

KOMENDA POWIATOWA POLICJI W BEŁCHATOWIE

<http://belchatow.policja.gov.pl>

2024-04-26, 19:43

UWAGA NA OSZUSTWA METODĄ „NA PRACOWNIKA BANKU I APLIKACJĘ ANYDESK”!

Bełchatowscy policjanci prowadzą postępowania dotyczące oszustw, gdzie przestępcy działali metodą „na pracownika infolinii banku i aplikację zdalny pulpit”. Punktem wyjściowym w każdym przypadku było zainstalowanie przez pokrzywdzonych na swoim smartfonie lub komputerze aplikacji AnyDesk, która pozwoliła sprawcom przejąć całkowitą kontrolę nad rachunkiem bankowym. Zanim zainstalujesz taką aplikację na swoim urządzeniu, upewnij się, czy nie rozmawiasz z oszustem!

W sprawach, które są prowadzone przez policjantów z wydziału do walki z przestępczością gospodarczą KPP w Bełchatowie pokrzywdzonym zniknęły oszczędności z kont bankowych zaraz po zainstalowaniu na smartfonie lub komputerze aplikacji AnyDesk. Przy pomocy aplikacji zdalnego pulpitu przestępcy przejęli całkowitą kontrolę nad danymi, a następnie w dowolny sposób zarządzili kontem swojej ofiary. Ukradli oszczędności, a nawet zaciągnęli kredyt. W tych przypadkach wszystko zaczęło się od odebrania telefonu od rzekomego pracownika banku, który wykrył podejrzaną przelew, czy transakcję. W każdym przypadku punktem wyjściowym było zainstalowanie przez pokrzywdzonych aplikacji AnyDesk.

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.

Taki mechanizm oszustwa miał miejsce w przypadku przestępstwa, którego ofiarą padła bełchatowianka. 14 maja 2021 roku kobieta odebrała telefon od osoby podającej się za pracownika banku, w którym posiadała rachunek. Pokrzywdzona sprawdziła, że numer ten odpowiadał numerowi kontaktowemu z jej bankiem. „Pracownik banku” informował o tym, że właśnie wykrył na jej rachunku bankowym podejrzaną przelew na konto należące w ocenie banku do przestępcy. Dla uwiarygodnienia informacji mężczyzna przedstawił się z imienia i nazwiska oraz podał imię i nazwisko rzekomego oszusta. Twierdził również, że sam zgłasza ten incydent na policję. Ostatecznie zapewnił, że

podejrzany przelew może jeszcze wstrzymać, jeśli kobieta na swoim smartfonie pilnie zainstaluje aplikację **AnyDesk**. Twierdził, że tylko dzięki posiadaniu tej aplikacji można powstrzymać podejrzaną transakcję. Oszust zmanipulował swoją ofiarę. Kobieta uwierzyła, iż rozmawia z pracownikiem banku, który chce jej pomóc. Będąc cały czas w kontakcie telefonicznym ze sprawcą, zgodnie z jego wskazówką, zainstalowała na swoim smartfonie żadaną aplikację. Od tego momentu przestępca przejął kontrolę nad rachunkiem bankowym pokrzywdzonej. W rozmowie wskazał, że aby zatrzymać niebezpieczną transakcję musi szybko potwierdzić kod, który "właśnie wysyła na jej telefon". Polecił jej akceptować wszystko co wyświetliło się na jej telefonie. Okazało się później, że kod oraz akceptowanie informacji pojawiających się na smartfonie dotyczyły zupełnie innej dyspozycji. W ten sposób złodzieje rozpoczęli kradzież pieniędzy z konta. Pokrzywdzona straciła wszystkie dostępne środki finansowe. Dodatkowo oszuści zaciągnęli kredyt na nazwisko pokrzywdzonej, a uzyskane w ten sposób pieniądze również padły ich łupem.

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.