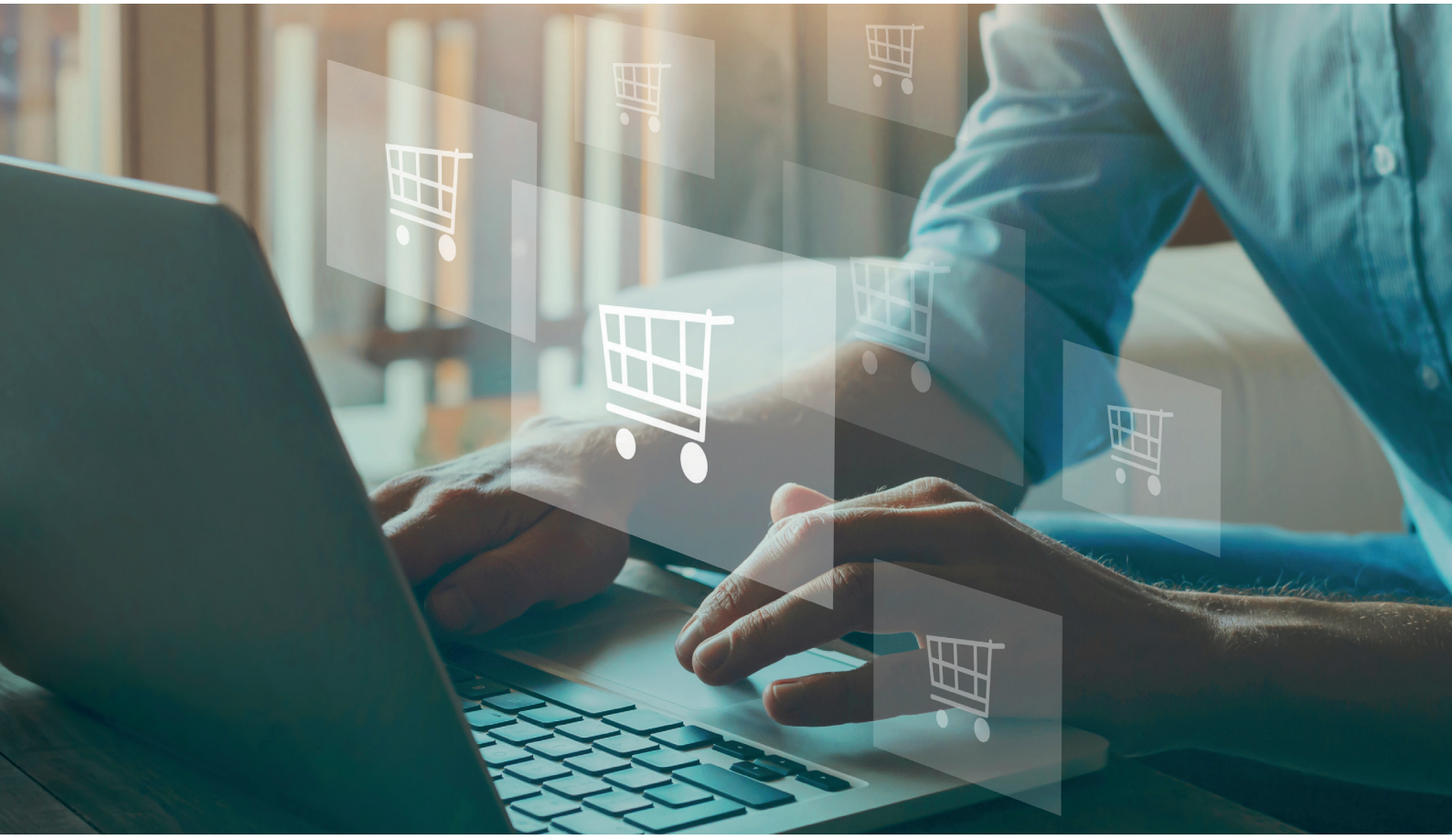
JAK BEZPIECZNIE KUPOWAĆ W INTERNECIE

Poradnik CERT Polska
2022/2023

CERT.PL
NASK

Na przełomie 2022 i 2023 roku nie trzeba już nikogo przekonywać, że internet stał się dla znacznej części konsumentów podstawowym sposobem dokonywania zakupów. Regularny wzrost tego trendu obserwowaliśmy od lat, ale warto wyróżnić dwa czynniki, które miały szczególny wpływ na obecną popularność e-commerce. W 2020 roku wybuch pandemii COVID-19 spowodował, że Polacy masowo przestawili się na zakupy dokonywane online, motywując to troską o własne bezpieczeństwo. Drugim istotnym, obserwowanym w 2022 roku czynnikiem wzmacniającym tendencję do kupowania online jest natomiast wysoki poziom inflacji, a co za tym idzie – większa potrzeba oszczędności[1], porównywania cen i kupowania możliwie najtaniej. W ten kontekst dobrze wpisuje się też coraz większa popularność paczkomatów (w grupie wiekowej 15-24 lata tę formę dostawy wybiera aż 87% badanych, nawet gdy bierzemy pod uwagę tylko sieć firmy InPost[2]), a co za tym idzie – niższe lub nawet zerowe koszty dostaw i ewentualnych zwrotów. Nic dziwnego, że 58% internautów uważa zakupy w internecie za bardziej opłacalne, a 31% z nich wprost deklaruje, że zamierza tą drogą kupować wszystko, co możliwe[3]. Aż 79% konsumentów zmieniło też w ostatnim czasie swoje zachowania zakupowe „w związku z nadchodzącym kryzysem”[4].

Pandemia i inflacja to czynniki negatywne, natomiast badani wymieniają też szereg zalet nabywania produktów w sieci, takich jak wygoda, większy wybór, oszczędność czasu oraz możliwość poznania opinii o produkcie. Wspólnie budują one obraz rynku, w ramach którego w samym 2022 roku spośród 37,6 miliona Polaków około 30 milionów (77-81% w zależności od badania[5]) miało już doświadczenie z realizowaniem zakupów w internecie. Co ważne, niewiele mniejszy odsetek (75%) regularnie kupuje online w polskich sklepach[6], a 62,3% transakcji zrealizowanych zostało w 2022 roku za pośrednictwem urządzeń mobilnych[7].

