PRACE KONKURSOWE „E-POMOCNI! KONKURS DL@ OSEHERO”

ose hero

ose OGÓLNOPOLSKA SIEĆ EDUKACYJNA

Uczestnicy naszego projektu **OSEhero** to nauczyciele, którzy szczególnie **dbają o bezpieczeństwo swoich uczniów w sieci**. Ponadto chętnie zdobywają wiedzę podczas szkoleń z ekspertami Ogólnopolskiej Sieci Edukacyjnej (OSE) i dzielą się nią z innymi: nauczycielami, uczniami, rodzicami.

Dzięki konkursowi „e-Pomocni" – skierowanemu specjalnie do OSEhero – z ich pomysłów na zorganizowanie kreatywnej lekcji na temat cyberbezpieczeństwa może skorzystać każdy!

Zadaniem w konkursie **„e-Pomocni! Konkurs dl@ OSEhero"** było przygotowanie **kart pracy dotyczących cyberzagrożeń**. Nasi szkolni superbohaterowie nowych technologii poradzili sobie doskonale! Spośród nadesłanych zgłoszeń wyłoniliśmy cztery zwycięskie prace – w najlepszy sposób **przybliżające młodym użytkownikom internetu zagadnienia związane z bezpieczeństwem online**. Uczestnicy projektu OSEhero udowodnili, że naprawdę są e-Pomocni!

Nagrodą w konkursie były bony o wysokości 2000 zł na zakup materiałów edukacyjnych. Trafiły do szkół naszych laureatów.

W publikacji, którą oddajemy w Wasze ręce, znajdziecie nagrodzone karty pracy. Zachowaliśmy ich oryginalny charakter. Mamy nadzieję, że zaproponowane przez naszych OSEhero **kreatywne ćwiczenia pomogą Wam zorganizować zajęcia na temat bezpieczeństwa w sieci i staną się inspiracją** do podejmowania innych działań w tym zakresie. A może Wy też zechcecie zostać OSEhero? Do tej wyjątkowej społeczności zapraszamy nauczycieli, ale też bibliotekarzy, pedagogów i dyrektorów szkół. Jak dołączyć do naszego projektu? Szczegóły znajdziecie na stronie osehero.pl.

Jeszcze raz serdecznie gratulujemy laureatom, a wszystkim nauczycielom życzymy, by byli dla swoich uczniów najlepszymi przewodnikami po wirtualnym świecie!

KARTA PRACY | „Cyfrowe bezpieczeństwo”

AUTOR | Tomasz Deresz
nauczyciel informatyki,
Technikum nr 3 w Suwałkach

Zagadnienia, których dotyczy karta pracy

- Bezpieczne korzystanie z usług internetowych, np. poczty, bankowości elektronicznej, komunikatorów i innych serwisów
- Zasady tworzenia bezpiecznych nazw użytkowników, silnych haseł i korzystania z uwierzytelniania dwuskładnikowego

Grupa wiekowa

Klasa 1 szkoły ponadpodstawowej

Czas trwania

45 minut (1 godzina lekcyjna)

Pomoce dydaktyczne

Karta pracy dla każdego ucznia, stacja robocza z dostępem do internetu, smartfon ucznia

Autor: Tomasz Deresz, nauczyciel z Technikum nr 3 w Suwałkach

Karta pracy „Cyfrowe bezpieczeństwo"

Opis: Aby właściwie zadbać o cyfrowe bezpieczeństwo, warto przyjrzeć się nawykom użytkownika końcowego, który narażony jest na wiele cyberzagrożeń. Najczęstszym błędem jest lekceważenie przez niego kwestii logowania do serwisów internetowych.

Podstawowym aspektem zapewniającym bezpieczeństwo jest korzystanie z unikalnych nazw użytkowników i silnych, łatwych do zapamiętania, ale trudnych do odgadnięcia haseł. Kolejnym elementem wpływającym na cyberbezpieczeństwo jest wprowadzenie uwierzytelniania wieloskładnikowego, co w połączeniu z silnym hasłem w znacznie większym stopniu chroni dane użytkownika.

Czas trwania: 45 minut (1 godzina lekcja)

Typ: zajęcia praktyczne

Pomoce dydaktyczne: stacja robocza ucznia z dostępem do internetu, smartfon ucznia

Sprawozdanie: wykonany dokument należy wysłać na skrzynkę e-mail prowadzącego zajęcia

Zadanie 1: Ustawienie bezpiecznej nazwy użytkownika

Czas trwania: 10 minut

Opis: Pierwszym krokiem w kierunku zadbania o własne bezpieczeństwo w sieci jest wybór unikalnej nazwy użytkownika, czyli loginu (username). Często zapominamy o tym, aby nie posługiwać się standardowymi nazwami użytkowników, np. admin, tomek itp., czyli takimi, które mogą być oczywiste dla osoby próbującej przejąć dostęp do naszego konta.

Zadaniem uczniów jest wygenerowanie przykładowego loginu za pomocą portalu https://www.lastpass.com/features/username-generator (lub innej podobnej witryny).
Kryteria: minimum 8 znaków, zawierających małe i wielkie litery.
W karcie pracy dla ucznia przygotowane zostało miejsce na wklejenie zrzutu ekranu dokumentującego wykonanie zadania.

Zadanie 2: Ustawienie bezpiecznego hasła

Czas trwania: 15 minut

Opis: Najważniejszym elementem zapewniającym bezpieczeństwo w serwisach internetowych jest silne hasło. Poza kierowaniem się zdrowym rozsądkiem przy ustawianiu trudnego do złamania hasła trzeba też wiedzieć, że takie rzeczy reguluje również prawo, jeżeli chodzi o systemy teleinformatyczne przetwarzające np. dane osobowe.

Zadaniem uczniów jest stworzenie własnego, silnego hasła uwzględniającego nowe rekomendacje podane poniżej. W karcie pracy dla ucznia przygotowane zostało miejsce na jego zapisanie.

PAMIĘTAJ:

- hasło powinno składać się z więcej niż 12 znaków i przynajmniej 5 słów;
- może, ale nie musi zawierać znaków specjalnych, cyfr czy dużych liter;
- podczas tworzenia hasła warto używać pełnych zdań, które łatwo zapamiętać, np. nieco zmodyfikowanych cytatów lub powiedzeń;
- w haśle warto połączyć słowa pochodzące z dwóch języków – wtedy trudniej je złamać;
- silnego hasła nie trzeba cyklicznie zmieniać.

Przykładowe metody tworzenia silnych haseł można znaleźć w rekomendacjach CERT Polska. Warto polecić uczniom:

- broszurę „Jak budować silne hasła" (https://cert.pl/uploads/2022/01/hasla/resources/plakaty_informacyjne_hasla_a4.pdf);
- zbiór materiałów dotyczący haseł (https://cert.pl/hasla/).

Miejsce na zapisanie przykładowego hasła

Zadanie 3: Konfigurowanie uwierzytelniania dwuskładnikowego (2FA)

Czas trwania: 20 minut

Opis: Unikalna nazwa użytkownika i silne hasło zawsze powinny iść w parze. W dzisiejszych czasach warto do tego dołączyć również uwierzytelnianie dwuskładnikowe (w skrócie 2FA – z ang. *Two-Factor Authentication*). Ten sposób ochrony zapewnia „podwójne sprawdzanie", czy na pewno jesteś osobą, za którą się podajesz, gdy korzystasz z usług online. Zmniejsza to ryzyko nieuprawnionego dostępu do naszych danych. Uwierzytelnianie dwuskładnikowe jest dostępne w większości powszechnych usług online, takich jak bankowość, poczta e-mail lub media społecznościowe.

Podczas konfigurowania usługi 2FA zostaniesz poproszony o podanie „drugiego składnika", do którego masz dostęp tylko Ty. Najczęściej jest to kod przesłany SMS-em lub poprzez aplikację. Szczegóły można znaleźć na stronie: https://www.gov.pl/web/baza-wiedzy/konfigurowanie-uwierzytelniania-dwuskladnikowego-2fa.

