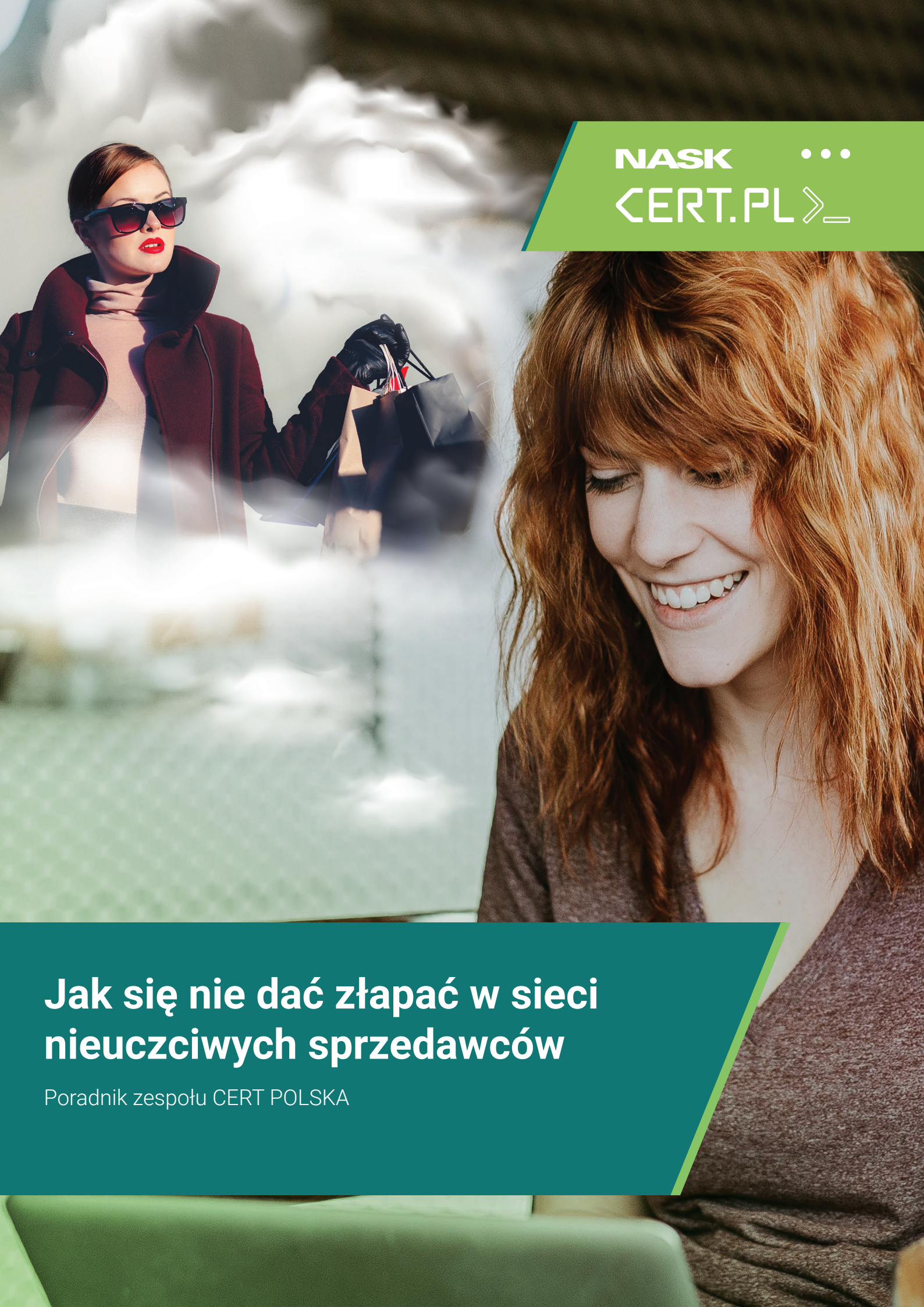
