Spoofing i vishing
to oszustwa z wykorzystaniem połączeń telefonicznych. Przestępcy podszywają się pod przedstawicieli zaufanych instytucji, naszych bliskich i znajomych, by namówić nas do podjęcia określonych działań.

#Halo!
Tu cyberbezpieczny Senior

Najpopularniejsze metody oszustw:

na wnuczka
(np. wypadek, zepsuty telefon, pilnie potrzebne pieniądze)

na policjanta, lekarza
(np. zatrzymanie członka rodziny, próba kradzieży pieniędzy, pilna konsultacja lekarska)

na przedstawiciela banku i pomoc techniczną
(np. zablokowanie środków finansowych)

na pracownika ZUS lub innej instytucji
(np. problem z wypłaceniem emerytury)

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

Jak się chronić przed oszustwami telefonicznymi?

- Nie działaj pod wpływem emocji i presją czasu, nie podejmuj żadnych pochopnych decyzji.
- Unikaj odbierania telefonu słowami: „Tak, słucham”.
- Zwracaj uwagę na wszelkie nieścisłości w komunikatach lub pytania, których nie rozumiesz albo wydają się podejrzane. Zwracaj uwagę na błędy językowe lub zagraniczny akcent.
- Nigdy nie podawaj nikomu wrażliwych informacji (np. PESEL, nazwisko panieńskie), numerów kart płatniczych, danych logowania i kodów autoryzacyjnych.
- Nie pobieraj ani nie instaluj aplikacji lub oprogramowania za czyjąś namową.
- Rozłącz się i zweryfikuj rozmówcę. Zadzwoń pod znany numer instytucji lub odwiedź oddział stacjonarny. W przypadku telefonu od rodziny, skontaktuj się bezpośrednio z osobą, za którą ktoś się podaje.
- Jeśli otrzymasz nietypowy telefon, porozmawiaj o tym z kimś zaufanym np. rodziną, przyjaciółmi i powiedz o niepokojącym połączeniu.

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