Zadaniem uczniów jest zainstalowanie na swoim telefonie aplikacji do 2FA, np. Google Authenticator lub innej, bądź użycie tej, którą już posiadają. Niektóre serwisy mają też własne, dedykowane aplikacje, np. Poczta Wirtualnej Polski posiada aplikację o nazwie 1login.

Dla testowego konta pocztowego wykorzystywanego do zajęć w pracowni uczeń ma ustawić uwierzytelnianie dwuskładnikowe, postępując zgodnie z instrukcją portalu pocztowego.

W razie trudności podczas ustawiania uwierzytelniania dwuskładnikowego uczeń może skorzystać z opcji pomocy dostępnej na większości portali. Najczęściej znajdziemy ją na dole strony, w stopce.

Wykonanie zadania uczeń powinien zgłosić prowadzącemu zajęcia i zademonstrować logowanie z wykorzystaniem uwierzytelniania dwuskładnikowego.

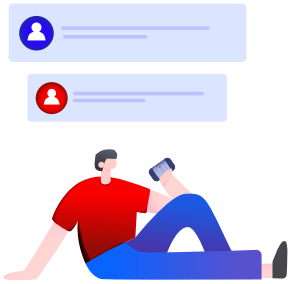
Przykładowo:

Logowanie dwustopniowe

Potwierdzaj logowanie w darmowej aplikacji 1login od WP lub przy pomocy klucza bezpieczeństwa USB, NFC czy Bluetooth. Dzięki temu nikt poza Tobą nie zaloguje się na Twoje konto 1login od WP bez Twojej zgody.

Masz włączone logowanie dwustopniowe

Od 16 czerwca 2021



W karcie pracy dla ucznia przygotowane zostało miejsce na wklejenie zrzutu ekranu.

Po wykonanych zadaniach uczniowie zapisują dokument i przesyłają go e-mailem do nauczyciela prowadzącego zajęcia.

Karta pracy „Cyfrowe bezpieczeństwo"

Imię i nazwisko: ..... Klasa: ..... Data wykonania: .....

Aby właściwie zadbać o cyfrowe bezpieczeństwo, przyjrzyj się swoim nawykom w sieci. Użytkownik końcowy narażony jest na wiele cyberzagrożeń. Najczęstszym błędem jest lekceważenie kwestii logowania do serwisów internetowych.

Podstawowym aspektem zapewniającym bezpieczeństwo jest korzystanie z unikalnych nazw użytkowników i silnych, łatwych do zapamiętania, ale trudnych do odgadnięcia haseł. Kolejnym elementem wpływającym na cyberbezpieczeństwo jest wprowadzenie uwierzytelniania wieloskładnikowego, co w połączeniu z silnym hasłem w znacznie większym stopniu chroni dane użytkownika.

Zadanie 1: Ustawienie bezpiecznej nazwy użytkownika

Pierwszym krokiem w kierunku zadbania o własne bezpieczeństwo w sieci jest wybór unikalnej nazwy użytkownika, czyli loginu (username). Często zapominamy o tym, aby nie posługiwać się standardowymi nazwami użytkowników, np. admin, tomek itp., czyli takimi, które mogą być oczywiste dla osoby próbującej przejąć dostęp do naszego konta.

Instrukcja: Wygeneruj przykładowy login za pomocą portalu https://www.lastpass.com/features/username-generator (lub innej podobnej witryny) i wklej zrzut ekranu poniżej. Kryteria: minimum 8 znaków, zawierających małe i wielkie litery.

Miejsce na wklejenie zrzutu ekranu

Zadanie 2: Ustawienie bezpiecznego hasła

Najważniejszym elementem zapewniającym bezpieczeństwo w serwisach internetowych jest silne hasło. Poza kierowaniem się zdrowym rozsądkiem przy ustawianiu trudnego do złamania hasła trzeba też wiedzieć, że takie rzeczy reguluje również prawo, jeżeli chodzi o systemy teleinformatyczne przetwarzające np. dane osobowe.

Instrukcja: Stwórz silne hasło, uwzględniając nowe rekomendacje podane poniżej. Swoje hasło zapisz w wyznaczonym miejscu.

PAMIĘTAJ:

- hasło powinno składać się z więcej niż 12 znaków i przynajmniej 5 słów;
- może, ale nie musi zawierać znaków specjalnych, cyfr czy dużych liter;
- podczas tworzenia hasła warto używać pełnych zdań, które łatwo zapamiętać, np. nieco zmodyfikowanych cytatów lub powiedzeń;
- w haśle warto połączyć słowa pochodzące z dwóch języków – wtedy trudniej je złamać;
- silnego hasła nie trzeba cyklicznie zmieniać.

Przykładowe metody tworzenia silnych haseł można znaleźć w rekomendacjach CERT Polska:

- broszurze „Jak budować silne hasła" (https://cert.pl/uploads/2022/01/hasla/resources/plakaty_informacyjne_hasla_a4.pdf);
- zbiorze materiałów dotyczący haseł (https://cert.pl/hasla/).

Miejsce na zapisanie przykładowego hasła

Zadanie 3: Konfigurowanie uwierzytelniania dwuskładnikowego (2FA)

Unikalna nazwa użytkownika i silne hasło zawsze powinny iść w parze. W dzisiejszych czasach warto do tego dołączyć również uwierzytelnianie dwuskładnikowe (w skrócie 2FA – z ang. *Two-Factor Authentication*). Ten sposób ochrony zapewnia „podwójne sprawdzanie", czy na pewno jesteś osobą, za którą się podajesz, gdy korzystasz z usług online. Zmniejsza to ryzyko nieuprawnionego dostępu do naszych danych. Uwierzytelnianie dwuskładnikowe jest dostępne w większości powszechnych usług online, takich jak bankowość, poczta e-mail lub media społecznościowe.

Podczas konfigurowania usługi 2FA zostaniesz poproszony o podanie „drugiego składnika", do którego masz dostęp tylko Ty. Najczęściej jest to kod przesłany SMS-em lub poprzez aplikację. Szczegóły znajdziesz na stronie: https://www.gov.pl/web/baza-wiedzy/konfigurowanie-uwierzytelniania-dwuskladnikowego-2fa.

Instrukcja: Zainstaluj na swoim telefonie aplikację do 2FA, np. Google Authenticator lub inną, bądź użyj tej, którą już posiadasz. Niektóre serwisy mają też własne, dedykowane aplikacje, np. Poczta Wirtualnej Polski posiada aplikację o nazwie 1login.

Dla testowego konta pocztowego wykorzystywanego do zajęć w pracowni ustaw uwierzytelnianie dwuskładnikowe. Postępuj zgodnie z instrukcją portalu pocztowego, na którym masz konto.

PAMIĘTAJ:
W razie trudności w ustawieniu uwierzytelniania dwuskładnikowego skorzystaj z opcji pomocy dostępnej na większości portali. Najczęściej można znaleźć ją na dole strony, w stopce.

Wykonanie zadania zgłoś prowadzącemu zajęcia i zademonstruj logowanie z wykorzystaniem uwierzytelniania dwuskładnikowego.

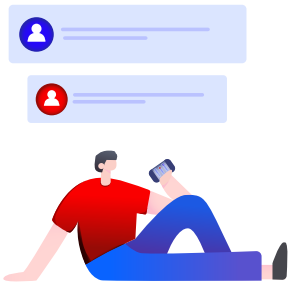
Przykładowo:

Logowanie dwustopniowe

Potwierdzaj logowanie w darmowej aplikacji 1login od WP lub przy pomocy klucza bezpieczeństwa USB, NFC czy Bluetooth. Dzięki temu nikt poza Tobą nie zaloguje się na Twoje konto 1login od WP bez Twojej zgody.

Masz włączone logowanie dwustopniowe

Od 16 czerwca 2021



Miejsce na wklejenie zrzutu ekranu

Po wykonanych zadaniach uczniowie zapisują dokument i przesyłają go e-mailem do nauczyciela prowadzącego zajęcia.