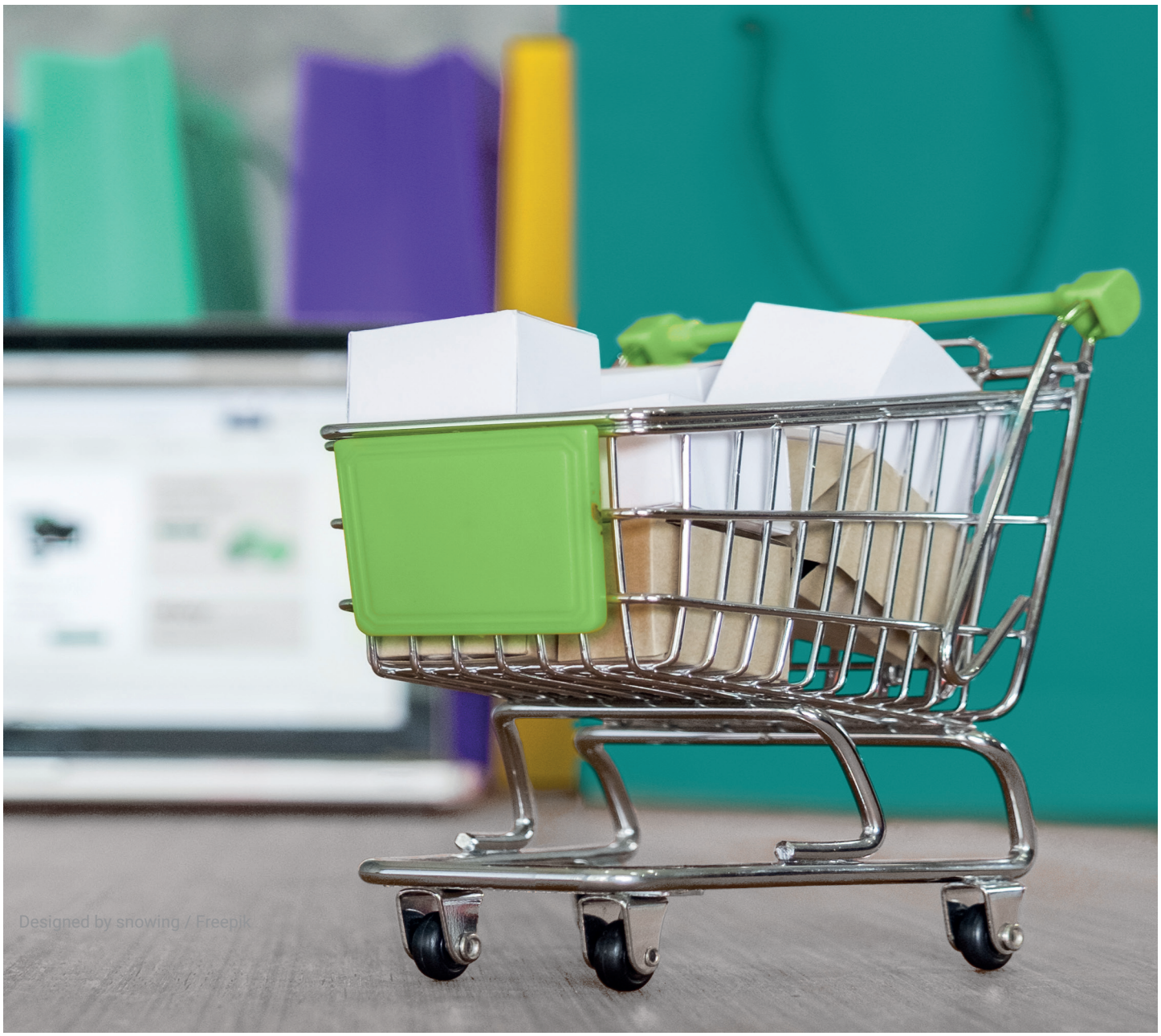


