



Oszustwo na pracownika Banku

Metoda wyłudzenia pieniędzy, w której oszuści podszywają się pod pracownika Banku i próbują nakłonić ofiarę przestępstwa do przekazania poufnych danych lub wykonania nieautoryzowanych przelewów. Sprawcy, stosując metodę „na pracownika Banku”, są w stanie przejąć dostęp do konta bankowego i środków na nim zgromadzonych. Przestępcy nie muszą wykorzystywać specjalistycznego oprogramowania do kradzieży danych lub pieniędzy. W popełnianiu przestępstwa pomaga im niestety pokrzywdzony. Sprawcy, manipulując, nakłaniają ofiary przestępstwa do podjęcia określonego działania.

Jak to działa?

- 1) Telefon z „Banku” Oszust dzwoni do ofiary, podając się za pracownika Banku. Często wykorzystuje spoofing, czyli technologię fałszowania numerów telefonów, przez co na ekranie może pojawić się prawdziwy numer Banku.
- 2) Rzekome zagrożenie Oszust informuje, że ktoś próbował włamać się na konto lub dokonać podejrzaną transakcji. Aby zapobiec rzekomej kradzieży pieniędzy „konsultant” poleca zainstalowanie aplikacji, która umożliwia mu zdalne wykonywanie działań na smartfonie czy komputerze rozmówcy. W ten sposób oszust ma dostęp do naszego urządzenia i tym samym konta, z którego dokonuje przelewów, a następnie wypłaca wszystkie zgromadzone na nim środki.
- 3) Presja i pośpiech Aby ofiara nie miała czasu na przemyślenie sytuacji, oszust twierdzi, że trzeba działać natychmiast, inaczej pieniądze zostaną utracone.
- 4) Prośba o poufne dane Oszust może poprosić o: - login i hasło do bankowości internetowej; - kod SMS do autoryzacji przelewu; - dane karty płatniczej.
- 5) Przelew na bezpieczne konto Oszust twierdzi, że pieniądze trzeba natychmiast przelać na nowe, bezpieczne konto. Po wykonaniu operacji fałszywy konsultant informuje o tym, że konto chwilowo zostaje zablokowane, a zgromadzone na nim środki z uwagi na zagrożenie zostaną chwilowo przelane na konto zastępcze. Przejęte środki przelewane są najczęściej na konta bankowe kantorów wymiany walut, skąd w formie gotówki są pobierane przez oszustów.

Jak się bronić?

- 1) Bank nigdy nie prosi o hasła, kody autoryzacyjne ani przelewy na inne konto;
- 2) Jeśli masz wątpliwości, rozłącz się i samodzielnie zadzwoń do Banku;
- 3) Nie podawaj żadnych danych wrażliwych przez telefon;
- 4) Zgłoś próbę oszustwa.

Pamiętaj!

- 1) Konsultanci Banków nigdy nie proszą o podanie poufnych danych takich jak np. numery dokumentów, numery kart bankowych, kody do zatwierdzenia transakcji internetowych;
- 2) Konsultanci Banków nigdy nie proszą o podanie swoich danych logowania do systemu bankowego;
- 3) Do swojego konta bankowego loguj się tylko przez samodzielnie wpisany adres strony internetowej Banku. Nie korzystaj z przesyłanych przez osoby trzecie linków przekierowujących na utworzone przez oszustów strony bankowe do zbierania danych logowania;
- 4) Konsultanci Banków nigdy nie zachęcają do pobierania żadnych aplikacji do szybkiej obsługi klienta. Jedynymi aplikacjami promowanymi przez Bank są te dedykowane do obsługi posiadanych rachunków i kart bankowych.

Dzień dobry, czy potwierdza Pani przelew na kwotę 800 zł dla Pana Dariusza? ... Nie? W takim razie musimy szybko go zablokować. Proszę zainstalować aplikację XXX, to pomogę Pani rozwiązać ten problem.

Witam serdecznie, jestem pracownikiem banku i kontaktuję się z Panem, ponieważ widzę, że z Pana konta 15 minut temu próbowano wykonać transakcję na rachunek XXX, który w naszym systemie znajduje się na czarnej liście. Proszę mi podać swój NIK...

Jestem pracownikiem działu technicznego i zajmuję się bezpieczeństwem naszych klientów. Dzwonię do Pani, ponieważ Pani środki, w kwocie 870 zł, zostały zablokowane. Aby je odblokować zadzwonię do Pani za kilka minut i zaloguje się Pani przy mnie na swój rachunek.

