2021-03-01

Bank Spółdzielczy w Strzegowie

Kliknij tutaj, aby wprowadzić tekst.

Bezpieczeństwo twojego rachunku

Oszuści dzwonią z numerów podszywających się pod numery banku

Ten rodzaj oszustwa wciąż występuje i co jakiś czas się nasila. Oszuści zmieniają jedynie pretekst, pod którym dzwonią. Ostatnio dzwonią i przekonują, że Bank zablokował podejrzany przelew. Następnie nakłaniają do zainstalowania niebezpiecznej aplikacji.

Dlaczego gdy dzwonią oszuści, widać numer naszego banku?

Oszuści wykorzystują słabe strony sieci GSM, które pozwalają im podszywać się pod dowolny numer telefonu - w tym numery banku. Nie jest to związane z jakimkolwiek przełamaniem naszych systemów bezpieczeństwa.

Jak przebiega oszustwo?

Oszust podszywa się pod pracownika działu bezpieczeństwa. Prawdopodobnie będzie znał Twoje imię i nazwisko, a może nawet adres - znajdzie je w internecie. Powie, że udało się zablokować przelew z Twojego konta. Zapewni, że sytuacja jest pod kontrolą i **zachęci Cię do pobrania i zainstalowania aplikacji** (np. Quicksuport od TeamViewer), pod pretekstem usprawnienia komunikacji z bankiem lub usunięcia wirusa.

Jeśli zainstalujesz aplikację, oszust przejmie kontrolę nad Twoim urządzeniem. Sprytnie pozyska od Ciebie dalsze dane, np.: login, hasło, kod z SMS-a autoryzacyjnego. W efekcie wyczyści Twoje konto ze wszystkich pieniędzy!

Jak się bronić?

Pracownicy banku nigdy nie będą zachęcali Cię do instalowania dodatkowego oprogramowania, poza naszą aplikacją . Jeżeli masz wątpliwości co do autentyczności konsultanta, rozłącz się i zadzwoń do Banku samodzienie. W ten sposób zagwarantujesz sobie, że dodzwonisz się do prawdziwego pracownika banku.

W tej sytuacji stosuj się do tych zasad bezpieczeństwa:

- Nigdy nie podawaj przez telefon loginu i hasła do bankowości internetowej.
- Nigdy nie instaluj dodatkowego oprogramowania by poprawić dostępność usług bankowych.
- Poproś rozmówcę o podanie imienia i nazwiska, jeżeli ich sam nie podał. Nasi pracownicy przedstawiają się już na początku rozmowy.
- Pod żadnym pozorem **nie przekazuj telefonicznie kodów z SMS-ów autoryzacyjnych**. SMS-y służą do potwierdzania przelewów czy dodawania nowych zaufanych urządzeń w Twojej bankowości internetowej. Dokładnie czytaj treść otrzymywanych od nas SMS-ów, żeby wiedzieć, czego konkretnie dotyczą!
- Bez dobrze uargumentowanej przyczyny nie podawaj przez telefon również swojego **numeru PESEL**.
- Zachowaj też ostrożność, jeżeli rozmówca wywiera na Tobie **presję czasu**. Oszuści często sugerują, że wszystko, o co proszą, musi być wykonane jak najszybciej. W pośpiechu dużo łatwiej podjąć nieprzemyślane decyzje.

Zarząd Banku Spółdzielczego w Strzegowie