno z oblicz sharentingu, czyli nadmiernego dzielenia się życiem dziecka w internecie. Różnica polega jednak na intencji – w troll parentingu chodzi o wywołanie reakcji publiczności, często kosztem emocji dziecka. Rodzice stają się tu nie tylko twórcami, ale też „reżyserami” sytuacji, w których syn czy córka pełni rolę nieświadomego aktora.

Należy pamiętać, że dziecku – podobnie jak każdej osobie dorosłej – przysługuje prawo do ochrony wizerunku, które wynika bezpośrednio z Kodeksu cywilnego (art. 23). Co więcej, zgodnie z prawem to rodzic odpowiada za ochronę dobra małoletniego, a więc także za to, by nie naruszać jego prywatności ani godności. Niczyje dzieciństwo nie powinno stać się internetowym widowiskiem!

Zanim więc wrzucicie do sieci zabawny filmik, zadajcie sobie kilka prostych pytań: Czy moje dziecko chciałoby, by to zobaczyli jego koledzy z klasy? Czy ten materiał będzie dla niego nadal zabawny za kilka lat? Czy naprawdę potrzebuję tych kilku sekund śmiechu – kosztem poczucia bezpieczeństwa syna lub córki?

Więcej o troll parentingu dowiecie się z kursu „Sharenting. Czy warto mieć rodzinny album w sieci?” oraz poradnika „Sharenting i wizerunek dziecka w sieci” dostępnych na platformie OSE IT Szkoła.

Trolling w sieci

„Troll” w sieci to nie mityczne stworzenie z bajek, ale użytkownik, który świadomie i celowo wywołuje kłótnie, ośmiesza innych lub swoimi komentarzami rozbija dyskusję. Jego celem nie jest rzeczowe komentowanie toczącej się rozmowy, ale wywołanie emocjonalnej reakcji innych użytkowników. Troll czuje się zwycięzcą wtedy, gdy uda mu się kogoś sprowokować, zdenerwować lub upokorzyć.

Choć wielu trolli tłumaczy swoje zachowanie „żartem”, za trollingiem często kryje się potrzeba władzy, kontroli lub kompensowania własnych frustracji. Pozorna anonimowość w internecie sprzyja takiemu zachowaniu: łatwiej być złośliwym, gdy nie patrzy się drugiej osobie w oczy.

Dziś trolling może być formą cyberprzemocy – obejmuje wyśmiewanie, nękanie, publikowanie obraźliwych komentarzy, a nawet manipulowanie cudzym wizerunkiem. W badaniach nad zachowaniami w sieci zwraca się uwagę, że trolling potrafi realnie wpływać na psychikę ofiar. Osoby regularnie nękane w internecie częściej doświadczają obniżonego nastroju, lęku i społecznego wykluczenia. Czasem jeden złośliwy komentarz wystarczy, by zniszczyć komuś reputację lub poczucie własnej wartości.

Troll, który umiejętnie podsyca dyskusję, obserwuje z satysfakcją, jak inni kłócą się między sobą. W ten sposób zyskuje uwagę i poczucie wpływu – dwa silne bodźce wzmacniające jego zachowanie. Dodatkowo media społecznościowe, poprzez swoje algorytmy, umożliwiają osiąganie większych zasięgów treściom wywołującym silne emocje. Im więcej reakcji, tym większy zasięg. Troll dostaje więc dokładnie to, czego chce – widzialność.

Jak reagować na trolling? Najprostsza zasada brzmi: nie karmić trolla. Każda emocjonalna odpowiedź to paliwo dla prowokatora. Zamiast wdawać się w dyskusję, warto zgłosić obraźliwy komentarz i zablokować użytkownika. W ten sposób lepiej zadbamy o bezpieczeństwo emocjonalne własne i innych osób zaangażowanych w rozmowę.

Ważne jest również edukowanie – szczególnie młodych użytkowników – że trolling to nie forma dowcipu, lecz internetowa agresja. Warto uczyć rozpoznawania różnic między konstruktywną krytyką a zachowaniem, które ma jedynie zranić lub ośmieszyć.

Gdy zapominamy, że po drugiej stronie ekranu jest człowiek, łatwiej o agresję, szyderstwo i prowokację. Budowanie kultury sieci opartej na szacunku i zrozumieniu to zadanie dla nas wszystkich – nauczycieli, rodziców i twórców platform.

Tryb incognito

Dobrze wiecie, że w internecie nic nie ginie, a każda nasza aktywność w sieci zostawia za sobą cyfrowy ślad. Strony, które przeglądamy, zbierają mnóstwo informacji na nasz temat, co w efekcie prowadzi np. do wyświetlania spersonalizowanych reklam. A co, gdybyśmy chcieli zadbać o swoją anonimowość online i chociaż częściowo się ukryć? Pomoże w tym tryb incognito (inaczej tryb prywatny), który możecie wybrać w swojej przeglądarce. Jak to działa?

Gdy korzystacie z trybu incognito, przeglądarka nie zapisuje na urządzeniu (komputerze, laptopie, smartfonie, tablecie) historii przeglądania, plików cookies ani danych, które podajecie w formularzach. Dzięki temu strony internetowe „nie wiedzą", kim jesteście, dopóki się nie zalogujecie, czyli w tym momencie jesteście dla nich nowymi użytkownikami. Za każdym razem, gdy zamykacie kartę incognito, przeglądarka usuwa wszystkie dane stron i pliki cookies powiązane ze stronami, na których się pojawiliście. Wystarczy w ustawieniach wybrać „Nowe okno incognito" lub „Nowe okno prywatne" i gotowe!

Dlaczego warto korzystać z tego rozwiązania?

- Wasza aktywność w sieci nie będzie widoczna w historii przeglądarki, a więc nie zobaczą jej inni użytkownicy urządzenia (może się to okazać przydatne np. podczas kupowania prezentu niespodzianki dla Waszego domownika).
- W trybie incognito możecie bez obaw korzystać z loginów i haseł na różnych portalach – nie będą one przechowywane w pamięci urządzenia.
- Tryb incognito pomaga w korzystaniu z cudzych, ale zaufanych urządzeń (trzeba pamiętać, że nie chroni nas i naszych danych, gdy na urządzeniu zainstalowane jest malware – złośliwe oprogramowanie lub gdy odwiedziliśmy stronę phishingową).
- Gdy wyszukujecie w internecie jakąś frazę, otrzymujecie wyniki dopasowane do Waszych preferencji i pasujące do poprzednich wyszukiwań (co znaczy, że jeśli dwie osoby wpiszą w wyszukiwarkę to samo hasło, obie otrzymają różne wyniki). Włączając tryb prywatny, uzyskujecie wyniki, które nie uwzględniają danych na Wasz temat zebranych wcześniej przez przeglądarkę.

Choć korzystanie z trybu incognito ma swoje niezaprzeczalne plusy, warto wiedzieć, że nie zapewnia pełnej anonimowości w internecie. Mimo że w przeglądarce nie zapisują się informacje związane z Waszą aktywnością w sieci, to wciąż są one dostępne dla dostawcy usług internetowych, osób zarządzających odwiedzanymi stronami internetowymi i firm wykorzystujących algorytmy śledzące na tych stronach (np. serwisów społecznościowych). Oznacza to, że prywatność przeglądania ogranicza się wyłącznie do sprzętu, z którego korzystacie.

Uwaga: w trybie incognito musicie pamiętać o podstawowych zasadach bezpiecznego korzystania z sieci. Choć pozostajecie „w ukryciu", musicie dbać o siebie tak jak podczas swoich „jawnych" aktywności w internecie. Tryb prywatny nie jest niestety peleryną niewidką, dzięki której uchronicie się przed niebezpieczeństwami online!

Więcej o bezpiecznym korzystaniu z przeglądarek internetowych i ochronie swojej tożsamości w sieci przeczytacie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: przeglądarki internetowe", „Bezpieczni w sieci z OSE: kradzież danych i tożsamości", „Bezpieczni w sieci z OSE: ochrona danych osobowych".

Typosquatting

To kolejne popularne internetowe oszustwo, które związane jest z procederem tworzenia fałszywych paneli logowania. Pojęcie typosquatting zostało stworzone poprzez połączenie dwóch angielskich słów typo (literówka) oraz squatting (czaić się), co doskonale oddaje istotę problemu.

Na czym dokładnie polega typosquatting, zwany też URL hijackingiem (dosłownie oznaczającym porwanie adresu URL)? Cyberprzestępcy rejestrują fałszywe strony, wykorzystując nazwy powszechnie znanych firm, choć nieco zmienione. Warto więc uważnie przyglądać się adresowi, jaki widnieje w polu przeglądarki. Fałszywa domena może mieć w nazwie trudny do wychwycenia błąd: zawierać literówkę lub dodatkowy znak, np. kropkę lub łącznik (uważajcie też na brakujące znaki!).

Spreparowane strony na ogół na pierwszy rzut oka nie wzbudzają podejrzeń. Wyglądają tak samo jak ich oryginalne odpowiedniki: kolorystyka, krój czcionek, grafika, elementy nawigacji – niby wszystko się zgadza. Problem zaczyna się, gdy zalogujecie się na przygotowaną przez cyberoszustów witrynę: do poczty elektronicznej, banku, e-sklepu, mediów społecznościowych. Cena, jaką zapłacicie za chwilę nieuwagi, jest dość wysoka.

Skorzystanie z fałszywych paneli logowania wiąże się z utratą poufnych danych, loginów, haseł, numerów kart płatniczych, numerów PESEL czy dowodów osobistych, a co za tym idzie również z kradzieżą środków finansowych. Ponadto witryny wykorzystujące typosquatting mogą także udostępniać malware (złośliwe oprogramowanie), co oznacza, że niepostrzeżenie możecie zainstalować na swoim sprzęcie np. ransomware, adware czy spyware, sądząc, że to legalne oprogramowanie. Otwieracie tym samym cyberprzestępcom wirtualne drzwi do Waszych urządzeń. Warto pamiętać, że typosquatting uderza też w firmy, których markę wykorzystują oszuści. Straty wizerunkowe, ale też finansowe, to częsta konsekwencja URL hijackingu.

Jak się przed nim bronić? Jak zwykle sprawdzi się zachowywanie podstawowych zasad bezpieczeństwa w sieci.

- Pamiętajcie o instalacji oprogramowania antywirusowego, bieżącej aktualizacji przeglądarki internetowej i programów.
- Pobierajcie aplikacje i programy tylko z wiarygodnych źródeł.
- Sprawdzajcie, dokąd prowadzą otrzymane linki, np. najeżdżając kursorem myszki na adres URL.
- Jeśli jakaś wiadomość SMS lub e-mail wydadzą Wam się podejrzane, nie klikajcie w przesłane linki i nie pobierajcie załączników – to może być phishing.
- Uważnie wpisujcie adres do przeglądarki i sprawdzajcie, czy jesteście na oryginalnej stronie.
- Korzystajcie z uwierzytelniania dwuskładnikowego wszędzie tam, gdzie to możliwe.

Jeśli macie podejrzenie, że jakaś witryna internetowa wykorzystuje typosquatting w celu wyłudzenia danych lub pieniędzy, koniecznie zgłoście to do CERT Polska za pośrednictwem formularza dostępnego na stronie incydent.cert.pl. Eksperci ocenią, czy wypisać ją na listę ostrzeżeń przed niebezpiecznymi stronami.

U

Unboxing w grach cyfrowych

Gry komputerowe online przyciągają użytkowników na całym świecie. Nic w tym dziwnego: ta forma rozrywki to dla wielu osób doskonały sposób na relaks, okazja do spotkania się w sieci ze społecznością o wspólnych zainteresowaniach, możliwość rywalizacji, wyzwalania emocji, osiągania sukcesów – być może niedostępnych w „realu", a także sposobność do zdobywania wiedzy oraz nowych umiejętności.

Oczywiście każdy medal ma dwie strony. W przypadku gamingu łatwo wpaść w pułapkę nadużywania nowych technologii, a nawet e-uzależnienia. Częstym problemem jest również ukryty w grach hazard, jeśli wyposażenie wirtualnych postaci wiąże się z ciągłymi inwestycjami. Zwraca się też uwagę na pułapkę związaną z grami free-to-play, które tylko z pozoru są bezpłatne. W rzeczywistości wymuszają na użytkowniku mikropłatności, a te łatwo mogą wymknąć się spod kontroli.

W tym kontekście należy wspomnieć o lootboxach, nazywanych też skrzynkami z nagrodami czy paczkami. Kryją się w nich dodatki, z których gracz może skorzystać lub nie: wyposażenie postaci, broń czy nowa umiejętność, mogąca zwiększyć szanse na wygrane. Za unboxing, czyli rozpakowanie paczki-niespodzianki, oczywiście trzeba zapłacić – wirtualnymi lub prawdziwymi pieniędzmi. Podczas otwierania „pudełka" można liczyć na element zaskoczenia, bo nagrody przydzielane są losowo. Czy warto brać udział w takiej wirtualnej loterii?

Jeśli zasady kupowania lootboxów są jasne dla gracza i wybór tej opcji gry jest dowolny, nie ma w tym nic złego. Gorzej, jeśli warunkiem przejścia do kolejnego etapu jest zakup i unboxing skrzynki z nagrodami. Eksperci podkreślają też, że lootboxy pomagają w „zaszywaniu" elementów, które tradycyjnie występują w grach hazardowych. W tym przypadku inwestowanie w grę często wiąże się z dokonaniem nawet kilkuset mikropłatności. Łatwo wpaść w spiralę kosztów. Unboxing daje bowiem graczowi możliwość większego zaangażowania w rozgrywkę i przeżycia silnych emocji: ekscytacji związanej z nadzieją na odkrycie wyjątkowego przedmiotu.

Pamiętajcie, że zaangażowanie dzieci i młodzieży w gry o hazardowym charakterze niesie za sobą ryzyko uzależnienia od hazardu w dorosłym życiu. Z rozwagą sięgajcie więc po taką formę zabawy, która nie wiąże się z przykrymi konsekwencjami. Podczas wyboru gry kierujcie się ogólnoeuropejskim systemem klasyfikowania gier (PEGI), który określa, jaka rozrywka będzie dla dziecka bezpieczna.

