Oszustwa internetowe i sieciowe

Pigułka senioralna

Oszustwa internetowe i sieciowe to wszystkie rodzaje oszustw przeprowadzane za pośrednictwem internetu lub sieci komórkowych, wykorzystujące nowoczesne technologie cyfrowe np.: algorytmy, łamanie zabezpieczeń, szyfrowania sieci, sztuczną inteligencję.

Cześć z nich polega na powtarzaniu wzorców znanych już z przestrzeni realnej np.: oszustwa “na wnuczka”, “na policjanta”, niektóre z kolei są nowymi formami zagrożeń, na które narażeniu są również seniorzy.

Zadanie publiczne jest finansowane ze środków otrzymanych od Zleceniodawcy w ramach edycji w roku 2025 rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021–2025.

Na co jesteś narażony?

„Na wnuczka” / „Na policjanta” online lub telefonicznie

Opis: Oszust podaje się za wnuczka, krewnego lub policjanta i prosi o pieniądze (np. „miałem wypadek”, „trzeba wpłacić kaucję”).
Cel: Wyłudzenie gotówki lub przelewu.
Wskazówka: Nigdy nie przekazuj pieniędzy osobom, które dzwonią z prośbą o pomoc – zawsze zadzwoń sam do bliskiego.

Fałszywe wiadomości e-mail lub SMS (phishing)

Opis: Wiadomości wyglądają jak od banku, urzędu, kuriera czy znanej firmy. Zawierają link do „potwierdzenia danych” lub „śledzenia przesyłki”.
Cel: Kradzież danych osobowych lub bankowych.
Wskazówka: Nie klikaj w linki w podejrzanych wiadomościach, nie wpisuj haseł z takich stron.

Fałszywy pracownik banku lub technik komputerowy

Opis: Dzwoni osoba, która twierdzi, że konto jest zagrożone i trzeba „przelać pieniądze na bezpieczne konto” lub „zainstalować program pomocy zdalnej”.
Cel: Przejęcie konta bankowego.
Wskazówka: Bank nigdy nie prosi o instalację programów ani przelewy bezpieczeństwa.

ALARM, seniorze!

Fałszywe loterie i nagrody

Opis: Wiadomość lub reklama informuje o „wygranej” - by ją odebrać, trzeba zapłacić niewielką „opłatę” lub podać dane karty.
Cel: Wyłudzenie pieniędzy lub danych.
Wskazówka: Prawdziwe konkursy nie wymagają opłat za odbiór nagrody.

Podszywanie się pod urzędy i instytucje

Opis: Fałszywe e-maile „z ZUS”, „z urzędu skarbowego” lub „z policji” – proszą o podanie danych lub otwarcie załącznika.
Cel: Instalacja wirusa lub kradzież danych.
Wskazówka: Urzędy nie wysyłają wezwań przez e-mail z załącznikami ZIP lub PDF z hasłem.

Fałszywe zbiórki charytatywne

Opis: Strony lub posty w mediach społecznościowych proszą o wsparcie chorego dziecka lub ofiar wojny. Często to fałszywe konta.
Cel: Wyłudzenie datków.
Wskazówka: Wspieraj tylko znane organizacje (np. Caritas, WOŚP) przez ich oficjalne strony.

NIE DAJ SIĘ OSZUKAĆ!

BEZPIECZNY SENIOR TO SZCZĘŚLIWY SENIOR!

Czujesz, że mogłeś zostać oszukany? Zgłoś!

- na policję (nr alarmowy 997) lub w lokalnym komisariacie policji,
- zespołowi ds. reagowania na incydenty zagrożenia komputerowego CERT Polska - strona https://incydent.cert.pl
- za pośrednictwem portalu GOV - zgłoszenia zagrożenia online https://www.gov.pl/cyfryzacja/zglos-incydent

Pigułka senioralna to seria materiałów edukacyjnych Fundacji Nowy Przemysł Śląska mająca na celu realizowanie zadań związanych z działaniem na rzecz społeczności województwa śląskiego.
Opracowanie merytoryczne: mgr Klaudia Żubryk, Szkoła Doktorska Uniwersytetu Śląskiego w Katowicach
Opracowanie graficzne i przygotowanie do druku: Marta Warczek