KARTA PRACY

„Pierwsze kroki w mediach społecznościowych"

AUTORKA

Anna Sośniak

nauczycielka informatyki i chemii,
Szkoła Podstawowa im. Władysława Reymonta
w Rębielicach Królewskich

Zagadnienia, których dotyczy karta pracy

- Bezpieczeństwo w mediach społecznościowych
- Dbanie o prywatność w sieci
- Unikanie zagrożeń związanych z udostępnianiem informacji o sobie
- Tworzenie bezpiecznych haseł

Grupa wiekowa

Klasy 4–6 szkoły podstawowej

Czas trwania

45 minut (1 godzina lekcyjna)

Pomoce dydaktyczne

Karta pracy dla każdego ucznia, długopisy

Autor: Anna Sośniak, nauczycielka ze Szkoły Podstawowej im. Władysława Reymonta w Rębielicach Królewskich

Karta pracy „Pierwsze kroki w mediach społecznościowych"

Wskazówki do prowadzenia zajęć:

Przed przeprowadzeniem zajęć warto zorientować się, czy uczniowie wiedzą, czym są media społecznościowe, jakie znają portale społecznościowe i czy z nich korzystają.

Pierwsza część karty pracy pokazuje krok po kroku, jak stworzyć bezpieczne hasło. Druga część uczy rozpoznawać, które dane możemy udostępniać w sieci jako publiczne, a które lepiej pokazywać tylko w kręgu znajomych. Ostatnia część wskazuje, jak wyrażać konstruktywną krytykę.

Sugerowane odpowiedzi do zadań zostały zapisane kolorem czerwonym.

Czy jesteś odpowiednio chroniony?

Sprawdź swoje bezpieczeństwo i uporządkuj podane hasła od najsłabszego do najsilniejszego. W rozwiązaniu zadania pomogą Ci zasady tworzenia silnych haseł, które znajdziesz na rysunku smartfona.

NUMER	HASŁO
5	WlazlKostekNaBridgelStuka
2	AlaMaKota
4	WlazlKostekNaMostekIStuka
3	WlazlKotekNaPlotekIMruga
1	kot

Już wiesz, jak chronić swoje dane!

Wymyśl bezpieczne hasło, które będzie łatwe dla Ciebie, a trudne dla innych.

NaGorzeRosesNaPrawoBez

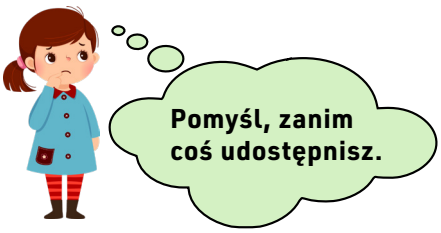
Czy udostępniasz z głową?

Zaznacz krzyżykiem, komu udostępnisz daną informację o sobie.

Już wiesz, jak udostępniać z głową!

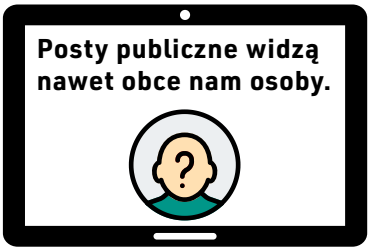
W smartfonie masz zapisane śmieszne zdjęcie z przyjaciółmi i chcesz im je pokazać. Zastanów się, czy możesz umieścić fotografię na portalu społecznościowym, czy lepiej wysłać ją do przyjaciół na zamkniętej grupie, do której nikt oprócz Was nie ma dostępu. Narysuj strzałkę wskazującą właściwy sposób postępowania.

INFORMACJE O TOBIE	ZNAJOMI	PUBLICZNE
Zdjęcie profilowe		X
Numer telefonu	X	
Zdjęcie z wakacji	X	
Informacja o zaginięciu Twojego psa z prośbą o pomoc w jego odnalezieniu		X



Udostępniam zdjęcie na portalu społecznościowym. Ładnie na nim wyglądam, a Kuba i Zuzia mają głupie miny. Na pewno wszystkim się ono spodoba.

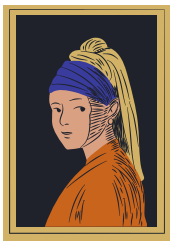
Wysyłam zdjęcie ze znajomymi na naszą grupę. Nie wszyscy muszą wiedzieć, w jaki sposób spędzamy razem czas.



Czy jesteś życzliwy w sieci?

Pokoloruj ekrany, na których komentarz wyraża konstruktywną krytykę i nie obraża autora posta.

Widać, że ciężko pracowałaś nad tym obrazem. Można dostrzec drobne niedociągnięcia, ale są sposoby, żeby następnym razem ich nie było. W miejskim domu kultury ruszają darmowe warsztaty plastyczne dla młodzieży. Tam na pewno Ci pomogą.



Co to za bazgroły? Dzieci w przedszkolu ładniej rysują! Aż oczy bolą od patrzenia!

Nie da się tego słuchać! Zajmij się czymś innym, bo do śpiewania się nie nadajesz.

Muzyka musi być Twoją pasją. Myślałeś o tym, aby zamiast śpiewem zająć się grą na instrumencie? Filharmonia w naszym mieście prowadzi lekcje gry dla początkujących.

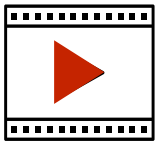
Chwalisz się przypalonym kotletem? Co za głupota. Od razu widać, że to coś jest niejadalne. Nie przypuszczałam, że można zepsuć tak proste danie. Od dziś jesteś „mistrzem przypalonego kotleta". Hahahaha

Nie przejmuj się. Każdemu zdarzyło się zepsuć jakieś danie. Następnym razem pamiętaj, żeby ustawić czas pieczenia na minutniku piekarnika. Wiele razy uratowałem w ten sposób swoje wypieki, bo z natury jestem zapominalski.

Już wiesz, jak być życzliwym w sieci!

Napisz życzliwy komentarz, który pomoże autorowi filmu.

Konstruktywna krytyka jest rodzajem nieagresywnego zwrócenia komuś uwagi, powinna odnosić się tylko do rzeczy, które dana osoba może zmienić. Intencją osoby przekazującej uwagi jest chęć pomocy drugiej stronie w osiągnięciu celu lub w rozwoju.



Jak zrobić kwiatek z bibuły? Instrukcja krok po kroku

Co sądzicie o moim pierwszym filmiku? Czekam na Wasze komentarze.

Twój komentarz:

Dzięki Tobie zrobiłam mój pierwszy w życiu kwiatek z bibuły. Bardzo mi pomogłeś. Następnym razem postaraj się mówić nieco wolniej.

Początkujące osoby, takie jak ja, potrzebują więcej czasu na wykonanie kolejnych kroków.

Karta pracy „Pierwsze kroki w mediach społecznościowych”

Czy jesteś odpowiednio chroniony?

Sprawdź swoje bezpieczeństwo i uporządkuj podane hasła od najsłabszego do najsilniejszego. W rozwiązaniu zadania pomogą Ci zasady tworzenia silnych haseł, które znajdziesz na rysunku smartfona.

NUMER	HASŁO
5	WlazlKostekNaBridgeIStuka
2	AlaMaKota
4	WlazlKostekNaMostekIStuka
3	WlazlKotekNaPlotekIMruga
1	kot

Już wiesz, jak chronić swoje dane!

Wymyśl bezpieczne hasło, które będzie łatwe dla Ciebie, a trudne dla innych.

Twoje hasło:

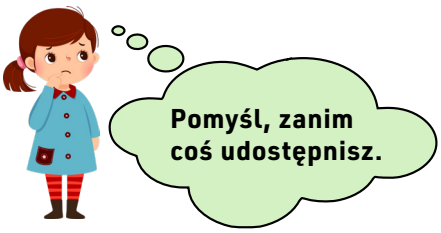
Czy udostępniasz z głową?

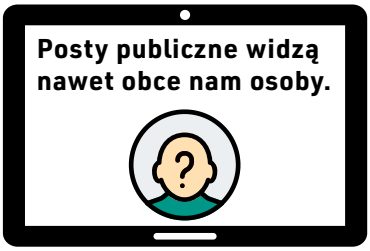
Zaznacz krzyżykiem, komu udostępnisz daną informację o sobie.

