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

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. 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 anty-wirusowe, najlepiej z modułem antyphishingowym.
- Czytaj powiadomienia push z aplikacji bankowych i na bieżąco kontroluj przelewy na swoim koncie.

Vishing i spoofing

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.

Fałszywe inwestycje

To metoda oszustwa, która polega na **podszywaniu się pod maklerów i brokerów giełdowych**. Proponują nowe możliwości zainwestowania Twoich środków, które np. wcześniej nie były dostępne na rynku dla każdego. Doskonale przedstawiona oferta staje się przekonująca, przez co ciężko rozpoznać kłamstwo. Co więcej, oszuści bardzo często wykorzystują wizerunki znanych osób czy firm. Dzięki temu oferta i możliwość szybkiego oraz wysokiego zarobku wydają się jeszcze bardziej wiarygodne. Oszuści stosują oprogramowanie do zdalnej obsługi urządzenia.

Jak się chronić?

- Nie podawaj loginu i hasła do bankowości internetowej oraz danych karty płatniczej (numer karty, CVV, data ważności).
- Nie instaluj dodatkowego oprogramowania (np. AnyDesk) na urządzeniach, z których logujesz się do aplikacji bankowej.
- Jeśli otrzymasz przelew z obcego rachunku, który wygląda jak „zwykły" od innej osoby, nie przekazuj go dalej. Jeśli to zrobisz, weźmiesz udział w przestępstwie – praniu pieniędzy.
- Omijaj podejrzane inwestycje. Zawsze przemyśl wszystkie za i przeciw.
- Jeśli masz podejrzenie, że to oszustwo, zadzwoń na policję.