Chcecie dowiedzieć się więcej o pozytywnych i negatywnych aspektach grania? Skorzystajcie z materiałów dostępnych na platformie e-learningowej OSE IT Szkoła. Szczególnie polecamy: poradnik dla rodziców „Nastolatki i gry cyfrowe", ekspercki webinar „Gry komputerowe – dobra zabawa, rozwojowa szansa czy niebezpieczna rozrywka?", zbiór felietonów „O grach cyfrowych", kurs dla starszych uczniów „Cyberprzemoc w grach internetowych" i kurs dla młodszych dzieci „Owce w sieci – Zamęt w głowach".

User experience (UX)

Na co dzień korzystamy ze stron internetowych i aplikacji, jednak nie wszystkie lubimy w tym samym stopniu. Od czego to zależy? Przede wszystkim od user experience (UX), czyli doświadczenia użytkownika, a więc wrażeń i odczuć, które budzi w nas cyfrowy (w tym przypadku) produkt.

Strony i aplikacje zaprojektowane z uwzględnieniem UX w centrum stawiają człowieka i jego komfort. Liczą się zatem intuicyjność, przejrzystość nawigacji, jasny przekaz informacji i maksimum funkcjonalności. Nie bez znaczenia jest też atrakcyjny projekt interfejsu, a także ogólny wygląd strony. Im lepiej dana witryna jest przygotowana pod kątem user experience, tym większe szanse na to, że użytkownicy wrócą, polecą ją znajomym, zrobią zakupy – będą często z niej korzystać. Za projektem UX stoją specjaliści z zakresu IT, którym nieobce są zagadnienia związane z wzornictwem przemysłowym, dostępnością cyfrową, a nawet… psychologią i socjologią.

U

Czy UX może mieć coś wspólnego z cyberbezpieczeństwem? Okazuje się, że tak. Badania (Rybak, Dudczyk, 2019) wykazują, że osoby, które korzystają z portali społecznościowych, nie zawsze mają pełną świadomość zagrożeń związanych z udostępnianiem tam swoich danych osobowych. Dzielą się w sieci prywatnymi informacjami, kierując się… pozytywnymi wrażeniami wywoływanymi przez dany serwis. Pamiętajcie – zasada ograniczonego zaufania przede wszystkim!

Źródło:

Rybak Ł., Dudczyk J., (2019), „User experience w aspekcie zagrożenia dla bezpieczeństwa cyfrowego", Journal of Modern Science, tom 2/41, s. 127–140.

Usługi bezpieczeństwa OSE

W ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) oferujemy szkołom w całej Polsce dostęp do bezpłatnego, szybkiego, szerokopasmowego internetu o prędkości 100/100 Mb/s. Na tym nie koniec – nasi użytkownicy mogą liczyć także na profesjonalne, bezpłatne usługi bezpieczeństwa:

- **Bezpieczny internet OSE**. To usługa, która jest aktywna w każdej szkole podłączonej do OSE. Zapewnia zabezpieczenie sieci i jej użytkowników przed dostępem do treści potencjalnie szkodliwych, szkodliwym oprogramowaniem, atakami sieciowymi oraz wirusami na poziomie podstawowym.
- **Ochrona przed szkodliwym oprogramowaniem (w ramach OSE plus)**. Usługa monitoruje, wykrywa i blokuje wirusy komputerowe podczas przeglądania stron internetowych czy pobierania plików z sieci. Dodatkowo zapewnia ochronę przed zaawansowanymi atakami sieciowymi oraz blokuje transmisję szkodliwego oprogramowania na poziomie sieci OSE. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych zagrożeniach.
- **Ochrona użytkowników OSE (w ramach OSE plus)**. To bezpłatna usługa, która chroni przed dostępem do stron zawierających treści potencjalnie szkodliwe i nielegalne, w tym materiały pornograficzne czy pokazujące agresję i przemoc. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach.
- **Bezpieczne treści (w ramach OSE plus)**. Usługa pozwala na uzyskanie informacji o trendach związanych z dostępem do treści potencjalnie szkodliwych w sieci szkolnej. Dzięki algorytmom uczenia maszynowego (ML), klasyfikuje materiały, z którymi zetknęli się użytkownicy (teksty, obrazy, wideo) i przypisuje je do odpowiednich kategorii. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach.

Szczegółowych informacji na temat naszych usług bezpieczeństwa szukajcie w zakładkach FAQ i Internetowe usługi OSE na stronie ose.gov.pl oraz w aktualności „5 pytań o… usługi bezpieczeństwa OSE". Nie znaleźliście tam odpowiedzi na swoje pytanie? Wyślijcie e-mail na adres: wsparcie-techniczne_ose@nask.pl lub zadzwońcie na infolinię OSE (+48 22 182 55 55), czynną od poniedziałku do piątku w godzinach 7:30–16:00.

Ustawa o krajowym systemie cyberbezpieczeństwa

Kto jest odpowiedzialny za cyberbezpieczeństwo w Polsce? Jakie są główne cele zapewniania bezpieczeństwa cyfrowego na poziomie kraju? Czym są incydenty bezpieczeństwa i kto na nie reaguje? Odpowiedzi na te i inne pytania znajdziecie w Ustawie o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 5), która włącza do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. Dyrektywa NIS.

Dokument opisuje również Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej, czyli wytyczne określające kierunki działań państwa w zakresie ochrony infrastruktury krytycznej, edukacji

w obszarze bezpieczeństwa cyfrowego oraz przygotowania do reagowania na zagrożenia. Ustawa kładzie nacisk na profilaktykę, wykrywanie i szybkie reagowanie na incydenty, a także na współpracę z partnerami zagranicznymi i organizacjami międzynarodowymi.

Dzięki tym regulacjom Polska buduje spójny system ochrony cyberprzestrzeni, który obejmuje zarówno instytucje państwowe, jak i sektor prywatny. Ustawa wskazuje wyraźnie, że cyberbezpieczeństwo jest wspólną odpowiedzialnością: państwa, przedsiębiorstw i obywateli. W praktyce oznacza to, że wszystkie podmioty mają określone obowiązki – od zgłaszania incydentów i stosowania odpowiednich zabezpieczeń, po udział w szkoleniach i edukacji w zakresie bezpieczeństwa cyfrowego.

W skrócie, Ustawa o krajowym systemie cyberbezpieczeństwa nie tylko tworzy ramy prawne, ale też wyznacza standardy ochrony cyfrowej w Polsce, zapewniając spójność działań, minimalizację ryzyka i zwiększenie odporności państwa na zagrożenia w sieci. To fundament, na którym opiera się bezpieczeństwo polskiej infrastruktury krytycznej i ochrona danych obywateli w erze cyfrowej.

Uwierzytelnianie dwuskładnikowe

O tym, jak cenne są nasze dane, w tym dane osobowe czy dane do logowania, dowiadujemy się najczęściej w przypadku… ich utraty. Jak się przed tym zabezpieczyć? Przede wszystkim postawcie na silne hasła, które będą strzegły dostępu do Waszych kont w serwisach pocztowych, społecznościowych czy bankowości elektronicznej. Dobre hasło składa się z minimum 14 znaków i jest zmodyfikowaną frazą – łatwą do zapamiętania, ale trudną do odgadnięcia, np. ze względu na obcojęzyczny wtręt (DwaBialeLatajaceSophisticatedKroliki) lub sprytne zmiany (WlazlKostekNaMostekIStuka). Jeśli nie znacie jeszcze nowych wytycznych CERT Polska dotyczących zasad tworzenia silnych haseł, koniecznie się z nimi zapoznajcie i sprawdźcie, czy Wasze zabezpieczenia są wystarczające!

W dzisiejszych czasach silne hasło to niestety nie wszystko. Warto pomyśleć o włączeniu dodatkowej weryfikacji, tzw. uwierzytelniania dwuskładnikowego (ang. *Two Factor Authenticaton*, 2FA). Pomoże nam ono skutecznie chronić nasze konta. Decydując się na uwierzytelnienie dwuskładnikowe, mamy do wyboru kilka możliwości. To przede wszystkim jednorazowe kody generowane w aplikacji lub wysyłane SMS-em („coś, co znasz"), ale też klucz sprzętowy („coś, co posiadasz") – małe urządzenie, które pozwala potwierdzić, że to właśnie my próbujemy zalogować się do komputera, serwisu czy aplikacji. Drugim składnikiem może być też „coś, czym jesteś", a więc zabezpieczenie biometryczne w postaci odcisku palca, skanu twarzy czy obrazu tęczówki. Po skonfigurowaniu 2FA podczas logowania z nowego urządzenia – za każdym razem – oprócz hasła będziemy wprowadzać także np. specjalny kod. Ten dodatkowy składnik jest znany tylko nam, więc nawet jeśli hasło wycieknie lub stracimy je w inny sposób, cyberprzestępca nie włamie się na nasze konto.

Nierzadko hasła chronią to, co mamy najcenniejszego – dostęp do konta w banku czy danych osobowych. Dlatego warto stosować najsilniejsze z możliwych sposoby zabezpieczeń, w tym również uwierzytelnianie dwuskładnikowe.

Wszystkie nasze konta są ważne, jednak szczególną opieką powinniśmy otoczyć konta o „wysokiej wartości", gdzie znajdują się informacje, na których naprawdę nam zależy i których nie możemy stracić. Pamiętajcie przede wszystkim o właściwym zabezpieczeniu nie tylko swojej bankowości elektronicznej, ale przede wszystkim poczty e-mail. Przestępcy, którym uda się włamać do naszej skrzynki odbiorczej, mogą ją później wykorzystać do resetowania haseł na innych kontach!

Więcej porad dotyczących zabezpieczania swoich kont znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe" i „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe".

Źródło:

„Kompleksowo o hasłach", (2022), artykuł na stronie cert.pl.

Uwierzytelnianie wieloskładnikowe

Przezorny zawsze ubezpieczony – zapewne znacie to powiedzenie, ale czy zastanawialiście się, czy w kontekście bezpieczeństwa w sieci istnieją jakieś granice ochrony? Wielokrotnie zachęcaliśmy Was do włączania uwierzytelniania dwuskładnikowego (2FA), czyli takiej metody potwierdzenia swojej tożsamości podczas logowania, która wymaga podania dwóch informacji, np. hasła i kodu generowanego w aplikacji. A co powiecie na uwierzytelnianie wieloskładnikowe (ang. *Multi-Factor Authentication*, MFA)?

W takim przypadku nie wystarczą dwa elementy potwierdzające tożsamość użytkownika – będzie trzeba ich podać np. trzy. Dodatkowe składniki mogą być te same, co w uwierzytelnianiu dwuskładnikowym, czyli:

- **„coś, co znasz”**: np. hasło, kod PIN lub odpowiedź na ustawione wcześniej pytanie zabezpieczające;
- **„coś, co masz”**: np. klucz U2F lub kod z aplikacji uwierzytelniającej na smartfonie użytkownika – hasło jednorazowe (OTP) lub hasło jednorazowe ograniczone czasowo (TOTP);
- **„coś, czym jesteś”**: informacje biometryczne: np. odcisk palca, rozpoznawanie twarzy lub skan tęczówki.

Co istotne, MFA wymaga od użytkowników podania co najmniej dwóch składników z dwóch różnych kategorii (np. „coś, co znasz” i „coś, czym jesteś”). Jak wygląda taki proces logowania? W pierwszym kroku podajecie login i hasło, w drugim – np. jednorazowy kod z aplikacji, a w trzecim – np. odcisk palca. Taka metoda uwierzytelniania jest bezpieczniejsza od 2FA: to praktycznie niemożliwe, że oszust, który wejdzie w posiadanie Waszych danych dostępowych, uzyska dostęp także do dwóch dodatkowych składników zabezpieczających.

Uwierzytelnianie wieloskładnikowe może uwzględniać różne typy czynników umożliwiających identyfikację, np. lokalizację, ocenę ryzyka czy czas logowania. Mówimy wówczas o adaptacyjnym MFA. Ta metoda polega na analizie zachowań kontekstowych w celu przewidzenia poziomu ryzyka nieuprawnionego dostępu.

W przypadku gdy adaptacyjne MFA wykryje nietypowe zachowania, takie jak próba logowania z nieznanego urządzenia lub z nierozpoznanej lokalizacji, zażąda od użytkownika dowodów na potwierdzenie jego tożsamości (np. umożliwi logowanie dopiero po kliknięciu potwierdzenia na innym urządzeniu). Wykorzystanie wzorców zachowań, do których „przyzwyczajone” jest Wasze urządzenie, pozwala jeszcze lepiej dbać o Wasze bezpieczeństwo. Warto zauważyć, że o wprowadzenie tej dodatkowej warstwy bezpieczeństwa zostaniecie poproszeni tylko wtedy, gdy zostanie wykryta podejrzana aktywność – co znaczy, że proces logowania nie będzie za każdym razem ciągnął się w nieskończoność.

Więcej o 2FA i dodatkowych składnikach uwierzytelniania dowiecie się z aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe” i „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe”. Zajrzyjcie też do poradnika „Kompleksowo o hasłach” na stronie cert.pl – pamiętajcie, że hasła również są bardzo istotnym zabezpieczeniem!

Uzależnienie od gier komputerowych

W dobie powszechnego dostępu do internetu i urządzeń cyfrowych coraz łatwiej wpaść nam w pułapkę różnego rodzaju uzależnień behawioralnych, związanych z nowymi technologiami. Należy do nich m.in. zaburzenie grania w gry cyfrowe lub wideo (ang. *gaming disorder*), objawiające się wewnętrznym przymusem grania w grę, uporczywym powtarzaniem tej czynności, nawet jeśli jest szkodliwa (np. prowadzi do zaniedbania innych sfer życia i wielu negatywnych konsekwencji zdrowotnych) oraz zakończonymi niepowodzeniem próbami kontrolowania lub zakończenia grania.

Choć uzależnienie od gier jest zaburzeniem, które dotyka jedynie kilka procent populacji, to coraz częściej obserwujemy rosnącą zależność młodych użytkowników od aktywności online. Powodów, dla których dzieci i młodzież nadużywają lub szkodliwie używają gier cyfrowych, może być bardzo wiele. Często to potrzeba wrażeń, nuda czy chęć sprawdzenia się. Gry umożliwiają dzieciom
i nastolatkom ucieczkę od realnego świata w stworzoną przez siebie rzeczywistość, którą w pełni kontrolują i do której dorośli nie mają dostępu.

