



Bezpieczna bankowość z Bankiem Spółdzielczym w Kaliszu Pomorskim

Nie daj się oszustom zachowaj ostrożność!



Jak dbamy o bezpieczeństwo naszych klientów?



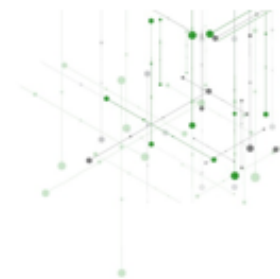
Dbamy o bezpieczeństwo technologiczne
dane i pieniądze klientów
Banku Spółdzielczego w Kaliszu Pomorskim są bezpieczne



Na bieżąco **ostrzegamy** przed oszustami

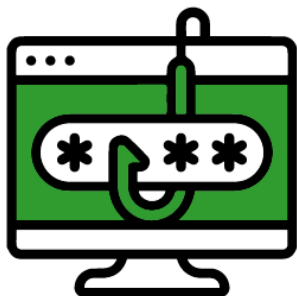


Edukujemy naszych klientów jak bezpiecznie bankować





Z jakich metod najczęściej korzystają oszuści?



Phishing



Vishing i spoofing



Wangiri





Phishing

Co to jest?

Uważaj na phishing



To metoda oszustwa, która polega na **wysyłaniu e-maili lub SMS-ów z załącznikami czy linkami do fałszywych stron internetowych.** Wiadomości mają nakłonić Cię do kliknięcia w link albo otwarcia załącznika.



Bank Spółdzielczy w Kaliszu Pomorskim



Uważaj na phishing

Co ważne, oszuści mogą podszywać się pod pewne osoby lub firmy. Chcą uśpić Twoją czujność, więc dbają o to, aby skala podobieństwa była jak największa. Fałszywe strony wyglądają ładząco podobnie do stron firm, które znasz.



Bank Spółdzielczy w Kaliszu Pomorskim



Czego najczęściej dotyczą fałszywe wiadomości?



Niewielkiej kwoty, którą masz dopłacić do przesyłki

Bonów, kuponów oraz innych darmowych „nagród”, które możesz zdobyć



Podejrzanych logowań na Twoim koncie

Problemów z Twoim kontem lub płatnością



Niekompletnych danych, które musisz potwierdzić

Niezapłaconej faktury, którą masz opłacić



Jak przebiega oszustwo?

1 Dostajesz e-maila lub SMS-a. Wiadomość wygląda jak z firmy, którą dobrze znasz.

2 Masz pilnie zalogować się na stronę banku przez link z wiadomości. Najczęściej po to, aby odebrać rzekome pieniądze.

3 Link przekierowuje Cię na fałszywą stronę, która przypomina stronę Twojego banku.

4 Logujesz się – podajesz swoje dane oraz kod z SMS-a.

5 Masz wpisać kolejne kody SMS, aby zaktualizować swoje dane.

6 Widzisz komunikat o błędzie, więc wpisujesz je kilka razy.

! Pamiętaj: zawsze dokładnie czytaj kody SMS – czy treść powiadomienia z kodem odpowiada temu co akurat chcesz zrobić na stronie? Zwracaj też uwagę na to, które urządzenia dodajesz do zaufanych.

7 Oszust dostał dostęp do Twojego konta. Od teraz może się na nie logować i z niego korzystać.



Jak się chronić?



Pamiętaj o zasadzie **ograniczonego zaufania**.

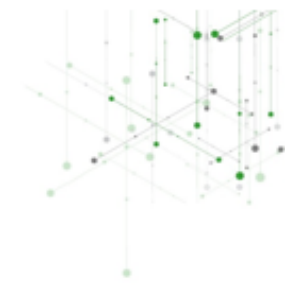
Zanim klikniesz w link lub pobierzesz jakiś plik, upewnij się, że pochodzą one z zaufanych źródeł.

Filtruj spam i zainwestuj w **oprogramowanie antywirusowe**, najlepiej z modułem antyphishingowym.

Czytaj powiadomienia push z aplikacji bankowych i na bieżąco **kontroluj** przelewy na swoim koncie.



Bank Spółdzielczy w Kaliszu Pomorskim





Vishing i spoofing

Czym są?

Uważaj na vishing



Vishing to metoda oszustwa, która polega na podszywaniu się pod pracowników banków i innych zaufanych instytucji, np. policjantów.