NASK
CERT.PL

Jak się nie dać złapać w sieci nieuczciwych sprzedawców

Poradnik zespołu CERT POLSKA



Raport „E-commerce w Polsce 2019. Gemius dla e-Commerce Polska" przygotowany przez firmę Gemius we współpracy z Izbą Gospodarki Elektronicznej nie pozostawia wątpliwości – coraz więcej Polaków robi zakupy przez internet! W 2019 odsetek kupujących przez internet wyniósł 62 % i był wyższy o 6 p.p. niż rok wcześniej. Co ciekawe, zakupy on line przestają być domeną młodych ludzi. W 2019 roku kupujący poniżej 34 rż stanowili 42% (rok wcześniej było to 64% kupujących). Zainteresowanie internetowymi sklepami wzrosło w grupach starszych. Osoby 50+ to 26% wśród osób kupujących online, a internauci w wieku 35-49 to 32% nabywców.

Niestety, im popularniejszy staje się handel w sieci, tym większą kreatywnością wykazują się nieuczciwi sprzedawcy i cyberprzestępcy. Sposoby ich działania są coraz bardziej doskonałe, wyrafinowane i sprawiające, że kupujący powinien zachować czujność i rozwagę na każdym z etapów robienia internetowych zakupów, a czasami nawet wcześniej, zanim trafi do e-sklepu.

Aby pomóc Państwu w bezpiecznych zakupach przez internet, zespół **CERT Polska** działający w **NASK**, przygotował poradnik z praktycznymi radami, na co zwracać uwagę, jak działać, czego się wystrzegać, aby kupowanie online było tylko przyjemnością!

Czy niezadowolenie z zakupów online zawsze wynika z nieuczciwości sprzedawcy?

Nie, często sprzedawca jest uczciwy, ma dobrą wolę i prowadzi uczciwy biznes. Niestety, zdarzają się sytuacje losowe, kiedy coś pójdzie niezgodnie z dobrymi chęciami – dostaniemy towar uszkodzony, niezgody z zamówieniem, będzie opóźnienie w dostawie lub haker włamie się na stronę uczciwego sprzedawcy i na jego konto dokona przestępstwa. Czasami też sami, szukając oszczędności, decydujemy się na kupno towaru mniej rozpoznawalnej marki, o trudnej do oceny jakości.

Zdarza się też tak, że na rozpoznawalnych i sprawdzonych już przez nas portalach sprzedaży może pojawić się nieuczciwa oferta. Jest to jedna z technik, gdzie atakujący próbuje przemycić swoje oszustwo w gąszczu legalnych ogłoszeń. Ma to na celu utrudnienie przeciwdziałania nadużyciom w tym zakresie, a także późne wykrycie w celu oszukania jak największej liczby ofiar. Dedykowane zespoły bezpieczeństwa nie ustają w wysiłkach, aby skutecznie typować oraz usuwać takie ogłoszenia.

Co robić by nie wpaść w sidła złodziei kupując z wiarygodnej strony, np., internetowej aukcji lub serwisu z ogłoszeniami?

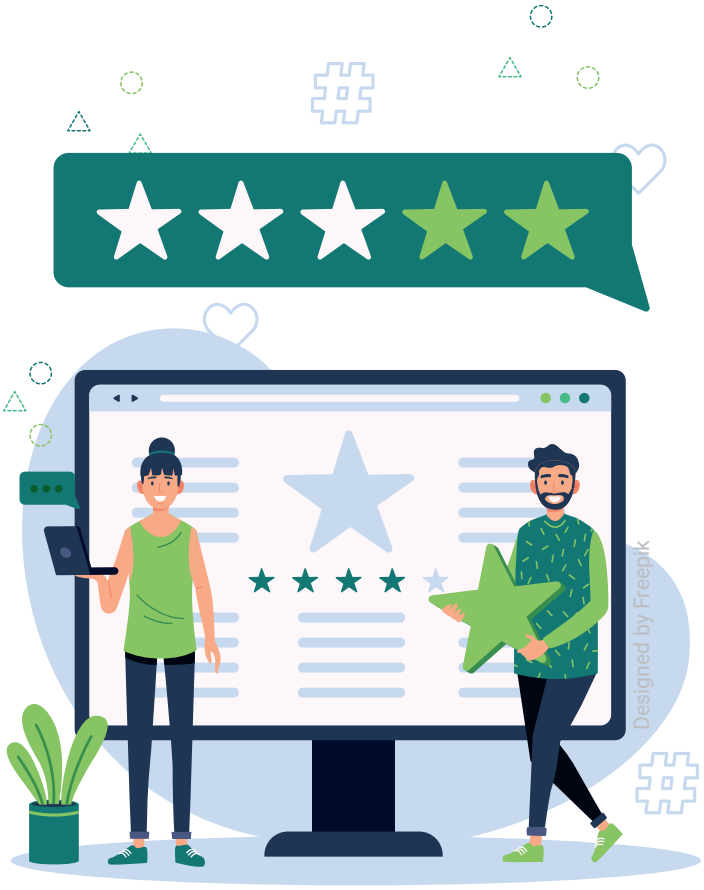
Przede wszystkim zapoznajmy się dokładnie z ofertą. Jeżeli w treści jest jakiś link, kierujący rzekomo do dokładniejszego opisu, sprawdźmy to dokładnie. Zwróćmy uwagę na pasek adresowy po kliknięciu w interesujący nas link – czy nie odsyła nas do jakiejś podejrzanej strony, znajdującej się w nieznanej domenie, czy nie pojawia się tam literówka, która ma na celu podszycie się pod znany podmiot, np. aukcjje.cc, oglozsenia.pl