Oczywiście nie każdy, kto poświęca dużo czasu grom komputerowym, korzysta z nich w sposób szkodliwy. O problemie mówimy, gdy ten czas wymyka się spod kontroli lub na korzyść gier zaniedbujemy codzienne sprawy. Jak rozpoznacie, czy Wasze dziecko nadmiernie angażuje się w gry? Obserwujcie je i zwracajcie uwagę na to, czy nie wycofuje się z kontaktów społecznych, czy rezygnuje z innych aktywności poza graniem, czy porzuca dotychczasowe hobby na rzecz grania lub zaniedbuje obowiązki. Jeśli zauważycie u niego powyższe symptomy, a także jeśli temat grania wywołuje w Waszym domu coraz większe konflikty, a próby ograniczania czasu przed ekranem spotykają się z agresją ze strony dziecka – zareagujcie!

Wskazówki dotyczące rozpoznawania uzależnienia od gier oraz ustalania z dzieckiem reguł korzystania z urządzeń cyfrowych znajdziecie w poradnikach „Nastolatki i gry cyfrowe”, „O grach cyfrowych” oraz „FOMO i nadużywanie nowych technologii” dostępnych na platformie
OSE IT Szkoła. Sięgnijcie też do naszych aktualności, w których mówimy o jasnych i ciemnych stronach grania: „Gaming – uzależnienie od gier komputerowych” i „Grać czy nie grać? Oto jest pytanie!”.

Użytkownik

Nie ma przesady w stwierdzeniu, że wszyscy jesteśmy użytkownikami – korzystamy przecież ze smartfonów i innych urządzeń cyfrowych, z internetu, aplikacji. Czy jednak zawsze posługujemy się tymi narzędziami w bezpieczny sposób?

Lista wskazówek, o których powinniście pamiętać, chcąc zadbać o swoje bezpieczeństwo w sieci, może nie jest zbyt krótka, mimo to warto upewnić się, że odhaczacie wszystkie ważne punkty. Bezpieczny użytkownik to ten, który mądrze i świadomie korzysta z zasobów oraz dobrodziejstw internetu – warto zatem poświęcić chwilę na wdrożenie zasad!

Zacznijcie od zabezpieczeń: to silne hasła, uwierzytelnianie dwuskładnikowe, ale też regularne aktualizacje, które chronią Was przed różnymi atakami sieciowymi i działaniem złośliwego oprogramowania (malware). A skoro mowa o szkodnikach – uważajcie również na oszustów, którzy w podstępny sposób rozsyłają niebezpieczne maile lub próbują zagrozić Wam podczas rozmowy telefonicznej, a także za pośrednictwem niebezpiecznych SMS-ów. Świadomy użytkownik internetu nie otwiera też podejrzanych załączników i nie klika w linki pochodzące z nieznanych źródeł. W dzisiejszych czasach z dużą ostrożnością podchodzi też do informacji, które znajduje w sieci: uważa na zmanipulowane wiadomości, deepfake i dezinformację. A przede wszystkim kieruje się zasadą ograniczonego zaufania!

W aktualnościach (na platformie OSE IT Szkoła, ale też na stronie ose.gov.pl) na bieżąco podpowiadamy Wam, jak zadbać o siebie w internecie. Najnowsze wskazówki znajdziecie np. w artykule „Dekalog bezpiecznego internauty”.

U

V

Viral

Zapewne widzieliście krążące w sieci zdjęcie kota z niezadowoloną miną, do którego internauci dodają różne komentarze i udostępniają grafikę w formie memów. A może oglądaliście popularne w ostatnim czasie filmiki przedstawiające piosenki stworzone przez sztuczną inteligencję? Jest duża szansa, że trafiliście na tego typu materiały określane mianem viralowych.

Viral to termin, który dosłownie możemy przetłumaczyć z języka angielskiego jako „wirusowy". Uspokajamy, nie chodzi tu o wirusa komputerowego, a o naturę takich treści – udostępniane są one w intrenecie na masową skalę i zyskują ogromną popularność w krótkim czasie. Mówiąc o treściach viralowych, możemy mieć na myśli różne materiały: zdjęcia, memy, filmy, artykuły czy posty w mediach społecznościowych. Jakie cechy powinien mieć viral, żeby był rozpowszechniany przez ludzi z całego świata?

Najczęściej taki materiał jest zabawny, wywołuje w odbiorcach różne emocje (radość, wzruszenie, współczucie, smutek), wiąże się z czymś zaskakującym, innowacyjnym oraz łatwo można go przekazać dalej. Te cechy starają się wykorzystywać firmy podczas tworzenia strategii polegającej na viral marketingu, czyli marketingu wirusowym. Ich zadaniem jest tworzenie treści, które będą miały potencjał viralowy i dotrą do jak największej liczby odbiorców.

Oczywiście viral może mieć też ciemniejszą stronę. Gorzej, gdy popularność zyska zdjęcie lub filmik przedstawiający daną osobę oraz obiegnie świat bez jej wiedzy i zgody. Pamiętacie dziewczynkę ze smutną, zniesmaczoną miną, która zyskała nawet w sieci swój przydomek – side-eyeing Chloe? Jej zdjęcie doczekało się niezliczonej liczby przeróbek i stało się powodem do żartów.

Często pod wpływem emocji zamieszczamy w mediach społecznościowych komentarze, opinie, publikujemy zdjęcia, filmy. Pamiętajcie, że takie materiały mogą dotrzeć nie tylko do znajomych, ale i obcych ludzi, którzy nie zawsze mają dobre zamiary. Co więcej – mogą zacząć żyć własnym życiem: ktoś może je powielić, wykorzystać Wasz wizerunek do stworzenia prześmiewczego memu, ale też do przestępczych procederów, np. kradzieży tożsamości czy szantażu.

Zanim więc opublikujecie coś w sieci, pomyślcie, jak dany materiał wpłynie na Wasz cyfrowy ślad, który zostanie z Wami na długo. Zastanówcie się też, czy każdy viralowy materiał warto udostępniać innym. Przed kliknięciem przycisku „przekaż dalej", sprawdźcie, czy dany materiał nie promuje szkodliwych treści, materiałów obrazujących przemoc, szerzących dezinformację. Eksperci przestrzegają – nawet sporadyczny kontakt z niebezpiecznymi treściami wpływa na emocje i samopoczucie dziecka!

Virtual Private Network (VPN)

Wirtualna sieć prywatna to technologia, która tworzy zaszyfrowany prywatny tunel podczas łączenia z internetem. Dzięki temu nasze aktywności w sieci są trudniejsze do monitorowania i obserwowania przez innych. VPN ukrywa również naszą lokalizację, co utrudnia odwiedzanym przez nas stronom internetowym zidentyfikowanie naszego położenia – także kraju, w jakim aktualnie przebywamy.

Jak działa VPN? Gdy z niego korzystamy, nasze aktywności sieciowe przechodzą przez zaszyfrowany, wspomniany już, tunel i następnie przesyłane są do zamierzonego celu. Co ważne, dzięki VPN-owi ruch jest odpowiednio zabezpieczony, nasza prywatność – chroniona, a korzystanie z internetu – bezpieczniejsze. Mechanizm tej technologii opiera się głównie na ukryciu rzeczywistego adresu IP naszego urządzenia oraz szyfrowaniu danych, które przesyłamy w trakcie połączenia internetowego. Sieci VPN wykorzystują architekturę klient–serwer.

Z VPN-ów korzystają głównie korporacje oraz banki. Takie rozwiązanie służy do bezpiecznego połączenia pracowników z firmową siecią, zapewniając poufność danych poprzez tworzenie zaszyfrowanego tunelu. Umożliwia pracę zdalną, dostęp do zasobów firmowych z dowolnego

miejsca, a także łączenie wielu lokalizacji firmy w jedną prywatną sieć. Jak czytamy na stronie cert.pl, „wirtualna sieć prywatna rzeczywiście dodaje kolejną warstwę szyfrowania i anonimizacji, co jest korzystne dla ochrony prywatności. Jednakże, VPN nie jest jedynym ratunkiem ani absolutną koniecznością dla zapewnienia podstawowego bezpieczeństwa w większości typowych sytuacji podczas korzystania z publicznego Wi-Fi. Powszechne stosowanie protokołu HTTPS oraz nowoczesne standardy zabezpieczeń Wi-Fi, takie jak WPA3, już zapewniają solidną ochronę".

Nic nie stoi na przeszkodzie, żeby korzystać z VPN-a również w celach niesłużbowych. Zanim wybierzecie dostawcę wirtualnej sieci prywatnej, upewnijcie się, że jest godny zaufania. W tym celu warto pamiętać m.in. o szukaniu usługi, która nie zapisuje logów i skupia się na zachowaniu prywatności użytkowników. Sprawdźcie też koniecznie, gdzie znajduje się siedziba przedsiębiorstwa (czy w tym kraju gwarantowane jest prawo do prywatności?) oraz wystrzegajcie się darmowych programów.

Źródło:

„Bezpieczeństwo twojej kieszeni, czyli jak ochronić swój telefon", artykuł na stronie cert.pl.

W

Wideokonferencje

To wirtualna forma komunikacji przy wykorzystaniu urządzeń cyfrowych (np. laptopa, smartfona) i internetu. Wideokonferencje umożliwiają zdalne rozmowy w czasie rzeczywistym przy użyciu mikrofonu i kamery – niezależnie od odległości, jaka dzieli uczestników spotkania. Ponadto wraz z oprogramowaniem, które daje nam dostęp do wideokonferencji, otrzymujemy wiele funkcji: udostępniania obrazu, prezentacji i innych plików, nagrywania spotkań czy wykorzystania czatu.

Wideokonferencje wykorzystywane są w pracy, edukacji bądź przy organizacji różnych wydarzeń, np. ważnych uroczystości czy wykładów. Mimo że ułatwiają komunikację, korzystając z nich, musicie również zadbać o bezpieczeństwo i pamiętać o zasadach, które uchronią Was przed różnymi incydentami i nieprzyjemnościami, takimi jak wyciek danych czy naruszenia prywatności. O czym warto pamiętać?

- **Nie ignorujcie aktualizacji!** Nowe wersje programów i aplikacji zawierają poprawki błędów oraz zabezpieczeń, które zwiększają Wasze bezpieczeństwo. Jeśli często zapominacie o ich instalacji, warto włączyć automatyczne aktualizacje.
- **Konfiguracja ustawień audio i wideo**. Dobrą praktyką jest automatyczne wyciszenie mikrofonu i wyłączenie kamery przy dołączaniu do spotkania. Dodatkowo można zasłonić kamerkę, gdy jej nie używacie, zwiększy to Wasze poczucie prywatności.
- **Tło podczas spotkania**. Zadbajcie o porządek za swoimi plecami lub skorzystajcie z funkcji wirtualnego albo rozmytego tła. Widoczne za Wami przedmioty osobiste czy bałagan mogą robić złe wrażenie.
- **Udostępnianie ekranu**. Zanim zaczniecie dzielić się swoim ekranem, warto zamknąć wszystkie zbędne aplikacje i okna. Powiadomienia z komunikatorów czy innych programów mogą nie tylko rozpraszać uczestników, ale też przypadkowo ujawnić prywatne lub służbowe informacje.
- **Udostępnianie zaproszeń**. Nie przesyłajcie linków do spotkań osobom postronnym. Jeśli ktoś nie otrzymał zaproszenia, powinien skontaktować się z organizatorem.
- **Ochrona danych**. Nie róbcie zrzutów ekranu i nie nagrywajcie spotkań bez pozwolenia! W ten sposób narażacie innych np. na upublicznienie poufnych informacji.

Więcej praktycznych informacji o bezpiecznych wideokonferencjach znajdziecie na ose gov.pl w aktualności „Bezpieczni w sieci z OSE: wideokonferencje". Przeczytajcie też koniecznie biuletyn „OUCH! – Bezpieczeństwo wideokonferencji".

Źródło:

„Bezpieczne wideokonferencje i spotkania online", (2025), artykuł na stronie kompetencjecyfrowe.gov.pl [online, dostęp dn. 24.10.2025].

Wirtualna rzeczywistość (ang. *virtual reality*, VR)

Chcielibyście w sekundę przenieść się w dowolne miejsce na ziemi – istniejące lub już nieistniejące, znaleźć się na pokładzie statku kosmicznego, łodzi podwodnej, na największym stadionie piłkarskim, szczycie Mount Everestu, wcielić się w chirurga albo kaskadera? Jeśli tak, skorzystajcie z technologii wirtualnej rzeczywistości, która stwarza pozory realnie istniejącego świata i pozwala się w nim zanurzyć.

Wirtualna rzeczywistość (ang. *virtual reality*, VR) to rzeczywistość wykreowana komputerowo, która umożliwia tworzenie trójwymiarowego obrazu. Specjalne narzędzia, takie jak gogle, kontrolery czy kostiumy pozwalają użytkownikom poruszać się po wirtualnym świecie, odkrywać go,

a nawet wchodzić w interakcje z jego elementami. Obiekty w technologii VR mogą mieć rzeczywiste wymiary, można też je oglądać z różnych perspektyw, ponieważ obraz zmienia się wraz z naszym położeniem, np. jeśli obrócimy głowę, położymy się lub usiądziemy.

Co sprawia, że technologia VR jest niezwykle atrakcyjna i potrafi pochłaniać nas tak mocno, że możemy zapomnieć o otaczającym świecie rzeczywistym? W tym kontekście warto przytoczyć trzy pojęcia (Witkowska, 2024).

- **Immersja** – czyli „zanurzenie", którego doświadczamy wtedy, kiedy świat wirtualny działa na nasze zmysły podobnie do otaczającej nas rzeczywistości.
- **Psychologiczna obecność**– poczucie osobistego zaangażowania w wirtualną sytuację, realnego uczestnictwa w niej.
- **Ucieleśnienie** – uczucie znajdowania się w wirtualnym ciele, mające bezpośredni wpływ na odczuwanie prawdziwości danego doświadczenia.

Przez długi czas technologia VR kojarzona była głównie z grami. Dziś znajduje zastosowanie w wielu dziedzinach, np. edukacji, medycynie, motoryzacji, transporcie czy marketingu. Dzięki tej technologii uczniowie mogą przenieść się np. do starożytności i dosłownie zanurzyć się w historii. Studenci są w stanie uczyć się anatomii, przeprowadzać operacje czy doświadczenia, uczestniczyć w symulacjach lotu lub trudnych zdarzeń, na które w przyszłości będą musieli reagować. VR wykorzystują też firmy, np. do odzwierciedlenia procesów technologicznych, zdobywania nowych kompetencji. Z kolei liderom i menadżerom wirtualna rzeczywistość pomaga np. zrozumieć emocje innych, wyrabiać empatię czy ćwiczyć wystąpienia przed dużą publicznością. To wszystko w bezpiecznym, kontrolowanym środowisku.

