Fałszywe sklepy i SMS-y premium - jak unikać oszustw mobilnych

Cyberprzestępcy nieustannie opracowują nowe metody, aby wyłudzić nasze dane osobowe, pieniądze lub zainstalować złośliwe oprogramowanie na naszych urządzeniach.

Ta prezentacja pomoże Ci zrozumieć, jak działają najpopularniejsze oszustwa mobilne, jak je rozpoznać oraz - co najważniejsze - jak się przed nimi skutecznie chronić. Poznasz praktyczne wskazówki, które pomogą Ci bezpiecznie korzystać z urządzeń mobilnych.

Co to są oszustwa mobilne?

Wyłudzenie danych

Kradzież loginów, haseł, numerów kart płatniczych i innych wrażliwych informacji.

Niechciane płatności

Naciąganie na nieautoryzowane opłaty lub subskrypcje.

Złośliwe oprogramowanie

Instalacja programów szpiegujących lub blokujących urządzenie.

Najczęstsze formy oszustw mobilnych to fałszywe sklepy internetowe, które wyglądają jak prawdziwe, ale nie wysyłają zamówionego towaru lub zbierają dane płatnicze, oraz SMS-y premium, które powodują wysokie opłaty za ich odebranie lub wysłanie.

Fałszywe sklepy – jak działają?

Atrakcyjna oferta

Kuszą wyjątkowo niskimi cenami i promocjami typu „tylko dziś", aby skłonić do szybkiej, nieprzemyślanej decyzji.

Profesjonalny wygląd

Mają strony internetowe łudząco podobne do znanych marek, co wzbudza zaufanie potencjalnych ofiar.

Brak kontaktu

Nie podają danych kontaktowych lub podany adres e-mail nie działa, co uniemożliwia późniejszą reklamację.

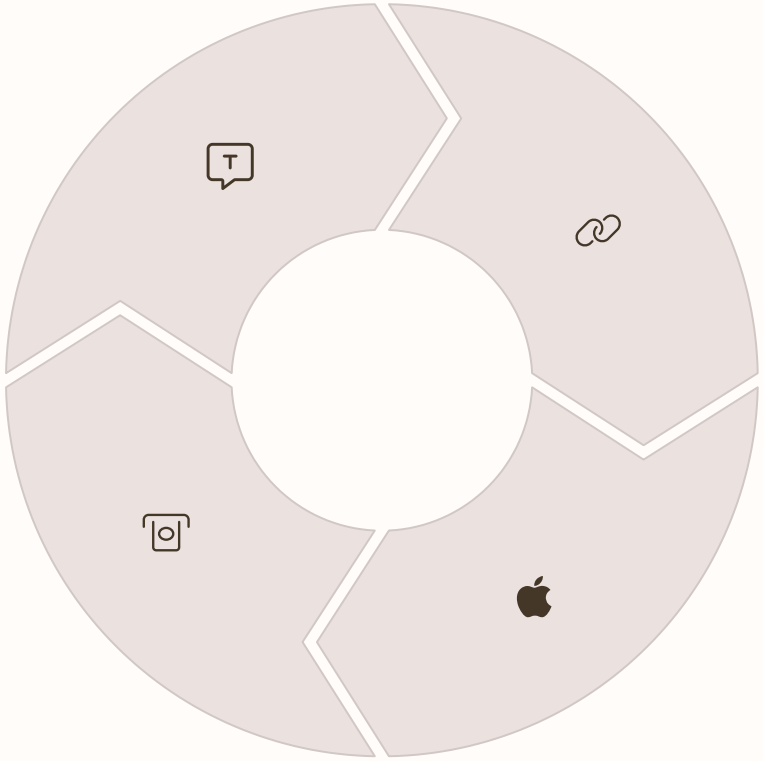
Płatność z góry

Wymagają płatności przed wysyłką, często kartą lub przelewem ekspresowym, po czym kontakt się urywa.

SMS-y premium – gdzie czyha pułapka?

Wiadomość-przynęta

Przychodzi SMS z informacją o paczce, wiadomości głosowej lub wygranej nagrodzie.



Niebezpieczny link

W treści znajduje się link prowadzący do podejrzanej strony internetowej.

Aktywacja opłat

Uruchamiana jest subskrypcja płatnych wiadomości lub usługa SMS premium.

Fałszywa aplikacja

Strona prosi o instalację aplikacji, która często zawiera złośliwe oprogramowanie.

