POLICJA ŚLĄSKA

https://slaska.policja.gov.pl/kat/informacje/wiadomosci/321763,Policjanci-ostrzegaja-przed-spoofingiem.html
2021-11-28, 22:39

POLICJANCI OSTRZEGAJĄ PRZED SPOOFINGIEM!

Data publikacji 07.10.2021

Oszustwo metodą „spoofingu" jest coraz częściej powodem strat oszczędności całego życia. Spoofing to nowa metoda wyłudzania danych wrażliwych lub pieniędzy. Polega na wykorzystaniu oprogramowania do zmiany numeru telefonicznego lub nazwy dzwoniącego połączenia, które widzi na wyświetlaczu swojego telefonu je odbierający. Policjanci apelują o ostrożność przy tego typu kontaktach i weryfikację tożsamości dzwoniących do nas osób. Pamiętajmy! Oszuści umiejętnie manipulują rozmową tak, by uzyskać jak najwięcej informacji i wykorzystać naszą naiwność. W kontaktach z nieznajomymi kierujmy się zawsze zasadą ograniczonego zaufania.

Spoofing telefoniczny to nic innego jak coraz popularniejsze oszustwo polegające na podszywaniu się dzwoniącego pod inne numery, by móc następnie dzwonić z nich do ofiar i udawać inną osobę.

Technicznie spoofing jest dziś możliwy głównie dzięki nowym rozwiązaniom technologicznym. Przy ich wykorzystaniu dzwoniący może w niemal dowolnej usłudze ręcznie wprowadzić numer, który ma się wyświetlić adresatowi połączenia jako numer dzwoniącego. Policjanci nie mają możliwości technicznego zablokowania spoofingu, gdyż telefon przestępcy nie jest podłączony do sieci komórkowej, lecz komputerowej.

W ten sposób coraz częściej oszuści podszywają się pod konsultantów banków, przedstawicieli urzędów czy nawet policjantów.

Sprawcy wykorzystują różne triki socjotechniczne po to, by zmanipulować rozmówcę i uzyskać dostęp do jego smartfona lub komputera, a w konsekwencji do rachunku bankowego. Ofiara spoofingu, sugerując się numerem, który wyświetlił się na telefonie jest przekonana, że prowadzi rozmowę z infolinią banku, pracownikiem urzędu lub policjantem. W większości rozmów pojawiają się jednak dwa elementy: presja czasu i poczucie zagrożenia. Zwykle oszuści namawiają ofiary do przelania pieniędzy na dane konto.

Scenariusz ataków wykorzystujących spoofing telefoniczny jest zwykle taki sam, a przynajmniej zbliżony. Oszust stara się wystraszyć rozmówcę, by działał pod wpływem emocji, najczęściej informując go o rzekomym włamaniu na konto bankowe i konieczności podjęcia szybkich działań, by zablokować możliwości włamywaczy.

Każdą telefoniczną prośbę o przesłanie pieniędzy lub podanie danych konta bankowego powinno się traktować jako próbę oszustwa. Najlepiej w takiej sytuacji samodzielnie wpisać numer banku, zadzwonić, poinformować o otrzymanym połączeniu i zweryfikować przekazane informacje.

(Biuro dw. z Cyberprzestępczością KGP/ mw)