Przebywanie w wirtualnej rzeczywistości stwarza ogromne szanse, ale może być też źródłem zagrożeń. Warto zwrócić uwagę szczególnie na młodszych użytkowników nowych technologii. Z nauki i rozrywki VR na pewno nie powinny korzystać małe dzieci – rekomendowany wiek to minimum 12–13 lat. Zanim złapiecie VR-owego bakcyla, pamiętajcie o bezpieczeństwie i potrzebie zachowania cyfrowej higieny:

- Używanie gogli może powodować mdłości, zmęczenie oczu, zawroty czy ból głowy – zachowajcie umiar i róbcie częste przerwy, podczas których postawicie na odpoczynek od ekranów i aktywności offline.
- Nie korzystajcie z wirtualnej rzeczywistości przed snem – taka rozrywka może wpłynąć na jego jakość.
- Zanurzając się w świecie VR, pamiętajcie o otaczającej Was realnej rzeczywistości. Każdy Wasz ruch może nieść niebezpieczeństwo upadku, urazu czy zderzenia z przedmiotami znajdującymi się w Waszym otoczeniu.
- Badacze podkreślają, że korzystanie z technologii VR niesie ryzyko tworzenia fałszywych wspomnień, szczególnie wśród dzieci. Każdą przygodę z takimi narzędziami poprzedźcie więc rozmową, która przygotuje dziecko na nowe doświadczenia.
- Immersja i poczucie obecności nasilają przeżywane emocje, dlatego należy dbać, by treści przekazywane za pomocą technologii VR były dostosowane do wieku i etapu rozwoju dziecka.
- VR zwiększa przeżycia, co sprawia, że dziecko może być bardziej podatne na prezentowane treści. Sprawdźcie, czy nie są one zbyt intensywne i sugestywne.
- Pamiętajcie, że w każdej chwili możecie zdjąć gogle, szczególnie gdy doświadczycie uczucia przytłoczenia, lęku czy zakłopotania (por. Witkowska, 2024).

Więcej o technologii VR przeczytacie w naszym poradniku dla nauczycieli „Bezpiecznie w wirtualnej rzeczywistości".

Wirus komputerowy

Wirusy komputerowe to jedno z najstarszych zagrożeń w świecie cyfrowym. Choć ich nazwa jest powszechnie znana, wielu użytkowników wciąż nie do końca rozumie, jak działają i w jaki sposób mogą zaszkodzić urządzeniu. W praktyce wirus to fragment złośliwego kodu, który po przedostaniu się do komputera infekuje pliki lub system operacyjny, a następnie zaczyna się samodzielnie rozprzestrzeniać. Celem jego złośliwego działania może być kradzież danych, trwałe uszkodzenie plików, spowolnienie pracy systemu albo umożliwienie przestępcom zdalnego dostępu do urządzenia.

Nazwa „wirus" nie jest przypadkowa – podobnie jak w świecie biologii, infekcja przenosi się pomiędzy urządzeniami, np. przez połączenie w sieci, przesyłanie plików lub korzystanie z tych samych nośników danych. Zainfekowany plik może wydawać się zupełnie bezpieczny, a jego uruchomienie często następuje nieświadomie. Wtedy szkodliwy kod zostaje aktywowany, a użytkownik traci kontrolę nad częścią działań swojego systemu.

Wirusy dostają się do naszych urządzeń na różne sposoby. Najczęściej trafiają tam poprzez linki i załączniki z niechcianych e-maili, fałszywe strony internetowe, oprogramowanie pobierane z nieoficjalnych źródeł czy zainfekowane pendrive'y.

Istnieje wiele rodzajów wirusów, które różnią się sposobem działania. Wirusy plikowe przyczepiają się do programów i uruchamiają razem z nimi. Makrowirusy wykorzystują dokumenty tekstowe lub arkusze kalkulacyjne, a wirusy sektora rozruchowego atakują najgłębsze warstwy systemu – dysk, z którego komputer startuje. Niektóre z nich, jak tzw. robaki sieciowe, rozprzestrzeniają się samodzielnie, wykorzystując luki w zabezpieczeniach.

Skutki infekcji mogą być różne – od niewinnych, lecz uciążliwych zmian w systemie, po utratę wszystkich danych lub kradzież informacji logowania. Zdarza się, że wirusy szyfrują dane na dysku, żądając później okupu za ich odblokowanie (tzw. ransomware).

Aby chronić się przed wirusami komputerowymi, warto stosować kilka prostych zasad:

- regularnie aktualizować system operacyjny i oprogramowanie;
- instalować oprogramowanie wyłącznie z zaufanych źródeł;
- korzystać z oprogramowania antywirusowego i zapory sieciowej;
- weryfikować przed kliknięciem linki otrzymane z nieznanych źródeł, zwracać szczególną uwagę na rozszerzenie pliku załączników do wiadomości mailowych i nie uruchamiać ich, jeśli budzą nasze wątpliwości;
- unikać pobierania plików z nieznanych stron;
- tworzyć kopie zapasowe ważnych danych.

Wirus komputerowy to nie tylko techniczne zagrożenie, ale również przypomnienie o tym, jak ważna jest świadomość cyfrowa. Nawet najlepszy antywirus nie zastąpi zdrowego rozsądku użytkownika – to właśnie on stanowi pierwszą linię obrony przed cyfrowymi infekcjami. Dbajcie o swoje bezpieczeństwo!

Źródło:

„Wirus komputerowy – czym jest? Jakie są rodzaje wirusów?", (2025), artykuł w serwisie bezpiecznyinternet.edu.pl.

Wizerunek online

Każde nasze działanie w internecie zostawia po sobie cyfrowy ślad. Z jednej strony są to informacje, które udostępniamy automatycznie, podczas każdego kliknięcia. Przeglądając internet, robiąc

zakupy online, instalując różne aplikacje, zdradzamy np. szczegóły dotyczące systemu operacyjnego swojego urządzenia, adresu IP, używanej przeglądarki internetowej, ale też własne preferencje czy dane geolokalizacyjne. Z drugiej strony wiele wiadomości o nas samych zostawiamy w sieci intencjonalnie – szczególnie w mediach społecznościowych. Prywatne posty, komentarze, „lajki", zastosowane nakładki na profile, opublikowane filmy i zdjęcia stanowią prawdziwą kopalnię wiedzy o nas samych.

Jedno jest pewne – generujemy ogromną ilość materiałów, które często mówią o nas więcej, niż byśmy przypuszczali. Kto może skorzystać z tej wiedzy? Wszyscy zainteresowani: obecni i przyszli pracodawcy, rodzina, znajomi, reklamodawcy, ale też cyberprzestępcy, dla których ważny jest każdy szczegół z naszego życia – prywatnego i zawodowego – by przeprowadzić skuteczny, sprecyzowany atak, np. phishingowy. Ponadto aktywność w internecie wpływa na nasz unikalny e-wizerunek. Warto więc nauczyć się świadomie zarządzać upublicznianymi informacjami.

Od czego zacząć? Na początek warto ustawić w przeglądarce tryb prywatny (incognito), kontrolować pliki cookies, zapoznać się z polityką prywatności aplikacji, które chcecie zainstalować na swoim urządzeniu – niektóre apki żądają dostępu do zbyt wielu danych (np. listy kontaktów czy zdjęć w galerii na telefonie). Podczas aktywności w sieci należy wziąć jeszcze pod uwagę kilka innych kwestii:

- **Publikujcie świadomie**. Nie działajcie pod wpływem emocji. Przed wrzuceniem jakiegoś materiału do sieci zastanówcie się, jak wpłynie on na Waszą reputację – teraz i za jakiś czas. Ponadto z rozwagą dzielcie się materiałami w internecie – nie powielajcie niesprawdzonych newsów, nie siejcie dezinformacji.
- **Pamiętajcie o ukrytych danych**. Zdjęcia, filmy i inne cyfrowe materiały mogą zawierać informacje o ich autorze, czasie utworzenia czy lokalizacji. Zanim coś opublikujecie, sprawdźcie, jakie dane dodatkowo udostępniacie. Część z nich możecie ukryć, stosując ustawienia prywatności na swoich urządzeniach. Pomocne może być np. wyłączenie funkcji geolokalizacji w smartfonie.
- **Chrońcie swoją prywatność w sieci**. W mediach społecznościowych wybierzcie konto prywatne zamiast publicznego – w ten sposób nie każdy będzie miał dostęp do publikowanych przez Was treści.
- **Zachowajcie ostrożność i poufność**. Nie zdradzajcie w internecie informacji dotyczących Waszej pracy (może to doprowadzić do ujawnienia tajemnic służbowych lub ustawowo chronionych) oraz osobistych – takich jak numer telefonu, adres zamieszkania czy miejsce, w którym aktualnie przebywacie. Nigdy nie publikujcie też online zdjęć dokumentów (nawet ich fragmentów), aby nie paść ofiarą kradzieży tożsamości.
- **Korzystajcie z prawa do bycia zapomnianym**. Zawsze możecie prosić o usunięcie z internetu materiałów, które Was dotyczą. Takie prawo wynika z rozporządzenia unijnego RODO.

Jeśli ktoś bezprawnie wykorzystał Wasz wizerunek w sieci, reagujcie – prawo stoi po Waszej stronie! W tej sytuacji możecie podjąć następujące kroki:

- zażądać od osoby, która naruszyła Wasz wizerunek, zaniechania takiego działania;
- jeśli pierwszy krok nie przyniósł efektów, możecie wnieść sprawę do sądu;
- gdy w wyniku bezprawnego rozpowszechniania Waszego wizerunku doszło do powstania szkody niemajątkowej, np. utraty dobrego imienia czy doświadczenia wstydu, upokorzenia, możecie żądać usunięcia skutków takiego działania, np. w formie przeprosin na łamach prasy czy zadośćuczynienia pieniężnego;
- jeżeli wskutek naruszenia Waszego wizerunku została wyrządzona szkoda majątkowa, np. utraciliście zarobek, możecie żądać naprawienia szkody poprzez zasądzenie odszkodowania równoważnego powstałej szkodzie.

Źródło:

„Jak cię widzą, tak cię piszą… Zadbaj o swój wizerunek w sieci”, (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

Wtyczka (plug-in, add-on)

Zdarza się czasem, że podczas korzystania z przeglądarki internetowej brakuje Wam jakiejś dodatkowej funkcjonalności, prawda? Chcecie porządkować swoje zakładki, mieć łatwy dostęp do translatora, listy zadań, menedżera haseł lub innych ulubionych narzędzi? To nie kłopot: możecie zainstalować sobie wtyczkę (ang. *plug-in*, *add-on*), która pozwoli dopasować opcje przeglądarki do Waszych potrzeb.

Wtyczka to nic innego niż dodatkowe oprogramowanie bądź jego moduł, rozszerzający wyjściowy program o nowe funkcjonalności, niezawarte w jego oryginalnej, wyjściowej wersji. Takie rozszerzenia dostępne są w oficjalnych sklepach – osobno dla poszczególnych przeglądarek.

Choć wtyczki mają sprawiać, że korzystanie z przeglądarek będzie łatwiejsze i przyjemniejsze, instalowanie ich może nieść za sobą niemałe ryzyko. Możecie bowiem natrafić na takie plug-iny, które zamiast rozszerzać możliwości przeglądarek, są wykorzystywane do oszustw internetowych, w tym wykradania danych.

Złośliwe wtyczki (ang. *malicious browser extensions*) mogą:

- gromadzić wrażliwe dane,
- śledzić aktywność użytkowników,
- przechwytywać dane z sesji przeglądania (np. informacje wpisywane w formularzach),
- wykorzystywać moc obliczeniową urządzenia do wydobywania kryptowalut,
- przekierowywać do fałszywych witryn,
- przejąć kontrolę nad przeglądarką.

Warto pamiętać też o tym, że wiele złośliwych wtyczek podszywa się pod legalne rozszerzenia z przydatnymi funkcjami. Dlatego nigdy nie przekazujcie plug-inom wszystkich uprawnień, w tym dostępu do swoich danych!

Jednym z najbardziej powszechnych zagrożeń związanych z wtyczkami są rozszerzenia, które oprócz nowych funkcjonalności instalują także oprogramowanie typu adware, zawierające moduły odpowiadające za wyświetlanie niechcianych reklam lub przekierowujące na strony partnerów.

Nie ma niestety jednej uniwersalnej recepty pomocnej w rozpoznawaniu, które wtyczki są bezpieczne, a które tylko podszywają się pod prawdziwe rozszerzenia. Są jednak pewne alarmujące oznaki: jeśli nie możecie znaleźć informacji o autorze plug-ina, gdy brakuje danych o ostatniej aktualizacji, a opinie o wtyczce są podejrzane – powstrzymajcie się od instalacji i poszukajcie innej wtyczki. Dodatkowo nie zapominajcie o tym, żeby pobierać rozszerzenia wyłącznie z oficjalnych sklepów!

Źródło:

„Złośliwe rozszerzenia przeglądarek”, (2023), artykuł w serwisie trafficwatchdog.pl.

Wyciek danych

Ostatnio coraz częściej słyszymy o tym, że w wyniku ataku lub ludzkiego błędu doszło do wycieku bazy danych osobowych klientów niektórych firm. Być może Wasze dane również zostały upublicznione. To poważny problem, bo poufne informacje na nasz temat są niezwykle cenną walutą w internecie.

O jakich danych mówimy? To dane osobowe (imiona, nazwiska, numery PESEL, adresy, dane logowania i inne informacje, dzięki którym bez problemu można nas zweryfikować), dane finansowe (numery kart kredytowych i numery CVV, numery kont itp.) oraz zdrowotne (recepty, wyniki badań, historia leczenia). Można tu wymienić także dane biometryczne, ale też np. tajemnice handlowe czy znaki towarowe.

Upublicznienie tych informacji – które są dostępne w różnego rodzaju bazach i serwisach internetowych – to właśnie wyciek danych. Wiąże się on z dużym ryzykiem, że osoby nieuprawnione mogą wejść w posiadanie poufnych informacji i wykorzystać je w niepożądany sposób. Wycieki dotyczą najczęściej loginów, haseł lub innych danych osobowych. Mogą być celowe (zaplanowane jako atak cyberprzestępców) lub przypadkowe (powstałe w wyniku ludzkiego błędu). Oszuści polują na podatności, czyli luki w zabezpieczeniach, i w ten sposób uzyskują dostęp do informacji na nasz temat.