Sprawdź sprzedawcę. Pamiętaj,że czas jego obecności w serwisie nie powinien być gwarantem uczciwości – jego konto mogło zostać przejęte przez atakującego. Oceń jego pozostałe oferty a także ich spójność. Sprawdź przede wszystkim, czy nie jest tworzony jakiś dodatkowy warunek zakupowy na aukcji, która Cię interesuje, np. prośba o zalogowanie się w innym miejscu, pobranie i zainstalowanie czegokolwiek, albo sfinalizowanie transakcji w innym miejscu. Bądź wyczulony na sztuczki w stylu „Nie musi Pan/Pani przelewać środków, ale dla potwierdzenia tożsamości poproszę o zdjęcie karty kredytowej" lub „Oddam za darmo, proszę tylko opłacić kuriera". Brzmi uspokajająco, ale najczęściej niesie konsekwencje dla ofiary, która uległa takiej socjotechnice.

Jeżeli cokolwiek wyda Ci się podejrzane nie bój się pytać. W pierwszej kolejności samego sprzedającego, bliskich nam osób a także dedykowanych zespołów bezpieczeństwa, które na „chłodno" ocenią znalezioną przez Ciebie „gorącą" ofertę.

Czy warto sprawdzać opinie o sklepie?

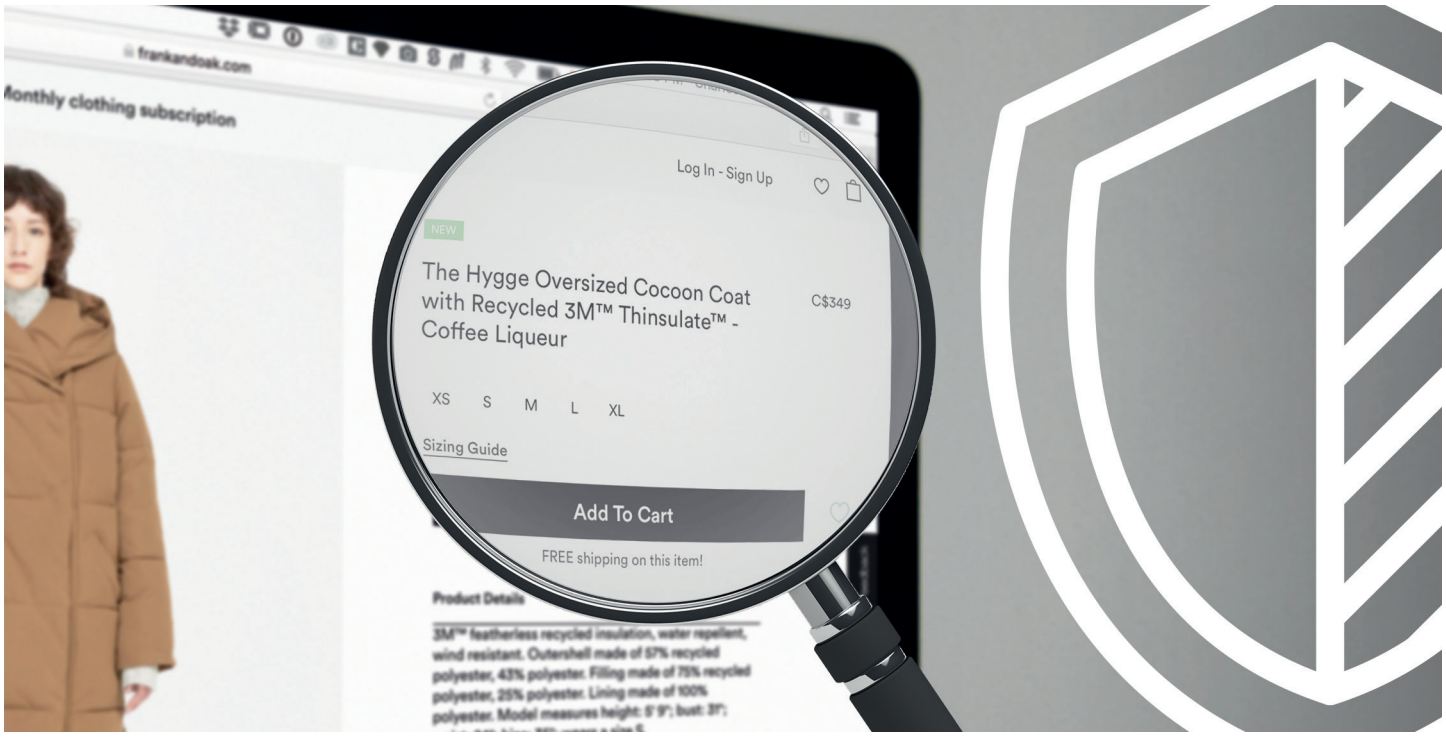
Oczywiście, że tak, ale sprawdzajmy, kto te opinie napisał. Na pierwszy rzut oka wydaje się to trudne. Jednak wiodące i liczące się serwisy uniemożliwiają fałszowanie oszustwa. Dlatego sprawdzajmy czy strona lub same opinie nie zostały przygotowane przez atakujących (np. oppinnie.cc). Zwróćmy też uwagę na historię wystawianych opinii – jeśli istnieje luka np. najnowsze opinie są z ostatnich dwóch tygodni, a wcześniejsze sprzed roku lub wcześniej – ograniczmy zaufanie. Zawsze warto skorzystać z pomocy wyszukiwarki. Jest szansa, że oszukani klienci zdążyli zostawić w sieci jakieś ostrzeżenie na temat sklepu, który wydał się nam interesujący.



