POLICJA MAŁOPOLSKA

https://malopolska.policja.gov.pl/krk/aktualnosci/8332,Spoofing-telefoniczny-na-Sadecczyznie-Ostrzegamy-przed-oszustwem-na-zdalny-doste.html
2021-05-17, 00:38

SPOOFING TELEFONICZNY NA SĄDECCZYŹNIE. OSTRZEGAMY PRZED OSZUSTWEM NA ZDALNY DOSTĘP DO TELEFONU KOMÓRKOWEGO

Data publikacji 01.03.2021

Cyberprzestępcy wykorzystają możliwość podszycia pod telefoniczny numer banku by podstępnie wyłudzać dane do konta ofiary. Tym razem ich ofiarą padło troje mieszkańców Sądecczyzny, którzy na prośbę fałszywych pracowników banku zainstalowali na swoich komórkach aplikację umożliwiającą zdalny dostęp do telefonu. Ta fatalna w skutkach decyzja kosztowała ich łącznie ponad 55 tys. złotych.

W ostatnim czasie do sądeckich policjantów zgłosiło się dwóch mężczyzn i kobieta, którzy zostali oszukani w bardzo podobny sposób. Cyberoszuści wykorzystując tzw. spoofing* wykonywali połączenie, które identyfikowało się w telefonach pokrzywdzonych jako infolinia banku. Później fałszywi konsultanci (mówiący ze wschodnim akcentem), informowali o nieprawidłowościach na rachunku np. nieuprawnionym przelewie. Osoby podające się za pracowników banku prosiły o wykonanie kilku prostych czynności, które rzekomo miały na celu przeciwdziałanie niebezpieczeństwu utraty oszczędności. Między innymi polecały, by na telefonie komórkowym zainstalować aplikację umożliwiającą zdalny dostęp do telefonu – dzięki temu w łatwy i szybki sposób, bez konieczności przychodzenia do placówki bankowej, problem miał zostać rozwiązany. Następnie fałszywi konsultanci prosili o zmianę hasła do bankowości mobilnej, uzyskując tym samym pełny dostęp do rachunków swoich ofiar. Informowali przy tym, że będą przychodziły kody autoryzacyjne, które trzeba im przekazywać.

Pokrzywdzeni postępowali zgodnie z otrzymywanymi instrukcjami, a dzięki temu cyberoszuści przy pomocy otrzymywanych kodów BLIK i otrzymanych od ofiar kodów autoryzacyjnych przelewali środki z kont poszkodowanych na inne konta, zaciągali kredyty lub wypłacali pieniądze z bankomatu. W efekcie sądeczanie stracili łącznie 55 300 złotych.

Policjanci ostrzegają i apelują o rozwagę, a także radzą jak nie dać się oszukać w podobny sposób:

• Bądź ostrożny w kontaktach telefonicznych z nieznajomymi, nawet rzekomymi pracownikami banku.

• Chroń swoje dane, w tym również numery telefonów – nawet nie zorientujesz się, że zamiast smsa od krewnych czy znajomych, do których masz zaufanie, dostaniesz wiadomość od cyberoszustów (np. z prośbą o podanie kodu BLIK czy zlecenie przelewu) i stracisz swoje pieniądze.

• Nie instaluj dodatkowych programów na urządzeniach, z których logujesz się do bankowości elektronicznej. Czerwona lampka powinna zapalić się, zwłaszcza gdy osoba podająca się za pracownika banku wymaga zainstalowania jakiegokolwiek oprogramowania czy aplikacji do zdalnej obsługi telefonu komórkowego czy pulpitu. W takiej sytuacji rozłącz się i najlepiej z innego aparatu telefonicznego zadzwoń do biura obsługi klienta banku.

• Nie udostępniaj telefonicznie nikomu swoich danych do logowania w internetowym systemie bankowości elektronicznej, nawet pracownikom banku.

• Nie autoryzuj przelewów, których sam nie wykonujesz. Nie podawaj żadnych kodów autoryzacyjnych w przypadku kiedy ktoś do Ciebie dzwoni (niezależnie z jakiego numeru).

• Nie otwieraj przesłanych linków, nie znając ich nadawcy ani zawartości.

• Podejrzewając, że ktoś próbuje Cię oszukać, natychmiast powiadom Policję.

*Spoofing telefoniczny, czyli podszywanie się pod dowolny numer lub nazwę oznacza, że mimo wyświetlanej w telefonie nazwy (np. mama, Tomek itp.) czy numeru telefonu (np. numeru infolinii banku czy innej instytucji), tak naprawdę

dzwoni lub pisze wiadomości zupełnie inna osoba.