15.11.2021

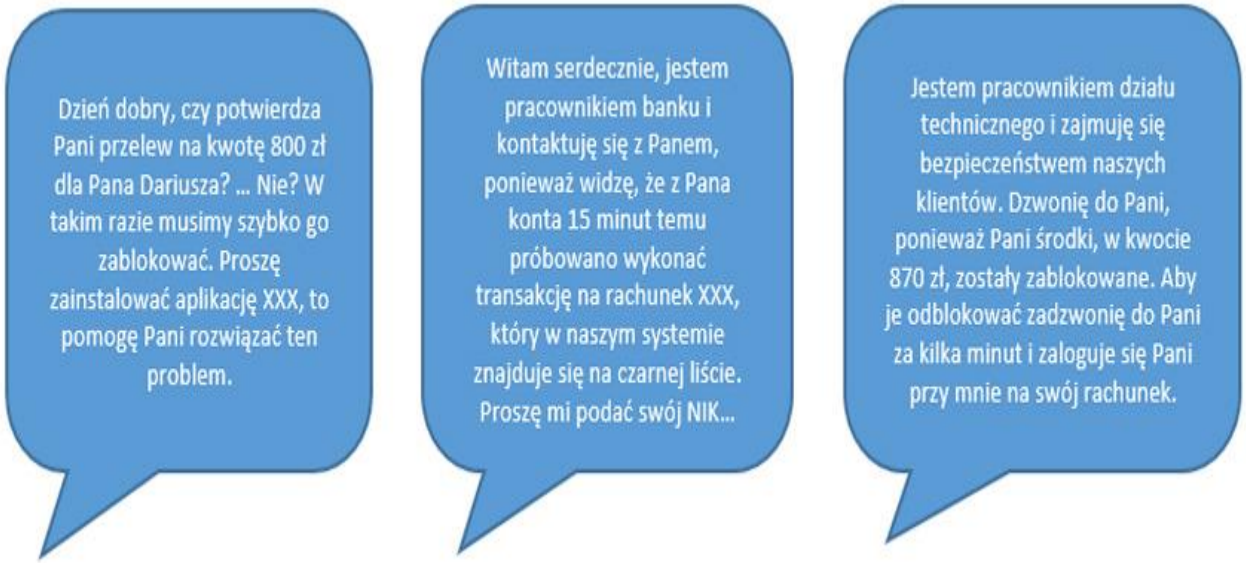
Uwaga – Fałszywe połączenia telefoniczne przestępców podszywających się pod banki!

Komunikat – ostrzeżenie – Komendy Głównej Policji, FinCERT.pl – BCC ZBP i Polskiej Izbie Informatyki i Telekomunikacji z dnia 15 listopada 2021 r.

W ostatnich miesiącach częstym sposobem dokonywania przestępstw na szkodę klientów banków jest wykorzystanie telefonicznego połączenia głosowego z osobą, która jest przekonywana, że rozmawia z pracownikiem banku lub inną osobą godną zaufania (np. policjantem).

Jest to rodzaj phishingu, nazywany vishingiem. Nazwa jest połączeniem słów „voice phishing", czyli phishing głosowy. Celem jest pozyskanie poufnych informacji lub nakłonienie ofiary do wykonania określonych czynności (np. zainstalowania aplikacji dającej przestępcom zdalny dostęp do komputera ofiary).

Najpopularniejsze przykłady rozmowy:



Przestępcy bardzo dobrze potrafią posługiwać się technikami manipulacji. Ponadto w celu uwiarygodnienia kontaktu, potrafią na telefonie ofiary wyświetlić numer telefonu lub nazwę zaufanej instytucji (np. banku).

Oszuści przed wykonaniem połączenia przygotowują się do rozmowy, tak by była ona wiarygodna i uśpiła czujność klienta. Przede wszystkim dokonują wyboru, za kogo poda się osoba dzwoniąca. Znane są przypadki, w których przestępcy podszywali się pod:

- doradców bankowych,
- dział techniczny lub bezpieczeństwa,
- pośrednika,
- przedstawiciela jednostek państwowych,
- znajomego itp.

Następnie przestępca wybiera numer telefonu z jakiego wykona połączenie, co skutkuje wyświetleniem na telefonie ofiary innego numeru telefonu lub nazwy kontaktu niż w rzeczywistości np. na telefonie Klienta wyświetli się numer infolinii jego banku. Pozwala na to technika określana jako spoofing numeru telefonu.

Czym jest spoofing?

Spoofing polega na podszywaniu się pod inne urządzenie lub innego użytkownika, może dotyczyć m.in. numeru telefonu, ale także adresu e-mail, IP, nadawcy SMS i innych. Przestępcy wykorzystują znane sobie technologie, które oprócz podmiany numeru telefonu pozwalają m.in. na:

- wybór płci osoby dzwoniącej,
- wybór pochodzenia,
- wybór akcentu,
- dodawanie efektów dźwiękowych
- zastosowanie menu głosowego.

Tak przygotowany przestępca wykonuje połączenie do ofiary i zgodnie z wcześniej ułożonym scenariuszem rozpoczyna rozmowę. Najgroźniejszą bronią takiego przestępcy jest dobra umiejętność stosowania socjotechniki. Poniżej kilka przykładowych metod socjotechnicznych, jakie mogą wykorzystywać przestępcy.