Jak uniknąć wejścia na stronę sprzedawcy oszusta?

Zawsze miejmy świadomość, co lub kto nas tutaj przyprowadził. Jeśli zachętę do zakupów (często okraszoną atrakcyjną ofertą, promocją, kuponem rabatowym) dostajemy przez media społecznościowe, komunikatory – pocztę elektroniczną – miejmy się na baczności. To są znane sposoby złowienia klientów-ofiar przez cyberprzestępców.

- Wyniki wyszukiwania. Jeśli szukamy np. butów sportowych męskich i wpisujemy takie hasło w wyszukiwarkę internetową, w wynikach możemy otrzymać nie tylko popularne i uczciwe sklepy, ale również wyniki, które mogą być dla nas niebezpieczne.
- Oferta sklepu. Jeśli nie znamy sklepu, który pokazał się w wynikach, sprawdźmy jakie towary poza „męskimi butami sportowymi" oferuje dany sklep. Jeśli będą to maszyny budowlane, bielizna damska oraz terakota – powinniśmy włączyć czujność, taki rozrzut oferowanego asortymentu może budzić wątpliwości.
- Wygląd strony internetowej. Poza tym sprawdźmy inne elementy strony – czy jest pisana poprawną polszczyzną, czy nie ma błędów ortograficznych, gramatycznych, językowych. Jakiej jakości są zdjęcia, grafika. Jeśli mamy wrażenie, że ktoś zrobił tę stronę w przysłowiowe 5 minut i na kolanie, lepiej wycofajmy się z dokonywania na niej zakupów.
- Informacje na temat działania sklepu. Kolejna rzecz, którą warto zrobić to sprawdzenie wszystkich niezbędnych elementów e-sklepów, takich jak: regulamin, sposób dostarczenia przesyłki, sposób płatności, sposób zwrotu towaru. Weryfikując obecność wyżej wskazanych pamiętajmy, żeby być wyczulonym na wszelkie niespójności pomiędzy nimi.
- Dane sprzedawcy. Sprawdźmy, czy firma podana na stronie jako jej właściciel istnieje w KRS, sprawdźmy dane teleadresowe – czy taki adres istnieje fizycznie i co się pod nim znajduje – tę możliwość dają niektóre serwisy mapowe. Jeśli w KRS pod nazwą rzekomego właściciela sklepu wpisany jest np. sklep stacjonarny lub firma prowadząca inną działalność niż handlowa – włączmy czujność, bo możliwe, że oszust podszywa się pod istniejącą firmę, która nie ma sklepu internetowego lub przejął nieużywaną domenę internetową innego podmiotu gospodarczego.
- Bezpośredni kontakt ze sprzedawcą. Jeśli na stronie sklepu, który budzi nasze wątpliwości podany jest kontakt, użyjmy go i „przepytajmy" osobę, która go odbierze. Jeśli rozmówca nie będzie znał odpowiedzi na nasze pytania, będzie się irytował, lub wychwycimy jakieś niespójności, odstąpmy od zamiaru robienia zakupów w tym sklepie.