Jakie są przyczyny wycieków danych? Według „Raportu rocznego z działalności CERT Polska 2022" należą do nich:

- niezamierzone działanie osoby przetwarzającej dane (np. niewłaściwe korzystanie z funkcji „do wiadomości" zamiast „ukryte do wiadomości" przy wysyłce maila);
- błędy w konfiguracji wycieków (np. upublicznienie danych osobowych części studentów Szkoły Głównej Handlowej w Warszawie spowodowane błędnym zabezpieczeniem interfejsu);
- łańcuch wycieków (np. w sytuacji, gdy przestępcy raz zdobyte dane logowania wykorzystują metodą prób i błędów w różnych serwisach – tzw. ataki typu credential stuffing);
- działania cyberprzestępców (np. rozbudowywanie szkodliwego oprogramowania typu ransomware o funkcje pozwalające na kradzież danych z zainfekowanych maszyn).

Gdy zorientujecie się, że Wasze dane zostały upublicznione, przede wszystkim użyjcie programu antywirusowego, żeby sprawdzić bezpieczeństwo swojego komputera. Następnie bezzwłocznie zmieńcie dotychczasowe hasła do logowania, w tym również hasła pokrewne, które łatwo zgadnąć.

Pamiętajcie o unikalnych hasłach w każdym serwisie! Ponadto – tam, gdzie to możliwe – ustawcie też uwierzytelnianie dwuskładnikowe lub wieloskładnikowe, czyli dodatkowe zabezpieczenie, którym będzie np. jednorazowy kod z aplikacji, odcisk palca lub klucz U2F. W zależności od zakresu danych, które wyciekły, konieczne może być np. zastrzeżenie numeru PESEL, co pomoże powstrzymać oszustów np. przed zaciągnięciem pożyczki na Wasze nazwisko.

Aby chronić się przed wyciekiem danych, musicie pamiętać o stosowaniu silnych haseł i innych skutecznych zabezpieczeń, separacji tożsamości i ograniczaniu liczby informacji na swój temat, jakie podajecie w sieci. Ponadto raz na jakiś czas sprawdzajcie, czy Wasze dane nie wyciekły, logując się na stronie bezpiecznedane.gov.pl. Śledźcie komunikaty administratorów danych, którzy mają obowiązek informować klientów o wycieku. Zaglądajcie też na Facebooka CERT Polska, gdzie zawsze znajdziecie aktualne informacje o cyberzagrożeniach.

O przyczynach wycieków i metodach ochrony danych osobowych przeczytacie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: wyciek danych" i „Bezpieczni w sieci z OSE: ochrona danych osobowych".

Źródło:

CERT Polska, (2023), „Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu", Warszawa: Państwowy Instytut Badawczy NASK.

Wyzwanie (challenge)

Wyzwania w sieci, znane jako challenge'e, to jeden z najbardziej wiralowych trendów mediów społecznościowych. Mają przyciągać uwagę, zaskakiwać, bawić, a czasem wzruszać. W idealnym

świecie kończyłyby się na tańcach, akcjach charytatywnych i kreatywnych zabawach. Niestety, wiele z nich przeradza się w niebezpieczne eksperymenty, które narażają uczestników na ryzyko kontuzji i mogą doprowadzić do tragedii.

Challenge'e internetowe narodziły się z potrzeby wspólnoty i zabawy. Użytkownicy mediów społecznościowych lubią uczestniczyć w najpopularniejszych wyzwaniach – bo to sposób na wyrażenie siebie, poczucie przynależności i zdobycie popularności. Często challenge zaczyna się niewinnie: ktoś wymyśla zabawny filmik, inni go naśladują i zaczyna się lawina reakcji.

Problem pojawia się, gdy granica między zabawą a ryzykiem zaczyna się zacierać. Wyzwania typu „cinnamon challenge" (połknięcie łyżki cynamonu), „Tide Pod challenge" (rozgryzanie kapsułek do prania) czy „blackout challenge" (chwilowe podduszanie się) pokazują, że niektóre trendy mogą być skrajnie niebezpieczne dla zdrowia i życia. Choć to brzmi absurdalnie, takie filmy zyskują tysiące odsłon – a dla młodych użytkowników to często wystarczająca motywacja, by spróbować samemu.

Moda na udział w challenge'ach nie mija. Jak czytamy w raporcie „Nastolatki", w 2024 r. przynajmniej raz podjęło je 26% badanych (a tylko 11% rodziców zauważa udział swojego dziecka w takich praktykach). Wyzwania podejmuje 33% chłopców i 19% dziewcząt (Ładna i in., 2025).

Dlaczego tak wielu młodych ludzi ulega takim pomysłom? Odpowiadają za to m.in. potrzeba akceptacji i presja grupy. Media społecznościowe budują świat, w którym widoczność jest równoznaczna z wartością. Lajki i reakcje, szczególnie od rówieśników, podkreślają prestiż, wyrażają uznanie i akceptację, a to bardzo istotne dla nastolatków. Adolescencja to taki okres rozwoju, w którym mózg intensywnie się rozwija, a obszary odpowiadające za kontrolę impulsów nie są jeszcze w pełni ukształtowane – nastolatkowi trudniej przewidzieć konsekwencje swoich zachowań, za to łatwiej podejmuje on ryzyko i przekracza granice. Z drugiej strony ciekawość i chęć odkrywania świata pchają go do eksperymentowania, które nie zawsze jest bezpieczne. Wreszcie młody mózg ma szczególnie wrażliwy układ nagrody. Każdy lajk pod relacją z realizacji wyzwania jest niezwykle przyjemny, a im więcej reakcji, tym silniejsze poczucie satysfakcji i chęć powtarzania takich doświadczeń.

Nie bez znaczenia są również algorytmy mediów społecznościowych, które promują treści wzbudzające emocje. Im bardziej kontrowersyjny lub szokujący materiał, tym większy zasięg. To błędne koło: użytkownicy chcą być zauważeni, więc podejmują coraz bardziej ryzykowne wyzwania, a platformy – kierując się logiką zaangażowania – pokazują je kolejnym osobom.

W ten sposób niebezpieczne challenge'e rozprzestrzeniają się błyskawicznie, często zanim ktokolwiek zdąży zareagować. Dla wielu młodych ludzi są one testem odwagi lub sposobem na zdobycie uznania w grupie rówieśniczej. Problem w tym, że niebezpieczne challenge'e często udają niewinną zabawę, a ich potencjalne skutki są bagatelizowane.

Pamiętajcie, że nie wszystkie wyzwania są szkodliwe i złe. W sieci pojawiały się również inicjatywy niosące dobro – jak „Ice Bucket Challenge", wyzwanie, które pomogło zebrać miliony dolarów na badania nad stwardnieniem zanikowym bocznym (ALS), albo „Hot16Challenge", w którym artyści w śpiewanych na potrzeby wyzwania 16-wersowych piosenkach zachęcali do wpłat wspierających środowisko medyczne podczas pandemii COVID-19.

Źródło:

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

Z

Zabezpieczenia biometryczne

Wiemy doskonale, że podstawowym zabezpieczeniem naszych kont – a co za tym idzie: danych osobowych – są silne hasła. Coraz częściej ich funkcję pełnimy… my sami, np. odblokowując telefon odciskiem palca czy używając wizerunku twarzy do logowania się do banku. To przykłady zabezpieczeń biometrycznych, czyli takich, które wykorzystują nasze unikatowe cechy.

Najczęściej spotykane metody biometryczne to skanowanie odcisku palca, rozpoznawanie twarzy i analiza tęczówki oka. Coraz częściej stosuje się również błyskawiczne selfie, biometrię głosu, analizę układu naczyń krwionośnych dłoni, geometrię dłoni czy rozpoznawanie sposobu chodu i dynamiki pisania na klawiaturze. W niektórych systemach testowane są także bardziej zaawansowane formy uwierzytelniania, łączące kilka cech jednocześnie – np. rozpoznawanie twarzy z potwierdzeniem głosowym – co zwiększa poziom bezpieczeństwa i ogranicza ryzyko oszustw.

Zabezpieczenia biometryczne mają kilka istotnych zalet. Po pierwsze, trudno je skopiować – nie da się „zgubić" swojego odcisku palca ani „pożyczyć" czyjejś tęczówki oka. Po drugie, są wygodne i szybkie – wystarczy jedno spojrzenie w kamerę lub dotknięcie czytnika, aby uzyskać dostęp do urządzenia lub konta. Po trzecie, trudniej o błędy użytkownika – nie ma ryzyka, że zapomni on hasła lub użyje tego samego ciągu znaków w wielu miejscach. Wydaje się również, że biometryczne hasła są niemożliwe do podrobienia przez cyberprzestępców (jednak nie można ufać im bezgranicznie – wystarczy np. nagrać czyjś głos, by oszukać urządzenie, które go rozpoznaje). Przyzwyczajcie się do myśli, że biometria będzie wykorzystywana nie tylko w kryminologii (do badań daktyloskopijnych lub DNA), ale też na coraz szerszą skalę w naszym codziennym życiu. A może już teraz ustawiliście zabezpieczenie biometryczne jako dodatkowy element uwierzytelniania dwuskładnikowego lub wieloskładnikowego?

Warto też wspomnieć, że biometria znajduje zastosowanie nie tylko w urządzeniach mobilnych czy bankowości elektronicznej, ale także w np. kontroli dostępu w instytucjach publicznych i na lotniskach. W medycynie ułatwia identyfikację pacjentów, a w sektorze transportowym – usprawnia odprawę podróżnych.

Na koniec biometryczna ciekawostka: choć wydaje się, że tego typu zabezpieczenia są znakiem obecnych czasów, ich pierwszych śladów można szukać nawet w III/II tysiącleciu p.n.e. Istnieją bowiem dowody, że starożytni Babilończycy umieszczali odciski palców w formie podpisów na kontraktach!

Więcej informacji o silnych hasłach i sposobach zabezpieczania kont znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe" i „Bezpieczni w sieci z OSE: płatności biometryczne".

Zachowania ryzykowne

Internet, zwłaszcza media społecznościowe, stają się dla młodych ludzi przestrzenią, w której mogą obserwować, prezentować i – niestety – podejmować ryzykowne zachowania. Wirtualny świat, często ukazujący wyidealizowane, wykreowane obrazy rzeczywistości, kształtuje niebezpieczne wzorce – ich powielanie może prowadzić do poważnych problemów psychicznych i fizycznych.

Jednym z niebezpieczeństw jest promowanie zaburzeń odżywiania. W sieci można natrafić na profile i treści, ukazujące anoreksję w sposób estetyczny, co może zachęcać młodych do drastycznych działań w celu osiągnięcia „idealnej" sylwetki. W mediach społecznościowych ludzkie ciało często przedstawiane jest jako produkt, który musi być piękny i doskonały, a sukces utożsamiany jest z osiągnięciem właśnie takiego wyglądu. Nastolatki dążą do nierealistycznych standardów, nierzadko narażając swoje zdrowie i życie.

Innym ryzykownym zachowaniem są internetowe wyzwania, tzw. challenge'e, które często stanowią zagrożenie dla zdrowia, a nawet życia. Młodzi ludzie, ze względu na swoją impulsywność i potrzebę akceptacji, są szczególnie podatni na tego typu treści. Podejmują wyzwania, aby zdobyć uznanie rówieśników, nie zawsze zdając sobie sprawę z konsekwencji.

Czy możecie pomóc swoim dzieciom i uczniom odnaleźć się w wirtualnym świecie? Jak najbardziej. Ważne jest, aby młodzi ludzie nauczyli się krytycznie oceniać treści, które widzą w internecie i nie wierzyć ślepo we wszystko, co usłyszą od influencerów. Niezbędne jest również rozwijanie odporności psychicznej, aby mogli dystansować się od presji idealizowanego świata online. Uczcie ich rozpoznawać i odrzucać niebezpieczne wzorce oraz wspierajcie ich w kształtowaniu wewnętrznego, przyjaznego głosu, który w odpowiedniej chwili powie nastolatkowi: „Jesteś wystarczający", „Wszystko z tobą w porządku".

Chcecie dowiedzieć się więcej? Obejrzycie wystąpienie ekspertki OSE Marty Witkowskiej „Glamouryzacja zaburzeń i zachowa ryzykownych w internecie" zarejestrowane podczas Kongresu OSE 2023, dostępne na kanale Ogólnopolskiej Sieci Edukacyjnej na YouTubie.

Zakupy online

Zakupy online robimy coraz chętniej. Eksperci z CERT Polska w poradniku „Jak bezpiecznie kupować w internecie" podają, że tylko „w 2022 r. spośród 37,6 miliona Polaków około 30 milionów (77–81% w zależności od badania) miało już doświadczenie z realizowaniem zakupów w internecie" (CERT Polska, 2023). Do korzystania z e-sklepów, zakupowych aplikacji mobilnych czy portali aukcyjnych przekonuje nas głównie wygoda. Wszystkie produkty mamy na wyciągnięcie ręki, szybko możemy też znaleźć najatrakcyjniejszą ofertę. I co ważne – nie musimy tracić czasu na dojazdy do sklepów i stanie w kolejkach.

Zanim jednak wrzucicie coś do wirtualnego koszyka i klikniecie „zamawiam", sprawdźcie, czy nie kupujecie kota w worku. Podczas polowania na atrakcyjne ceny warto pamiętać o kilku zasadach bezpieczeństwa i dobrych cyfrowych nawykach. Jakich?

