Kradną pieniądze z kont bankowych - policja ostrzega

11-02-2021

Fot: Pixabay.com

W ostatnim czasie do Komendy Powiatowej Policji w Dzierżoniowie zgłosiło się kilka osób, których konta bankowe zostały okradzione. Przestępcy wymyślają cały czas nowe metody. Osoby okradzione mogły tego uniknąć. Bądźmy czujni!

Przestępcy są bardzo kreatywni aby nas okraść. Co ciekawe w ostatnio funkcjonujących przestępstwach, posiadacze kont bankowych sami udostępniają dane potrzebne oszustowi. Dwie najbardziej popularne metody to na „Portal ogłoszeniowy” i „Na pracownika banku”

Na czym to polega oszustwo na „Portal ogłoszeniowy”:

- Wystawiasz coś na portalu ogłoszeniowym. Znajduje się kupiec. Twierdzi, że chce zapłacić za wystawiony do sprzedaży towar, a pieniądze możesz odebrać po wejściu w link. W ten sposób oszust zastawia na Ciebie pułapkę. Teraz oszust wysyła Ci linka. Klikasz i trafiasz na stronę łudząco podobną do strony portalu ogłoszeniowego. Na stronie jest formularz z prośbą o podanie danych Twojej karty i stan Twojego konta. Wypełniasz formularz. Oszust ma już prawie wszystko żeby Cię okraść.

- Przychodzi do Ciebie SMS z banku, z kodem do autoryzacji. Ty nie czytasz go uważnie i wpisujesz kod do formularza. W SMS-ie napisaliśmy, że autoryzujesz dodanie Twojej karty do Google Pay lub Apple Pay. Oszust Cię okrada. Płaci Twoją kartą za pomocą aplikacji płatniczej lub wypłaca nią gotówkę w bankomacie”. Koniec. Twoje konto jest puste.

Jak uniknąć oszustwa:

- czytaj SMS-y od Banków. Zwróć uwagę na to, co autoryzujesz;
- poznaj zasady bezpieczeństwa swojego banku i stosuj się do nich gdy korzystasz z portali aukcyjnych miej ograniczone zaufanie do potencjalnych kontrahentów;
- rozliczaj się bezpośrednio przez dany portal, unikaj bezpośrednich transakcji, uważaj na próby nawiązania kontaktu poza portalem, np. przez WhatsApp czy Messenger
- zobacz instrukcje płatności portali ogłoszeniowych;
- oszuści mogą podrobić stronę portalu aukcyjnego – tak samo jak i każdą inną stronę, również naszą, dlatego zwracaj uwagę na adres widoczny w przeglądarce.
- zwróć uwagę na poprawność językową strony, na której przekazujesz dane karty. Fałszywe strony często zawierają błędy, są napisane niegramatycznie.

Na czym to polega oszustwo na „Pracownika banku”

- oszuści podszywają się pod pracowników banków. Dzwonią do klientów z numerów bardzo podobnych do numeru infolinii i informują, że bank udaremnił nieuprawnioną wypłatę pieniędzy z konta. Aby zapobiec takim sytuacjom w przyszłości proszą o zainstalowanie na smartfonie pewnej aplikacji. W rzeczywistości jest to narzędzie do przejęcia kontroli nad naszym telefonem i hasłami bankowości mobilnej. Niektórzy podejrzliwi klienci po rozmowie z oszustem kontaktują się z prawdziwą infolinią banku. Wtedy okazuje się, że żadna taka sytuacja nie miała miejsca;
- pracownicy banku nigdy nie proszą podczas rozmowy o login lub hasło do bankowości internetowej;
- pracownicy banku nigdy nie proszą o zainstalowanie dodatkowego oprogramowania lub uzyskanie zdalnego dostępu do komputerów klientów;
- pracownicy Banku nigdy nie proszą o pełen numer karty i kod CVV;
- jeśli masz wątpliwości czy rozmawiasz z pracownikiem Banku - rozłącz się - sprawdź numer na stronie internetowej i oddzwoń.

Bezpieczeństwo naszych pieniędzy w dużej mierze zależy od nas samych!

kom. Marcin Ząbek, KPP w Dzierżoniowie