Cyberdefence 24

01.06.2020

„NIE DAJ SIĘ ZROBIĆ W BAMBUKO", CZYLI KRÓTKI PORADNIK O TYM JAK NIE PAŚĆ OFIARĄ PRZESTĘPCÓW PRZY ZAKUPACH ONLINE

Co zrobić by nie wpaść w sidła złodziei kupując sieci? Rady na temat prawidłowych zachowań w sieci przy dokonywaniu transakcji przygotował dla konsumentów CERT Polska.

Zakupy online są szybkie, sprawne i przyjemne. Jednak, aby były one bezpieczne i nie naraziły nas nie tylko na szkody finansowe, ale również na możliwość utraty danych konieczne jest podchodzenie do nich „z głową" na karku. Jak nie stać się ofiarą? To pytanie nurtuje niejednego ostrożnego użytkownika sieci. CERT Polska przygotował krótki poradnik dla użytkowników i zbierał w nim najważniejsze i chyba najbardziej podstawowe zasady zakupów online. Czy ich stosowanie uchroni nas w 100%? Niestety nie, ale może znacznie ograniczyć ryzyko, że staniemy się ofiarą.

„Jeżeli w treści jest jakiś link, kierujący rzekomo do dokładniejszego opisu, sprawdźmy to dokładnie" – radzi CERT Polska. Wystarczy poświęcić zaledwie chwilę i sprawdzić pasek adresowy. W szczególności powinniśmy zwrócić uwagę, czy nie znajduje się on w nieznanej domenie, nie zawiera literówek w adresie mających upodobnić go do innych podmiotów – np. znanych portali aukcyjnych czy stron z ogłoszeniami.

„Sprawdź sprzedawcę. Pamiętaj, że czas jego obecności w serwisie nie powinien być gwarantem uczciwości – jego konto mogło zostać przejęte przez atakującego". Szczególnie nasza uwaga powinna być wyostrzona na dodatkowe warunki sprzedaży jak np. prośba o zalogowanie się w innym miejscu, pobranie czy zainstalowanie czegoś. Sygnałem alarmowym powinno być również prośba o sfinalizowanie transakcji w innym miejscu. Zawsze warto sprawdzić opinię o sklepie w sieci. Naszą uwagę powinno szczególnie przyciągnąć znaczna luka w wystawianiu ocen – np. roczna przerwa w wystawianiu jakichkolwiek ocen. Jeśli wyszukiwanie pokazało nam również liczne opinie o tym, że klienci zostali oszukani warto się im przyjrzeć.

„Miejmy się na baczności" – kiedy? Zawsze wtedy, kiedy zachętą do zakupów jest oferta okraszona atrakcyjną promocją, kuponem rabatowym które dostajemy poprzez media społecznościowe czy pocztę elektroniczną. Często super promocje to sposoby na łowienie ofiar przez cyberprzestępców. CERT Polska w swoim krótkim poradniku wskazuje na szereg rzeczy, które powinny zwrócić naszą uwagę:

- **Rodzaj asortymentu w sklepie –** jeśli w wyszukiwarce pojawi się nam oferta sklepu, z produktem którego szukamy warto sprawdzić jakiego rodzaju produkty są w nim sprzedawane. Jeśli „rozrzut" produktów jest zbyt duży (np. szukamy butów sportowych a sklep oferuje również maszyny budowlane czy terakotę) może on budzić spore wątpliwości.
- **Wygląd strony internetowej –** czy wygląda jakby została stworzona „na kolanie"? Zwróć uwagę czy nie ma w niej błędów ortograficznych, gramatycznych czy jest pisane poprawną

polszczyzną. Sklep powinien posiadać również regulamin, jasny sposób dostarczania zamówienia, sposób płatności oraz warunki zwrotu towaru.
- **Dane sprzedawcy –** nie tylko przy kosztownych zakupach warto sprawdzić czy firma podana na stronie widnieje w KRS. Możemy również sprawdzić jej dane teleadresowe - czy podany adres istnieje i co się pod nim mieści – wystarczy nam do tego przeglądarka.
- **Kontakt ze sprzedawcą –** jeśli jest wskazany kontakt do sprzedawcy, wykorzystaj go i pobaw się w detektywa. Jeśli osoba po drugiej stronie telefonu nie będzie znała odpowiedzi na nasze pytania, podawała sprzeczne wiadomości czy będzie się irytował odpowiadając na nasze pytania – dla własnego bezpieczeństwa zrezygnuj z ze zrobienia zakupów w tym sklepie.

Pamiętajmy, że przestępcy stosują przeróżne chwyty, aby nakłonić nas do „zakupu". CERT zwraca uwagę na „popychacze" do zakupu. Cóż to takiego? To zabiegi socjotechniczne, które mają uśpić naszą czujność np. „super rabat – ale tylko dzisiaj". Ale powinniśmy również uważać czy płatność, którą dokonujemy jest w rzeczywistości faktycznie wykonywana na rzecz tego podmiotu, u którego chcemy nabyć produkt. Natychmiastowe przerwanie transakcji powinno nastąpić w momencie, kiedy sprzedawca poprosi nas o login do mediów społecznościowych czy bankowości mobilnej.

Reagujmy również na to co podpowiada nam nasz komputer – antywirus szaleje? Przeglądarka podpowiada, że strona jest niebezpieczna? Nie bagatelizuj tych sygnałów.

A co, jeśli padniemy ofiarą przestępcy?

Utrata środków finansowych za produkt, którego nigdy nie dostaniemy to tyko próbka kłopotów, które mogą nas spotkać. CERT Polska ostrzega o możliwości utraty oszczędności czy utrata danych, jeśli podczas „zakupów" zostanie zainstalowane na urządzeniu złośliwe oprogramowanie.

Jeśli w miarę szybko zorientujemy się, że daliśmy się „wykiwać" skontaktujmy się z bankiem, a następnie zgłośmy incydent na stronie incydent.cert.pl. Zespół CERT Polska radzi również, aby zgłosić się na policję. Zadbajmy również o bezpieczeństwo innych użytkowników sieci i zostawmy stosowną informację na serwisach z opiniami zarówno w mediach społecznościowych jak i na dedykowanych temu stronach.

W zależności od tego jakiego sposoby płatności użyliśmy odzyskanie płatności może być mniej lub bardziej problematyczne. Możemy poprosić o pomoc bank i skorzystać z mechanizmu tzw. obciążenia zwrotnego (chargeback) składając reklamację. Jednak przy najbardziej pesymistycznym scenariuszu, kiedy płatności dokonamy przy pomocy przelewu niewykluczone, że będziemy musieli czekać aż organy ścigania zatrzymają oszusta.