POLICJA ŚLĄSKA

https://slaska.policja.gov.pl/kat/informacje/wiadomosci/312522,Ostrzezenie-dla-klientow-bankow-w-zwiazku-z-pojawiajacymi-sie-oszustwami-w-inter.html
2021-11-28, 22:07

OSTRZEŻENIE DLA KLIENTÓW BANKÓW W ZWIĄZKU Z POJAWIAJĄCYMI SIĘ OSZUSTWAMI W INTERNETOWYCH SERWISACH OGŁOSZENIOWYCH

Data publikacji 27.05.2021

Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegają klientów banków przed pojawiającymi się oszustwami w internetowych serwisach ogłoszeniowych. FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP coraz częściej odnotowuje aktywność przestępców nakierowaną na wyłudzanie danych i środków od osób fizycznych i podmiotów sprzedających na internetowych serwisach ogłoszeniowych.

Masowo dochodzi do wyłudzeń informacji o numerach kart płatniczych lub danych dostępowych do usług bankowości elektronicznej od osób sprzedających (wystawiających ogłoszenia) na przykład na portalu OLX. Przestępcy wyłudzają dane pod pretekstem przekazania zapłaty za towar lub usługę. Robią to poprzez wysłanie linku do fałszywej strony WWW, na której pokrzywdzony podaje swoje dane. **Komenda Główna Policji oraz FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegają klientów banków przed niebezpieczeństwem związanym z tego typu atakami.**

Jak przebiega atak?

1. Sprzedający wystawia produkt lub usługę na portalach ogłoszeniowych, np. OLX.

2. Do sprzedającego odzywa się osoba rzekomo zainteresowana zakupem i wypytuje o szczegóły. Kontakt najczęściej następuje przez komunikator WhatsApp.

3. W trakcie prowadzonej rozmowy, potencjalnie zainteresowany kupujący - przestępca proponuje sprzedającemu płatność poprzez nową usługę.

4. Sprzedający otrzymuje link do strony, na której ma podać dane swojej karty lub dane do logowania do usług bankowości elektronicznej. Link może być przesłany:

- bezpośrednio w rozmowie przez komunikator,
- w wiadomości e-mail lub SMS podszywającej się np. pod portal ogłoszeniowy lub usługę kurierską.

5. Klikając w przesłany link, otwiera się specjalnie przygotowana strona, wyglądająca dla sprzedającego wiarygodnie, gdyż może tam zobaczyć np. zdjęcie i cenę swojego produktu.

Na tej stronie znajduje się ponadto miejsce do wpisania:

- karty płatniczej (dane posiadacza karty, pełen numer karty, CVV, data ważności, kod 3DS)

- lub danych dostępowych do bankowości elektronicznej (login, hasło, SMS kody).

6. Po podaniu powyższych danych nie dochodzi do sprzedaży i dodatkowo sprzedający traci swoje środki, stając się pokrzywdzonym.

Co zatem robić by chronić swoją tożsamość i pieniądze?

Prosimy, aby zawsze pamiętać, że:

- dane dostępowe do konta, dane karty płatniczej oraz dane osobowe to informacje, które powinny być zawsze chronione - nie należy ich udostępniać osobom nieuprawnionym! Ujawniając je narażamy się na utratę swoich pieniędzy, a nawet zaciągnięcie kredytu lub pożyczki;
- jeśli ktoś wywiera na Państwa presję i wymusza podjęcie natychmiastowej decyzji lub działań – **proszę zastanowić się dwa razy**, to może być próba ataku;
- warto upewnić się w innym kanale komunikacji (np. oficjalny numer telefonu podany w Internecie), że nadawca rzeczywiście wysłał do Państwa wiadomość – zarówno w przypadku wiadomości e-mail, jak i wiadomości SMS lub wysyłanych w komunikatorach, nazwę nadawcy można dowolnie zmodyfikować i w ten sposób podszyć się pod prawdziwą firmę;
- warto zweryfikować wiadomość pod kątem poprawności językowej (np. czy jest napisana poprawną polszczyzną, nie zawiera literówek lub innych błędów).

Jeśli zostaliście Państwo pokrzywdzeni w wyniku przeprowadzenia takiego ataku, prosimy o niezwłoczne złożenie zawiadomienia o popełnieniu przestępstwa Policji oraz skontaktowanie się z Państwa bankiem. Jeśli posiadacie Państwo relacje biznesowe w kilku bankach, warto poinformować wszystkie o zdarzeniu.

(Komenda Główna Policji, FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP/ mw)