VOICE PHISHING

CZYLI OSZUSTWO Z WYKORZYSTANIEM POŁĄCZENIA TELEFONICZNEGO

Vishing polega na podszywaniu się pod osobę pracującą w danej instytucji, aby zdobyć zaufanie ofiary i wyłudzić od niej poufne dane

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

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

Jak się bronić?

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