- **Zastanówcie się, jak trafiliście na daną witrynę**. Jeśli informacje o wyjątkowych promocjach i kuponach rabatowych otrzymaliście w wiadomości SMS, e-mail, w komunikatorze lub kliknęliście w baner reklamowy w sieci – zachowajcie czujność. Przestępcy wykorzystują różne kanały komunikacji, żeby dotrzeć do potencjalnych ofiar i za pomocą przesłanych linków przekierować je na niebezpieczną stronę.
- **Poszukajcie istotnych informacji**. Na stronie e-sklepu powinny być zamieszczone podstawowe informacje: adres, pod jakim zarejestrowana jest firma, telefon, numer w Krajowym Rejestrze Sądowym (KRS). Uwaga, jeśli w KRS pod nazwą rzekomego właściciela sklepu wpisana jest firma prowadząca inną działalność niż handlową – to ważne ostrzeżenie! Poszukajcie też na stronie sklepu regulaminu, a w nim zasad zwrotów, sposobów dostarczenia przesyłki. Ponadto upewnijcie się, czy dostępne są różne formy płatności. Jeśli nie znajdziecie takich informacji – poszukajcie ofert w innym sklepie.
- **Oceńcie jakość strony internetowej sklepu**. Jeśli strona jest przygotowana „na kolanie", w opisach występują liczne błędy językowe, zdjęcia i grafiki są słabej jakości, a sam sklep posiada bardzo szeroką ofertę i kusi podejrzanie wysokimi rabatami – opuśćcie tę witrynę. Z drugiej strony – niech Was nie zwiedzie profesjonalizm. Przestępcy wciąż doskonalą się w działaniu i są w stanie przygotować portal, który nie będzie wzbudzał zbyt wielu podejrzeń.
- **Skontaktujcie się ze sprzedawcą**. Wyślijcie wiadomość przez formularz kontaktowy na stronie lub na podany adres e-mail, napiszcie na czacie, zadzwońcie pod wskazany numer telefonu. Brak odpowiedzi to kolejny sygnał ostrzegawczy.
- **Zapoznajcie się z opiniami innych klientów**. Znaleźliście same pozytywne opinie? Nie spoczywajcie na laurach! Zweryfikujcie, czy zamieszczone oceny nie wydają się podobne, wygenerowane sztucznie, czy wszystkie nie zostały opublikowane w tym samym czasie i czy na pewno dotyczą sklepu, w którym zamierzacie dokonać zakupu. Skorzystajcie też

z wyszukiwarki internetowej – jest szansa, że wcześniej oszukani klienci zdążyli ostrzec innych przed fałszywą witryną. Sami także wystawcie opinię, jeśli poczuliście się oszukani, dzięki temu być może ktoś inny uniknie groźnej pułapki.

- **Dokładnie przeczytajcie adres strony**. Zwróćcie uwagę, czy w adresie sklepu (ale też bramki z płatnościami online, na którą finalnie zostaniecie odesłani) nie kryją się łatwe do przeoczenia literówki. Być może witryna, na której się znaleźliście, podszywa się pod znaną markę.
- **Uważajcie na nietypowe prośby sprzedawcy**. Jeśli podczas zakupów dostaniecie dodatkowe prośby: o pobranie aplikacji z niezaufanego źródła, podanie loginu do bankowości mobilnej, przesłanie zdjęcia karty kredytowej – uciekajcie!

CERT Polska ostrzega, że przy okazji nierozważnych zakupów online możemy się narazić na wiele przykrych konsekwencji. Utrata gotówki za towar, który nigdy do nas nie dotrze, to stosunkowo niewielka strata. Gorzej, gdy podczas e-zakupów stracimy wszystkie oszczędności lub przestępca przejmie nasze dane wrażliwe. Może się tak stać, jeśli zdoła zainstalować na naszym urządzeniu złośliwe oprogramowanie.

Gdy okaże się, że zrobiliście zakupy w fałszywym sklepie, powinniście jak najszybciej poinformować o tym swój bank. Możecie złożyć reklamację i poprosić o uruchomienie mechanizmu tzw. obciążenia zwrotnego (chargeback). Zgłoście też incydent na stronie incydent.cert.pl oraz na policji. Zostawcie także informację w sieci o nieuczciwym sprzedawcy. Być może uda Wam się w ten sposób uchronić innych użytkowników internetu przed cyberatakiem!

Więcej informacji znajdziecie w aktualnościach z serii „Bezpieczne zakupy" na stronie ose.gov.pl: „Bezpieczne zakupy: przygotuj się na Black Friday", „Bezpieczne zakupy: platformy sprzedażowe", „Bezpieczne zakupy: płatności online".

Źródło:

„Bezpieczne zakupy: fałszywe e-sklepy", (2024), artykuł na stronie ose.gov.pl.

CERT, (2023), „Jak bezpiecznie kupować w internecie. Poradnik CERT Polska 2022/2023", Warszawa: Państwowy Instytut Badawczy NASK.

Zbiórki charytatywne online

„Na leczenie", „na zwierzaka", „na Ukrainę" – to najczęstsze cele zbiórek, z jakimi mamy obecnie do czynienia w internecie. Jako społeczeństwo coraz bardziej angażujemy się w pomoc potrzebującym, musimy więc wiedzieć, że możemy natknąć się na oszustów.

Przestępcy grają na naszych emocjach i bez mrugnięcia okiem wykorzystują różne metody – wyszukują w internecie zdjęcia chorych dzieci i zwierząt, podrabiają dokumentację medyczną, w swoje zbiórki angażują celebrytów. Wszystko po to, by wyłudzić od nas pieniądze.

To oczywiście nie znaczy, że powinniście zrezygnować z udziału w akcjach charytatywnych! Jeżeli chcecie komuś pomóc, wybierajcie zaufane platformy organizujące zbiórki (tam również zdarzają się próby oszustw, jednak organizatorzy zrzutek są szczegółowo weryfikowani) oraz miejcie oczy i uszy szeroko otwarte. Zapoznajcie się dokładnie z celem zbiórki i jej opisem, sprawdzajcie, jak długo istnieje organizacja, która ją prowadzi, szukajcie jej regulaminu, terminu rozpoczęcia i zakończenia akcji. Starajcie się też weryfikować adres strony internetowej – pamiętajcie, że przestępcy często przygotowują fałszywą stronę, do złudzenia przypominającą witrynę np. danej organizacji pozarządowej. Zalecamy też sprawdzanie, czy zbiórka jest powiązana z jakąś wiarygodną instytucją, np. domem dziecka czy szpitalem, która potwierdzi, że współpracuje z organizatorem zrzutki. Koniecznie zajrzyjcie też na stronę zbiorki.gov.pl, gdzie prowadzony jest rejestr zbiórek publicznych organizowanych na terenie kraju.

A może chcecie wrzucić pieniądze do puszki? Spójrzcie więc czujnie na osobę prowadzącą zbiórkę. Powinna być ona wyposażona w identyfikator zawierający imię i nazwisko, nazwę zbiórki, jej cel i numer, a także informacje o organizatorze.

Jeśli macie podejrzenia co do legalności jakiejś zbiórki pieniędzy, zgłoście tę sprawę na policję.

Źródła:

Gańko K., (2022), „(Cyber)bezpieczne święta z OSE”, Warszawa: Państwowy Instytut Badawczy NASK.

„Rozsądek online – jak się nie dać oszukać w sieci! Fałszywe zbiórki”, artykuł na stronie bezpiecznymiesiac.pl.

Zero trust security

Z pewnością wielokrotnie zetknęliście się ze stwierdzeniem, że pomocne w wystrzeganiu się zagrożeń jest zachowywanie zasady ograniczonego zaufania. To bardzo ważna reguła! Nieprzyjmowanie obcych osób do grona znajomych w social mediach, nieotwieranie załączników z podejrzanych maili, ograniczanie informacji na swój temat podawanych w sieci – takie nawyki mogą ochronić Was przed bardzo nieprzyjemnymi skutkami ataków cyberoszustów.

Na poziomie firm i dużych organizacji konieczne jest jeszcze większe zaostrzenie rygoru, którym jest wdrożenie polityki zero trust (brak zaufania). Podstawą tego modelu bezpieczeństwa jest założenie, że nie wolno ufać nikomu i niczemu (żadnemu użytkownikowi, nowemu sprzętowi czy adresowi IP), dopóki nie udowodni, że nie stanowi zagrożenia. Kluczowe okazują się tu: uwierzytelnianie użytkowników na podstawie wszystkich możliwych punktów dostępowych, ograniczanie do minimum ryzyka nieuprawnionych dostępów, bieżące wykrywanie zagrożeń, ograniczanie uprawnień „dokładnie na czas” i udzielanie ich tylko w niezbędnym zakresie.

Choć te zasady w teorii odnoszą się do zarządzania bezpieczeństwem w dużych instytucjach, nic nie stoi na przeszkodzie, żeby politykę zero trust stosować także w mniejszej skali. Nie spodziewaliście się maila z informacją o nagrodzie w konkursie? Nie wypełniajcie formularza potwierdzającego Waszą tożsamość. Nie macie pewności, że dzwoni do Was znajomy, który potrzebuje pomocy? Upewnijcie się, że po drugiej stronie słuchawki jest faktycznie ktoś, kogo znacie. Za każdym razem, gdy stykacie się w sieci z czymś nieoczywistym, uważajcie i podchodźcie z duża dozą ostrożności do „okazji dostępnych tylko dziś”, doniesień budzących silne emocje, wiadomości wymuszających natychmiastowe działanie pod groźbą „poważnych konsekwencji”.

Zespół ds. nadużyć (zespół abuse)

Internet to przestrzeń, w której codziennie powstają miliony wiadomości, postów, filmów i stron. Większość z nich służy wymianie informacji i komunikacji, ale wśród nich pojawiają się też treści szkodliwe – spam, próby wyłudzeń, ataki hakerskie, a nawet materiały niezgodne z prawem. Właśnie w takich sytuacjach do akcji wkracza zespół ds. abuse – niewidoczny dla większości użytkowników, ale kluczowy dla bezpieczeństwa całej sieci.

Abuse (ang. nadużycie) w kontekście internetu odnosi się do wszelkich działań, które łamią zasady korzystania z sieci – od rozsyłania spamu i złośliwego oprogramowania po naruszenia praw autorskich, phishing czy cyberprzemoc.

Zespół ds. abuse (często działający w ramach operatorów sieci, dostawców usług internetowych lub instytucji publicznych) zajmuje się przyjmowaniem i analizowaniem takich zgłoszeń. Jego zadaniem jest reagowanie na nadużycia – wykrywanie, blokowanie i zapobieganie szkodliwym działaniom w internecie.

Praca specjalistów ds. abuse to połączenie informatyki, analizy danych i cyberbezpieczeństwa. Zespół:

- monitoruje ruch w sieci i reaguje na zgłoszenia o podejrzanych działaniach;
- analizuje adresy IP, z których wysyłany jest spam lub prowadzony atak;
- weryfikuje, czy dana domena nie służy do phishingu lub dystrybucji malware;
- współpracuje z innymi operatorami, organizacjami i służbami w celu neutralizacji zagrożeń;

- podejmuje działania naprawcze – np. blokuje dostęp do niebezpiecznych stron lub zawiesza konta użytkowników łamiących regulamin.

Choć wiele z tych czynności odbywa się w tle, ich efekt odczuwa każdy z nas: mniej spamu, szybsze reagowanie na oszustwa, większe bezpieczeństwo użytkowników sieci.

Każdy użytkownik sieci może wesprzeć działania zespołów ds. abuse, zgłaszając podejrzane sytuacje. Warto to robić, gdy: otrzymamy wiadomość e-mail z podejrzanym linkiem lub prośbą o podanie danych, zauważymy stronę podszywającą się pod instytucję publiczną, bank lub sklep lub trafimy na treści łamiące prawo (np. nawoływanie do nienawiści, pornografia dziecięca, kradzione oprogramowanie). Należy wówczas zwrócić się do CERT Polska (za pośrednictwem formularza na stronie incydent.cert.pl) lub Dyżurnet.pl (na stronie dyzurnet.pl, mailowo na adres: dyzurnet@dyzurnet.pl lub telefonicznie: 801 615 005).

Zielona kłódka

Cyberbezpieczeństwo to bardzo dynamiczna dziedzina – razem z nowymi metodami ataków powstają nowe zabezpieczenia, musicie więc śledzić na bieżąco pomocne wskazówki i doniesienia. Jednym z przykładów może być przełamany w ostatnim czasie mit zielonej kłódki w pasku adresu, rzekomo gwarantującej bezpieczeństwo odwiedzanej strony.

Kłódka mówi tylko o tym, że połączenie jest szyfrowane, czyli strona korzysta z certyfikatu SSL zapewaniającego poufność przesyłanych danych. Zdobycie takiego darmowego certyfikatu nie nastręcza zbyt wielu problemów – okazuje się, że większość stron phishingowych, które CERT Polska wpisuje na listę ostrzeżeń przed niebezpiecznymi stronami, ma adres zaczynający się od https i jest poprzedzony kłódką!

O czym powinniście pamiętać? **Ważny jest adres odwiedzanej strony, nie to, czy znajduje się przy nim kłódka**. Zwracajcie uwagę, czy w adresie strony nie pojawiają się:

- literówki, np. „0” zamiast „o”;
- nietypowe rozszerzenia, np. „.tk”, „.top”, „.ru”, czy „.xyz” zamiast najpopularniejszych w Polsce „.pl”, „.com”, czy „.eu”;
- długie lub niepasujące subdomeny, np. „bank.security.login.example.com”;
- dodatkowe znaki, np. „paypal-secure.com” zamiast „paypal.com”.

Wasz niepokój powinny wzbudzić częste przekierowania, zwłaszcza jeśli po wejściu na jakąś witrynę natychmiast zmienia się adres w przeglądarce, a Wy trafiacie na podejrzaną stronę z reklamami lub stronę umożliwiającą pobieranie np. dodatkowego oprogramowania. Uważajcie też na linki ukryte w e-mailach – zamaskowane pod hiperłączami czy przyciskami. Przed kliknięciem zawsze najeżdżajcie myszką na link, aby zobaczyć, dokąd naprawdę prowadzi.

Coraz częściej phishingowe i inne niebezpieczne strony różnią się od swoich legalnych pierwowzorów jedynie nieznacznymi szczegółami. Niestety to właśnie te drobiazgi, których w pośpiechu nie zauważycie, mogą Was kosztować utratę danych osobowych lub nawet oszczędności życia. Wystarczy bowiem, że na podstawionej przez oszustów stronie podacie swój login i hasło do bankowości elektronicznej…

Zielona kłódka nie może uśpić Waszej czujności! Zawsze sprawdzajcie, na jakiej stronie się znajdujecie (nawet jeśli wydaje Wam się, że dana witryna wygląda tak samo jak zawsze), a jeśli coś wzbudzi Wasze podejrzenia – zgłoście incydent do CERT Polska. Możecie skorzystać z formularza dostępnego na stronie incydent.cert.pl lub nowej funkcji w aplikacji mObywatel.

Źródła:

„Cyberbombki – podsumowanie”, artykuł w serwisie cert.pl.

„Funkcja Bezpieczni w sieci już dostępna w mObywatelu. Jak działa?”, (2024), artykuł w serwisie cyberdefence24.pl.