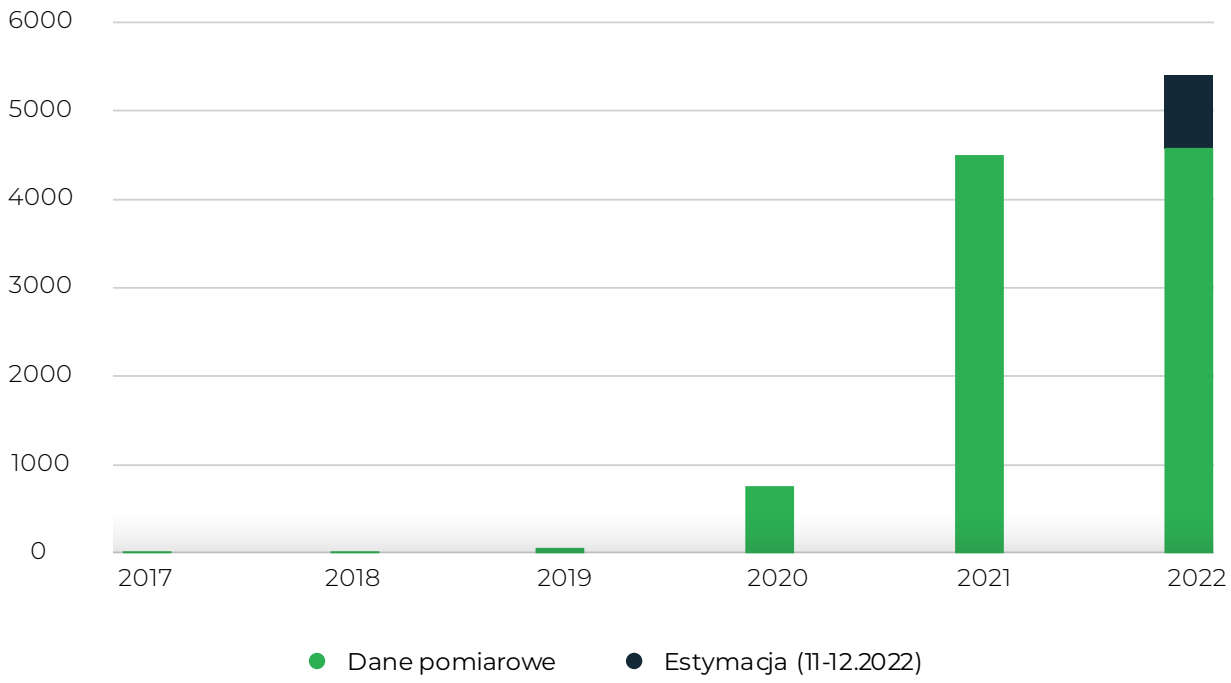


1 Raport „W kryzysie do E-commerce” zrealizowany w 2022 roku przez Izbę Gospodarki Elektronicznej.
2 Raport „E-commerce w Polsce 2022” zrealizowany przez Gemius, Polskie Badania Internetu i IAB Polska.
3 Raport „W kryzysie do E-commerce”.
4 Tamże.
5 Raporty „E-commerce w Polsce 2022” oraz „Polaków portret własny. Bezpieczni na e-zakupach 2022” zrealizowany przez Santander Consumer Bank.
6 Raport „E-commerce w Polsce 2022”.
7 Raport „Trendy na rynku e-commerce w Polsce 2022” zrealizowany przez Ceneo.

PRZESTĘPCY DZIAŁAJĄ TAM, GDZIE SĄ PIENIĄDZE

Skoro konsumenci przenieśli swoje działania zakupowe do sieci, ten sam obszar stał się automatycznie polem coraz intensywniejszych działań przestępców. Jak pokazują statystyki zagrożeń rejestrowanych przez zespół CERT Polska, działający w strukturach Państwowego Instytutu Badawczego NASK, już w 2021 roku ponad 5-krotnie (w stosunku do poprzedniego roku) wzrosła liczba incydentów cyberbezpieczeństwa związanych z oszustwami na najpopularniejszych polskich portalach zakupowych (Allegro, OLX, Vinted). W 2022 roku liczba realnych incydentów tego typu była już (w porównaniu z rokiem 2020) niemal 7-krotnie wyższa. Warto w tym kontekście przypomnieć, że niemal co trzeci internauta (32,5%) rozpoczyna proces zakupowy od wizyty na portalu Allegro[8], a zatem na ten typ oszustw narażony jest znaczący odsetek konsumentów.

