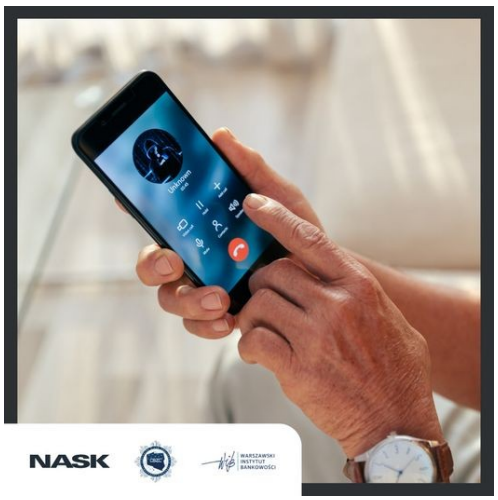
Socjotechnika a oszustwa online: W jaki sposób seniorzy mogą bronić się przed oszustami?

W dzisiejszym świecie coraz więcej rzeczy dzieje się w internecie, co może być zarówno korzystne, jak i stwarzać trudności. Jednym z tych problemów jest zagadnienie zwane "socjotechniką online".



Osoby starsze, które urodziły się i dorastały w czasach, kiedy nie było jeszcze dostępu do internetu i smartfonów, mogą być szczególnie narażone na tego rodzaju zagrożenia. Ponieważ: są bardziej ufni, otwarci na pomoc innych, a także chętniej sami pomagają, a ponadto lubią rozmawiać z innymi, są uprzejmi i cenią kontakt z innymi ludźmi.

Te wspaniałe cechy, takie jak ufność, otwartość i życzliwość, które są często charakterystyczne dla osób starszych, mogą stanowić pułapkę, szczególnie w świecie online, gdzie oszuści doskonale wiedzą, jak wykorzystać te cechy. Dodatkowo brak pełnej wiedzy na temat dzisiejszych możliwości technologicznych powoduje, że seniorzy stają się łatwiejszym łupem dla oszustów, którzy wiedzą, jak manipulować naszymi emocjami i zachęcać nas do podejmowania działań, służących ich celom.
Dlatego tak ważne jest, abyśmy, pomimo naszej naturalnej skłonności do ufania i dostrzegania dobra w innych, **zachowali szczególną ostrożność i zdrową dawkę podejrzliwości w świecie internetu**. Musimy być świadomi, że oszuści mogą wykorzystać naszą dobroć i ufność przeciwko nam. **Dlatego warto być czujnym wobec potencjalnych zagrożeń i znać skuteczne metody obrony przed nimi**.

Oszustwa polegające na wykradaniu pieniędzy czy danych osobowych to problem, który istnieje od dawna, a internet, często uważany za sferę anonimowości, otwiera nowe drzwi dla osób dążących do manipulacji i pozyskiwania korzyści w sposób nieuczciwy.
Oszustwa online nie znikną, ale możemy się przed nimi bronić, działając mądrze i świadomie w przestrzeni internetowej.

Jak więc można chronić się przed socjotechniką? Zapoznaj się z naszymi wskazówkami!

- **Bądź ostrożny w kontaktach z nieznajomymi i pozornie znajomymi, czyli:**

- nie udzielaj poufnych informacji ani nie podejmuj działań, gdy otrzymujesz niespodziewane wiadomości od nieznanych osób online;
- sprawdzaj tożsamość osoby, która prosi o poufne informacje lub pieniądze;
- pamiętaj, że nie każdy jest tym, za kogo się podaje;
- nie przekazuj pieniędzy online, jeśli ktoś nieznajomy prosi Cię o ich przelanie nawet na bardzo ważny cel.

- **Działaj bez pośpiechu, uważaj na naciski i presję czasu, czyli:**

- nie daj się zwieść wyrażeniom typu: „natychmiast", „szybko", „niezwłocznie", „to wymaga pilnego wykonania", „tylko natychmiastowa reakcja" - takie sformułowania mają na celu nakłonić Cię do działania bez zastanowienia;
- nie otwieraj załączników ani nie klikaj w podejrzane linki w e-mailach czy wiadomościach - to częsty sposób na rozprzestrzenianie wirusów komputerowych!

- **Bądź świadomy i wyedukowany, czyli:**

- dowiedz się więcej na temat różnych rodzajów oszustw online;
- przeczytaj o popularnych schematach oszustw, takich jak phishing, oszustwa telefoniczne i fałszywe strony internetowe, aby poznać sposoby wyłudzania pieniędzy i danych osobowych;
- śledź najnowsze wiadomości i bądź na bieżąco - wiedza jest kluczem do ochrony przed oszustwami;
- ustaw mocne hasła do swoich kont online oraz unikaj używania tych samych haseł do różnych usług internetowych.

- **Pytaj, rozmawiaj, zgłaszaj podejrzane działania, czyli:**

- nie obawiaj się pytać i sprawdzać oraz przyznać, że czegoś nie wiesz - brak wiedzy to nic złego;
- rozmawiaj z bliskimi i dziel się swoimi doświadczeniami i obawami z rodziną lub przyjaciółmi;
- jeśli masz wątpliwości co do wiadomości lub prób oszustwa online, zgłoś je odpowiednim służbom ścigania lub organom regulacyjnym;
- jeśli coś jest dla Ciebie niezrozumiałe, poproś kogoś ze swojego otoczenia, aby Ci wytłumaczył i pomógł rozwiązać problem.

Jakie triki wykorzystują oszuści:

- udają kogoś innego np. członków rodziny, pracowników banków czy instytucji, by skłonić nas do ujawnienia poufnych informacji (hasło do konta, kodu PIN) lub przekazania pieniędzy;
- dzwonią lub wysyłają fałszywe e-maile albo wiadomości tekstowe, które wyglądają jak wiadomości od zaufanych źródeł, np. banków, firm czy serwisów internetowych;
- straszą konsekwencjami i wykorzystują presję czasu, np. mogą twierdzić, że twoje konto bankowe jest zagrożone lub że musisz działać natychmiast, aby uniknąć konsekwencji;
- manipulują naszymi emocjami i wykorzystują uczucia innych ludzi, np. udają, że są osobą potrzebującą pomocy finansowej lub emocjonalnej;
- obiecują atrakcyjne nagrody, zniżki lub oferty na tanie leki lub cudowne środki na różne dolegliwości zdrowotne albo znakomite urządzenia domowe, a następnie proszę o płatność, dostęp do konta bankowego lub inne informacje, aby skorzystać z tych pozornie korzystnych ofert;
- gratulują wygranej w loterii lub konkursie online, w którym nie uczestniczyłeś, i proszą o opłatę wstępną lub dostarczenie swoich danych osobowych w celu odbioru nagrody.

Podcast „3 grosze o ekonomii"

Schematy oszustw w Internecie - rozmowa z Panią Karoliną Wiązowską, Ekspertką ds. cyberbezpieczeństwa z BLIK/PSP. Link do audycji: 3 grosze o ekonomii - Schematy oszustw w internecie (google.com)

***

Materiał przygotowany w ramach kampanii pt. *#Halo! Tu cyberbezpieczny Senior*! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

***