Już wiesz, jak udostępniać z głową!

W smartfonie masz zapisane śmieszne zdjęcie z przyjaciółmi i chcesz im je pokazać. Zastanów się, czy możesz umieścić fotografię na portalu społecznościowym, czy lepiej wysłać ją do przyjaciół na zamkniętej grupie, do której nikt oprócz Was nie ma dostępu. Narysuj strzałkę wskazującą właściwy sposób postępowania.

INFORMACJE O TOBIE	ZNAJOMI	PUBLICZNE
Zdjęcie profilowe		
Numer telefonu		
Zdjęcie z wakacji		
Informacja o zaginięciu Twojego psa z prośbą o pomoc w jego odnalezieniu		





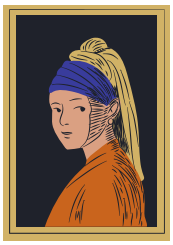
Udostępniam zdjęcie na portalu społecznościowym. Ładnie na nim wyglądam, a Kuba i Zuzia mają głupie miny. Na pewno wszystkim się ono spodoba.

Wysyłam zdjęcie ze znajomymi na naszą grupę. Nie wszyscy muszą wiedzieć, w jaki sposób spędzamy razem czas.

Czy jesteś życzliwy w sieci?

Pokoloruj ekrany, na których komentarz wyraża konstruktywną krytykę i nie obraża autora posta.

Widać, że ciężko pracowałaś nad tym obrazem. Można dostrzec drobne niedociągnięcia, ale są sposoby, żeby następnym razem ich nie było. W miejskim domu kultury ruszają darmowe warsztaty plastyczne dla młodzieży. Tam na pewno Ci pomogą.



Co to za bazgroły? Dzieci w przedszkolu ładniej rysują! Aż oczy bolą od patrzenia!

Nie da się tego słuchać! Zajmij się czymś innym, bo do śpiewania się nie nadajesz.

Muzyka musi być Twoją pasją. Myślałeś o tym, aby zamiast śpiewem zająć się grą na instrumencie? Filharmonia w naszym mieście prowadzi lekcje gry dla początkujących.

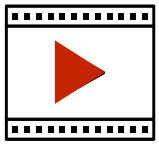
Chwalisz się przypalonym kotletem? Co za głupota. Od razu widać, że to coś jest niejadalne. Nie przypuszczałam, że można zepsuć tak proste danie. Od dziś jesteś „mistrzem przypalonego kotleta". Hahahaha

Nie przejmuj się. Każdemu zdarzyło się zepsuć jakieś danie. Następnym razem pamiętaj, żeby ustawić czas pieczenia na minutniku piekarnika. Wiele razy uratowałem w ten sposób swoje wypieki, bo z natury jestem zapominalski.

Już wiesz, jak być życzliwym w sieci!

Napisz życzliwy komentarz, który pomoże autorowi filmu.

Konstruktywna krytyka jest rodzajem nieagresywnego zwrócenia komuś uwagi, powinna odnosić się tylko do rzeczy, które dana osoba może zmienić. Intencją osoby przekazującej uwagi jest chęć pomocy drugiej stronie w osiągnięciu celu lub w rozwoju.



Jak zrobić kwiatek z bibuły? Instrukcja krok po kroku

Co sądzicie o moim pierwszym filmiku? Czekam na Wasze komentarze.

Twój komentarz:

KARTA PRACY | „e-Pomocni: bezpieczny internet"

AUTORKA | Edyta Sadowska
nauczycielka edukacji wczesnoszkolnej,
Publiczna Szkoła Podstawowa nr 15
im. Władysława Syrokomli w Radomiu

Zagadnienia, których dotyczy karta pracy

- Podstawowe zasady bezpiecznego korzystania z internetu
- Zagrożenia związane z udostępnianiem swoich danych
- Podstawowe pojęcia dotyczące cyberbezpieczeństwa (wirus, program antywirusowy, dane osobowe, nieznane linki, znajomy z internetu)

Grupa wiekowa

Klasy 1–3 szkoły podstawowej

Czas trwania

45 minut (1 godzina lekcyjna) lub kilka krótkich spotkań tematycznych

Pomoce dydaktyczne

Karta pracy dla każdego ucznia, długopisy

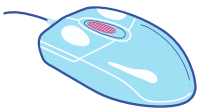
Autor: Edyta Sadowska nauczycielka z Publicznej Szkoły Podstawowej nr 15 im. Władysława Syrokomli w Radomiu

Karta pracy „e-Pomocni: bezpieczny internet"

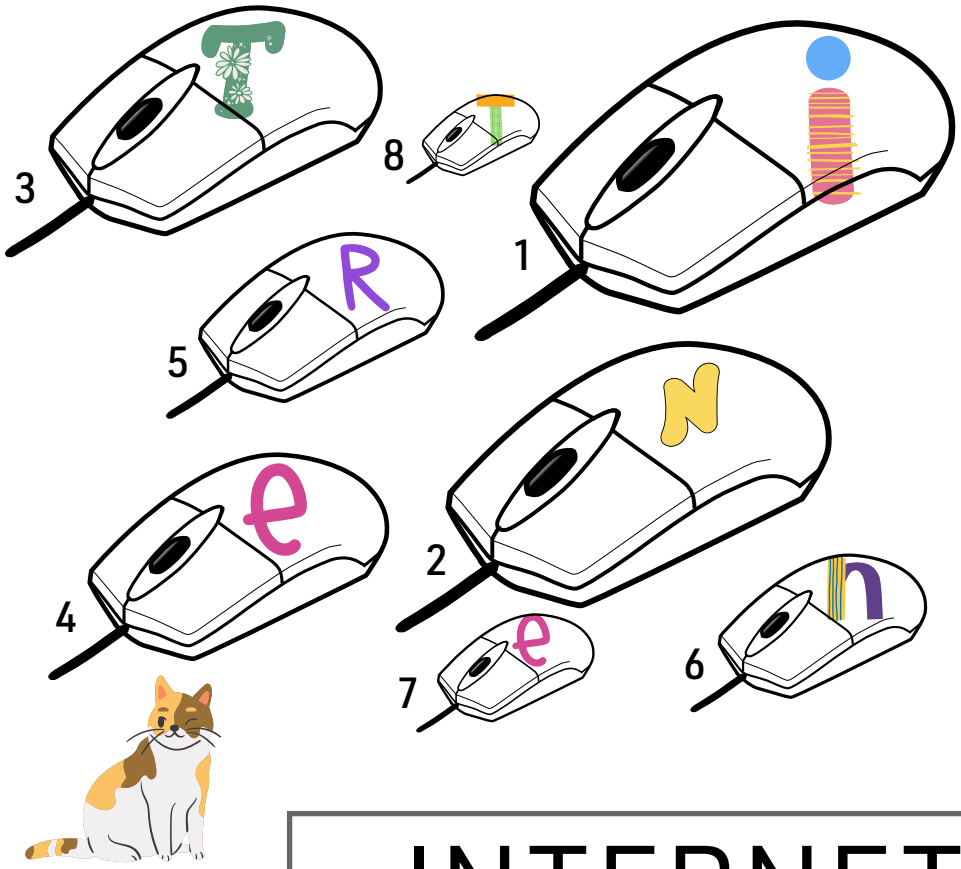
Imię _____ Nazwisko _____

Klasa _____

Uciekaj, myszko...



Wyobraź sobie, że jesteś kotem. Złap – połącz ze sobą wszystkie ponumerowane myszy. Zacznij od 1, a skończ na 8. Odczytaj hasło i zapisz je w ramce na dole strony. Następnie pokoloruj myszki.



Hasło: INTERNET

Spróbuj odpowiedzieć na pytanie: **CO TO JEST INTERNET?**

BURZA MÓZGÓW

Do czego potrzebny jest internet?

Zastanów się, dlaczego Twoim zdaniem warto korzystać z internetu. Swoje odpowiedzi zapisz lub narysuj w poniższych polach.

Np. źródło wiedzy

Np. zabawa

Np. kontakt ze znajomymi

Np. rozwijanie zainteresowań (tworzenie, słuchanie muzyki)

GRZECZNOŚĆ NA CO DZIEŃ...

