Smishing *to rodzaj oszustwa polegający na wysyłaniu fałszywych wiadomości tekstowych na telefon potencjalnej ofiary.*

#Halo!
Tu cyberbezpieczny Senior

Bądź czujny wobec zagrożeń i poznaj skuteczne metody obrony przed nimi. Pamiętaj! Nie każdy kto do Ciebie pisze, ma dobre zamiary.

Metody oszustw:

nieopłacona faktura

dopłata do przesyłki

problemy z rachunkiem bankowym (zablokowane konto, wniosek o pożyczkę)

wygrane w loteriach, informacje o niespodziewanej nagrodzie

Jak się chronić przed oszustwami typu smishing?

- Nie działaj pochopnie, nie podejmuj decyzji pod wpływem emocji i presją czasu.
- Zweryfikuj nadawcę. Zadzwoń pod numer instytucji, od której dostałeś/-aś wiadomość lub odwiedź jej oddział.
- Nie klikaj w linki i nie otwieraj załączników, jeśli nie wiesz co zawierają.
- Stosuj silne hasła oraz weryfikację dwuetapową. Jeśli nie wiesz jak to zrobić, poproś o pomoc kogoś bliskiego.
- Zwracaj uwagę na komunikaty i ostrzeżenia, które otrzymujesz od banku lub innych instytucji.
- Podejrzane wiadomości SMS możesz bezpośrednio przekazać do zespołu CERT Polska.

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