1. Osoba, która odbiera telefon, informowana jest o rzekomej transakcji na swoim rachunku bankowym, a dzwoniący prosi o potwierdzenie jej wykonania. Oczywiście żadnego obciążenia nie ma, ale zdezorientowana ofiara, myśląc, że ratuje swoje środki, odpowiada na pytania dzwoniącego. Ten tłumaczy, że ma to na celu zidentyfikowanie klienta, a w rzeczywistości zadawane są pytania daleko odbiegające od standardowej weryfikacji, a które mają na celu zdobycie wiedzy pozwalającej przestępcy np. na dostęp do konta ofiary.
2. Ten zabieg socjotechniczny w początkowej rozmowie podobny jest do tzw. „metody na wnuczka”. Ofiara informowana jest, że jej środki są w niebezpieczeństwie i jedynym sposobem ich ochrony jest podanie danych uwierzytelniających do bankowości elektronicznej lub dane karty płatniczej. Jeżeli je poda, to dopiero teraz środki naprawdę są zagrożone.
3. Osoba dzwoniąca przedstawia się jako doradca kredytowy, informuje, że zgodnie z rzekomo złożonym w nocy wnioskiem o pożyczkę pieniądze zostały przyznane, należy jednak dokończyć formalności. Ofiara oczywiście żadnego wniosku o kredyt nie składała. Dalej scenariusz jest już mocno zbliżony do poprzednich. Zdenerwowana osoba zaczyna odpowiadać na serię pytań, wierząc, że dzwoniący chce jej pomóc, a w rzeczywistości oszust wchodzi w posiadanie interesujących go danych i kończy rozmowę.

4. Zdarzyć się może, że przestępca nie musi nawet uciekać się do kłamstwa o potencjalnej operacji finansowej czy środkach w niebezpieczeństwie. Wystarczy, że na początku rozmowy przedstawi się np. jako pracownik instytucji państwowej i poprosi rozmówcę o identyfikację. Pomiędzy bardzo standardowymi pytaniami pojawiają się i te mniej oczywiste, na które ofiara często nie zwróci początkowo uwagi. Tym sposobem przestępca może wejść w posiadanie danych wrażliwych.
5. Przestępcy śledzą rynek i dostosowują często swoje działania również do obecnych trendów. O możliwości wyłudzeń poprzez połączenia głosowe informował również zbp.pl oraz policja.pl, przy okazji składania przez przedsiębiorców wniosków o subwencje z programu Tarczy Finansowej PFR.

Żeby wzmocnić wiarygodność przekazywanych informacji oszust podczas rozmowy będzie posługiwał się fachowym słownictwem np. bankowym. Może również wykorzystać dodatkowe kanały komunikacji, np. wysłać wiadomość e-mail. Nie oznacza to jeszcze, że jest tym, za kogo się podaje. Adres e-mail mógł znaleźć w Internecie, jeżeli ktoś wpisał go np. na portalu społecznościowym lub ofiara często adres e-mail podaje sama, a później po prostu o tym nie pamięta.

Scenariuszy jest znacznie więcej, wszystkie one mają cechę wspólną: wpłynięcie na emocje rozmówcy, w celu wprowadzeniu ofiary w stan zmartwienia, zaniepokojenia lub zaciekawienia. Tak, żeby podczas rozmowy była rozkojarzona i mniej uważna. To pozwala oszustom, którzy są osobami sprawnie posługującymi się metodami manipulacji, na pozyskanie interesujących ich danych osobowych i/lub finansowych ofiary.

Co dzieje się dalej? Zależy od tego, jakie informacje pozyskał przestępca. Cel jest jeden – zyski finansowe, m.in. poprzez pobieranie pożyczki na ofiary (dzięki pozyskaniu danych osobowych), wyprowadzanie pieniędzy bezpośrednio z rachunku klienta czy wykonywanie operacji kartowych.

Jak się chronić?

Należy stosować się do kilku ważnych zasad:

- nie podawaj loginu i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, daty ważności, imienia i nazwiska posiadacza karty) – te informacje są poufne, powinny być tylko w posiadaniu użytkownika i nikt nie ma prawa wymagać ich podania, prawdziwy przedstawiciel banku nigdy o to nie zapyta,
- nigdy nie ujawniaj kodów do bankowości internetowej oraz kodów 3D Secure wykorzystywanych do autoryzacji transakcji kartowych w Internecie, przychodzących na telefon,
- zawsze czytaj treść SMS-ów jakie przychodzą na twój telefon lub komunikatów w aplikacji mobilnej w trakcie połączenia z rzekomym przedstawicielem banku lub innej instytucji. Z ich treści może wynikać, iż akceptujesz transakcję, którą przygotowali przestępcy,

- jeżeli rozmowa wzbudza jakiekolwiek wątpliwości lub niepokój, należy rozłączyć się, odczekać minimum 30 sekund, a następnie samodzielnie połączyć z instytucją, której rzekomy przedstawiciel dzwonił, koniecznie wybierając oficjalny numer na klawiaturze numerycznej, a nie oddzwaniając na wcześniejsze połączenie
- zachować zdrowy rozsądek i zimną krew, nawet jeżeli zostało się poinformowanym o potencjalnym zagrożeniu np. utrata środków. Należy spokojnie przemyśleć, czy środki naprawdę mogą być w niebezpieczeństwie, czy może rozmowa prowadzona jest z oszustem, który dopiero sytuację chce wykorzystać. Dobrym krokiem będzie przerwanie połączenia i ponowne jego zainicjowanie zgodnie z zasadą powyżej.
- należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym przedstawicielem banku.

Każdy klient banku powinien pamiętać, że każdorazowo ma prawo zgłosić nietypową sytuację do banku, a w sytuacji podejrzenia, że doszło lub mogło dojść do popełnienia przestępstwa, również zawiadomić policję.

Komenda Główna Policji

FinCERT.pl–BCC ZBP

Polska Izba Informatyki i Telekomunikacji