Czy zielona kłódka przy adresie sklepu nas zabezpiecza?

Niestety nie. W dobie pomysłowości hakerów, mit zielonej kłódki upadł i nie należy sugerować się pozytywnie jej obecnością przy adresie internetowym. Dlatego, pamiętajmy, że nawet jeśli przy adresie wyświetla się kłódka, ale inne elementy strony lub dotarcia na tę stronę budzą nasze wątpliwości, nie bagatelizujmy tych ostrzeżeń.

Co jeszcze powinno wzbudzić czujność kupującego?

- Uważajmy na zniżki i wszelkiego rodzaju „popychacze" do działania. Jeżeli ktoś wyjątkowo zachęca dodatkowo oferując nam „super rabat" i tylko dzisiaj, bądź szczególnie czujny. Jest to znany zabieg socjotechniczny.
- Uważaj na próby podsunięcia nam legalnej płatności w fałszywym sklepie. Jest to bardzo niebezpieczna technika, która może uśpić nawet obeznanego w zakupach internautę. Sprawdzaj czy płatność, której dokonujemy jest wykonywana faktycznie na rzecz podmiotu, w którym kupujemy. W przeciwnym wypadku towar może zostać wysłany do atakującego.
- Zwracajmy uwagę na to, o co prosi nas sprzedający. Prośba o login do Facebooka, do bankowości mobilnej z pewnością powinna spowodować nasze natychmiastowe „wyjście" z takiego sklepu.
- Szczególnie zwróćmy uwagę na pasek z adresem internetowym podczas dokonywania płatności. Sprawdź, czy na pewno jest to właściwy adres, zgodny z nazwą serwisu, bez literówek, a także czy strona banku, do której zostaliśmy odesłani, to na pewno strona naszego banku.

Czego absolutnie nie powinniśmy ignorować?

Jeśli podczas robienia zakupów w sklepie internetowym „odezwie" się zainstalowany na komputerze program antywirusowy lub sama przeglądarka wyświetli informację, że strona jest niebezpieczna, nie ignorujmy tego.

Podobnie w momencie, kiedy zlecając płatność odezwie się do nas nasz bank z prośbą lub informacją odnośnie działania na naszym koncie. Jeżeli masz wątpliwości, że dzwoni do ciebie bank, sam podejmij z nim kontakt.

Co nam grozi jeśli jednak dokonamy zakupu w fałszywym sklepie internetowym?

Utrata gotówki, w kwocie, którą zapłaciliśmy za towar, którego nigdy nie dostaniemy to stosunkowo niewielki problem. Może zdarzyć się też tak, że stracimy wszystkie oszczędności, a w przypadku zainstalowania przez hakera wirusa podczas robienia zakupów, możemy też utracić inne swoje dane wrażliwe. Dlatego nigdy nie ignorujmy nawet najmniejszych niepokojących nas sygnałów.

Co zrobić, gdy zorientujemy się, że zrobiliśmy zakupy w fałszywym sklepie?

Należy jak najszybciej poinformować dostawcę płatności, czyli bank, w którym prowadzony jest rachunek bądź karta płatnicza. Następnie powinniśmy zgłosić incydent na stronie incydent.cert.pl oraz policji. Dzięki tym działaniom zwiększamy szansę na zatrzymanie szkodliwego procederu, a także na podjęcie działań w celu ujęcia sprawców. Warto też ostrzec innych, zostawiając informację w serwisach z opiniami, na forach, na FB fundacji i organizacji broniących praw konsumentów.

Czy jest szansa na odzyskanie skradzionych pieniędzy?

W przypadku, gdy płaciliśmy kartą, odzyskanie pieniędzy jest stosunkowo łatwe. Wystarczy skorzystać z mechanizmu tzw. obciążenia zwrotnego (chargeback), składając reklamację w banku i opisując problem. Przy płatności przelewem szanse na odzyskanie pieniędzy są dużo mniejsze. Zdarzają się przypadki, gdy bankowi uda się zatrzymać przelew, jednak przy pesymistycznym scenariuszu, musimy poczekać aż organy ścigania zatrzymają sprawców.

NASK

CERT.PL