Rejonowy Bank Spółdzielczy
w Lututowie

Rejonowy Bank Spółdzielczy w Lututowie ostrzega – przestępcy podszywają się pod pracowników banków

Dbaj o bezpieczeństwo!

Zobacz, przed czym ostrzegamy.

Bezpieczeństwo to nasze prawo, ale również nasza odpowiedzialność. Troska o bezpieczeństwo danych nabiera szczególnego znaczenia w okresie zagrożenia pandemią. Niestety, wielu przestępców, wykorzystując sytuację, próbuje wyłudzić nasze dane osobowe. Świadomość tego, że możemy zostać oszukani, jest pierwszym krokiem na drodze właściwej ochrony. Żyjemy w przekonaniu, że w pełni chronimy swoje dane, w rzeczywistości jednak każdy z nas jest narażony na ich kradzież, niezależnie od tego, jak dobrze pilnujemy swojego dowodu osobistego czy numeru karty bankomatowej.

Metody oszustów zmieniają się. **Nowym sposobem oszustów jest podszywanie się pod pracownika Rejonowego Banku Spółdzielczego w Lututowie w celu wyłudzenia danych. Często nr telefonu, z którego dzwoni oszust, wyświetla się Klientowi, jakby rzeczywiście pochodził z banku**. W niektórych przypadkach oszust będzie znał imię i nazwisko ofiary, a może nawet adres – znajdzie je w Internecie. Celem działania przestępców jest potwierdzenie posiadanych informacji i pozyskanie innych dodatkowych danych. Przestępca zapewnia, że troszczy się o bezpieczeństwo pieniędzy zdeponowanych na rachunku. Przedstawia Klientowi, że doszło do włamania na jego konto i usiłowania dokonania przelewu. Informuje, że sprawa dotyczy wielu osób, u których zaistniała taka sytuacja i dlatego dzwoni w tej sprawie również do Klienta.

Możliwe jest także, że stosując metody socjotechniczne, przestępca będzie nakłaniał ofiarę do podania danych, np. do logowania do bankowości elektronicznej lub do zainstalowania oprogramowania na komputerze czy telefonie. Oszust pyta Klienta o dowód tożsamości, o jego zwyczaje podczas dokonywania zakupów, np. jak często dokonuje transakcji w Internecie, czy pobiera potwierdzenia zakupów kartą. Prosi także o dane karty płatniczej oraz na wyrażenie zgody na instalację aplikacji zewnętrznej tzw. zdalny pulpit, np. TeamViewer. Gdy Klient odmawia, oszust informuje, że za ewentualne kradzieże z rachunku będzie odpowiedzialny sam Klient. Jeśli Klient dokona instalacji aplikacji zewnętrznej, to oszuści mogą przejąć kontrolę nad urządzeniem ofiary i w ten sposób pozyskać dalsze dane, np.: login, hasło, kod z SMS-a autoryzacyjnego. Efektem tych działań może być kradzież pieniędzy z rachunku bankowego lub zaciągnięcie zobowiązania finansowego w naszym imieniu.

Warto podjąć wszelkie możliwe działania, aby zapewnić sobie bezpieczeństwo.

Pamiętaj, pracownicy banku nigdy:

- nie będą próbowali uzyskać od Ciebie poufnych danych, w szczególności związanych z obsługą bankowości (kodów pin/SMS lub innych danych pozwalających na dokonanie transakcji);
- w żadnym wypadku nie będą zachęcali Cię do instalowania dodatkowego oprogramowania.

W starciu z dobrze zorganizowanym, a przy tym bezwzględnym przeciwnikiem, jakim są krajowe i międzynarodowe grupy przestępcze i cybergangi, warto wiedzieć, jak skutecznie zapewnić sobie bezpieczeństwo.

Pamiętaj!

- Nigdy nie podawaj przez telefon loginu i hasła do bankowości internetowej oraz danych karty.
- Nigdy nie instaluj dodatkowego oprogramowania, by poprawić dostępność usług bankowych. Wyjątkiem są bankowe aplikacje mobilne, ale informacja o nich jest dostępna na stronie internetowej banku **www.rbs.lututow.pl**.
- Poproś rozmówcę o podanie imienia i nazwiska, jeżeli ich sam nie podał, oraz zanotuj numer telefonu, z którego dzwoni.
- Każdorazowo sprawdź, czy w pasku adresu strony internetowej pojawia się symbol kłódki. Adres witryny internetowej strony Bankowości Elektronicznej Banku powinien rozpoczynać się od **https://online.rbs.lututow.pl**.
- 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 banku SMS-ów, żeby wiedzieć, czego konkretnie dotyczą.
- Nie wykonuj działań, o które prosi nieznany Ci nadawca w SMS-ie / wiadomości e-mail itp. Nie klikaj w link.
- 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.

W sytuacji, gdy odbierzesz telefon od osoby podającej się za pracownika banku, jeżeli masz wątpliwości co do autentyczności połączenia, jak również w każdym innym przypadku, w którym podczas korzystania z elektronicznych kanałów dostępu spotkasz się z sytuacją, która wyda ci się nietypowa, podejrzana lub wzbudzi Twoje zaniepokojenie:

- rozłącz się / odłóż słuchawkę – upewnij się, że się rozłączyłeś;
- połącz się z placówką banku, w której została podpisana umowa na dostęp do usług Internet Bankingu, w celu potwierdzenia przekazanych informacji (numery telefonu dostępne są na stronie internetowej banku – **www.rbs.lututow.pl**);
- przed ponownym korzystaniem z bankowości internetowej – przy użyciu nowych środków dostępu – należy upewnić się, że urządzenie, z którego się korzysta, jest wolne od wszelkich podejrzanych instalacji oraz zabezpieczone aktualnym oprogramowaniem antywirusowym.

O każdym przypadku, który wyda się Państwu podejrzany, prosimy poinformować bank. To pozwoli nam na szybką reakcję i ułatwi zatrzymanie przestępców.

Przypominamy – najważniejsza jest zasada ograniczonego zaufania i zachowania zdrowego rozsądku. Tylko ostrożność oraz dokładne weryfikowanie informacji i internetowych kontaktów pozwoli ograniczyć ryzyko zdobycia przez cyberprzestępców dostępu do naszego komputera czy smartfonu, a za ich pośrednictwem do naszego konta bankowego. Pilnujmy swoich dokumentów, informacje na swój temat przekazujmy tylko, jeśli mamy pewność do kogo trafią i w jaki sposób zostaną wykorzystane. Ważne, aby działać świadomie, a gdy już padniemy ofiarą cyberataku, wiedzieć, jak go rozpoznać i gdzie szukać pomocy.