Cieszyn: Straciła 20 tysięcy zł

Data publikacji: 18.07.2023 11:48

Zaczęło się o „pracownika banku”, który poinformował, że zamyka konto z kryptowalutami. Skończyło się kradzieżą 20 tys. oszczędności.

Policjanci z Cieszyna prowadzą postępowanie dotyczące oszustwa, gdzie przestępca działał metodą “na pracownika infolinii banku i aplikację zdalny pulpit”.

- ***O sprawie oszustwa policjanci zostali powiadomieni w piątek (14.07.2023). Pokrzywdzona pozwoliła się zmanipulować fałszywemu pracownikowi banku, który poinformował, że właśnie zamyka konto związane z kryptowalutami. Pokrzywdzona, wierząc rozmówcy, postępowała zgodnie z instrukcjami „pracownika banku”, który polecił zainstalowanie aplikacji służącej przestępcom do zdalnego dostępu do telefonu i komputera. Wszystko po to, aby „ być ciągłym kontakcie”. To wystarczyło, aby pokrzywdzonej z konta zniknęły oszczędności sięgające blisko 20 tysięcy złotych. Przy pomocy aplikacji zdalnego pulpitu przestępcy przejęli całkowitą kontrolę nad danymi, a następnie w dowolny sposób zarządzili kontem swojej ofiary. W tym przypadku wszystko zaczęło się od odebrania telefonu od rzekomego pracownika banku*** – relacjonuje podkomisarz Krzysztof Pawlik z Komendy Powiatowej Policji w Cieszynie.

Policjanci przypominają, że w każdym przypadku punktem wyjściowym dla tego typu oszustw jest zainstalowanie przez pokrzywdzonych aplikacji AnyDesk lub Team Viewer.

Mechanizm działania sprawców tego typu oszustwa:

• Przestępcy dzwonią do swojej ofiary z prawdziwego numeru telefonu banku. Po sprawdzeniu na stronie banku okazuje się, że numer „jest prawdziwy”, bo jest podawany na jego oficjalnej stronie internetowej jako numer do kontaktu. Pamiętaj, pod numer telefonów można się podszyć. Od tego momentu pokrzywdzonym wyłącza się czujność, bo przecież dzwoni pracownik banku z poprawnego numeru telefonu z ważną informacją dotyczącą rachunku bankowego. Taka sytuacja wielu osobom „wyłącza” czujność.

• Dzwoniący przedstawia się jako pracownik banku, który kontaktuje się w istotnej sprawie dotyczącej bezpieczeństwa rachunku. Oszust najczęściej twierdzi, że bank wykrył podejrzaną transakcję na rachunku, dlatego prosi o współpracę, aby nie dopuścić do oszustwa. Często „proszą” o sprawdzenie ruchów na koncie, podstępnie wypytując o stan konta i dostępne środki finansowe.

• Sprawcy nalegają również na to, by „zgodnie z regulaminem banku”, pracownik działu technicznego, czy informatyk przeskanował (urządzenie: telefon lub komputer) pod kątem wirusów. W tym celu chcą się połączyć z Tobą przez aplikację np. AnyDesk, którą rzekomo trzeba mieć zainstalowaną. W czasie rozmowy nalegają na zainstalowanie tej aplikacji, bo “regulamin banku tego wymaga” .

• Prowadzą rozmowę w taki sposób, że osoba nie ma czasu zastanowić się i wykonuje wszystkie polecenia, jakich żąda przestępca. W ten sposób oszust z pomocą pokrzywdzonego wykonuje operacje na koncie. Dzięki aplikacji AnyDesk oszuści wiedzą wszystko, co osoba robi na smartfonie czy komputerze, widzą też kody potrzebne do autoryzowania transakcji. W taki sposób przejmują kontrolę nad rachunkiem i „czyszczą” konto z dostępnych środków finansowych.

Jak nie stać się ofiarą?

Zawsze zachowaj czujność, nie działaj pochopnie. Koniecznie upewnij się z kim rozmawiasz, nie daj się zmanipulować. Jeśli zadzwoni do Ciebie ktoś z banku, ROZŁĄCZ SIĘ. Skontaktuj się z bankiem, najlepiej osobiście

udaj się na placówki bankowej lub natychmiast samodzielnie zadzwoń na infolinię swojego banku (pod numer, który znajdziesz na stronie swojego banku). Jeśli telefon z banku był prawdziwy, to konsultant z infolinii, na którą dzwonisz, będzie wiedział o co chodzi. W podejrzanej sytuacji, dla własnego bezpieczeństwa, przelej część swoich oszczędności na inny rachunek w innym banku, wówczas nie stracisz dostępu do całości swoich środków.

Pamiętaj, że tego rodzaju przestępstwa są trudne do wykrycia, a szanse na odzyskanie utraconych w ten sposób środków finansowych, praktycznie są znikome. Często również bank nie uwzględnia reklamacji, ponieważ pokrzywdzeni sami umożliwili oszustom dostęp do swojego konta, instalując na ich polecenie aplikację zdalnego pulpitu.

Jeśli padłeś ofiarą takiego oszustwa, zgłoś ten fakt na Policji i złóż reklamację do banku.

red.