Bibliografia i literatura uzupełniająca

(dostęp do wszystkich treści online: 14.11.2025)

Artykuły na stronie ose.gov.pl

a) Z serii „Bezpieczni w sieci z OSE: aplikacje mobilne", „Bezpieczni w sieci z OSE: ataki słownikowe", „Bezpieczni w sieci z OSE: bezpieczeństwo urządzeń mobilnych", „Bezpieczni w sieci z OSE: bezpieczne logowanie", „Bezpieczni w sieci z OSE: bezpieczny login i hasło", „Bezpieczni w sieci z OSE: BLIK i płatności internetowe", „Bezpieczni w sieci z OSE: CAPTCHA", „Bezpieczni w sieci z OSE: child grooming", „Bezpieczni w sieci z OSE: cyberbullying", „Bezpieczni w sieci z OSE: dezinformacja w mediach społecznościowych", „Bezpieczni w sieci z OSE: doxing", „Bezpieczni w sieci z OSE: fake newsy", „Bezpieczni w sieci z OSE: internet rzeczy (IoT)", „Bezpieczni w sieci z OSE: internetowi oszuści i socjotechnika", „Bezpieczni w sieci z OSE: kampanie phishingowe w 2024 roku", „Bezpieczni w sieci z OSE: komunikatory internetowe", „Bezpieczni w sieci z OSE: kontrola rodzicielska", „Bezpieczni w sieci z OSE: kradzież danych i tożsamości", „Bezpieczni w sieci z OSE: kody QR", „Bezpieczni w sieci z OSE: kontrola rodzicielska", „Bezpieczni w sieci z OSE: lista ostrzeżeń przed fałszywymi stronami", „Bezpieczni w sieci z OSE: malware", „Bezpieczni w sieci z OSE: metody i techniki dezinformacji", „Bezpieczni w sieci z OSE: ochrona danych osobowych", „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci", „Bezpieczni w sieci z OSE": online'owy nudging", „Bezpieczni w sieci z OSE na wakacje: oversharing i cyfrowy ślad", „Bezpieczni w sieci z OSE: phishing", „Bezpieczni w sieci z OSE: płatności biometryczne", „Bezpieczni w sieci z OSE: poczta e-mail", „Bezpieczni w sieci z OSE: podatności i luki bezpieczeństwa", „Bezpieczni w sieci z OSE: przechowywanie danych w chmurze", „Bezpieczni w sieci z OSE: przeglądarki internetowe", „Bezpieczni w sieci z OSE: ransomware", „Bezpieczni w sieci z OSE: silne hasła i uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: szyfrowanie end-to-end", „Bezpieczni w sieci z OSE: trolling w mediach społecznościowych", „Bezpieczni w sieci z OSE: uwaga na okazje w Black Friday", „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe", „Bezpieczni w sieci z OSE: wideokonferencje", „Bezpieczni w sieci z OSE na wakacje: fałszywe oferty", „Bezpieczni w sieci z OSE: wakacyjne przyjaźnie – uwaga na niebezpieczne kontakty!", „Bezpieczni w sieci z OSE: wyciek danych"

b) Inne: „5 pytań o… aplikację mOchrona", „5 pytań o… FOMO i problemowe używanie internetu", „5 pytań o… gaming", „5 pytań o… równowagę cyfrową", „5 pytań o… usługi bezpieczeństwa OSE", „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!", „Bezpieczne media społecznościowe", „Bezpieczne zakupy: fałszywe e-sklepy", „Bezpieczne zakupy: platformy sprzedażowe", „Bezpieczne zakupy: płatności online", „Bezpieczne zakupy: przygotuj się na Black Friday", „Bezpieczni w sieci z OSE na wakacje: bankowość mobilna", „Bezpieczni w sieci z OSE na wakacje: catfishing i letnie kontakty online", „Bezpieczni w sieci z OSE na wakacje: offline challenge", „Bezpieczni w sieci z OSE na wakacje: kopie zapasowe", „Bezpieczni w sieci z OSE na wakacje: sharenting i wizerunek dziecka w sieci", „Cyfrowa higiena i bezpieczeństwo w sieci z OSE", „Cyfrowe gry a rozwój dziecka", „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa", „Czas na wiosenne – cyfrowe – porządki!", „Czy to nagranie może kłamać? Uwaga na deepfake!", „Doomsurfing – jak wyrwać się z błędnego koła śledzenia złych informacji", „Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!", „Dzień bez Telefonu Komórkowego – czy to możliwe?", „Dzień Bezpiecznego Komputera: zadbaj o swój sprzęt", „Europejski Miesiąc Cyberbezpieczeństwa z OSE: naucz się reagować na incydenty bezpieczeństwa", „Europejski Miesiąc Cyberbezpieczeństwa z OSE: phishing", „Dekalog bezpiecznego internauty", „Europejski Miesiąc Cyberbezpieczeństwa z OSE: uważaj na różne typy oszustw w internecie", „Jak nie kupić kota w worku, czyli bezpieczne zakupy online", „Jak nie wpaść w pułapkę fake newsów?", „Kongres OSE 2024: szkodliwe treści w internecie", „Majówka – cyfrowy detoks czy balans?", „Netykieta, czyli jak zostać mistrzem słowa w internecie", „Niebezpieczne zjawiska w internecie: FOMO", „Niebieski Poniedziałek – zadbajmy o zdrowie

psychiczne dzieci", „Sekrety sztucznej inteligencji: chatboty na usługach cyberprze stępców", „Skimming, czyli co się może kryć w bankomacie", „Smombie są wśród nas", „Stres cyfrowy – czym jest i jak go pokonać?", „Tylko zerknę. Sprawdź, czy Twoje dziecko doświadcza phubbingu", „Ukryte znaczenie emocji – jak zrozumieć swoje dziecko?", „Uwaga na spoofing!", „Uwaga na romance scam!", „Uwaga, złodziej!", „Walentynki online? Sexting – niebezpieczny trend", „Wirtualna miłość – realne zagrożenie", „Zadbaj o siebie z OSE: cyfrowy detoks", „Zadbaj o siebie z OSE: cyfrowy stres", „Zadbaj o siebie z OSE: doomsurfing", „Zadbaj o siebie z OSE: Dzień bez Komputera", „Zadbaj o siebie z OSE: media społecznościowe", „Zadbaj o siebie z OSE: odzyskaj kontrolę nad czasem ekranowym", „Zadbaj o siebie z OSE: oversharing", „Zadbaj o siebie z OSE: problemowe używanie internetu", „Zadbaj o siebie z OSE: prywatność w mediach społecznościowych", „Zadbaj o siebie z OSE: seksting", „Zadbaj o siebie z OSE: zrób coś dobrego dla swojego mózgu", „Zanim uwierzysz, sprawdź!", „Złote zasady internetowych znajomości", „Zrób kopię zapasową!"

Artykuły na platformie OSE IT Szkoła

„Dzień Bota – dowiedz się więcej o sztucznej inteligencji!", „Cyberbezpieczna biblioteczka: cyfrowy ślad", „Cyberbezpieczna biblioteczka: szkodliwe treści", „Gaming – uzależnienie od gier komputerowych", „Gra pod choinkę? Poradnik świętego Mikołaja", „Grać czy nie grać? Oto jest pytanie", „Lekcja o cyberbezpieczeństwie: prywatność online", „Lekcja o cyberbezpieczeństwie: prywatność online cz. 2", „Letnia Akademia Cyfrowej Higieny: czas na social media sabbatical", „Letnia Akademia OSE 2022: hazard online", „Letnia Akademia Cyfrowej Higieny: o nudgingu i cyfrowych sztuczkach", „Masz już swój plan B?", „Netykieta, czyli jak zostać mistrzem słowa w internecie", „Nie krzycz w internecie, czyli ściągawka z netykiety", „Niebezpieczne zjawiska w internecie: szkodliwe treści", „Silne hasło to podstawa!", „Temat lekcji: FOMO i problemowe używanie internetu wśród uczniów", „Temat lekcji: gry cyfrowe", „Temat lekcji: manipulacje w sieci i teorie spiskowe", „Temat lekcji: nadużywanie internetu", „Temat lekcji: przemoc w sieci", „Temat lekcji: sexting"

Artykuły na stronie kompetencjecyfrowe.gov.pl

„Bezpieczne wideokonferencje i spotkania online", „Jak cię widzą, tak cię piszą… Zadbaj o swój wizerunek w sieci", „Jak zgodnie z prawem korzystać z materiałów dostępnych w internecie?", „Nauczyciel w świecie deepfake – czy uwierzyłbyś swoim oczom?", „Ochrona przed dezinformacją", „Ochrona przed oprogramowaniem szpiegującym"

Artykuły – inne

„ALFA, BRAVO, CHARLIE, DELTA – stopnie alarmowe CRP", (2025), artykuł na stronie kompetencjecyfrowe.gov.pl.

„Bezpieczeństwo twojej kieszeni, czyli jak ochronić swój telefon", artykuł na stronie cert.pl.

„Co to jest Backdoor?", (b.r.), artykuł na stronie nflo.pl.

„Co to jest bot?", (b.r.), artykuł na stronie nflo.pl.

„Co to jest Botnet?", (b.r.), artykuł na stronie nflo.pl.

„Co to jest certyfikat SSL, podstawowe informacje o certyfikatach SSL", (b.r.), artykuł w serwisie instytutcyber.pl.

„Co to jest firewall? Jak działa zapora sieciowa?", (2025), artykuł na stronie bezpiecznyinternet.edu.pl.

„Co to jest kryptowaluta?", (b.r.), artykuł w serwisie coinbase.com.

„Co to jest kryptowaluta i jak funkcjonuje?", (2021), artykuł w serwisie skrill.com.

„Co to jest OSINT (biały wywiad) i jak przebiega?”, (2024), artykuł w serwisie bezpiecznyinternet.edu.pl.

„Co to jest spyware? Jak się chronić i usunąć oprogramowanie szpiegujące?”, (2025), artykuł na stronie cyberacademy.com.pl.

„Co wycieki danych mówią o hasłach”, (2022), artykuł na stronie cert.pl.

„Cyberbombki – podsumowanie”, artykuł w serwisie cert.pl.

„Cybersquatting w praktyce – na czym polega? Jak się przed nim zabezpieczyć?”, (2023), artykuł w serwisie netia.pl.

„Czym jest adware?”, (b.r.), artykuł na stronie malwarebytes.com.

„Czym jest atak DoS”, (2022), artykuł w serwisie instytutcyber.pl.

„Czym jest GPS Jamming?”, (2025), artykuł na stronie instytutcyber.pl.

„Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?”, (2022), artykuł na stronie gov.pl.

„Czym jest stalking?”, (2021), artykuł na stronie mazowiecka.policja.gov.pl.

Dębski M., (2024), „10 tricków patoinfluencera”, grafika dostępna na stronie Fundacja Dbam o Mój Zasięg na Facebooku.

Dzieciuchowicz N., (2024), „Naruszenie prywatności – co oznacza, jakie może mieć skutki i kto ponosi odpowiedzialność”, artykuł na stronie lexdigital.pl.

„Encyklopedia cyberbezpieczeństwa: APT”, (2022), artykuł w serwisie instytutcyber.pl.

„Fonoholizm, czyli uzależnienie od telefonu”, (b.r.), artykuł w serwisie gov.pl.

„Funkcja Bezpieczni w sieci już dostępna w mObywatelu. Jak działa?”, artykuł w serwisie cyberdefence24.pl.

„Gotowi na RODO”, (b.r), Generalny Inspektor Ochrony Danych Osobowych, Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego.

Górecki M., (2021), „Bezpieczne przesyłanie dużych plików”, artykuł w serwisie politykabezpieczenstwa.pl.

„Jak chronić własność intelektualną firmy w internecie”, (2021), artykuł w portalu Biznes.gov.pl.

„Jak i gdzie kupić bitcoin?”, (b.r.), artykuł w serwisie odkryjbitcoin.pl.

„Jak pomóc dziecku wciągniętemu w hazard? Rozmowa z ekspertem”, (b.r.), wywiad z Barbarą Wojewódzką na portalu uzaleznieniabehawioralne.pl.

„Jak sobie radzić z przeciążeniem informacyjnym?”, (2024), artykuł w serwisie pw.edu.pl.

„Kompleksowo o hasłach”, (2022), artykuł na stronie cert.pl.

Krauzowicz M., (b.r.), „Hardening od podstaw, czyli jak ze swojej organizacji zrobić twierdzę nie do zdobycia?”, artykuł w serwisie integritypartners.pl.

„Ktoś od miesiąca zawiesza smartfony w warszawskim metrze. Jak to robi?”, (2023), artykuł w serwisie niebezpiecznik.pl.

„Lektura obowiązkowa: cyfrowa odporność”, (2020), artykuł w serwisie vertiv.com.

Łużak T., (2024), „Atak słownikowy – na czym polega i jak się przed nim chronić?”, artykuł w serwisie netia.pl.

Łużak T., „Bomba logiczna, czyli liczy się czas”, (2025), artykuł na stronie www.netia.pl.

Łużak T., „Browser hijacker – ataki w przeglądarkach wykorzystywanych przez pracowników. Czym grożą?”, (2025), artykuł na stronie netia.pl.

„Na czym polega kradzież tożsamości?”, (2024), artykuł na stronie wojtanis.com.pl.

„Niebezpieczne reklamy w wyszukiwarkach – jak się nie dać złapać cyberoszustom?”, (2023), artykuł na stronie gov.pl.

„Nowa kampania reklamowa ad hijacking za pośrednictwem Google Ads”, (2023), artykuł na stronie cert.pl.

„Ochrona danych zgodnie z RODO”, (2025), artykuł na stronie europa.eu.

Olszewski D., (2022), „Czy łączność bezprzewodowa Bluetooth jest bezpieczna?”, artykuł w serwisie computerworld.com.

„Oszustwa na portalach z ogłoszeniami”, (2022), artykuł w serwisie cert.pl.

„Oszustwa typu BEC”, (2023), artykuł na stronie gov.pl.

„People snubbed on Facebook feel less meaningful existence study finds”, (2014), artykuł w serwisie cbsnews.com.

„Pojęciownik Demagoga”, (2022), artykuł w serwisie demagog.pl.

„Rozsądek online – jak się nie dać oszukać w sieci! Fałszywe zbiórki”, artykuł na stronie bezpiecznymiesiac.pl.