Zawsze powinniśmy dobrze postępować – zarówno w internecie, jak i w domu lub szkole. Pokoloruj na zielono chmurki z przykładami pozytywnego zachowania, a na czerwono – niedozwolonego.

mówienie PROSZĘ

przezywanie koleżanki lub kolegi

mówienie DZIĘKUJĘ

krzyczenie na koleżankę lub kolegę

mówienie PRZEPRASZAM

obrażanie na forum

BEZPIECZEŃSTWO W SIECI

W internecie konieczne jest przestrzeganie ustalonych zasad.
Wykonaj zadanie, a poznasz kilka z nich.
Połącz ze sobą kostki zawierające tyle samo oczek.
Odczytaj powstałe zdania (zasady) i zapisz je w liniach.
Pamiętaj o kropce na końcu zdania.

Nie	w nieznane	od znajomych.
Nie podawaj	z programów	do odgadnięcia.
Stosuj hasła	wiadomości tylko	danych osobowych.
Nie klikaj	swoich	z nieznajomymi.
Korzystaj	rozmawiaj	linki.
Otwieraj	trudne	antywirusowych.

Komentarz dla nauczyciela: *Po zakończeniu pracy przez uczniów porozmawiaj z nimi o zasadach, które odgadli. Wyjaśnij nowe lub trudne pojęcia, np.: program antywirusowy czy dane osobowe (podaj przykłady takich danych). Porozmawiajcie o tym, jakie hasła są trudne do odgadnięcia, co to są nieznane linki oraz kim jest znajomy i nieznajomy z internetu.*

Nie rozmawiaj z nieznajomymi.

Nie podawaj swoich danych osobowych.

Stosuj hasła trudne do odgadnięcia.

Nie klikaj w nieznane linki.

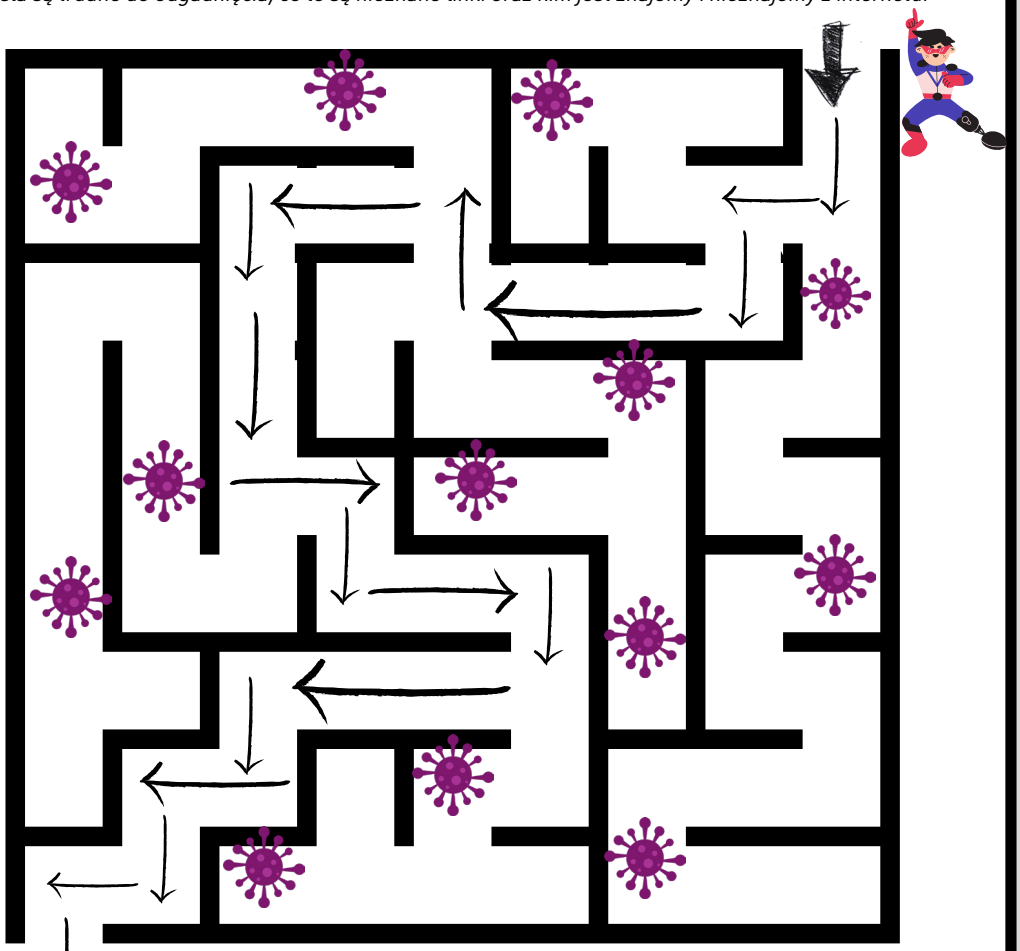
Korzystaj z programów antywirusowych.

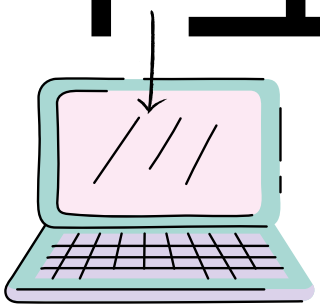
Otwieraj wiadomości tylko od znajomych.

UNIKAM WIRUSÓW

Czasami do naszych komputerów dostają się „nieproszeni goście" – WIRUSY, które potrafią nieźle napsocić w naszych plikach i folderach! Dlatego staramy się z nimi walczyć, używając np. programów antywirusowych. Pomóż superbohaterowi odnaleźć drogę do komputera. Pamiętaj, aby wybrać trasę, na której nie ma wirusów.

Komentarz dla nauczyciela: *Po zakończeniu przez uczniów pracy, wyjaśnij im nowe lub trudne pojęcia, np: program antywirusowy czy dane osobowe (podaj przykłady takich danych). Porozmawiajcie o tym, jakie hasła są trudne do odgadnięcia, co to są nieznane linki oraz kim jest znajomy i nieznajomy z internetu.*





Jak Ci się pracowało?

Narysuj na ekranie komputera:

uśmiechniętą buzię – jeśli zadania były ciekawe

lub

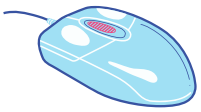
smutną buzię – jeśli uważasz, że zadania były mało interesujące.

Karta pracy „e-Pomocni: bezpieczny internet"

