Wstęp

Co to jest Vishing?

Vishing to oszukańcze pozyskanie poufnej informacji z wykorzystaniem telefonu. Przestępca podszywa się pod osoby lub instytucje godne zaufania. Jest to rodzaj ataku opartego na inżynierii społecznej, mającego swoje podstawy w phishingu. Nazwa Vishing to zlepek słów z wyrażenia ‘voice phishing’ - phishing głosowy.

Metody ataku

Jedną z metod ataku jest rozesłanie wiadomości zawierającej numer telefonu, pod którym odbiorca e-maila lub SMS-a ma zaktualizować swoje poufne dane. Po połączeniu się z podanym numerem telefonu włącza się automat, który poprosi o podanie nazwy użytkownika i hasła do aplikacji bankowej lub dane o karcie płatniczej takie jak numer kart, data ważności, PIN.
Inna metoda ataku polega na wykorzystaniu programu, który sam telefonuje do Klienta korzystając z listy pozyskanych wcześniej numerów telefonów. Podobnie jak w poprzednim ataku następuje uruchomienie automatu odtwarzającego informacje mające przekonać ofiarę o konieczności podania poufnych danych.

Jak chronić się przed Vishingiem?

Po pierwsze, jeśli masz wątpliwości czy osoba dzwoniąca jest pracownikiem banku, nie podawaj swoich poufnych informacji. Zadzwoń do banku w celu potwierdzenia tożsamości osoby dzwoniącej. Numery telefonów znajdziesz tutaj: http://www.ingbank.pl/kontakt.

Po drugie zachowaj zdrowy rozsądek. Traktuj z dystansem wszystkie maile, SMS’y i telefony, w których jesteś proszony o dane osobowe, PIN czy hasło. Jeżeli zostałeś poproszony o podanie danych, o które do tej pory bank nie pytał, zadzwoń do banku i sprawdź czy na pewno o te dane pyta bank!

Pamiętaj!

Nie korzystaj z numeru podanego przez osoby dzwoniące. W przypadku podejrzeń o wyłudzenie danych zgłoś ten przypadek policji oraz powiadom bank o tym fakcie.