POLICJA OPOLSKA

https://opolska.policja.gov.pl/op/aktualnosci/58759,Nie-wierz-w-scenariusz-oszustow.html
2022-06-27, 14:22

NIE WIERZ W SCENARIUSZ OSZUSTÓW

Data publikacji 26.01.2022

Współczesna technologia ułatwia i udoskonala życie w wielu dziedzinach. Niestety, wykorzystują ją również przestępcy w oszustwie zwanym spoofingiem. Dzwonią wówczas z numerów imitujących oficjalne połączenia bankowe. W rozmowie podszywają się pod konsultantów finansowych lub bankowców. Nakłaniają na przelanie swoich oszczędności na podane konta, proszą o zainstalowanie jakiegoś oprogramowania lub o kliknięcie w przesłany link i zalogowanie się na swoje konto. W efekcie wchodzą w posiadania naszych pieniędzy. Zobaczcie, jak wygląda przykładowy scenariusz takiej rozmowy.

Wyróżniamy różne rodzaje spoofingu - głównie 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.

Zdarza się, że w przesłanej wiadomości otrzymujemy link do strony internetowej. 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.

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.

Film VID-20220125-WA0000.mp4

Aby obejrzeć film włącz obsługę JavaScript w swojej przelądarce.

Pobierz plik VID-20220125-WA0000.mp4 (format mp4 - rozmiar 8.53 MB)

PLIKI DO POBRANIA

Transkrypcja
13.68 KB