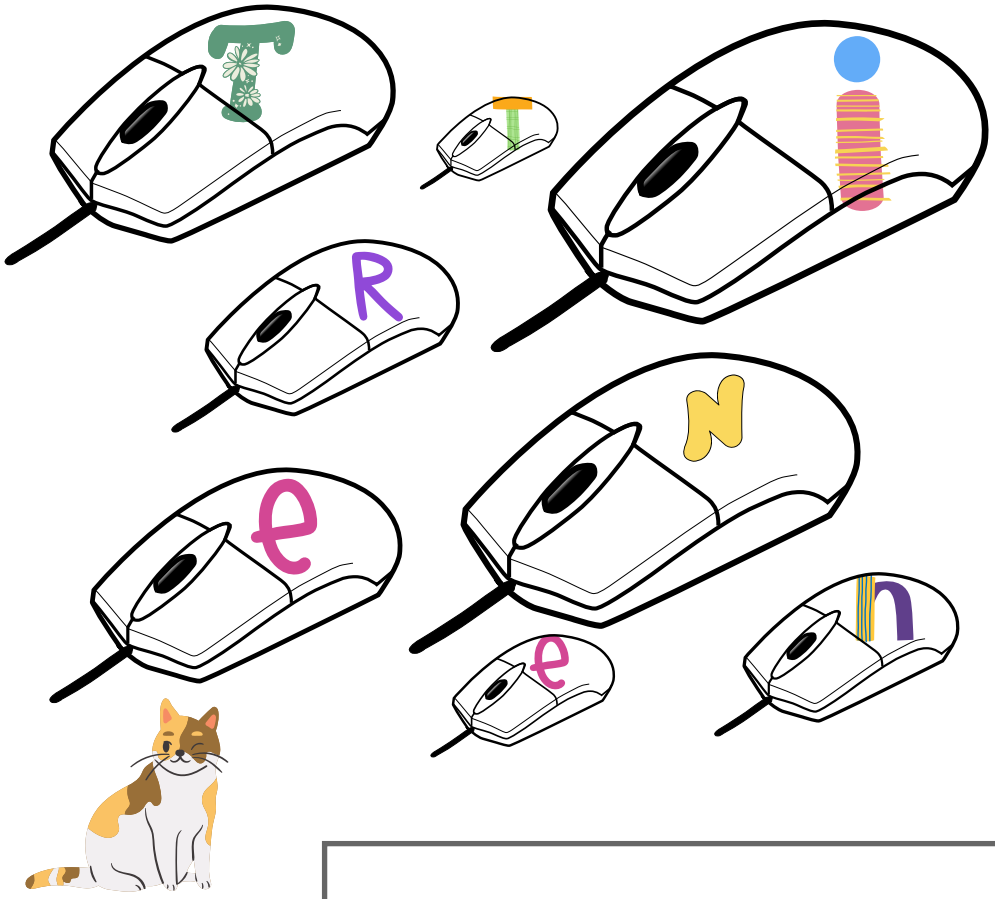
Imię _____ Nazwisko _____

Klasa _____

Uciekaj, myszko...



Wyobraź sobie, że jesteś kotem. Złap – połącz ze sobą wszystkie ponumerowane myszy. Zacznij od 1, a skończ na 8. Odczytaj hasło i zapisz je w ramce na dole strony. Następnie pokoloruj myszki.



Hasło:

Spróbuj odpowiedzieć na pytanie: **CO TO JEST INTERNET?**

BURZA MÓZGÓW

Do czego potrzebny jest internet?

Zastanów się, dlaczego Twoim zdaniem warto korzystać z internetu.
Swoje odpowiedzi zapisz lub narysuj w poniższych polach.

GRZECZNOŚĆ NA CO DZIEŃ...

Zawsze powinniśmy dobrze postępować – zarówno w internecie, jak i w domu lub szkole. Pokoloruj na zielono chmurki z przykładami pozytywnego zachowania, a na czerwono – niedozwolonego.

mówienie PROSZĘ

przezywanie koleżanki lub kolegi

mówienie DZIĘKUJĘ

krzyczenie na koleżankę lub kolegę

mówienie PRZEPRASZAM

obrażanie na forum

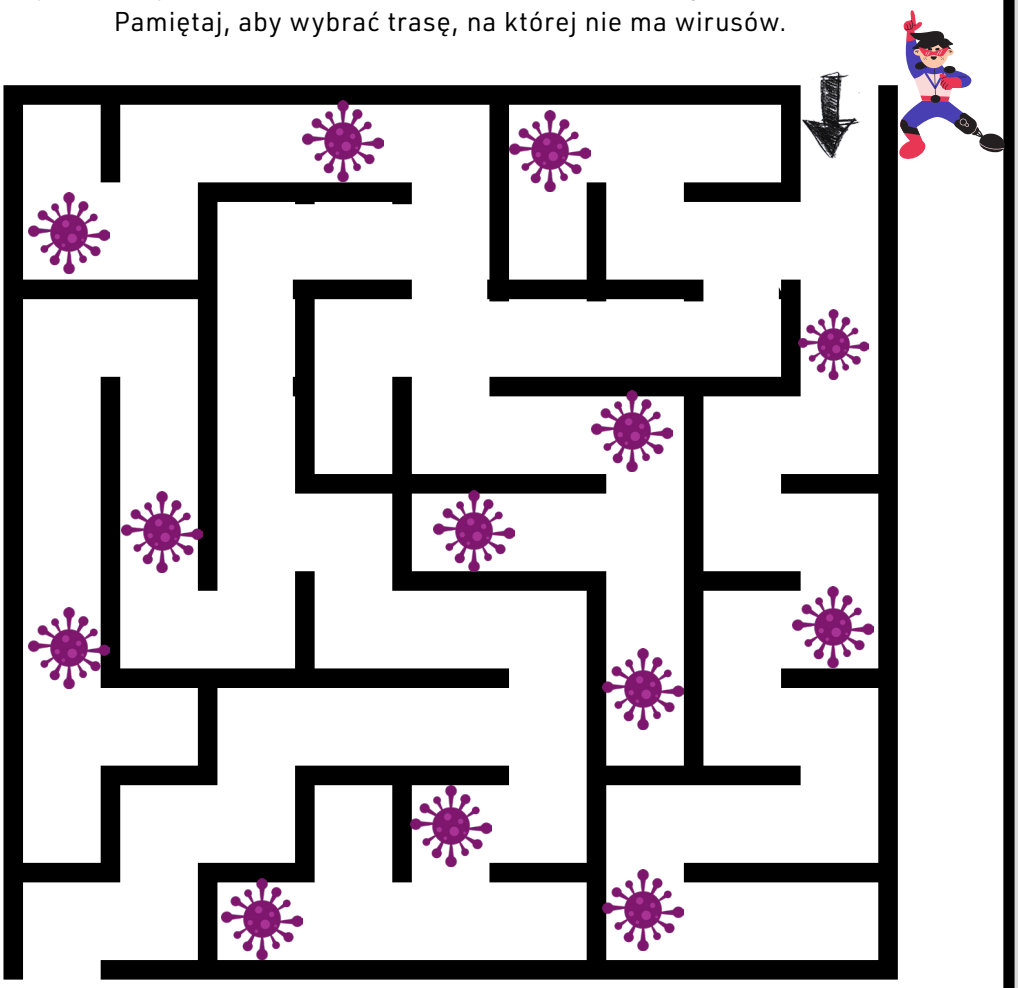
BEZPIECZEŃSTWO W SIECI

W internecie konieczne jest przestrzeganie ustalonych zasad.
Wykonaj zadanie, a poznasz kilka z nich.
Połącz ze sobą kostki zawierające tyle samo oczek.
Odczytaj powstałe zdania (zasady) i zapisz je w liniach.
Pamiętaj o kropce na końcu zdania.

Nie	w nieznane	od znajomych.
Nie podawaj	z programów	do odgadnięcia.
Stosuj hasła	wiadomości tylko	danych osobowych.
Nie klikaj	swoich	z nieznajomymi.
Korzystaj	rozmawiaj	linki.
Otwieraj	trudne	antywirusowych.

UNIKAM WIRUSÓW

Czasami do naszych komputerów dostają się „nieproszeni goście" – WIRUSY, które potrafią nieźle napsocić w naszych plikach i folderach! Dlatego staramy się z nimi walczyć, używając np. programów antywirusowych. Pomóż superbohaterowi odnaleźć drogę do komputera. Pamiętaj, aby wybrać trasę, na której nie ma wirusów.



Jak Ci się pracowało?

Narysuj na ekranie komputera:

uśmiechniętą buzię – jeśli zadania były ciekawe

lub

smutną buzię – jeśli uważasz, że zadania były mało interesujące.

KARTA PRACY

„Nasze dane osobowe w wirtualnym świecie"

AUTORKA

Dorota Ługowska

nauczycielka informatyki,
Publiczna Szkoła Podstawowa nr 15
im. Władysława Syrokomli w Radomiu

Zagadnienia, których dotyczy karta pracy

- Ochrona danych osobowych
- Zagrożenia związane z udostępnianiem w sieci informacji o sobie (wyłudzanie danych osobowych, phishing)

Grupa wiekowa

Klasy 5–6 szkoły podstawowej

Czas trwania

45 minut (1 godzina lekcyjna)

Pomoce dydaktyczne

Karta pracy dla każdego ucznia oraz smartfony wyposażone w czytnik kodów QR, długopisy

Autor: Dorota Ługowska, nauczycielka z Publicznej Szkoły Podstawowej nr 15 im. Władysława Syrokomli w Radomiu

Karta pracy „Nasze dane osobowe w wirtualnym świecie"

Karta pracy adresowana jest do uczniów klas 5–6 szkoły podstawowej. Dotyczy zagadnień związanych z ochroną danych osobowych w internecie oraz zagrożeń, jakich mogą doświadczyć jego użytkownicy – czyli wyłudzania danych osobowych. Szczególną uwagę zwracamy na przypomnienie, czym są dane osobowe, czego o sobie nie „mówić" innym w wirtualnym świecie, na czym polega phishing i jak działają mechanizmy wyłudzania danych.