Oszuści chcą w ten sposób zdobyć Twoje poufne dane (np. login i hasło do bankowości internetowej) lub nakłonić Cię do określonych czynności (np. zainstalowania aplikacji do zdalnej obsługi urządzenia).



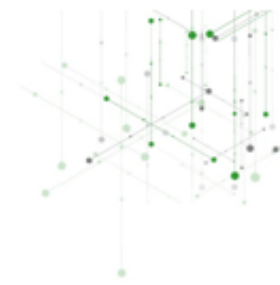
Bank Spółdzielczy w Kaliszu Pomorskim



Uważaj na spoofing



Spoofing to metoda oszustwa, która polega na podszywaniu się pod inne urządzenia lub innego użytkownika. Oszuści zmieniają numer telefonu, adres e-mail czy adres IP, z których się kontaktują. Mogą też wybrać i zmienić płeć osoby dzwoniącej, jej kraj pochodzenia, a nawet akcent. Zawsze dobrze przygotowują się do rozmowy, aby była ona wiarygodna i uśpiła Twoją czujność



Jak przebiega takie oszustwo?

1

Odbierasz telefon od oszusta.

2

Oszust przekazuje Ci informację o płatności na Twoim koncie i prosi o potwierdzenie jej wykonania. Często oszuści przekazują też informację o logowaniu spoza granic Polski.

3

Odpowiadasz na wszystkie pytania, których oficjalnym celem jest zweryfikowanie klienta.

4

Oszust informuje Cię, że musi zablokować fałszywą transakcję lub przeprowadzić „zdalne skanowanie antywirusowe”. W tym celu masz zainstalować specjalną aplikację.

5

Instalujesz aplikację, a Twoje dane trafią do oszusta – ma dostęp do Twojego konta i pieniędzy na nim.




Pamiętaj: Oszuści stosują wyćwiczone techniki manipulacji. Podszywają się pod prawdziwe numery telefonów! Kiedy dzwonią, na Twoim telefonie może wyświetlić się inny, znany numer lub nazwa banku.



Bank Spółdzielczy w Kaliszu Pomorskim




Jak się chronić?




Nigdy nie podawaj loginu i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, data ważności).




Zawsze czytaj treść SMS-ów i komunikatów z aplikacji mobilnej, które dostajesz.



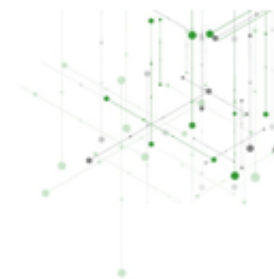
Jeżeli jakakolwiek rozmowa wzbudza Twoje wątpliwości, rozłącz się. Odczekaj minimum 30 sekund, a następnie samodzielnie połącz się z instytucją, z której dzwonił rzekomy przedstawiciel.



Nie instaluj dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do aplikacji bankowej.



Nie zgadzaj się na alternatywny kontakt mailowy czy SMS-owy. Oszust może chcieć wysłać link lub załącznik, który może zainfekować Twoje urządzenie.



Jak się chronić?

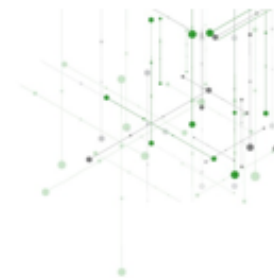


Pamiętaj, że pracownicy banku podczas rozmowy telefonicznej nigdy nie poproszą Cię o:

- instalację dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do bankowości internetowej i mobilnej,
- hasła dostępu, kody PIN/SMS lub inne dane do transakcji.



Bank Spółdzielczy w Kaliszu Pomorskim



Jak się chronić?

Weryfikacja tożsamości w aplikacji mobilnej Nasz Bank – jak to przebiega?



W trakcie rozmowy możesz poprosić o potwierdzenie tożsamości przez pracownika Banku