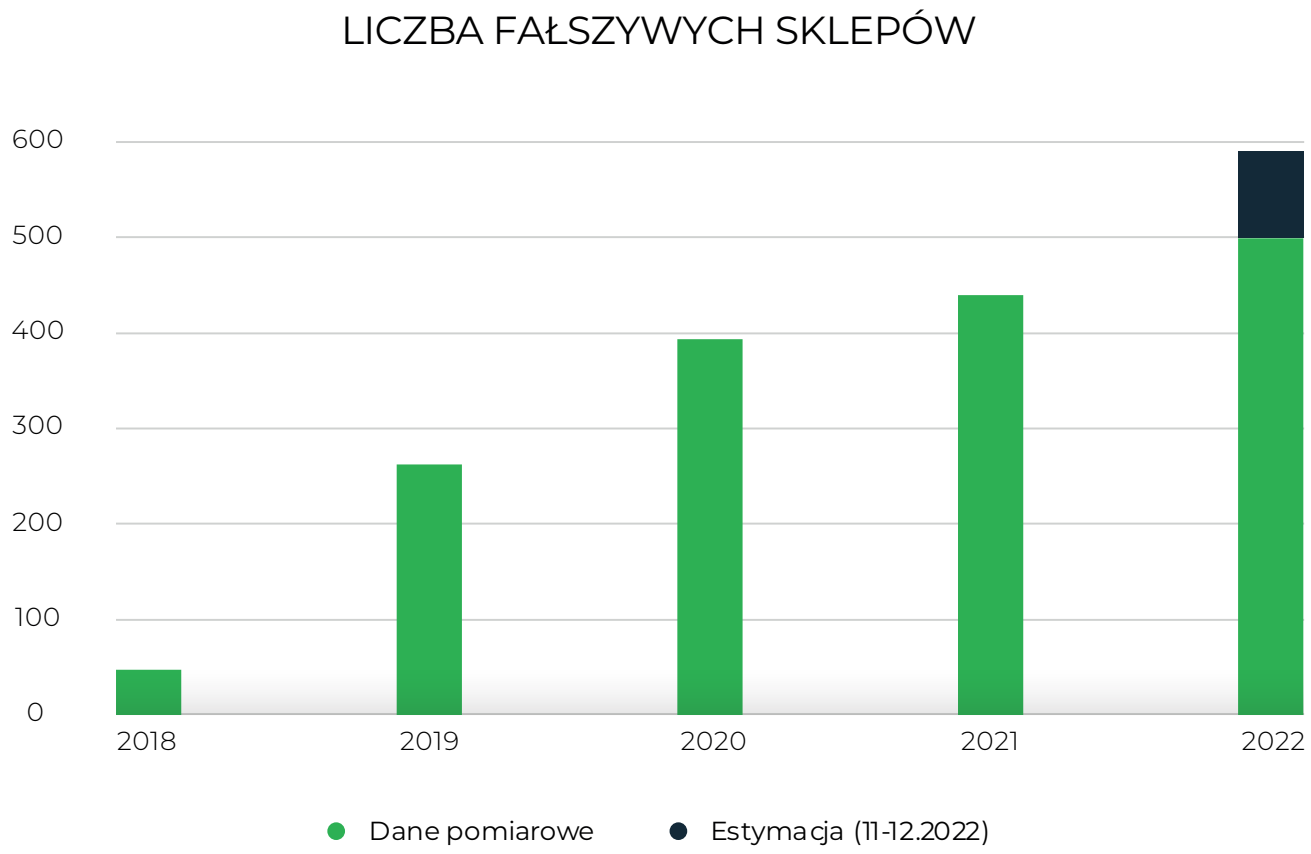
INCYDENTY CYBERZAGROŻEŃ NA PORTALACH ALLEGRO, OLX, VINTED



Liczba incydentów zagrożeń związanych z najpopularniejszymi portalami zakupowymi w Polsce gwałtownie wzrosła już w roku 2021. Źródło: Dane zespołu CERT Polska.

8 Tamże.

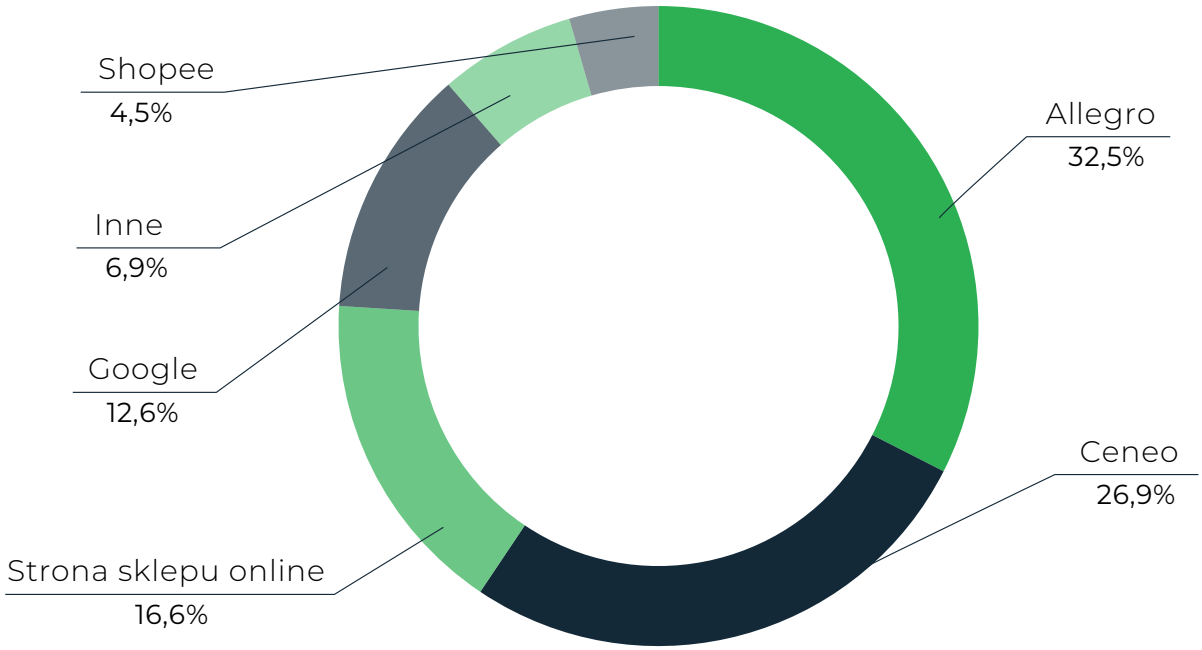
Od 2019 roku CERT Polska rejestruje też rosnącą falę przestępstw polegających na tworzeniu fałszywych sklepów internetowych, sprzedających fikcyjne towary lub wyłudzających dane dostępowe do kont bankowych. W 2020 roku (w porównaniu z rokiem 2018) ich odsetek wzrósł o 1256 punktów procentowych, ale nawet porównanie 2022 z rokiem ubiegłym wykazuje zwiększenie liczby stron internetowych podszywających się pod sklepy online o 34 p.p. Ten typ oszustw także traktować należy jako poważne zagrożenie, ponieważ 16,6% kupujących online rozpoczyna swój proces wyszukiwania produktów online właśnie od wizyty na stronie sklepu, a kolejne 12,6% korzysta w pierwszym kroku ścieżki zakupowej z wyszukiwarki Google[9].