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej. Phishing jest bardzo prostym rodzajem ataku cybernetycznego. Nie wymaga szukania luk w zabezpieczeniach ani posiadania zaawansowanej wiedzy technicznej. Phishing bazuje na najsłabszym ogniwie ochrony sieci komputerowej, czyli błędach użytkownika. Twórcy fałszywych informacji podszywają się pod realnie istniejące instytucje, nakłaniając użytkownika do udzielenia osobistych informacji.

(źródło: https://pl.wikipedia.org/wiki/Phishing)

Zamieszczone w karcie pracy ćwiczenia uczniowie mogą wykonać na telefonie czy tablecie lub w wersji papierowej, uzupełniając zadania na wydrukowanej karcie pracy.

zadanie w wersji elektronicznej zadanie w wersji papierowej

Zadanie 1: Polega na wskazaniu prawidłowej odpowiedzi na pytanie, kto jest bezpieczniejszy w internecie? Odpowiedzi należy udzielić na podstawie podanych wypowiedzi.

Zadanie 2: W zamieszczonej wykreślance należy wyszukać i zaznaczyć przykłady danych osobowych oraz wpisać odpowiedzi w wyznaczonych miejscach. Ważne, aby wspomnieć, że niektóre dane osobowe składają się z dwóch wyrazów. Zadanie może zostać wykonane również w formie cyfrowej poprzez zeskanowanie kodu QR.

Zadanie 3: Na początku zajęć nauczyciel przybliża uczniom pojęcie phishingu. Na podstawie omówionych przykładów uczniowie zaznaczają prawidłową definicję tego niebezpiecznego zjawiska.

Zadanie można wykonać także w wersji elektronicznej poprzez skanowanie definicji ukrytych w kodach QR i zaznaczenie na karcie pracy poprawnej odpowiedzi. Podczas omówienia zadania warto podać uczniom kilka przykładów ataków phishingowych, tak aby potrafili je zidentyfikować w praktyce. Informacje o aktualnych kampaniach phishingowych znajdują się np. na fanpage'u CERT Polska pod linkiem https://www.facebook.com/CERT.Polska. Można również zachęcić uczniów do samodzielnego zapoznania się z materiałami zamieszczonymi pod tym linkiem.

Zadanie 4: W zadaniu podane zostały przykłady prawidłowych i nieprawidłowych reakcji po otrzymaniu podejrzanej wiadomości e-mail. Zadaniem ucznia jest wskazanie właściwego zachowania – poprzez połączenie odpowiedzi z wesołą kopertą oraz niewłaściwego, które należy połączyć ze smutną kopertą. Zadanie można wykonać także w wersji elektronicznej, skanując kod QR.

Nasze dane osobowe są bardzo cenne.
To informacje, które pozwalają na zidentyfikowanie konkretnej osoby. Do takich danych należą m.in.: imię, nazwisko, adres zamieszkania czy numer telefonu (to dane osobowe zwykłe).
Dane dotyczące zdrowia, pochodzenia czy przekonania religijnego – to dane osobowe wrażliwe. Sprawdź, czy potrafisz je chronić i bezpiecznie korzystać z internetu.
Podejmij kolejne wyzwania.

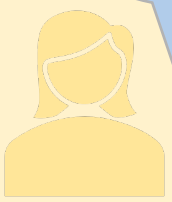
Zadanie 1

Zapoznaj się z wypowiedziami użytkowników internetu.
W wyznaczonym miejscu zaznacz znakiem „X", kto jest bezpieczniejszy w internecie i zachował się odpowiedzialniej.

Cześć,
mój ulubiony kolor
to zielony,
mam kota
i lubię czytać komiksy.

☒

Cześć,
mam na imię Ania,
mam 10 lat.
Chodzę do czwartej klasy
i mieszkam w Kołobrzegu
na ul. Internetowej 13.

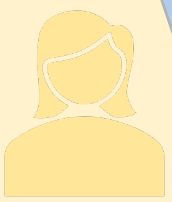


☐

Cześć, nazywam się
Janek Dzbanek,
jestem z Warszawy
i mam 12 lat.
Podaję mój e-mail...

☐

Cześć, mój nick to Zebra.
Czyli lubię biały
i czarny kolor
oraz grę,
w którą tu gramy.



☒

Zadanie 2

W zamieszczonej poniżej wykreślance ukrytych zostało sześć przykładów danych osobowych. Niektóre z nich składają się z dwóch członów (słów). Wykreśl dane osobowe i zapisz je we wskazanych obok miejscach. Odpowiedzi mogą występować pionowo lub poziomo.

r	x	e	i	m	l	c	w	k	l	e	y	b	n	k	u	y	h
d	a	t	a		u	r	o	d	z	e	n	i	a	d	r	e	s
h	r	t	w	h	u	w	v	s	l	v	h	b	z	y	a	i	s
s	r	h	z	n	x	f	i	h	g	t	t	m	w	s	h	q	e
q	a	g	n	j	m	b	j	e	g	f	o	u	i	m	i	ę	c
i	v	i	u	a	y	l	c	e	y	g	v	w	s	b	h	a	p
l	i	s	k	k	g	a	m	u	c	z	p	k	k	p	a	n	v
o	l	n	u	m	e	r		t	e	l	e	f	o	n	u	d	p
r	r	l	g	z	-	x	u	s	c	y	a	t	o	x	j	u	f
q	q	f	v	t	m	z	f	j	x	g	w	o	i	w	z	z	c
h	r	f	k	c	a	h	x	u	o	m	b	l	x	u	l	x	l
f	h	t	r	k	i	v	b	b	u	r	h	o	k	k	s	w	t
k	p	c	q	z	l	l	a	f	w	a	o	l	g	a	e	s	i

1. **data urodzenia**
2. **numer telefonu**
3. **e-mail**
4. **imię**
5. **adres**
6. **nazwisko**

**Wersja elektroniczna zadania – zeskanuj kod QR smartfonem lub tabletem i rozwiąż zadanie.*

Zadanie 3

Zeskanuj zamieszczone poniżej kody QR. Zaznacz, która definicja pojęcia phishing jest prawdziwa. Jeżeli nie posiadacz czytnika kodów QR, wykonaj zadanie w wersji papierowej, zaznaczając na karcie prawidłową odpowiedź.

Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS, za pomocą których cyberprzestępcy starają się wyłudzić nasze dane osobowe.

Phishing to popularny zabieg kosmetyczny.

Phishing to atak na nasz komputer. W ten sposób cyberprzestępcy starają się uszkodzić urządzenie.

Przykłady phishingu znajdziesz w materiałach dostępnych na fanpage'u CERT Polska:
https://www.facebook.com/CERT.Polska

Zadanie 4

Otrzymujesz wiadomość e-mail, w której znajdują się podejrzane linki i treści. Co należy zrobić, aby chronić swoje dane? Połącz prawidłowe zachowanie z wesołą kopertą, a nieprawidłowe ze smutną.

Sprawdzam nadawcę wiadomości i weryfikuję, czy jego adres wygląda na prawdziwy.

Sprawdzam poprawność językową i gramatyczną wiadomości.

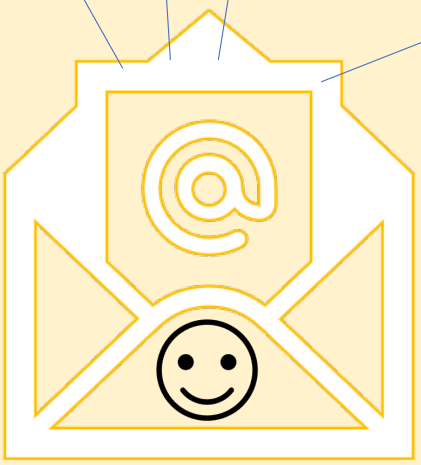
Klikam na zamieszczony w wiadomości link.

