Phishing *to oszustwo, w którym przestępcy podszywają się pod zaufany podmiot lub osobę przy pomocy fałszywych wiadomości e-mail, SMS/MMS czy połączeń telefonicznych chcąc wyłudzić nasze dane i wykraść pieniądze.*

#Halo!
Tu cyberbezpieczny Senior

Najpopularniejsze przykłady phishingu:

niezapłacona faktura

problemy z kontem bankowym (np. informacje o blokadzie lub podejrzanej aktywności na koncie)

wygrane w loterii, zniżki i kupony do popularnych sklepów

problemy z wypłaceniem dodatkowych świadczeń

Pamiętaj!
Fałszywe wiadomości do złudzenia przypominają te prawdziwe.

Jak się chronić przed fałszywymi wiadomościami?

- Uważaj na wiadomości, które wykorzystują Twoje emocje (np. stres, lęk, presję czasu) i namawiają do podjęcia natychmiastowych działań.
- Zweryfikuj nadawcę wiadomości i dokładnie przeczytaj jej treść. Sprawdź, czy nie zawiera błędów językowych, stylistycznych lub literówek.
- Nie klikaj w przesłane do Ciebie linki i nie otwieraj załączników, jeśli nie wiesz, co się w nich znajduje.
- Jeśli otworzyłaś/-eś link, sprawdź adres strony, na którą nastąpiło przekierowanie.
- Nie udostępniaj nikomu swoich danych poufnych (np. numeru PESEL, danych do logowania, numerów kart płatniczych).
- Włącz weryfikację dwuetapową na swoich kontach (m.in. poczta email, bankowość elektroniczna, serwisy społecznościowe). To dodatkowa ochrona, która utrudnia dostęp oszustom do Twoich danych.

Jeśli wiadomość budzi Twoje podejrzenia, zgłoś ją do zespołu CERT Polska. Poproś zaufaną osobę, aby pomogła Ci wypełnić formularz i przesłać zgłoszenie.

Bądź świadomy i poinformowany!

NIE WYKRĘCISZ MI TEGO NUMERU! SENIOR BEZPIECZNY W SIECI

NASK

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

WARSZAWSKI INSTYTUT BANKOWOŚCI

CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI CBZC