Nie daj się oszustom!
Poznaj metody, z których najczęściej korzystają

Vishing – co to jest?
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).

Spoofing – co to jest?
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. Zawsze dobrze przygotowują się do rozmowy, aby była ona wiarygodna i uśpiła Twoją czujność.

Jak się chronić?
- Nie podawaj loginu i hasła do bankowości internetowej oraz danych karty płatniczej (numer karty, CVV, data ważności).
- Dokładnie czytaj treść SMS-ów i komunikatów z aplikacji mobilnej, które dostajesz.
- Jeżeli jakakolwiek rozmowa wzbudza Twoje wątpliwości lub niepokój, rozłącz się. Chwilę później samodzielnie połącz się z instytucją, z której dzwonił rzekomy przedstawiciel. Koniecznie wpisz numer samodzielnie – nie oddzwaniaj na wcześniejsze połączenie.
- Nie instaluj dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do aplikacji bankowej.
- Nie zgadzaj się na alternatywny kontakt mailowy czy SMS-owy.

Phishing- co to jest?
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. Następnie masz przekazać swoje poufne dane, np. numer PESEL, numer dowodu, adres, login i hasło do bankowości internetowej czy numer karty płatniczej. Oszuści mogą podszywać się pod pewne osoby lub firmy.

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 się chronić?

- 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

Jeśli doszło do oszustwa, coś budzi Twoją wątpliwość lub nie działa tak jak powinno, jak najszybciej skontaktuj się ze swoim Bankiem Spółdzielczym lub zadzwoń na Infolinię SGB, czynną 24/7:

800 888 888 (bezpłatne połączenie)
61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora)

Więcej o bezpiecznym bankowaniu przeczytacie na stronie:
www.sgb.pl/bezpieczenstwo-w-sieci