„Dzień dobry, tu Policja…" Czy aby na pewno?

Data publikacji: 5.02.2022 17:11

Na policjanta, na CBS, na administratora danych, na pracownika banku… Wyobraźnia przestępców jest duża. Liczy się jedno – przekonać ofiarę, żeby wyłudzić dane i pieniądze. Przeczytaj, jak się chronić przed spoofingiem!

Kreatywność oszustów jest nieskończona: - ***Nie wahają się sięgać po najnowsze możliwości techniczne i internetowe. Nie wychodząc z domu, mogą w ten sposób pozbawić nas naszych oszczędności. Potrafią podszywać się pod konsultanta banku lub operatora sieci komórkowej. Wysyłają też fałszywe e-maile, by wyłudzić od nas dane wrażliwe. Skutecznym sposobem na ochronę jest czujność i zasada ograniczonego zaufania*** – informuje cieszyńska Policja.

Spppfing to inaczej „podszywanie się". Wyróżniamy różne rodzaje, najpopularniejszy jest spoofing internetowy i telefoniczny. ***- Ten w wersji internetowej to najczęściej wysyłanie maili na nasze skrzynki. Przestępcy podszywają się wówczas pod firmy, instytucje lub np. agencje pośrednictwa pracy. Oszuści wciągają nas w swój proceder i wyłudzają dane wrażliwe, takie jak loginy i hasła do bankowości elektronicznej, numery kart kredytowych lub bankomatowych czy też numer PESEL. Dzięki temu mogą dostać się na nasze konta bankowe lub zaciągać kredyty*** – ostrzegają policjanci.

Czasami w naszej skrzynce może wylądować mail z zaufanego źródła, w którym znajduje się lin. - ***Po kliknięciu wchodzimy na podstawioną witrynę, która łudząco przypomina zaufaną stronę. Również tam, niczego nie świadomi, możemy wprowadzać hasła i loginy. W ten sposób udostępniamy swoje oszczędności przestępcom*** – funkcjonariusze opisują zasadę działania oszustów.

Spoofing telefoniczny podszywanie 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 – ostrzegają policjanci.

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 podobny. Oszust stara się wystraszyć rozmówcę, np. 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 –*** radzą funkcjonariusze.