POLICJA LUBELSKA

https://lubelska.policja.gov.pl/lub/aktualnosci/121956,Oszustwo-metoda-spoofingu-przez-osoby-podajace-sie-za-pracownikow-banku.html
2022-09-27, 01:34

OSZUSTWO METODĄ „SPOOFINGU" PRZEZ OSOBY PODAJĄCE SIĘ ZA PRACOWNIKÓW BANKU

Data publikacji 24.01.2022

Około 20 tysięcy złotych stracił 26 -letni mieszkaniec gminy Ułęż po telefonicznym kontakcie z osobą podającą się za pracownika banku. Na wyświetlaczu telefonu pojawiło się połączenie z nazwą jednego z banków. Po rozmowie z „pracownikiem" banku, zalogował się do bankowości elektronicznej. Jak się później okazało na jego dane oszuści wzięli kredyt i zdążyli wypłacić pieniądze. Apelujemy o zachowanie ostrożności w przypadku otrzymania tego typu telefonów.

Do ryckiej komendy zgłosił się mieszkaniec gminy Ułęż, który padł ofiarą oszustów. Mężczyzna poinformował policjantów, że zadzwonił do niego mężczyzna podający się za pracownika banku. Na wyświetlaczu telefonu 26-latka pojawiło się połączenie z nazwą jednego z banków. Dzwoniący poinformował pokrzywdzonego, że prawdopodobnie ktoś włamał się na jego konto i próbował podjąć kwotę 700 zł. Prowadził również rozmowę na temat oszustw bankowych. Po rozmowie z „bankowcem" 26 -latek zalogował się do swojej aplikacji bankowej i nie stwierdził nieprawidłowości. Po jakimś czasie otrzymał wiadomość ze swojego banku z której wynikało, że na jego dane został wzięty kredyt w wysokości około 44 tysięcy złotych. Zanim pokrzywdzony skontaktował się z bankiem i zablokował konto, oszuści zdążyli już wypłacić w kilku transakcjach około 20 tysięcy złotych. Dodatkowo jak się później okazało miał zablokowany dostęp do swojej poczty elektronicznej. Mężczyzna kolejnego dnia zgłosił sprawę na policji.

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.

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.

starszy aspirant Agnieszka Marchlak