Oszuści często podszywają się pod znane firmy kurierskie, banki lub operatorów telefonicznych, aby wzbudzić zaufanie i skłonić ofiarę do kliknięcia w link.

Jak rozpoznać oszustwo?

Podejrzane sklepy

- **Brak opinii lub same pozytywne recenzje na stronie**
- **Strona powstała niedawno (można sprawdzić przez serwisy Whois)**
- **Brak certyfikatu bezpieczeństwa (adres zaczyna się od „http" zamiast „https")**
- **Niezrozumiały regulamin, błędy językowe, dziwna nazwa domeny**

Podejrzane SMS-y

- **Treść wiadomości jest ogólna, bez imienia, numeru zamówienia**
- **Link prowadzi do strony z dziwnym adresem**
- **Prośba o instalację aplikacji lub podanie danych logowania**
- **Presja czasu i emocji ("Ostatnia szansa!", "Pilne!")**

Oszuści często wykorzystują techniki socjotechniczne, wzbudzając poczucie pilności lub strachu, aby skłonić ofiarę do szybkiego, nieprzemyślanego działania.

Jak się chronić?

Zachowaj ostrożność

Nie klikaj w podejrzane linki w SMS-ach i komunikatorach. Zawsze weryfikuj nadawcę wiadomości.

Bezpieczne źródła

Nie instaluj aplikacji spoza oficjalnych sklepów (Google Play, App Store). Sprawdzaj uprawnienia aplikacji.

Ochrona urządzenia

Zainstaluj program antywirusowy na telefonie i włącz filtrowanie SMS-ów premium u operatora.

Bezpieczne płatności

Płać przy odbiorze lub przez bezpieczne pośrednictwo (np. BLIK, PayU). Sprawdzaj opinie o sklepie.

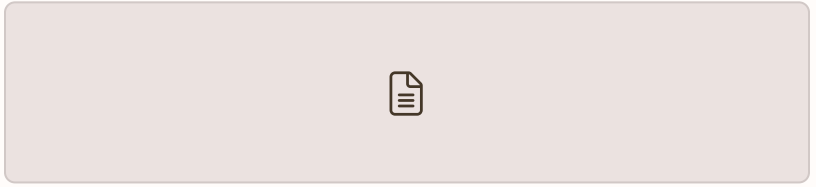
Co robić, jeśli padniesz ofiarą?

Kontakt z bankiem

Niezwłocznie skontaktuj się z bankiem - możliwe, że uda się cofnąć transakcję

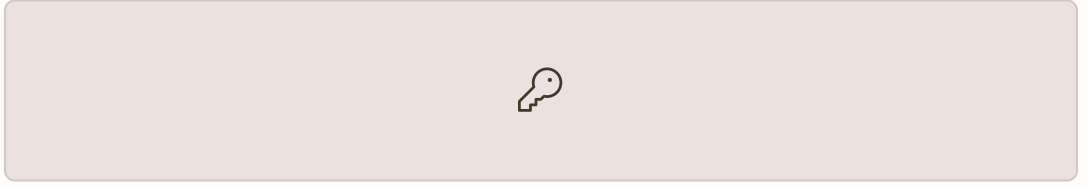
Zgłoszenie operatorowi

Poinformuj operatora, jeśli zostały aktywowane usługi premium



Zgłoszenie oszustwa

Zgłoś sprawę do CERT Polska lub na stronie incydent.cert.pl



Zmiana haseł

Zmień hasła do kont, które mogły zostać przejęte

Pamiętaj, aby usunąć wszystkie podejrzane aplikacje z telefonu i wykonać pełne skanowanie urządzenia w poszukiwaniu złośliwego oprogramowania.

Pamiętaj:

Zbyt piękne, by było prawdziwe

Jeśli oferta wygląda zbyt dobrze, by była prawdziwa – najpewniej taka właśnie jest. Wyjątkowo niskie ceny powinny wzbudzić Twoją czujność.

Podszywanie się

Cyberprzestępcy potrafią podszywać się nawet pod znane firmy kurierskie, operatorów i sklepy. Zawsze weryfikuj tożsamość nadawcy.

Ostrożność przede wszystkim

Zachowuj ostrożność – telefon to dziś komputer z Twoimi danymi, kontami i finansami. Chroń go tak samo jak swój portfel.

Pamiętaj, że cyberprzestępcy liczą na Twoją nieuwagę i pośpiech – nie daj im tej satysfakcji!