Oszustwa internetowe: jak je rozpoznać i jak się chronić?

W dobie cyfryzacji ...

W dobie cyfryzacji i powszechnego dostępu do internetu, **oszustwa internetowe stają się coraz bardziej powszechne.**

Oszuści wykorzystują różne metody, aby wyłudzić pieniądze lub dane osobowe. Dowiedz się, jak je rozpoznać i skutecznie się przed nimi chronić.

Czym są oszustwa internetowe?

Oszustwa internetowe to działania mające na celu **wyłudzenie pieniędzy lub danych osobowych.** Najczęściej odbywają się za pośrednictwem e-maili, SMS-ów, rozmów telefonicznych lub fałszywych stron internetowych.

Banki

Podszywanie się pod instytucje finansowe

Firmy kurierskie

Fałszywe powiadomienia o przesyłkach

Sklepy internetowe

Nieistniejące oferty zakupowe

Bliskie osoby

Wyłudzenia "na znajomych"

Oszuści często podszywają się pod zaufane instytucje, takie jak banki, firmy kurierskie, sklepy internetowe, a nawet bliskie osoby.

Najczęstsze rodzaje oszustw

1

Phishing

To metoda polegająca na wysyłaniu fałszywych wiadomości, które zachęcają do kliknięcia w podejrzane linki. Przykłady takich wiadomości to: **„Twoje konto zostanie zablokowane"** lub **„Dopłać 1,99 zł do paczki"**.

2

Fałszywe sklepy internetowe

Kuszą wyjątkowo niskimi cenami, ale po dokonaniu wpłaty towar nigdy nie zostaje dostarczony.

3

Wyłudzenia „na znajomego"

Oszuści podszywają się pod znajomych lub członków rodziny, prosząc o pilną pożyczkę.

Przykład z życia

> Wyobraź sobie, że otrzymujesz SMS od „kuriera" z informacją, że Twoja paczka nie może zostać dostarczona, chyba że dopłacisz 2 zł.

SMS od kuriera

Wiadomość z linkiem do dopłaty

Podejrzana strona

Adres zawiera literówki, układ budzi wątpliwości

Prośba o dane

Żądanie danych do logowania do banku

W wiadomości znajduje się link prowadzący do strony, która wygląda podejrzanie — adres zawiera literówki, a układ strony budzi wątpliwości. Po wejściu na stronę proszą Cię o podanie danych do logowania do banku. To klasyczny przykład oszustwa.

Jak się chronić? Krok po kroku

01

Nie klikaj w podejrzane linki

Jeśli nie zamawiałeś/-aś żadnej paczki, zignoruj wiadomość.

02

Sprawdzaj adresy stron internetowych

Upewnij się, że adres strony jest poprawny i zaczyna się od „https://".

03

Nie podawaj danych do banku

Nigdy nie wpisuj danych logowania na stronach, które otrzymałeś/-aś w wiadomości SMS lub e-mail.

04

Ustaw powiadomienia o transakcjach w banku

Dzięki temu szybko wykryjesz nieautoryzowane operacje na swoim koncie.

Włącz dwuskładnikowe uwierzytelnianie (2FA)

2FA to dodatkowa warstwa zabezpieczeń, która sprawia, że samo hasło nie wystarczy, aby ktoś uzyskał dostęp do Twojego konta.

Najczęściej stosowane formy 2FA to:

Kod SMS

Jednorazowy kod wysyłany na telefon

Aplikacje uwierzytelniające

np. Google Authenticator, Microsoft Authenticator

Klucze bezpieczeństwa

np. YubiKey

Dlaczego warto?

Nawet jeśli cyberprzestępca pozna Twoje hasło, bez dodatkowego kodu nie zaloguje się do konta. To jeden z najskuteczniejszych sposobów ochrony przed przejęciem profilu w banku, mediach społecznościowych czy poczcie e-mail.

Co zrobić, jeśli podejrzewasz oszustwo?

1

Skontaktuj się z bankiem

Niezwłocznie poinformuj o sytuacji

2

Zgłoś incydent

Na stronie: https://incydent.cert.pl

Pamiętaj

Pamiętaj, że **ostrożność i zdrowy rozsądek to Twoi najlepsi sprzymierzeńcy** w walce z oszustami internetowymi.

Dbaj o swoje dane i nie daj się oszukać!

RIG REGIONALNA IZBA GOSPODARCZA W KALISZU
UŁATWIAMY BIZNES • ŁĄCZYMY PRZEDSIĘBIORCÓW •

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych
Moc Małych Społeczności