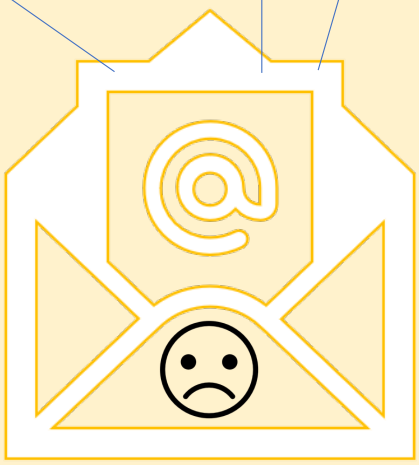
Otwieram dodany do wiadomości załącznik.

Usuwam podejrzaną wiadomość.

Przesyłam wiadomość do kolejnej osoby.

Oznaczam tę wiadomość jako spam.





**Wersja elektroniczna zadania – zeskanuj kod QR smartfonem lub tabletem i rozwiąż zadanie.*

Karta pracy „Nasze dane osobowe w wirtualnym świecie"

Zamieszczone w karcie pracy ćwiczenia można wykonać na telefonie czy tablecie poprzez skanowanie kodów QR, a także w wersji papierowej, uzupełniając zadania na wydrukowanej karcie pracy.

zadanie w wersji elektronicznej

zadanie w wersji papierowej

Nasze dane osobowe są bardzo cenne. To informacje, które pozwalają na zidentyfikowanie konkretnej osoby. Do takich danych należą m.in.: imię, nazwisko, adres zamieszkania czy numeru telefonu (to dane osobowe zwykłe), dane dotyczące zdrowia, pochodzenia czy przekonania religijnego – to dane osobowe wrażliwe. Sprawdź, czy potrafisz je chronić i bezpiecznie korzystać z internetu. Podejmij kolejne wyzwania.

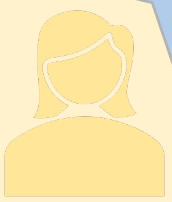
Zadanie 1

Zapoznaj się z wypowiedziami użytkowników internetu.
W wyznaczonym miejscu zaznacz znakiem „X", kto jest bezpieczniejszy w internecie i zachował się odpowiedzialniej.

Cześć,
mój ulubiony kolor
to zielony,
mam kota
i lubię czytać komiksy.

☐

Cześć,
mam na imię Ania,
mam 10 lat.
Chodzę do czwartej klasy
i mieszkam w Kołobrzegu
na ul. Internetowej 13.

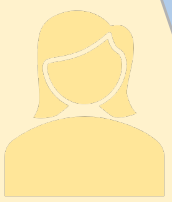


☐

Cześć, nazywam się
Janek Dzbanek,
jestem z Warszawy
i mam 12 lat.
Podaję mój e-mail...

☐

Cześć, mój nick to Zebra.
Czyli lubię biały
i czarny kolor
oraz grę,
w którą tu gramy.



☐

Zadanie 2

W zamieszczonej poniżej wykreślance ukrytych zostało sześć przykładów danych osobowych. Niektóre z nich składają się z dwóch członów (słów). Wykreśl dane osobowe i zapisz je we wskazanych obok miejscach. Odpowiedzi mogą występować pionowo lub poziomo.

r	x	e	i	m	l	c	w	k	l	e	y	b	n	k	u	y	h
d	a	t	a		u	r	o	d	z	e	n	i	a	d	r	e	s
h	r	t	w	h	u	w	v	s	l	v	h	b	z	y	a	i	s
s	r	h	z	n	x	f	i	h	g	t	t	m	w	s	h	q	e
q	a	g	n	j	m	b	j	e	g	f	o	u	i	m	i	ę	c
i	v	i	u	a	y	l	c	e	y	g	v	w	s	b	h	a	p
l	i	s	k	k	g	a	m	u	c	z	p	k	k	p	a	n	v
o	l	n	u	m	e	r		t	e	l	e	f	o	n	u	d	p
r	r	l	g	z	-	x	u	s	c	y	a	t	o	x	j	u	f
q	q	f	v	t	m	z	f	j	x	g	w	o	i	w	z	z	c
h	r	f	k	c	a	h	x	u	o	m	b	l	x	u	l	x	l
f	h	t	r	k	i	v	b	b	u	r	h	o	k	k	s	w	t
k	p	c	q	z	l	l	a	f	w	a	o	l	g	a	e	s	i

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....

**Wersja elektroniczna zadania – zeskanuj kod QR smartfonem lub tabletem i rozwiąż zadanie.*

Zadanie 3

Zeskanuj zamieszczone poniżej kody QR. Zaznacz, która definicja pojęcia phishing jest prawdziwa. Jeżeli nie posiadacz czytnika kodów QR, wykonaj zadanie w wersji papierowej, zaznaczając na karcie prawidłową odpowiedź.

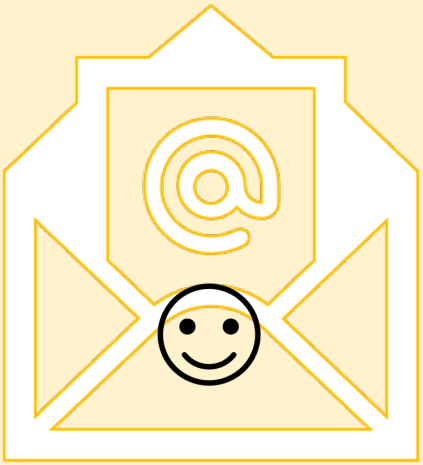
Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS, za pomocą których cyberprzestępcy starają się wyłudzić nasze dane osobowe.	**Phishing to popularny zabieg kosmetyczny.**	**Phishing to atak na nasz komputer. W ten sposób cyberprzestępcy starają się uszkodzić urządzenie.**

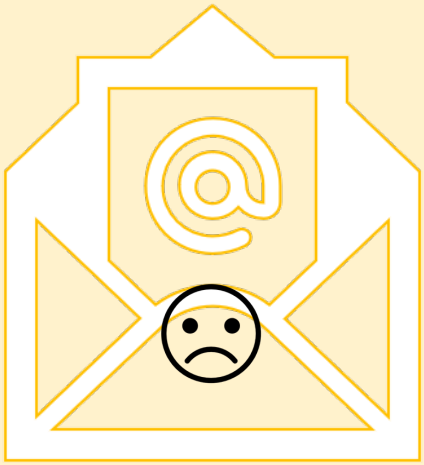
Przykłady phishingu znajdziesz w materiałach dostępnych na fanpage'u CERT Polska:
https://www.facebook.com/CERT.Polska

Zadanie 4

Otrzymujesz wiadomość e-mail, w której znajdują się podejrzane linki i treści. Co należy zrobić, aby chronić swoje dane? Połącz prawidłowe zachowanie z wesołą kopertą, a nieprawidłowe ze smutną.

- Sprawdzam nadawcę wiadomości i weryfikuję, czy jego adres wygląda na prawdziwy.
- Sprawdzam poprawność językową i gramatyczną wiadomości.
- Klikam na zamieszczony w wiadomości link.
- Otwieram dodany do wiadomości załącznik.
- Usuwam podejrzaną wiadomość.
- Przesyłam wiadomość do kolejnej osoby.
- Oznaczam tę wiadomość jako spam.





**Wersja elektroniczna zadania – zeskanuj kod QR smartfonem lub tabletem i rozwiąż zadanie.*

DOWIEDZ SIĘ WIĘCEJ

O OSEHERO NA STRONIE

https://osehero.pl

ose hero

ose OGÓLNOPOLSKA SIEĆ EDUKACYJNA

Fundusze Europejskie Polska Cyfrowa

Rzeczpospolita Polska

NASK

Unia Europejska Europejski Fundusz Rozwoju Regionalnego