Vishing i spoofing – czym są?

Vishing to metoda oszustwa, która polega na **podszywaniu się pod pracowników banków i innych zaufanych instytucji**, np. policjantów. Oszuści chcą w ten sposób zdobyć Twoje poufne dane (np. identyfikator i hasło do bankowości internetowej) lub nakłonić Cię 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 Twoją czujność.

Jak przebiega takie oszustwo?

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

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

- Odbierasz telefon od oszusta.
- Oszust przekazuje Ci informację o rzekomej płatności na Twoim koncie i prosi o potwierdzenie jej wykonania. Często oszuści przekazują też informację o logowaniu spoza granic Polski.
- Odpowiadasz na wszystkie pytania, których oficjalnym celem jest zweryfikowanie klienta.
- Oszust informuje Cię, że musi zablokować rzekomą fałszywą transakcję lub przeprowadzić „zdalne skanowanie antywirusowe”. W tym celu masz zainstalować specjalną aplikację, np. AnyDesk lub TeamViewer.
- Instalujesz aplikację, a Twoje dane trafią do oszusta – ma dostęp do Twojego konta i pieniędzy na nim.

Jak się chronić?

- Nigdy nie podawaj identyfikatora i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, data ważności). To informacje poufne, powinny być znane tylko Tobie.
- Zawsze czytaj treść SMS-ów i komunikatów z aplikacji mobilnej, które dostajesz. Zwróć na nie szczególną uwagę podczas połączenia z rzekomym przedstawicielem banku lub innej instytucji. Z ich treści może wynikać, że akceptujesz transakcję, którą przygotowali przestępcy.
- Jeżeli jakakolwiek rozmowa wzbudza Twoje wątpliwości lub niepokój, rozłącz się. Odczekaj minimum 30 sekund, a następnie samodzielnie połącz się z instytucją, z której dzwonił rzekomy przedstawiciel. Koniecznie wpisz numer samodzielnie – **nie oddzwaniaj na wcześniejsze połączenie.**
- Nie instaluj dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do aplikacji bankowej.
- Nie zgadzaj się na alternatywny kontakt mailowy czy SMSowy. Oszust może chcieć wysłać link lub załącznik, który może zainfekować Twoje urządzenie.

Jeśli dojdzie do oszustwa…

Nie czekaj, reaguj! Jak najszybciej zablokuj dostęp do bankowości elektronicznej oraz skontaktuj się z Bankiem!