Liczba fałszywych sklepów w polskiej przestrzeni internetowej wyraźnie rośnie już od 2019 roku, przy czym w 2022 roku odnotowano – w porównaniu z rokiem poprzednim – aż 34% więcej tego typu zagrożeń. Źródło: Dane zespołu CERT Polska.

9 Tamże.

W JAKI SPOSÓB NAJCZĘŚCIEJ POLACY ROZPOCZYNAJĄ ZAKUPY W SIECI



Źródło: Raport „Trendy na rynku e-commerce w Polsce 2022”, bazujący na badaniu dokonanym wśród użytkowników serwisu Ceneo.

CO POLACY ROBIĄ PRZED ZŁOŻENIEM ZAMÓWIENIA W SKLEPIE INTERNETOWYM

65%
Czytają komentarze na temat e-sklepu

58%
Porównują ceny towarów

41%
Zapoznają się z warunkami zwrotu/ reklamacji towaru

39%
Szukają najtańszej opcji dostawy

34%
Szukają najszybszej formy dostawy

34%
Sprawdzają dostępność płatności za pobraniem

33%
Sprawdzają dostępność znanych operatorów płatności

25%
Czytają regulamin

22%
Sprawdzają, czy strona ma zabezpieczenia

22%
Sprawdzają dane rejestrowe firmy

19%
Czytają zgody marketingowe

8%
Zapisują się do newslettera

Źródło: Raport „Polaków portret własny. Bezpieczni na e-zakupach 2022”

POTRZEBA EDUKACJI E-KONSUMENTÓW W POLSCE

W kontekście wzrastającej liczby zagrożeń związanych z zakupami online pogłębia się również potrzeba przeciwdziałania tego typu oszustwom, zwłaszcza poprzez edukację polskich internautów. O tym, jak niezbędne i pilne jest uświadamianie konsumentom zagrożeń związanych z dokonywaniem zakupów w sklepach internetowych świadczyć też mogą zatrważające wyniki badań zrealizowanych w 2022 roku, pokazujące chociażby, że aż 84% Polaków nie ma świadomości, czym jest phishing, a 77% nie rozumie pojęcia skimmingu[10].

Dlatego prezentowany przez nas poradnik ma za zadanie – w możliwie skondensowanej i przystępnej formie – pełnić rolę wzmacniającą świadomość polskich klientów e-commerce w obszarze zagrożeń, jakie mogą ich spotykać. Zdecydowaliśmy się przy tym na łatwy w odbiorze zestaw popularnych pytań i odpowiedzi, przygotowanych przez specjalistów z zespołu CERT. To maksimum wiedzy bazującej na praktyce przy minimum objętości, dlatego mamy nadzieję, że po zapoznaniu się z tym poradnikiem zakupy realizowane w sieci staną się znacznie przyjemniejsze, a przede wszystkim – bezpieczniejsze.

10 Raport „Polaków portret własny. Bezpieczni na e-zakupach 2022".

1. JAK ROZPOZNAĆ STRONĘ SPRZEDAWCY-OSZUSTA?

- **Sposób dotarcia do sklepu.** Zawsze miej świadomość, w jaki sposób znalazłeś się na danej stronie. Jeśli zachętę do zakupów (często okraszoną atrakcyjną ofertą, promocją, kuponem rabatowym) dostałeś przez media społecznościowe, komunikator lub pocztę elektroniczną – miej się na baczności. To typowe kanały łowienia potencjalnych ofiar przez cyberprzestępców.

- **Podejrzane wyniki wyszukiwania.** Pamiętaj, że jeśli szukasz np. butów sportowych męskich i wpisujesz takie hasło w wyszukiwarkę internetową, możesz otrzymać nie tylko odesłania do popularnych, uczciwych sklepów internetowych, ale również wyniki, które mogą okazać się niebezpieczne.

- **Dziwna oferta sklepu.** Jeśli nie znasz sklepu, który pokazał się w wynikach wyszukiwania, sprawdź jakie towary (poza „męskimi butami sportowymi") oferuje. Jeśli będą to m.in. maszyny budowlane, bielizna damska oraz terakota – należy wzmocnić czujność, bo tak szeroki przekrój oferowanego asortymentu budzi wątpliwości.