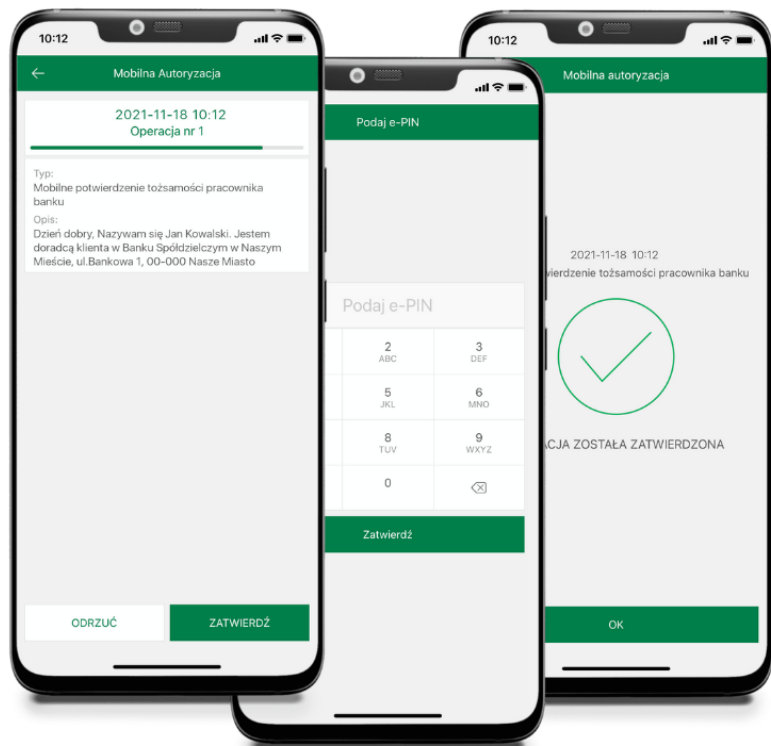
W aplikacji mobilnej Nasz Bank wyświetlana jest wiadomość z danymi pracownika

Pracownik wysyła z systemu bankowego wiadomość PUSH, w której podaje swoje imię i nazwisko



Jak się chronić?

Weryfikacja tożsamości w aplikacji mobilnej Nasz Bank – jak to przebiega?



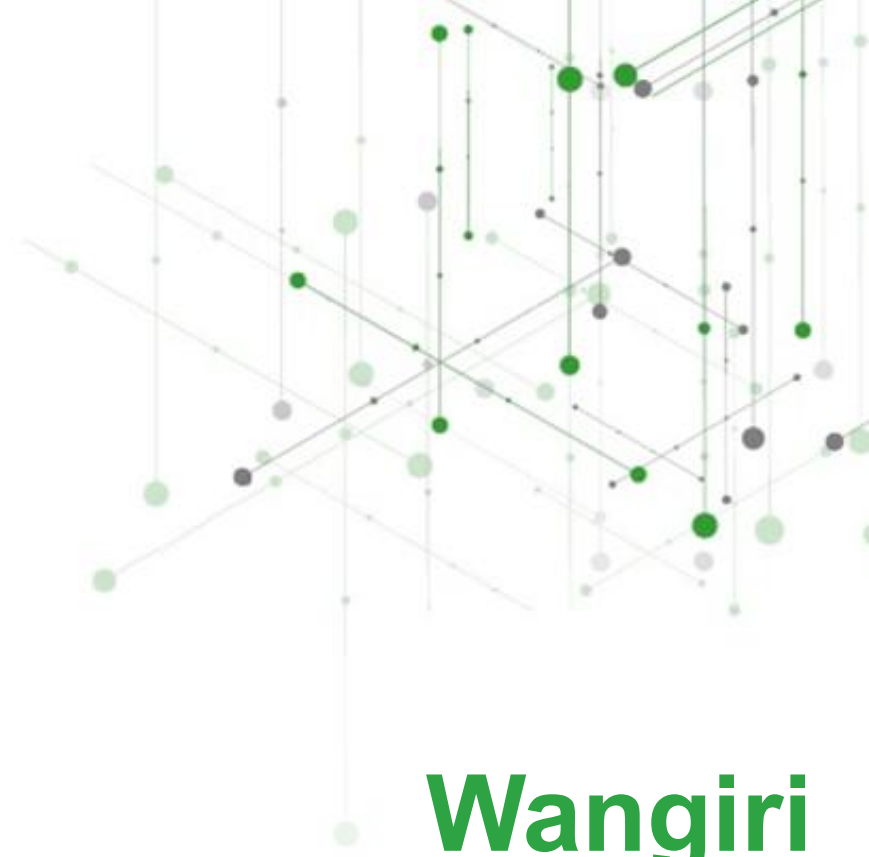
W trakcie rozmowy pracownik Banku może poprosić rozmówcę o potwierdzenie swojej tożsamości w aplikacji mobilnej

Pracownik wysyła z systemu bankowego wiadomość autoryzacyjną, potwierdzenia kontaktu z bankiem

W aplikacji mobilnej Nasz Bank wyświetlana jest wiadomość z potwierdzeniem prowadzenia rozmowy z pracownikiem banku

Po zatwierdzeniu autoryzacji pracownik Banku otrzymuje w systemie bankowych informację o autoryzacji rozmowy przez uprawnionego rozmówcę





Wangiri

Co to jest?

