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 wykorzystują metody spoofingu czyli podszywania się pod np. numer telefonu Banku.

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

Jak się bronić?

- Bank ani funkcjonariusze służb państwowych nie proszą o login i hasło oraz numer karty płatniczej i kod CVV poprzez infolinię, wiadomość sms czy email -zachowaj te dane dla siebie. Nigdy nie proszą również o dokonanie transakcji, przelewu, wypłaty środków z rachunku bankowego.
- Jeśli masz jakiekolwiek podejrzenia oszustwa – rozłącz się. Nie akceptuj żadnej propozycji alternatywnego kontaktu i samodzielnie zadzwoń do Banku.
- Zachowaj zdrowy rozsądek. Chroń swoje dane