Oszuści dzwonią z numerów podszywających się pod banki lub inne instytucje zaufania publicznego

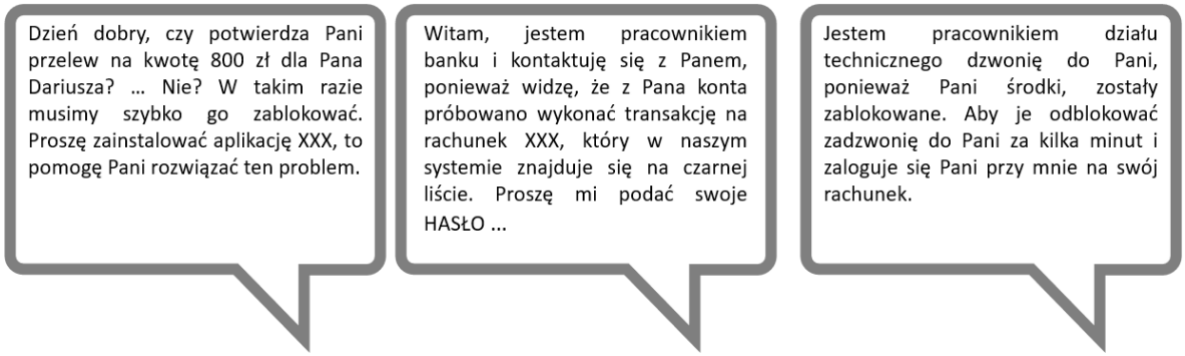
- Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
Centralnego Biura Zwalczania Cyberprzestępczości
Komendy Głównej Policji
z dnia 7 grudnia 2022 r.

Spoofing czyli fałszywe połączenia telefoniczne przestępców podszywających się pod banki lub inne instytucje zaufania publicznego takie jak Związek Banków Polskich, Urząd Komisji Nadzoru Finansowego, …!

Uważaj na połączenia telefoniczne, w których oszuści podszywają się pod pracownika banku lub inną osobę godną zaufania (np. pracownika Urzędu Komisji Nadzoru Finansowego, pracownika Zespołu Bezpieczeństwa Banków w Związku Banków Polskich, czy policjanta). Podczas fałszywego połączenia na Twoim telefonie może wyświetlić się numer telefonu lub nazwa zaufanej instytucji.

Przestępca będzie wpływał na Twoje emocje w celu wprowadzenia Ciebie w stan poczucia zagrożenia, zaniepokojenia, zmartwienia lub zaciekawienia. Oszust będzie rozmawiał z Tobą w języku ukraińskim, rosyjskim, rzadziej polskim.

Celem jest pozyskanie poufnych informacji (loginu i hasła do bankowości internetowej, kodów BLIK, danych dotyczących karty płatniczej) lub nakłonienie Ciebie do wykonania określonych czynności (np. zainstalowania aplikacji dającej przestępcom zdalny dostęp do Twojego komputera lub telefonu).
Poniżej przykłady rozmów:



Przestępcy kradną Twoje pieniądze m.in. poprzez wyprowadzanie oszczędności z rachunku bankowego, wykonanie transakcji kartowych czy pozyskanie pożyczki/kredytu z wykorzystaniem Twoich danych osobowych.

Jak się chronić by nie stracić pieniędzy?
Należy stosować się do kilku ważnych zasad:

1. nie podawaj loginu i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, daty ważności, imienia i nazwiska posiadacza karty) - prawdziwy przedstawiciel banku nigdy o to nie zapyta;
2. nigdy nie ujawniaj przychodzących na Twój telefon kodów do bankowości internetowej, kodów BLIK lub kodów 3D Secure wykorzystywanych do potwierdzenia przelewów lub innych płatności, w tym transakcji kartowych w Internecie;
3. zawsze czytaj treść SMS-ów jakie przychodzą na twój telefon lub komunikatów w aplikacji mobilnej banku. Z ich treści może wynikać, iż akceptujesz transakcję, którą realizują przestępcy;
4. za każdym razem czytaj treść otrzymywanych powiadomień, szczególnie podczas trwającej rozmowy z rzekomym konsultantem. Z ich treści może wynikać, iż dodajesz NOWE ZAUFANE urządzenie do swojego profilu (konta w bankowości elektronicznej), przy pomocy którego oszuści ukradną Tobie pieniądze lub zaciągną pożyczkę/ kredyt.

Jeśli rozmowa wzbudza niepokój lub wątpliwości:
rozłącz się, odczekaj minimum 30 sekund. Następnie połącz się z bankiem lub instytucją, której przedstawiciel dzwonił. Koniecznie wybierz oficjalny numer na klawiaturze numerycznej, nie oddzwaniaj z listy połączeń, które wyświetlają się na telefonie.

- zachowaj zdrowy rozsądek i zimną krew! Nawet jeżeli zostałeś poinformowany o potencjalnym zagrożeniu np. utrata środków, spokojnie przemyśl czy środki naprawdę mogą być w niebezpieczeństwie? Może jednak rozmawiasz z oszustem? Przerwij połączenie i skontaktuj się z bankiem zgodnie z powyższą zasadą;
- pamiętaj, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiasz z prawdziwym przedstawicielem banku;
- zawsze możesz zgłosić swoje podejrzenia do banku i jeśli doszło do popełnienia przestępstwa również zawiadom policję.

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.