

Strona znajduje się w archiwum.

ZDECYDOWANA REAKCJA PRACOWNICY BANKU ZAPOBIEGŁA OSZUSTWU

Są bezwzględni i wyjątkowo podli. Wykorzystują zaufanie swoich ofiar i grają na ich emocjach. Oszuści podszywają pod policjantów, prokuratorów lub pod pracownika banku. W tym ostatnim przypadku nakłaniają klientów do przekazywania środków oraz instalacji nieznanego oprogramowania. Przestraszona i zmanipulowana tą metodą mieszkanka Mrągowa straciła 7000 złotych. Straciłaby więcej, gdyby nie zdecydowana reakcja pracownicy banku.

Problemy mieszkanki Mrągowa zaczęły się w poniedziałek (07.02.22 r.), kiedy zadzwonił jej telefon. Odebrała i w słuchawce usłyszała męski głos z - według niej - rosyjskim akcentem. Mężczyzna przedstawił się, informując, że jest pracownikiem komórki cyberbezpieczeństwa banku, w którym kobieta ma konto. Wyjaśnił, że dzwoni w sprawie podejrzanego transakcji na jej koncie na kwotę 820 zł. Kobieta zaprzeczyła, by dokonała takiego przelewu. Wtedy oszust poinformował ją, że w takim razie ktoś włamał się na jej konto i muszą teraz zrobić zwrot tych pieniędzy, a jej telefon z pewnością został zainfekowany wirusem. Ponadto powiedział, że aby zapobiec dalszym problemom, trzeba pobrać specjalną aplikację - w rzeczywistości aplikację umożliwiającą przestępcom zdalny dostęp do jej telefonu. Co chwilę później się stało, bo otrzymała smsa ze „swojego banku” z linkiem, w który kliknęła.

Na tym etapie kobieta nie zdawała sobie sprawy, że rozmawia z oszustem, który nią manipuluje, stwarzając pozory profesjonalizmu i wiarygodności, dlatego na jego polecenie podała mu wszystkie numery karty bankomatowej oraz weszła przez telefon w swoją aplikację bankową. W ten sposób kradzież pieniędzy była tylko formalnością. Kobieta straciła 7 000 zł. Ale przestępcom było mało.

Oszust wmówił przestraszonej kobiecie, że jej dane zostały przekazane złodziejom przez kasjerki w banku. Pieniądze, które tam trzyma są zagrożone, bo pracują tam oszuści. Musi iść do swojej placówki i wypłacić zgromadzone tam środki. Kobieta zmanipulowana rozmową trwającą na przestrzeni kilku godzin, poszła do banku. Tam - cały czas kontynuując po cichu rozmowę telefoniczną z oszustem - poprosiła o wypłacenie pieniędzy. Na szczęście czujna pracownica banku zauważyła nietypowe zachowanie klientki. Najpierw powiedziała jej, że najprawdopodobniej padła ofiarą oszustwa, a potem stanowczo odmówiła wypłacenia jej pieniędzy. Przez to, że połączenie telefoniczne na tym etapie nie zostało jeszcze przerwane, usłyszał to również oszust, który kazał kobiecie wyjść z banku, po czym się rozłączył. W efekcie tej telefonicznej rozmowy i działania oszusta, kobieta straciła 7000 złotych, bo taki limit miała na koncie. Gdyby nie działanie czujnej pracownicy banku, straty mogłyby być dużo większe.

Jak odróżnisz oszusta od pracownika banku?

Przede wszystkim pamiętaj o tym, że jeśli masz konto w banku, to pracownik ma już część Twoich danych i nie musi o nie prosić. Oszust tymi danymi nie dysponuje, więc za wszelką cenę będzie starał się nakłonić Ciebie do ich podania. Najbardziej będzie mu zależało na loginie i hasle do Twojego konta. Prośba o podanie takich informacji to dowód, że masz do czynienia z oszustem.

Prawdziwy pracownik nigdy nie poprosi również o przekazanie mu całego numeru PESEL. Mogą pojawić się co najwyżej pytania weryfikacyjne - jedno o datę urodzenia, a drugie o 5 ostatnich cyfr numeru PESEL. Nigdy jednak pracownik banku nie zada tych dwóch pytań w jednej rozmowie. Nie poprosi też nigdy o podanie pełnego numeru i serii

dokumentu tożsamości, a także numeru karty płatniczej oraz kodu CVV/CVC.

Oczywiście cyberprzestępcy będą starali stworzyć niezwykle wiarygodną historię, żebyś te informacje pozyskać. Zrobią to nie na początku rozmowy, ale po krótkim wprowadzeniu, które będzie miało na celu uśpić Twoją czujność. Jeśli zapamiętasz nasze rady, to szybko i skutecznie rozpoznasz oszusta.

Podobnie jest z linkami i załącznikami. To metoda, którą bardzo często stosują cyberprzestępcy. Wysyłają maile z fałszywym załącznikiem albo linkiem, który kieruje na podstawioną stronę albo ściąga na Twój sprzęt złośliwe oprogramowanie. Pamiętaj jednak, że nigdy nie robią tego pracownicy banku. W komunikacji z klientem bank ogranicza umieszczanie linków i załączników w wiadomościach do niezbędnego minimum. Jeśli otrzymasz np. wiadomość, że Twoje konto jest zablokowane i w treści będzie link do odblokowania dostępu, albo pracownik banku poprosi o zainstalowanie dodatkowego certyfikatu lub oprogramowania, bądź niezwykle ostrożny. Najprawdopodobniej będzie to bowiem oszustwo.

Na co jeszcze zwrócić uwagę?

Oszuści mogą również próbować zdobyć dostęp do Twojego telefonu i znajdujących się tam informacji, np. wiadomości SMS. W tym celu będą próbowali skłonić Cię do zainstalowania pewnych aplikacji na Twoim sprzęcie. W tym przypadku również użyją wiarygodnych argumentów, np., że jest to nowsza wersja aplikacji bankowej lub aktualizacja, która poprawi bezpieczeństwo itd. Pracownik banku nigdy o to nie poprosi. Jeśli zatem odbierzesz telefon z dziwną prośbą chociażby o zainstalowanie aplikacji do zdalnej weryfikacji albo nowej aplikacji bankowej, od razu rozłącz się.

Więcej na ten temat można przeczytać na stronie

<https://bankomania.pkobp.pl/finanse/bezpieczenstwo/naucz-sie-odrozniac-oszusta-od-pracownika-banku/>

(dk/tm)