- **Nieprofesjonalny wygląd strony internetowej.** Sprawdź inne elementy strony – czy teksty pisane są poprawną polszczyzną, czy nie mają błędów ortograficznych, gramatycznych i językowych. Popatrz, jakiej jakości są zdjęcia i grafiki. Jeśli masz wrażenie, że ktoś zrobił tę stronę „na kolanie", lepiej wycofaj się z dokonywania na niej zakupów.

- **Zbadaj informacje na temat działania sklepu.** Jeśli nie znasz danego sklepu, sprawdź jakość wszystkich (tak, najlepiej wszystkich) niezbędnych elementów biznesu z obszaru e-commerce: regulaminu, sposobów dostarczenia przesyłki, sposobów płatności, sposobów zwrotu towaru. Weryfikując te elementy warto być wyczulonym na wszelkie niespójności pomiędzy nimi.

- **Sprawdź dane sprzedawcy.** Zbadaj, czy firma podana na stronie jako jej właściciel istnieje w KRS, sprawdź też jej dane teleadresowe (czy taki adres istnieje fizycznie i co się pod nim znajduje – taką możliwość dają niektóre serwisy mapowe). Jeśli w KRS pod nazwą rzekomego właściciela sklepu wpisany jest np. sklep stacjonarny lub firma prowadząca działalność inną niż handlowa – to ważny znak ostrzegawczy. Być może oszust podszywa się pod istniejącą firmę, która nie ma sklepu internetowego lub przejął nieużywaną domenę internetową innego podmiotu gospodarczego.

- **Spróbuj bezpośrednio skontaktować się ze sprzedawcą.** Jeśli na stronie sklepu, który budzi twoje wątpliwości, podane są dane kontaktowe, użyj ich i przepytaj osobę, z którą uda się skontaktować. Jeśli w żaden sposób nie udaje się nawiązać kontaktu, jeśli rozmówca nie zna odpowiedzi na nasze pytania lub szybko się irytuje, jeśli wychwycimy jakiekolwiek niespójności – najlepiej odstąpić od robienia zakupów w tym sklepie.

MIT ZIELONEJ KŁÓDKI

W dobie pomysłowości hakerów nie jest już dowodem bezpieczeństwa. Jeśli inne elementy strony budzą twoje wątpliwości, nie bagatelizuj podejrzeń.

2. CZY KŁÓDKA PRZY ADRESIE SKLEPU TO GWARANCJA BEZPIECZNYCH ZAKUPÓW?

Nie. Oszuści opracowali już metody wykorzystania tego typu oznaczenia, dlatego nie należy sugerować się pozytywnie jej obecnością przy adresie internetowym. Można nawet powiedzieć, że bezpieczeństwo zakupów dokonywanych na stronach oznaczonych kłódką to już niestety mit. Dlatego pamiętaj, że nawet jeśli przy adresie wyświetla się kłódka, ale inne elementy strony lub dotarcia na tę stronę budzą twoje wątpliwości, nie bagatelizuj tych ostrzeżeń.

CO DECYDUJE O TYM, ŻE SKLEP INTERNETOWY WYDAJE SIĘ POLAKOM GODNY ZAUFANIA

55%
Pozytywne opinie

44%
Znana marka sklepu

38%
Widoczność danych kontaktowych

28%
Możliwość płatności za pobraniem

21%
Możliwość płatności za pośrednictwem znanych operatorów

NIP

13%
Widoczność numeru NIP

12%
Certyfikat SSL

4%
Dostępność w mediach społecznościowych

Źródło: Raport „Polaków portret własny. Bezpieczni na e-zakupach 2022". Odpowiedzi nie muszą sumować się do 100.

3. CO ROBIĆ, BY NIE WPAŚĆ W SIDŁA ZŁODZIEI, JEŚLI ZACZYNAMY ZAKUPY Z WIARYGODNEJ STRONY INTERNETOWEJ (NP. ZNANEGO PORTALU AUKCYJNEGO LUB SERWISU Z OGŁOSZENIAMI)?

- Dokładnie zapoznaj się z ofertą. Jeżeli w treści jest jakiś link, kierujący rzekomo do dokładniejszego opisu, sprawdź go szczególnie uważnie. Zwróć uwagę na pasek adresowy po kliknięciu w link – czy nie odsyła do jakiejś podejrzanej strony, znajdującej się w nieznanej domenie, albo czy nie pojawia się w nim łatwy do przeoczenia błąd literowy, ukrywający podszywanie się pod znany podmiot, np. aukcjje.cc, ogloszenja.pl.
- Sprawdź sprzedawcę. Pamiętaj, że długi czas jego działalności w serwisie sprzedażowym nie musi być gwarantem uczciwości – konto mogło zostać przejęte przez atakującego.