Rożnowski J., (2024), „Na czym polega atak clickjacking? Jak się zabezpieczyć?”, artykuł w serwisie semcore.pl.

„Różnica między VR a AR”, (b.r.), artykuł w serwisie 4font.pl.

Rybak Ł., Dudczyk J., (2019), „User experience w aspekcie zagrożenia dla bezpieczeństwa cyfrowego”, Journal of Modern Science, tom 2/41, s. 127–140.

Sreenivas S., (2023), „What Is Digital Self-Harm?”, artykuł w serwisie webmd.com.

Stanecki J., (2023), „Zagrożenia związane z Chat GPT o innymi AI”, artykuł w serwisie gdpr.pl.

„Stopnie alarmowe i stopnie alarmowe CRP”, (b.r.), artykuł na stronie gov.pl.

Świerczek S., (2024), „Sztuczna inteligencja (AI) w cyberbezpieczeństwie”, artykuł w serwisie netcomplex.pl.

Tomaszewska I., (2023), „Czy strona jest wiarygodna – jak to sprawdzić samodzielnie?”, artykuł w serwisie demagog.org.

„Uwaga, fałszywa CAPTCHA, czyli nie daj się zainfekować”, (2024), artykuł na stronie cert.pl.

„Uważaj na fałszywe inwestycje w sieci”, (b.r.), informacje na stronie cert.pl.

„Uzależnienie od telefonu i nomofobia – przyczyny, objawy, leczenie”, (b.r), artykuł na stronie emc-sa.pl.

Vega N., (2017), „Co łączy króla wikingów, bezprzewodowe słuchawki i samochodowy zestaw głośnomówiący?”, artykuł w serwisie businessinsider.com.

Watemborski M., (2023), „Chat GPT – co to jest, jak działa, i do czego może być przydatny”, artykuł w serwisie tech.wp.pl.

WEC Communication, (2017), „Sprawdzamy, która metoda blokady ekranu jest najbezpieczniejsza”, artykuł w serwisie media.wec24.pl.

„Wirus komputerowy – czym jest? Jakie są rodzaje wirusów?”, (2025), artykuł w serwisie bezpiecznyinternet.edu.pl.

„Wystarczy jedno spojrzenie – płatności biometryczne”, (2023), artykuł w serwisie bezpiecznymiesiac.pl.

„Zaawansowane długotrwałe ataki (APT)”, (b.r), artykuł w serwisie 4consult.com.pl.

„Zgłoś nieuprawnione wykorzystanie swoich danych osobowych (kradzież tożsamości) – unieważnij dowód”, (b.r), artykuł na stronie gov.pl.

„Złośliwe rozszerzenia przeglądarek”, (2023), artykuł w serwisie trafficwatchdog.pl.

Publikacje

Borkowska A., (2024), „Mniej znaczy więcej – o multiscreeningu i wielozadaniowości”, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., (2023), „Cyberprzemoc. Włącz blokadę na nękanie. Poradnik dla rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., (2023), „Cyberprzemoc w szkole. Poradnik dla nauczycieli”, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Gańko K. Witkowska M., (2025), „O cyfrowej higienie”, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2025), „O grach cyfrowych”, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2023), „Sharenting i wizerunek dziecka w sieci”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., Gańko K., (2025), „O cyberprzemocy i hejcie w sieci”, Warszawa: Państwowy Instytut Badawczy NASK.

Bromiley M., (2019), „Czy robisz kopie zapasowe”, Biuletyn Bezpieczeństwa Komputerowego „OUCH!” nr 8, tłum. Wnuk B., Purzycki K., Urbanowicz J. SANS Security Awareness.

CERT Polska, (b.r.), „Poradnik ransomware”, Warszawa: Państwowy Instytut Badawczy NASK.

CERT Polska, (b.r.), „Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych”, Warszawa: Państwowy Instytut Badawczy NASK.

CERT, (2023), „Jak bezpiecznie kupować w internecie. Poradnik CERT Polska 2022/2023”, Warszawa: Państwowy Instytut Badawczy NASK.

CERT Polska, (2023), „Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu”, Warszawa: Państwowy Instytut Badawczy NASK.

CERT, (2025), „Raport roczny 2024 z działalności CERT Polska”, Warszawa: Państwowy Instytut Badawczy NASK.

Cherne L. (red.), (2020), „Bezpieczeństwo wideokonferencji”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 8.

Dudley T., (2018), „Powstrzymać phishing”, Biuletyn Bezpieczeństwa Komputerowego „OUCH!” nr 4, tłum. Kondraszuk S., Strzelczyk M., Sikorski J., SANS Security Awareness.

„Fake newsy, bańki informacyjne, teorie spiskowe”, (b.r.), Warszawa: Państwowy Instytut Badawczy NASK.

Gańko K., (2022), „(Cyber)bezpieczne święta z OSE”, Warszawa: Państwowy Instytut Badawczy NASK.

Gańko K., (2024), „Offline czyli zdrowiej. O cyfrowej higienie dla rodziców i wychowawców”, Warszawa: Państwowy Instytut Badawczy NASK.

Griffiths M., (1996), „Behavioural addiction: An issue for everybody?”, Journal of Workplace Learning, nr 8(3), s. 19–25, za: Makaruk K., Włodarczyk J., Skoneczna P., (2019), „Problematyczne używanie internetu przez młodzież. Raport z badań”, Warszawa: Fundacja Dajemy Dzieciom Siłę.

Izdebski, P., Kotyśko, M., (2016), „Problemowe korzystanie z nowych mediów”, w: B. Habrat (red.), „Zaburzenia uprawiania hazardu i inne tak zwane nałogi behawioralne” (s. 219–250), Warszawa: Instytut Psychiatrii i Neurologii, za: Makaruk K., Włodarczyk J., Skoneczna P., (2019), „Problematyczne używanie internetu przez młodzież. Raport z badań”, Warszawa: Fundacja Dajemy Dzieciom Siłę.

„Jak rozpoznać fake newsa?”, (b.r.), Warszawa: Państwowy Instytut Badawczy NASK.

Jupowicz-Ginalska i in., (2022), „FOMO 2022. Polacy a lęk przed odłączeniem”, Warszawa: Wydział Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego.

Kwaśnik A., (2025), „Internetowe love II – randkowanie, AI i cyberbezpieczeństwo”, Warszawa: Państwowy Instytut Badawczy NASK.

Kwaśnik A., (2023), „Sexting i nagie zdjęcia w sieci”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Kwaśnik A., (2023), „Sexting i nagie zdjęcia. Twoje dziecko i ryzykowne zachowania online”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Kwaśnik A., Melka-Roszczyk M., (2023/2024), „Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online”, Warszawa: Państwowy Instytut Badawczy NASK.

Lange R. (red.), (2023), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Ładna A. (red.), Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., (2025), „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców”, Warszawa: Państwowy Instytut Badawczy NASK.

Njoroge N., (2023), „Menedżer haseł”, Biuletyn Bezpieczeństwa Komputerowego „OUCH!” nr 8, tłum. Wnuk B., Węgrzynowicz A., SANS Security Awareness.

Piechna J., (2023), „Szkodliwe treści w internecie. Nie akceptuję, reaguję!”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Polak Z. (red.), Kwaśnik A., Sowiński P., (2021), „Cyfrowy ślad małego dziecka”, Warszawa: Państwowy Instytut Badawczy NASK.

Pyżalski J., Walter N., Iwanicka A., Bartkowiak K., (2023), „Wyniki badań ySKILLS. Druga fala (2022) Polska”, KU Leuven, Leuven: ySKILLS.

Reed T., (2021), „Bezpieczne przechowywanie danych w chmurze”, Biuletyn Bezpieczeństwa Komputerowego „OUCH!” nr 8, tłum. Wnuk B., Węgrzynowicz A., SANS Security Awareness.

Rywczyńska A., Piechna J., (2023), „Szkodliwe treści w internecie”, wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

„Sexting – skala zjawiska", (b.r), Warszawa: Państwowy Instytut Badawczy NASK.

Siemieniecka D., Skibińska M., Majewska K., (2020), „Cyberagresja – zjawisko, skutki, zapobieganie", Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

„Social Media 2023", (2023), Warszawa: Gemius, Polskie Badania Internetu, IAB Polska.

Witkowska M., (2023), „FOMO i nadużywanie nowych technologii. Poradnik dla rodziców", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Witkowska M., (2023), „FOMO i problemowe używanie internetu. Poradnik dla nauczycieli", wyd. II, Warszawa: Państwowy Instytut Badawczy NASK.

Witkowska M., (2024), „Bezpiecznie w wirtualnej rzeczywistości", Warszawa: Państwowy Instytut Badawczy NASK.

Witkowska M., (2024), „Media społecznościowe a dobrostan psychiczny", Warszawa: Państwowy Instytut Badawczy NASK.

Witkowska M., (2023), „Nastolatki i gry cyfrowe. Poradnik dla rodziców", Warszawa: Państwowy Instytut Badawczy NASK.

„Zagrożenia w internecie. Zapobieganie – reagowanie. Hazard online wśród młodzieży", (b.r.), Warszawa: Państwowy Instytut Badawczy NASK.

Zelster L., (2021), „Kradzież tożsamości – ochroń się przed nią", Biuletyn Bezpieczeństwa Komputerowego „OUCH!" nr 3, tłum. Wnuk B., Węgrzynowicz A., SANS Security Awareness.

Zelster L., (2018), „Ochrona przed złośliwym oprogramowaniem", Biuletyn Bezpieczeństwa Komputerowego „OUCH!" nr 6, tłum. Kondraszuk S., Strzelczyk M., Sikorski J., SANS Security Awareness.

Kursy e-learningowe na platformie OSE IT Szkoła

„Cyberprzemoc – anonimowość w sieci"; „Cyberprzemoc w grach internetowych"; „(Dez)informacja, czyli w co wierzyć w internecie"; „Krasnoludki 2.0 – Phishing, czyli kłopoty to nasza specjalność"; „Owce w sieci – Zabawa w śnieżki"; „Owce w sieci – Zamęt w głowach"; „Prawo autorskie – najważniejsze definicje"; „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu"; „Sharenting. Czy warto mieć rodzinny album w sieci?"; „Własność intelektualna"; „Techniki internetu"; „Zrozumieć FOMO"

Scenariusze zajęć

Borkowska A., Karelus K., (2022), „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole", Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2021), „Nie wywołuj hejtu z lasu. Czerwony Kapturek i cyberprzemoc. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6", Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2021), „Otwórz oczy – internet to nie wszystko. Śpiąca Królewna i FOMO. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6", Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2023), Scenariusze lekcji z serii #stopfomo", Warszawa: Państwowy Instytut Badawczy NASK.

Borkowska A., Witkowska M., (2021), „Złota Rybka i niebezpieczne kontakty online. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6", Warszawa: Państwowy Instytut Badawczy NASK.

Fenik-Gaberle K., (2021), „Czy wystarczy mi wyobraźnia? Ryzykowne zachowania w internecie:

szkodliwe treści. Scenariusz zajęć profilaktycznych dla uczniów w wieku 13–15 lat", Warszawa: NASK – Państwowy Instytut Badawczy.

Fenik-Gaberle K., (2021), „Decyzja. Ryzykowne zachowania w internecie: sexting. Scenariusz zajęć profilaktycznych dla uczniów w wieku 13–15 lat", Warszawa: NASK – Państwowy Instytut Badawczy.

Fenik-Gaberle K., (2021), „Jak się nie zaplątać w sieci? Scenariusz zajęć profilaktycznych dla uczniów w wieku 13–15 lat", Warszawa: Państwowy Instytut Badawczy NASK.

Inne materiały edukacyjne

Materiały z cykl „Bądź z innej bajki": animacja, podcast oraz broszura

Materiały opracowane w ramach kampanii edukacyjnej „FOMOwscy i JOMOwscy": kursy, scenariusze lekcji, komiksy

Materiały wideo

„Bezpieczni w sieci z OSE – Internet bez tajemnic", webinar z udziałem ekspertów OSE, wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

„Gry komputerowe – dobra zabawa, rozwojowa szansa czy niebezpieczna rozrywka?, webinar z udziałem ekspertów, wideo na kanale Nauka. To Lubię na YouTubie.

„Rodzinny album z wakacji, czyli czego o dzieciach nie powinien wiedzieć internet", webinar z udziałem ekspertów, wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Rowicka M., (2023), „Kongres OSE 2023. E-uzależnienia", wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

„Szkodliwe treści w internecie. Profilaktyka i reagowanie", webinar z udziałem ekspertów, wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Witkowska M., „Kongres OSE 2023: Glamouryzacja zaburzeń i zachowa ryzykownych w internecie", wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Witkowska M., (2024), „Niepokojące, nieodpowiednie, krzywdzące. Dzieci i szkodliwe treści w internecie", wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Zradzińska A., (2024), „AI, boty, awatary i szkodliwe treści", wideo na kanale Ogólnopolskiej Sieci Edukcyjnej na YouTubie.

Inne strony

Aplikacja mOchrona: ose.gov.pl/mochrona

Bezpłatny i anonimowy telefon zaufania dla dzieci: 116111.pl

Bezpłatny i anonimowy telefon zaufania dla rodziców i nauczycieli: 800100100.pl

Centrum wsparcia dla osób w stanie kryzysu psychicznego: centrumwsparcia.pl

CERT Polska: cert.pl

CERT Polska – Zgłoś incydent: incydent.cert.pl

Dyżurnet.pl: dyzurnet.pl

Europejski Miesiąc Cyberbezpieczeństwa: bezpiecznymiesiac.pl

Moje OSE: moje.ose.gov.pl

NASK – Państwowy Instytut Badawczy: nask.pl

No More Ransom: nomoreransom.org

#offlinechallenge: offlinechallenge.pl

Platforma e-learningowa Bezpieczni w sieci: bezpieczniwsieci.edu.pl

Polskie Centrum Programu Safer Internet (PCPSI): saferinternet.pl

Portal Uzależniania behawioralne: uzaleznieniabehawioralne.pl

Projekt OSEhero: osehero.pl

Sprawdź, czy Twoje dane są bezpieczne: bezpiecznedane.gov.pl

Telefon zaufania Rzecznika Praw Dziecka: brpd.gov.pl

Ujawnione luki w zabezpieczeniach cyberbezpieczeństwa: cve.org

Usługi moje.cert.pl: moje.cert.pl

Zgłoś dezinformację: zglos-dezinformacje.nask.pl