
POLICJANCI OSTRZEGAJ? PRZED SPOOFINGIEM!

Data publikacji

08.10.2021

POLICJANCI OSTRZEGAJ? PRZED SPOOFINGIEM!

Oszustwo metod? „spoofingu” jest coraz cz??ciej powodem strat oszcz?dno?ci ca?ego ?ycia. Spoofing to nowa metoda wy?udzania danych wra?liwych lub pieni?dzy. Polega na wykorzystaniu oprogramowania do zmiany numeru telefonicznego lub nazwy dzwoni?cego po??czenia, które widzi na wy?wietlaczu swojego telefonu je odbieraj?cy. Policjanci apeluj? o ostro?no?? przy tego typu kontaktach i weryfikacj? to?samo?ci dzwoni?cych do nas osób. Pami?tajmy! Oszu?ci umiej?tnie manipuluj? rozmow? tak, by uzyska? jak najwi?cej informacji i wykorzysta? nasz? naiwno??. W kontaktach z nieznajomymi kierujmy si? zawsze zasad? ograniczonego zaufania.

Spoofing telefoniczny to nic innego jak coraz popularniejsze oszustwo polegaj?ce na podszywaniu si? dzwoni?cego pod inne numery, by móc nast?pnie dzwoni? z nich do ofiar i udawa? inn? osob?.

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 wyświetli 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 działać pod wpływem emocji, najczęściej informując go o rzekomym włamaniu na konto bankowe i konieczności podjęcia szybkich działań, by zablokować możliwośći wamywaczy.

Każde telefoniczne próby o przesłanie pieniędzy lub podanie danych konta bankowego powinno się traktować jako próba oszustwa. Najlepiej w takiej sytuacji samodzielnie wpisać numer banku, zadzwonić, poinformować o otrzymanym połączeniu i zweryfikować przekazane informacje.

(Biuro dw. z Cyberprzestępczości KGP/ mw)

[Inne teksty z komend wojewódzkich na ten temat](#)

- [Udostępnij](#)
- [Drukuj](#)
- [PDF](#)