POLICJA KUJAWSKO-POMORSKA

https://kujawsko-pomorska.policja.gov.pl/kb/informacje/wiadomosci/121147,Bezpieczne-zakupy-w-sieci-Zachowajmy-czujnosc-by-nie-pasc-ofiara-oszustow.html
2022-05-18, 04:22

BEZPIECZNE ZAKUPY W SIECI. ZACHOWAJMY CZUJNOŚĆ, BY NIE PAŚĆ OFIARĄ OSZUSTÓW

Data publikacji 23.11.2021

Apelujemy o zachowanie ostrożności podczas zakupów w Internecie. Niestety pomysłowość i chciwość przestępców "nie zna granic". Płatności pobraniowe dokonywane powinny być tylko z zaufanych źródeł. Pod żadnym pozorem nie należy otwierać nieznanych nam linków, ponieważ mimo braku jakichkolwiek "objawów" w naszym komputerze zainstalowane zostaje oprogramowanie szpiegujące, którym wykraść można hasła do naszego konta bankowego itp. Przed zalogowaniem się zawsze zwracajmy uwagę czy dana witryna jest zaufana, a w pasku adresu znajduje się ikonka zamkniętej kłódki.

Wykonując transakcję w sieci, bez względu na to jakiego towaru dotyczą, musimy być ostrożni i kierować się zasadą ograniczonego zaufania, gdyż na popularnych portalach aukcyjnych lub społecznościowych nie brakuje nieuczciwych sprzedawców, którzy w łatwy i szybki sposób chcą osiągnąć zysk.

Kupując przez Internet należy zachować chociażby podstawowe środki ostrożności:

1. Podana cena produktu - dużo niższa cena niż w innych sklepach może sugerować ryzyko oszustwa.

2. Przed zakupem upewnij się kim jest osoba sprzedająca - mając pozytywne komentarze możemy być pewniejsi zakupu.

3. Przy płaceniu kartą kredytową zwracajmy uwagę, czy połączenie internetowe jest bezpieczne i czy przesyłane przez nas dane nie zostaną wykorzystane przez osoby nieuprawnione. Na stronie powinien pojawić się symbol zamkniętej kłódki, a na początku adresu – literki „https”.

4. Sprawdzajmy od kiedy konto sprzedawcy widnieje w serwisie i ilu użytkowników korzystało z jego usług.

5. Za każdym razem czytajmy regulamin sklepu i opis aukcji serwisu, z którego korzystamy.

6. Domagajmy się potwierdzenia nadania przesyłki, nie wpłacajmy pieniędzy przed potwierdzeniem wygranej licytacji.

7. Pamiętajmy, że mamy możliwość uzgodnienia sposobu płatności za wybrany przedmiot. Brak możliwości płatności przy odbiorze może sugerować w takich „sklepach” jedyną możliwą formę zapłaty przelewem na wskazane konto bankowe. Najbezpieczniej jest wybrać opcję „za pobraniem”.

8. Nie kasujmy korespondencji ze sprzedającym – w przypadku oszustwa jest ona dowodem potwierdzającym zakup.

9. Sprawdzajmy otrzymaną przesyłkę – czy towar jest zgodny z zamówieniem.

Jeśli mimo zachowania środków ostrożności, nie dostaniemy zamówionego towaru lub otrzymany produkt jest niezgodny z zamówieniem należy:

- jak najszybciej poinformować administratorów ds. bezpieczeństwa danego serwisu,
- zachować wszystkie dokumenty związane z transakcją, tj. dowód przelewu na konto bankowe, korespondencję mailową, jak również całą korespondencję ze sprzedawcą,

- zgłosić się wraz z powyższymi dokumentami do najbliższej jednostki policji.

Jeżeli zapłacimy za towar, a nie otrzymaliśmy go to z pewnością mamy do czynienia z oszustwem. Poinformuj o tym policję. Kodeks Karny za oszustwo przewiduje karę nawet do 8 lat pozbawienia wolności.

Oszuści działający w Internecie wymyślają nowe metody wyłudzania pieniędzy. Przełamują zabezpieczenia kont na portalach społecznościowych i podszywają się pod ich właścicieli. Działają jako pracownicy banku, którzy dzwonią z prośbą o zainstalowanie aplikacji antywirusowej. Zachowajmy czujność i nie dajmy się oszukać!

Uzyskiwanie danych personalnych lub danych do logowania w różnych serwisach, poprzez wprowadzanie w błąd lub za pomocą złośliwego oprogramowania, to dziś częste sposoby działania oszustów.

Policjanci odnotowują również przypadki oszustw na tzw. BLIKA. Oszuści, którzy wymyślili tę metodę, działają wyjątkowo bezczelnie. Najpierw odzywają się do potencjalnej ofiary z przejętego lub fikcyjnego konta na popularnym portalu społecznościowym, mającego rzekomo należeć do któregoś ze znajomych. W prywatnej wiadomości proszą ofiarę o pożyczenie pieniędzy. Pozornej wiarygodności całej sytuacji dodaje fakt, iż rzekomy znajomy nie prosi o gotówkę, a przedstawia zmyśloną historię o tym, że akurat jest przy kasie w sklepie, zapomniał portfela i jedynym ratunkiem jest podanie przez ofiarę kodu BLIK. Niestety, oszust wcale nie jest tym za kogo się podaje, a jedynie na czym mu zależy to wyciągnięcie od nas jak największej kwoty.

Pamiętajmy, że nie należy udostępniać nikomu danych do logowania w bankowości elektronicznej i mobilnej, haseł do konta. Nie powinniśmy także otwierać przesłanych linków, nie znając ich zawartości oraz instalować dodatkowych oprogramowań na urządzeniach, z których następuje logowanie do banku. Zwłaszcza jeśli wymaga tego rzekomy „doradca” inwestycyjny. Nie należy autoryzować przelewów, których sami nie wykonujemy. Podejrzewając, że ktoś próbuje dokonać oszustwa, należy powiadomić policję.

Autor: kom. Lidia Kowalska
Publikacja: kom. Lidia Kowalska