KOMENDA POWIATOWA POLICJI W CIESZYNIE

https://cieszyn.policja.gov.pl/ka6/informacje/wiadomosci/344481,Oszustwo-quotna-pracownika-bankuquot-pokrzywdzeni-stracili-wszystkie-oszczednosc.html
2022-12-02, 20:40

OSZUSTWO "NA PRACOWNIKA BANKU"- POKRZYWDZENI STRACILI WSZYSTKIE OSZCZĘDNOŚCI

Data publikacji 15.09.2022

Cieszyńscy policjanci ostrzegają przed oszustami podającymi się za pracowników banku, którzy dzwonią z oficjalnych numerów banków. Oszuści, twierdzący, że są konsultantami bankowymi, nakłonili pokrzywdzonych do wypłaty pieniędzy a następnie do wpłacenia gotówki i podania kodu BLIK. Pokrzywdzeni stracili w ten sposób blisko 85 000 złotych. Bądźmy czujni !!!

Policjanci odnotowują kolejne przypadki oszustwa „na pracownika banku". Pokrzywdzeni są tak manipulowani przez przestępców, że wypłacają posiadane w banku środki, a następnie wpłacają je we wpłatomacie innego banku przekazując kod BLIK przestępcom. W ten sposób 40-letni mężczyzna stracił blisko 35 000 złotych. Taką samą kwotę, w ten sam sposób straciła 29-latka. Z kolei 24-letnia kobieta została oszukana na niecałe 15 000 złotych po tym, jak usłyszała od „pracownika banku", że ktoś usiłował dokonać przelewu z jej konta. Uwierzyła rozmówcy, że bierze udział w akcji służb mającej na celu schwytanie przestępców. Po długiej rozmowie z „pracownikiem departamentu bezpieczeństwa", za którego podawał się przestępca, usłyszała jedyne prawdziwe, w toku całej rozmowy, zdanie- „została Pani oszukana, może to Pani zgłosić w banku i na policję". Wszystko wyglądało bardzo wiarygodnie, ale należy pamiętać o jednym- służby nie działają w taki sposób, nie informują przez telefon o działaniach operacyjnych...

A jak to wygląda w praktyce ?

Oszust dzwoni do konkretnej osoby i podaje się za konsultanta bankowego. Numer telefonu, z którego dzwoni fałszywy pracownik placówki bankowej wygląda na oficjalny numerem banku, który można potwierdzić na stronie internetowej. Dzwoniący informuje o niepokojących transakcjach na koncie ofiary. Aby zapobiec i unieważnić te przelewy „konsultant" wybiera różne formy oszustwa- jedną z nich jest zainstalowanie aplikacji AnyDesk, która umożliwia mu wykonywanie zdalnych działań na smartfonie lub komputerze rozmówcy. W ten sposób oszust uzyskuje dostęp do urządzenia ofiary i tym samym konta, z którego dokonuje przelewów, a następnie wypłaca zgromadzone na nim środki, a nawet próbuje też zaciągnąć kredyt na konto ofiary.

Drugą formą oszustwa jest wmówienie pokrzywdzonemu, że jest ważnym ogniwem w akcji zatrzymania sprawców włamań na konta bankowe. „Pracownik departamentu bezpieczeństwa" informuje, że zablokował przelew, który usiłowała wykonać inna osoba. „Konsultant" przekonuje pokrzywdzonego, że ten nie widzi podejrzanych ruchów na swoim koncie, ponieważ ma już najprawdopodobniej zmienione przez „włamywaczy" ustawienia i musi czym prędzej wypłacić pieniądze ze swojego konta. Tutaj „ostrzega" swoją ofiarę, że

pracownik banku może być w zmowie z przestępcami i też jest obserwowany ponieważ bierze **udział w procederze handlu danymi.** "Konsultant" informuje ofiarę, że wypłacone pieniądze to banknoty „emblematowe”, w związku z czym nie należą do ofiary. Wybrane z konta pieniądze ofiara ma wpłacić w wpłatomacie innego banku, który posiada „odpowiednią licencję”. Z tego tytułu po wpłacie pokrzywdzony namawiany jest do podania kodu BLIK-wówczas rozmówca zapewnia, że kod ten będzie potwierdzeniem wpłaty i jednocześnie podstawą odebrania „zabezpieczonej” gotówki po zakończonej "akcji".

Pamiętajmy, że przestępcy działają w różny sposób. Modyfikują swój sposób działania , żeby tylko uprawdopodobnić swoją historię. W przypadku oszustwa na pracownika banku mogą dzwonić np. dwie różne osoby. Najpierw otrzymamy informację z oficjalnego numeru konkretnego banku, o tym, że pewna osoba, która w bazach danych widnieje jako oszust, usiłowała zrobić przelew z naszego konta. Przestępca informuje, że w tej sytuacji trzeba podjąć środki zaradcze i pozabezpieczać konta także w innych bankach. Na koniec rozmowy dzwoniący podaje swoje imię i nazwisko oraz numer identyfikacyjny (często zgodny z prawdziwymi danymi), a następnie informuje, że przekazuje sprawę na policję. Po kilku minutach dzwoni inna osoba podająca się za pracownika innego banku, także z oficjalnego numeru banku. Podaje swoje imię i nazwisko oraz numer identyfikacyjny. Nie prosi o podawanie żadnych haseł, ani pinów do konta. Prosi „jedynie” o zainstalowanie aplikacji „AnyDesk, by ochronić środki na koncie. Pokrzywdzeni pobierają wówczas aplikacje i postępują zgodnie ze wskazówkami, jakie udzielała im konsultant. Rozmowa niejednokrotnie trwa kilka godzin...

Przestępcy doskonale znają aplikację mobilną i stronę internetową banku. Udzielają też merytorycznych odpowiedzi na wszystkie zadawane pytania, a wręcz przewidują kolejne kroki, jakie należy zrobić. Wiarygodności dodaje fakt, że w telefonie często słychać rozmowy innych konsultantów na tematy bankowe. Dzwoniący mówią płynnie w języku polskim, ale często ze wschodnim akcentem.

Policjanci przypominają i ostrzegają:
- pracownicy banku nigdy nie proszą o podanie loginu i hasła do konta, a tym bardziej kodu autoryzacyjnego SMS lub BLIK;
- nie polecają też instalowania aplikacji, z której mogą wykonywać ruchy na koncie klienta;
- **wykonując JAKIEKOLWIEK operacje finansowe, wykonuj je w placówce bankowej albo z własnej inicjatywy! NIGDY ZA NAMOWĄ osób kontaktujących się telefonicznie!!!!**

O wszelkich próbach wyłudzenia pieniędzy należy natychmiast poinformować policję dzwoniąc na numer alarmowy 112.