Jak przebiega oszustwo?



Pamięta: zawsze dokładnie sprawdzaj numery telefonów, które do Ciebie dzwonią, najczęściej oszuści dzwonią z numerów zaczynających się na: +373, +383, 216,, +252, +63, +223, +994, +93

1 Oszust dzwoni raz i natychmiast się rozłącza lub rozłącza się natychmiast po odebraniu połączenia

2 Z ciekawości oddzwaniamy na wyświetlony numer połączenia

3 Połączenie trafia na wysokopłatną infolinię

4 Oszust celowo przedłuża rozmowę aby rachunek za połączenie był jak najwyższy



Bank Spółdzielczy w Kaliszu Pomorskim



Jak się chronić?



Pamięta: zawsze dokładnie sprawdzaj numery telefonów, które do ciebie dzwonią, najczęściej oszuści dzwonią z numerów zaczynających się na: +373, +383, 216,, +252, +63, +223, +994, +93

1

Nie oddzwaniaj na podejrzane, zagraniczne numery

2

Sprawdzaj zawsze numery przed oddzwonieniem

3

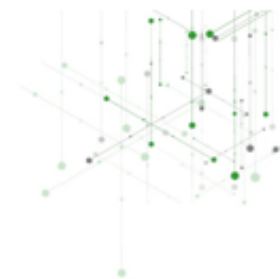
Gdy połączenie budzi Twoja wątpliwość natychmiast się rozłącz

4

Zablokuj podejrzane połączenia w telefonie



SGB Bank Spółdzielczy w Kaliszu Pomorskim





4 zasady bezpiecznego bankowania

Przestrzeganie zasad bezpiecznego korzystania z bankowości mobilnej i internetowej pozwoli na zminimalizowanie ryzyka włamania na konto bankowe ze strony cyberprzestępców

Jak się chronić?



Chron
swoje
hasła



Nie podawaj nikomu swojego hasła. Regularnie je zmieniaj. Używaj różnych haseł do różnych usług. Twórz skomplikowane hasła z wykorzystaniem znaków specjalnych. Nie zapisuj haseł na kartkach ani w plikach. Używaj managerów haseł o silnych algorytmach szyfrowania.



Bank Spółdzielczy w Kaliszu Pomorskim



Jak się chronić?

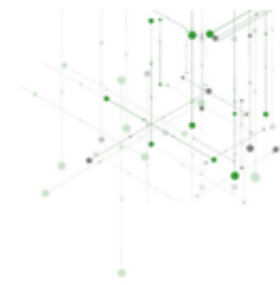
2.



! Nie otwieraj plików/linków nieznanego pochodzenia.
Czytaj SMS-y. Zwracaj uwagę na to co autoryzujesz.
Nie udostępniaj innym swojego komputera i telefonu.



Bank Spółdzielczy w Kaliszu Pomorskim



Jak się chronić?

3.

Weryfikuj
tożsamość
rozmówcy

Nigdy nie podawaj przez telefon poufnych danych, haseł dostępu, numeru PIN, kodów SMS. Pracownicy banku nigdy nie poproszą telefonicznie o takie informacje.
Wykorzystuj weryfikację tożsamości w aplikacji Nasz Bank.



Bank Spółdzielczy w Kaliszu Pomorskim



Jak się chronić?

4.

Ostrożnie
korzystaj




Ustal odpowiednie limity transakcji.
Nie loguj się do bankowości przez
publiczną sieć Wi-Fi. Zainstaluj
oprogramowanie antywirusowe.
Aktualizuj system operacyjny
i aplikacje. Pamiętaj o wylogowaniu.
Jeśli cokolwiek wzbudzi Twój niepokój
skontaktuj się z bankiem.



Bank Spółdzielczy w Kaliszu Pomorskim





**Zachowaj czujność!
Nie daj się oszustom!
Jeżeli coś zbudzi twoją wątpliwość skontaktuj się z bankiem**

**Oddział Kalisz Pomorski
94 3616348**

**Oddział Złocieniec
94 3671334**