



Oszustwa internetowe

Fałszywi znajomi

Oszuści podszywają się pod bliskich lub znajomych, wykorzystując np. komunikatory internetowe (WhatsApp, Messenger). Często proszą o szybką pomoc finansową, twierdząc, że znaleźli się w nagłej sytuacji (np. wypadek, zgubienie dokumentów).

Sygnały ostrzegawcze:

- Wiadomości od osób, które rzadko się kontaktują lub piszą w nietypowy sposób (np. błędna polszczyzna, nietypowe godziny kontaktu).
- Prośby o przelanie pieniędzy „natychmiast” lub „potajemnie”, w tym również od niedawno poznanej osoby, dalekiego krewnego lub „amerykańskiego żołnierza”
- Nieznany numer telefonu lub nowe konto na komunikatorze, rzekomo należące do bliskiej osoby.

Jak się bronić?

- Zawsze weryfikuj tożsamość osoby dzwoniącej lub piszącej, kontaktując się z nią w inny sposób (np. na komunikatorze).
- Nigdy nie przesyłaj pieniędzy bez upewnienia się, że prośba jest autentyczna.
- Ustaw silne hasła i pamiętaj o innych zasadach bezpieczeństwa w sieci.

Fałszywe biura podróży

Cyberprzestępcy tworzą strony internetowe podszywające się pod znane biura podróży, oferując wycieczki w atrakcyjnych cenach. Po opłaceniu „wyjazdu” klient nie otrzymuje żadnych dokumentów ani możliwości kontaktu.

Sygnały ostrzegawcze:

- Zbyt niskie ceny wycieczek w porównaniu do rynkowych ofert.
- Brak pełnych danych kontaktowych (tylko formularz, brak numeru telefonu).
- Strona internetowa o podejrzanej domenie (np. nietypowy rozszerzenie .xyz zamiast .pl lub .com).

Jak się bronić?

- Sprawdzaj opinie o biurze podróży na niezależnych stronach i forach.
- Weryfikuj stronę w publicznych rejestrach firm oraz sprawdzaj, czy biuro posiada odpowiednie licencje.
- Płać tylko za pomocą bezpiecznych metod (unikaj przelewów na prywatne konta).

Fałszywe bilety na wydarzenia

Oszuści sprzedają bilety na wydarzenia (koncerty, spektakle, mecze), które albo nie istnieją, albo są sfałszowane i nie dają prawa wstępu na stadion czy halę. Oferty często pojawiają się na portalach społecznościowych i w serwisach ogłoszeniowych.

Sygnały ostrzegawcze:

- Bilety sprzedawane po zaniżonych cenach lub na wydarzenia, które są już oficjalnie wyprzedane.
- Sprzedawca nalega na szybki przelew, często bez możliwości odbioru osobistego.
- Brak możliwości otrzymania faktury lub potwierdzenia zakupu.

Jak się bronić?

- Kupuj bilety tylko z oficjalnych źródeł lub zaufanych platform biletowych.
- Unikaj ofert na portalach społecznościowych i od nieznajomych osób.
- W przypadku zakupu od osoby prywatnej sprawdź możliwość płatności za pobraniem.

Fałszywe zbiórki charytatywne

Oszuści zakładają fałszywe zbiórki online, często wykorzystując emocje i dramatyczne historie (np. choroby dzieci, pomoc dla ofiar katastrof). Zebrane pieniądze trafiają na konto oszusta zamiast do potrzebujących.

Sygnały ostrzegawcze:

- Zbiórki bez dokładnych informacji o organizacji, brak numeru KRS w przypadku fundacji.
- Naglące prośby o wsparcie natychmiastowe", szantaż emocjonalny.
- Brak możliwości sprawdzenia, jak wykorzystane będą zebrane środki.

Jak się bronić?

- Wspieraj tylko zbiórki organizowane przez zaufane organizacje, które możesz zweryfikować.
- Sprawdzaj, czy zbiórka jest zarejestrowana na oficjalnych platformach, takich jak *Siepomaga* czy *Zrzutka*
- Unikaj przesyłania pieniędzy bezpośrednio na prywatne konta bankowe.

Fałszywe loterie i konkursy

Na czym polega oszustwo? Oferty wygrania atrakcyjnych nagród (np. elektroniki, wakacji) w zamian za „drobne opłaty administracyjne” lub podanie danych osobowych.

Sygnaly ostrzegawcze:

- Wiadomości o „wygranej” w konkursie, w którym senior nigdy nie brał udziału.
- Prośby o podanie danych osobowych lub wykonanie przelewu przed otrzymaniem nagrody.
- Brak regulaminu konkursu i szczegółowych informacji o organizatorze.

Jak się bronić?

- Nigdy nie podawaj danych osobowych ani nie płać za odbiór rzekomej nagrody.
- Sprawdzaj autentyczność konkursów, weryfikując organizatora i regulamin.
- Zgłaszaj podejrzane konkursy do odpowiednich instytucji, takich jak CERT Polska.