- Oceń pozostałe oferty sprzedającego – ich wiarygodność i spójność.
- Sprawdź, czy w aukcji nie pojawił się jakiś dodatkowy warunek zakupowy, np. prośby o zalogowanie się w innym miejscu, o pobranie i zainstalowanie jakiegoś oprogramowania albo o sfinalizowanie transakcji na innej stronie.
- Uważaj na pozornie opłacalne propozycje 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". Brzmią one uspokajająco, ale najczęściej niosą przykre konsekwencje dla ofiary, która uległa takim zagrywkom socjotechnicznym.
- Nie bój się pytać, jeżeli cokolwiek wydaje się podejrzane. W pierwszej kolejności poproś o wyjaśnienia samego sprzedającego, ale skonsultuj się także z bliskimi osobami, a także dedykowanymi zespołami bezpieczeństwa, które „na chłodno" ocenią znalezioną przez ciebie „gorącą" ofertę.

NISKA CENA... WYSOKIE RYZYKO

Zanim zrobisz zakupy – zbadaj wiarygodność sklepu. Możesz zweryfikować KRS/ CEIDG, dane adresowe, przeczytać opinie klientów, sprawdzić opcje dostawy i płatności. Jeśli coś wyda ci się podejrzane, prawdopodobnie takie jest!

4. CZY WARTO SPRAWDZAĆ OPINIE O SKLEPIE?

Zdecydowanie tak, ale równocześnie warto też sprawdzić, kto te opinie napisał. Na pierwszy rzut oka wydaje się to trudne, ale warto spróbować dokonać takiej weryfikacji, ponieważ wiodące, bezpieczne serwisy sprzedażowe uniemożliwiają fałszowanie opinii. Dlatego warto sprawdzić, czy strona internetowa (np. oppinnie.cc) lub same opinie nie zostały przygotowane przez atakujących.

Zwróćmy też uwagę na historię wystawianych opinii – jeśli istnieje w niej luka, np. najnowsze opinie pochodzą z ostatnich dwóch tygodni, potem następuje długa przerwa, a następnie wcześniejsze opinie są starsze niż rok – ograniczmy zaufanie.

Zawsze warto też skorzystać z wyszukiwarki, ponieważ jest szansa, że oszukani klienci zdążyli zostawić w sieci jakieś ostrzeżenie na temat sklepu, który wydał się nam interesujący.

5. JAKICH SYGNAŁÓW 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 wolno ignorować takich sygnałów.

Bardzo podejrzany jest również kontakt ze strony rzekomego banku w momencie, w którym realizujemy płatność, np. z prośbą o dodatkowe działania na naszym koncie. Podstawowa zasada brzmi: jeżeli masz wątpliwości, że dzwoni do ciebie ktoś z banku (nawet z numeru, który wyświetla się jako numer banku), przerwij rozmowę i samodzielnie podejmij próbę kontaktu z bankiem.

JEDYNA TAKA OKAZJA! (BY ZOSTAĆ OSZUKANYM...)

Wezwanie do szybkiego działania to częsty element działania cyberzbójów. Zabiegi socjotechniczne mają cię skłonić do podjęcia pochopnej decyzji, której skutki mogą być dramatyczne.

6. JAKIE INNE SYGNAŁY POWINNY WZBUDZIĆ NASZĄ CZUJNOŚĆ W TRAKCIE ZAKUPÓW?

- Zwracaj uwagę na wyjątkowe zniżki, niezwykłe okazje, a także „gorące" oferty limitowane czasowo, skłaniające do jak najszybszego działania. Jeżeli „super rabat" wygląda na niezwykle korzystny, a na dodatek dostępny jest „tylko dzisiaj", zachowaj szczególną czujność – bardzo atrakcyjna korzyść połączona z atmosferą pośpiechu to częsty zabieg socjotechniczny stosowany przez oszustów.
- Uważaj na próby podsunięcia ci legalnej płatności w fałszywym sklepie (oszust równolegle dokonuje realnych zakupów na swoje dane, natomiast nieświadomy internauta płaci za niego). To bardzo niebezpieczna technika, która może uśpić nawet doświadczonego internautę. Sprawdź też, czy płatność, której dokonujesz, wykonywana jest faktycznie na rzecz podmiotu, w którym dokonujesz zakupu. W przeciwnym wypadku towar może zostać wysłany do oszusta, a nie do ciebie.
- Zwracaj uwagę na to, o co prosi sprzedający. Prośba o login do Facebooka czy do bankowości mobilnej powinna spowodować natychmiastowe opuszczenie strony z takiego „sklepu".
- Szczególną uwagę zwróć 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 twojego banku.

