Bank Spółdzielczy w Zawadzkiem

NIE DAJ SIĘ NABRAĆ

Poznaj metody przestępców i nie pozwól się oszukać!

Jak działają oszuści ?

Prawdopodobny scenariusz:

1. Dzwoni telefon, odbierasz.
2. Osoba, z którą rozmawiasz przekonuje, że jest Pracownikiem Banku/Policjantem/Twoim wnuczkiem/krewnym lub inną osobą:

- osoba ta informuje, że pilnie potrzebuje pieniędzy/należy przekazać środki w ramach zabezpieczenia.
- lub wyłudza Twoje dane tj. numer Pesel, numer seryjny dowodu osobistego, numer karty itp.

3. Zostajesz pokierowany jak i gdzie przekazać środki.

4. Pamiętaj, Pracownik Banku/Policjant nigdy nie prosi o przekazanie pieniędzy i nie dzwoni z takim żądaniem.

Pomogłeś? Przekazałeś pieniądze?
Padłeś ofiarą oszusta!

Bądź ostrożny w kontaktach z nieznajomymi i pozornie znajomymi, czyli:

- nie udzielaj poufnych informacji ani nie podejmuj działań, gdy otrzymujesz niespodziewane wiadomości od nieznanych osób online;
- sprawdzaj tożsamość osoby, która prosi o poufne informacje lub pieniądze;
- pamiętaj, że nie każdy jest tym, za kogo się podaje;
- nie przekazuj pieniędzy online, jeśli ktoś nieznajomy prosi Cię o ich przelanie nawet na bardzo ważny cel.

Działaj bez pośpiechu, uważaj na naciski i presję czasu, czyli:

- nie daj się zwieść wyrażeniom typu: „natychmiast", „szybko", „niezwłocznie", „to wymaga pilnego wykonania", „tylko natychmiastowa reakcja" – takie sformułowania mają na celu nakłonić Cię do działania bez zastanowienia;
- nie otwieraj załączników ani nie klikaj w podejrzane linki w e-mailach czy wiadomościach – to częsty sposób na rozprzestrzenianie wirusów komputerowych!

Bądź świadomy i wyedukowany, czyli:

- **dowiedz się** więcej na temat różnych rodzajów oszustw online;
- **przeczytaj** o popularnych schematach oszustw, takich jak phishing, oszustwa telefoniczne i fałszywe strony internetowe, aby poznać sposoby wyłudzania pieniędzy i danych osobowych;
- **śledź** najnowsze wiadomości i bądź na bieżąco – wiedza jest kluczem do ochrony przed oszustwami;
- **ustaw** mocne hasła do swoich kont online oraz unikaj używania tych samych haseł do różnych usług internetowych.

Jakie triki wykorzystują oszuści:

- **udają** kogoś innego np. członków rodziny, pracowników banków czy instytucji, by skłonić nas do ujawnienia poufnych informacji (hasło do konta, kodu PIN) lub przekazania pieniędzy;
- **dzwonią lub wysyłają** fałszywe e-maile albo wiadomości tekstowe, które wyglądają jak wiadomości od zaufanych źródeł, np. banków, firm czy serwisów internetowych;
- **straszą** konsekwencjami i wykorzystują presję czasu, np. mogą twierdzić, że twoje konto bankowe jest zagrożone lub że musisz działać natychmiast, aby uniknąć konsekwencji;
- **manipulują** naszymi emocjami i wykorzystują uczucia innych ludzi, np. udają, że są osobą potrzebującą pomocy finansowej lub emocjonalnej;
- **obiecują** atrakcyjne nagrody, zniżki lub oferty na tanie leki lub cudowne środki na różne dolegliwości zdrowotne albo znakomite urządzenia domowe, a następnie proszę o płatność, dostęp do konta bankowego lub inne informacje, aby skorzystać z tych pozornie korzystnych ofert;
- **gratulują** wygranej w loterii lub konkursie online, w którym nie uczestniczyłeś, i proszą o opłatę wstępną lub dostarczenie swoich danych osobowych w celu odbioru nagrody.

Nim cokolwiek zrobisz albo będziesz mieć wątpliwości podejdź do Banku albo zgłosić się na Komisariat Policji.

NIE DAJ SIĘ OSZUKAĆ!