OUCH! Listopad 2021

Bezpieczne zakupy online

Mały krokami zbliża się sezon świąteczny. Wkrótce wiele ludzi będzie chciało zakupić prezenty na święta, a wielu z nas będzie robić to przez internet. Niestety, cyberprzestępcy również będą w tym czasie wyjątkowo aktywni, tworząc fałszywe sklepy internetowe i inne oszustwa związane z zakupami online. Te działania w głównej mierze mają na celu kradzież środków finansowych. Dowiedz się, jak znaleźć odpowiednie oferty i nie stać się ofiarą wyłudzenia.

Fałszywe sklepy internetowe

Przestępcy tworzą fałszywe sklepy internetowe, które swoim wyglądem przypominają te oficjalne, prawdziwe sklepy, ponadto używają nazw znanych sklepów lub marek. Gdy szukasz najlepszych ofert online, możesz znaleźć się na stronie fałszywego sklepu internetowego. Kupując w takich miejscach, musisz się liczyć z tym, że otrzymasz nieoryginalny przedmiot, a w najgorszym przypadku, że go w ogóle nie otrzymasz. Podejmij kroki, aby się zabezpieczyć:

- Jeśli to możliwe, kupuj w takich sklepach internetowych, które już znasz i w których robiłeś wcześniej zakupy. Aby o nich nie zapomnieć, możesz dodać te sklepy do zakładek przeglądarki.
- Bądź ostrożny, uważaj na reklamy w mediach społecznościowych i ceny, które są znacznie niższe niż ceny tych samych produktów dostępnych w innych sklepach internetowych. Jeśli oferta wygląda za dobrze, aby była prawdziwa, może to być oszustwo.
- Zachowaj ostrożność w przypadku witryn, które nie mają możliwości kontaktu, brak na nich regulaminu sklepu, mają niepełne formularze kontaktowe lub korzystają z prywatnych adresów e-mail.
- Bądź czujny, jeśli witryna wygląda tak samo, jak inna, z której korzystałeś w przeszłości, ale nazwa domeny lub nazwa sklepu są inne. Możesz być przyzwyczajony do zakupów w serwisie aukcyjnym Allegro, którego adres to www.allegro.pl, ale bądź ostrożny bo możesz trafić na fałszywą witrynę wyglądającą podobnie, ale z adresem np. www.alegroo.pl.
- Wpisz nazwę sklepu internetowego lub jego adres w wyszukiwarce, aby sprawdzić jakie są w internecie opinie o tym sklepie. Szukaj terminów takich jak "scam", "oszustwo", "nigdy więcej", "fake", "fałszywy".
- Chroń swoje konta online, używając unikalnego, silnego hasła do każdego z kont. Masz trudności z zapamiętaniem haseł? Skorzystaj z menedżera haseł.

Oszuści na prawdziwych stronach internetowych

Zachowaj czujność nawet podczas zakupów na zaufanych stronach. Sklepy internetowe często oferują produkty sprzedawane przez osoby trzecie - osoby fizyczne lub firmy - które mogą mieć nieuczciwe zamiary. Takie strony internetowe funkcjonują jak bazarki, na których niektórzy sprzedający są godni zaufania a inni mniej.

- Sprawdź opinie każdego sprzedawcy przed złożeniem zamówienia.
- Uważaj na sprzedawców, którzy niedawno założyli swoje konto, nie mają opinii lub sprzedają przedmioty po wyjątkowo niskich cenach.
- Zapoznaj się z polityką sklepu internetowego dotyczącą zakupów od osób trzecich.
- W razie wątpliwości kupuj przedmioty sprzedawane bezpośrednio przez sklep internetowy, a nie przez sprzedawców zewnętrznych.
- Nawet w przypadku prawdziwych dostawców, przed dokonaniem zakupu upewnij się, że zapoznałeś się z zasadami gwarancji i zwrotów sprzedawcy.

Płatności online za zakupy

Regularnie przeglądaj wyciągi z karty kredytowej, aby zidentyfikować podejrzane transakcje. Jeśli to możliwe, włącz opcję powiadamiania w aplikacji, SMS-em lub wiadomością e-mail o nowym obciążeniu karty. Jeśli znajdziesz podejrzaną aktywność na koncie, zgłoś to w banku. Do płatności online używaj kart kredytowych zamiast debetowych. Karty debetowe pobierają pieniądze bezpośrednio z konta bankowego. Jeśli zostaniesz okradziony, będzie Ci znacznie trudniej odzyskać pieniądze. Usługi płatności elektronicznych lub e-portfele, takie jak PayPal, PayU są również bezpieczniejszą opcją w przypadku zakupów online, ponieważ nie wymagają bezpośredniego podania numeru karty kredytowej sprzedawcy. Unikaj stron internetowych, które akceptują płatności tylko w kryptowalutach lub wymagają niejasnych metod płatności.

To, że sklep internetowy ma profesjonalny wygląd, nie oznacza, że jest prawdziwy. Jeśli strona wzbudza jakiekolwiek podejrzenia, nie korzystaj z niej. Zamiast tego udaj się na stronę, której używałeś w przeszłości. Być może nie znajdziesz tam oferty, która jest tak korzystna, jak przedstawiona na podejrzanej stronie, ale jest bardziej prawdopodobne, że unikniesz oszustwa i otrzymasz towar.

Redaktor gościnny

Mark Orlando jest dyrektorem ds. bezpieczeństwa, który odpowiadał za ochranę sieci w Pentagonie, Białym Domu oraz u licznych klientów z sektora prywatnego. Obecnie jest prezesem i współzałożycielem firmy Bionic zajmującej się cyberbezpieczeństwem, a także instruktorem i autorem kursów w Instytucie SANS. [Twitter: @markaorlando]

Źródła

Tworzenie haseł w prosty sposób: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Oszustwa bazujące na wiadomościach tekstowych: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Oszustwa za pośrednictwem mediów społecznościowych: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz