VOICE PHISHING

Oszustwo z wykorzystaniem połączenia telefonicznego

Uważaj na próby wyłudzenia poufnych danych przez telefon – przestępcy podszywają się pod pracowników naszego banku lub innych zaufanych instytucji (np. policjantów)!

Vishing to metoda oszustwa, która polega na **podszywaniu się pod pracowników banków i innych zaufanych instytucji**, np. policjantów. Oszuści chcą w ten sposób zdobyć poufne dane klienta (np. login i hasło do bankowości internetowej) lub nakłonić o do określonych czynności (np. zainstalowania aplikacji do zdalnej obsługi urządzenia).

Spoofing to metoda oszustwa, która polega na **podszywaniu się pod inne urządzenia lub innego użytkownika**. Oszuści zmieniają numer telefonu, adres e-mail czy adres IP, z których się kontaktują. Co więcej, mogą też wybrać i zmienić płeć osoby dzwoniącej, jej kraj pochodzenia, a nawet akcent. Zawsze dobrze przygotowują się do rozmowy, aby była ona wiarygodna i uśpiła czujność klienta.

Połączenie z nieznanego numeru od razu wzbudziłoby nasze podejrzenia, niestety atakujący także o tym wiedzą, dlatego też wykorzystują metody spoofingu, czyli podszywania się pod np. infolinię banku.

Jak przebiega takie oszustwo?

Scenariuszy ataku jest naprawdę wiele, w jednym z nich atakujący może podawać się za pracownika banku i poprosić o zainstalowanie aplikacji, aby usprawnić kontakt z bankiem. Następnie może zapytać o dane uwierzytelniające w celu zapobiegania dalszej utracie środków.

Oszuści stosują wyćwiczone techniki manipulacji. **Podszywają się pod prawdziwe numery telefonów!** Kiedy dzwonią, na telefonie klienta może wyświetlić się inny, znany numer lub nazwa banku.

Choć nie ma jednego schematu działania, przykładowa rozmowa może przebiegać tak:

- Klient odbiera telefon od oszusta.
- Oszust przekazuje klientowi informację o rzekomej płatności na jego koncie i prosi o potwierdzenie jej wykonania. Często oszuści przekazują też informację o logowaniu spoza granic Polski.
- Klient odpowiada na wszystkie pytania, których oficjalnym celem jest jego weryfikacja.
- Oszust informuje klienta, że musi zablokować rzekomą fałszywą transakcję lub przeprowadzić „zdalne skanowanie antywirusowe”. W tym celu klient ma zainstalować specjalną aplikację, np. AnyDesk lub TeamViewer.
- Klient instaluje aplikację, a jego dane trafią do oszusta – ma dostęp do konta klienta i pieniędzy na nim.

Jak się chronić?

- Nigdy nie wolno podawać loginu i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, data ważności). To informacje poufne, powinny być znane tylko klientowi.

- Zawsze warto czytać treść SMS-ów i komunikatów z aplikacji mobilnej. Należy zwrócić na nie szczególną uwagę podczas połączenia z rzekomym przedstawicielem banku lub innej instytucji. Z ich treści może wynikać, że akceptuje się transakcję, którą przygotowali przestępcy.
- Jeżeli jakakolwiek rozmowa wzbudza wątpliwości lub niepokój klienta, niech się rozłączy. Warto odczekać minimum 30 sekund, a następnie samodzielnie połączyć się z instytucją, z której dzwonił rzekomy przedstawiciel. Koniecznie należy wpisać numer samodzielnie –nie oddzwaniać na wcześniejsze połączenie.
- Nie powinno się instalować dodatkowego oprogramowania na urządzeniach, za pomocą których klient loguje się do aplikacji bankowej.
- Nie wolno zgadzać się na alternatywny kontakt mailowy czy SMSowy. Oszust może chcieć wysłać link lub załącznik, który może zainfekować urządzenie klienta.

- Bank nigdy nie poprosi o pełny login i hasło oraz o pełny numer karty płatniczej i kod CVV poprzez infolinię, widomość sms, czy email. **Zachowaj te dane wyłącznie dla siebie!**
- Jeśli masz jakiekolwiek podejrzenia oszustwa – rozłącz się. **Nie akceptuj żadnej propozycji alternatywnego kontaktu i samodzielnie zadzwoń do Banku.**
- **Zachowaj zdrowy rozsądek. Chroń swoje dane.**

Jeśli dojdzie do oszustwa…

Nie czekaj, reaguj! Jak najszybciej skontaktuj się z Bankiem lub zadzwoń pod Infolinię, czynną 24/7:

800 888 888 (bezpłatne połączenie)

61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).