Uważaj na oszustwa typu „na wnuczka”
– Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP,
Centralnego Biura Zwalczania Cyberprzestępczości oraz Komendy Głównej Policji
z dnia 27 lutego 2023 r.

Policja i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich odnotowują przypadki oszustw z wykorzystaniem zaawansowanej manipulacji polegającej na podszywaniu się pod osoby bliskie np. pod wnuczka lub pod inne osoby będące przedstawicielami instytucji zaufania publicznego, w tym policjantów czy pracowników banków, wywołując silny stan niepokoju w celu wyłudzenia pieniędzy.

Cechą charakterystyczną opisanych działań przestępczych jest z wykorzystaniem zaawansowanej socjotechniki podszycie się pod członka rodziny lub przyjaciela, który się znalazł w trudnej sytuacji i potrzebuje natychmiastowej pomocy finansowej. Przestępcy podszywają się również pod przedstawicieli instytucji zaufania publicznego takich jak Policja lub banki informując o zagrożeniu pieniędzy ulokowanych przez klienta i potrzebie podjęcia natychmiastowych działań w celu ich zabezpieczenia przed kradzieżą. Przedstawione powyżej schematy działań przestępców należy traktować jako przykładowe, gdyż przestępcy rozwijając swój proceder tworzą nowe scenariusze działania oparte na fikcyjnych historiach. Cechami wspólnymi tego typu przestępstw są:

- kontakt telefoniczny;
- stosowanie manipulacji;
- podszycie się pod osobę bliską lub wzbudzającą zaufanie;
- wprowadzenie w stan silnych emocji wywołujących ograniczone postrzeganie rzeczywistości i błędną ocenę sytuacji;
- nakłanianie do wypłaty pieniędzy ze swojego rachunku bankowego.

Poniżej przedstawiamy przykładowe warianty działania przestępców.

Wariant I – „na wnuczka” – osobę bliską

Przestępcy nawiązując kontakt telefoniczny z potencjalną ofiarą, który może trwać nawet kilka godzin, swoje działania dzielą na kilka etapów:

- w pierwszym etapie oszust podszywając się pod osobę bliską lub jej znajomego buduje poczucie zagrożenia dla bliskiej osoby i wskazują na konieczność udzielenia bardzo pilnej pomocy finansowej;
- w drugim etapie oszust włącza do gry inną osobę, która odbierze pieniądze, aby rzekomo przekazać je zagrożonej osobie bliskiej;
- w trzecim etapie ofiara wypłaca pieniądze z kasy w banku i przekazuje je zgodnie z instrukcją podaną przez oszusta;
- alternatywnie dla powyższych etapów: drugiego i trzeciego przestępcy mogą wskazywać potrzebę przelania pieniędzy na podany przez nich rachunek bankowy.

Wariant II – „na policjanta” – przedstawiciela instytucji zaufania publicznego

Podobnie jak to ma miejsce w wariancie nr I przestępcy nawiązują kontakt z potencjalną ofiarą z wykorzystaniem telefonu:

- w pierwszym etapie oszust podszywając się pod policjanta lub inną osobę reprezentującą instytucję zaufania publicznego kontaktuje się budując poczucie zagrożenia i informując o wysokim ryzyku utracenia pieniędzy;
- w drugim etapie oszust wskazuje bezpieczną metodę ochrony pieniędzy przed złodziejami – może to być tzw. „bezpieczne konto";
- w trzecim etapie zmanipulowana ofiara przelewa pieniądze na wskazany przez oszusta „bezpieczny rachunek" lub może dokonać wypłaty pieniędzy w oddziale banku i wpłaceniu ich w bankomacie z wykorzystaniem kodu BLIK lub porzuceniu ich we wskazanym przez przestępców miejscu.

Kiedy ktoś dzwoni i próbuje wywierać na Tobie presję, wymuszając wypłatę pieniędzy, stosuj się do poniższych zasad:

1. zachowaj spokój;
2. nie wykonuj ślepo poleceń;
3. rozłącz się i weź kilka głębokich wdechów;
4. zweryfikuj opisaną sytuację:
   - w przypadku scenariusza „na wnuczka" - powiadom najbliższych o zdarzeniu – zweryfikuj przedstawioną Ci historię;
   - w przypadku scenariusza „na policjanta" – skontaktuj się z najbliższą jednostką policji lub instytucją, pod którą podszył się oszust;
5. Powiadom Policję o usiłowaniu popełnienia przestępstwa lub o jego popełnieniu.
6. Powiadom swój bank, dzwoniąc do niego na numer infolinii znajdującej się na stronie internetowej banku – nigdy nie korzystaj z numeru podanego przez oszustów podczas rozmowy.

Zachęcamy do zapoznania się z filmem edukacyjnym traktującym o oszustwach typu „na wnuczka" zrealizowanego przez Komendę Powiatową Policji w Żorach – link: https://youtu.be/INnelwiQqLc oraz dostępnym na stronie Policji https://zory.policja.gov.pl/k31/informacje/wiadomosci/353753,To-gra-o-Twoje-pieniadze.html

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego
Centralne Biuro Zwalczania Cyberprzestępczości
Komenda Główna Policji

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków lub ich klientów.