7. CZY NIEZADOWOLENIE Z ZAKUPÓW ONLINE ZAWSZE WYNIKA Z NIEUCZCIWOŚCI SPRZEDAWCY?

Nie, często sprzedawca jest uczciwy, wykazuje dobrą wolę i prowadzi uczciwą działalność biznesową. Zdarzają się jednak sytuacje losowe, kiedy coś pójdzie niezgodnie z dobrymi chęciami – dostajemy towar uszkodzony lub niezgody z zamówieniem, pojawia opóźnienie w dostawie lub przestępcy włamią się na stronę uczciwego sprzedawcy i wykorzystają ją do dokonania oszustwa.

Czasami też sami, szukając oszczędności, decydujemy się na kupno towaru mniej znanej marki, co może powodować rozczarowanie jakością otrzymanego produktu lub opłaconej usługi.

Zdarza się też, że na rozpoznawalnych i sprawdzonych już przez nas portalach sprzedaży pojawia się nieuczciwa oferta. Wykorzystując tę technikę, atakujący próbują przemycić swoje oszustwo w gąszczu legalnych i uczciwych ogłoszeń. Ma to na celu utrudnienie przeciwdziałania nadużyciom w tym zakresie, a także opóźnienie wykrycia oszustwa, tak by złapała się na nie jak największa liczba ofiar. Dedykowane zespoły bezpieczeństwa starają się jednak skutecznie oznaczać i usuwać takie ogłoszenia.

TO TYLKO LITERÓWKA...

Drobny błąd, który może kosztować nas oszczędności życia. Recepta to uważne sprawdzanie adresu strony – szczególnie, gdy zostaliśmy już przekierowani do płatności.

8. CO ZROBIĆ, GDY ZORIENTUJEMY SIĘ, ŻE ZROBILIŚMY ZAKUPY W FAŁSZYWYM SKLEPIE?

Jak najszybciej poinformuj dostawcę płatności, czyli bank, w którym prowadzony jest twój rachunek bądź karta płatnicza. Następnie zgłoś incydent na stronie **incydent.cert.pl** oraz policji. Dzięki tym działaniom zwiększysz 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 oraz w mediach społecznościowych organizacji broniących praw konsumentów.

9. CO NAM GROZI, GDY DOKONAMY ZAKUPU W FAŁSZYWYM SKLEPIE INTERNETOWYM?

Niestety sama utrata kwoty, którą zapłaciliśmy za rzekomy produkt czy usługę, których nigdy nie otrzymamy, to jeszcze stosunkowo niewielki problem. W przypadku gorszego scenariusza wydarzeń stracimy wszystkie oszczędności, a jeśli w procesie zakupowym zainstalowaliśmy dodatkowo złośliwe oprogramowanie podsunięte przez przestępców, możemy też utracić wrażliwe dane. Dlatego w czasie zakupów online nigdy nie ignorujmy nawet najmniejszych niepokojących sygnałów.

10. CZY JEST SZANSA NA ODZYSKANIE PIENIĘDZY STRACONYCH W TRAKCIE ZAKUPÓW ONLINE?

W przypadku, gdy nastąpiła płatność 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 zazwyczaj musimy poczekać aż organy ścigania zatrzymają sprawców i wtedy próbować odzyskać utracone środki.

WŁĄCZ SIĘ W WALKĘ Z OSZUSTWAMI. MASZ NA TO REALNY WPŁYW!

Zgłaszając oszustwa zakupowe, pomagasz sobie i innym, którzy również narażeni są na utratę wrażliwych danych lub pieniędzy. Wspólnie nie dajmy się oszukać!
Podejrzane SMS-y, strony lub wiadomości mailowe:

prześlij na nr:
799 448 084

lub zgłoś przez formularz na stronie:
incydent.cert.pl

lub wyślij email na adres:
cert@cert.pl

Zespół CERT Polska uważnie weryfikuje każde zgłoszenie zagrożenia cyberbezpieczeństwa. Dzięki takim zgłoszeniom wpisaliśmy na listę ostrzeżeń już niemal **1300 szkodliwych stron** i zablokowaliśmy blisko **2 miliony prób wejścia** na fałszywe strony wyłudzające dane lub podszywające się pod legalne sklepy internetowe. We współpracy z odpowiednimi organami doprowadziliśmy też do skutecznego zatrzymania i skazania wielu oszustów.


CERT.PL
NASK