



Przykłady oszustw, które najczęściej zagrażają osobom starszym

na podstawie doświadczeń Policji

 podisnp. Jacek Rybicki

Wydział Profilaktyki Społecznej Biura Prewencji

Komendy Głównej Policji

Warszawa 9 czerwca 2025 roku

Kim są ofiary? Profil osoby narażonej na oszustwo



1. Charakterystyka społeczno-demograficzna
2. Czynniki psychologiczne sprzyjające podatności na oszustwo
3. Ograniczenia poznawcze i cyfrowe
4. Izolacja i brak natychmiastowego wsparcia
5. Zaufanie do instytucji i autorytetów





Najczęstsze schematy - oszustw

1. Oszustwa na tzw. legendę (na wnuczka, policjanta, pracownika banku)
2. Fałszywe sms, wiadomości e-mail
3. Oszustwa inwestycyjne, deepfaky
4. Oszustwa romantyczne



1. Przykład oszustwa na tzw. legendę

Seniorka została oszukana metodą „na policjanta”, 76-latka przekazała oszustom 96 tysięcy złotych. Pieniądze przelała na tzw. bezpieczne konto

Z 76 letnią kobietą skontaktował się telefonicznie mężczyzna, który przedstawił się jako funkcjonariusz CBA. Przekazał seniorce informację, że zajmuje się rozpracowaniem grup hackerskich, a jej pieniądze zgromadzone na koncie są zagrożone, fałszywy funkcjonariusz poinformował rozmówczynię, że aby nie dopuścić do utraty oszczędności należy je przenieść na tzw. konto bezpieczne. Niestety kobieta uwierzyła w historię mężczyzny i wykonując jego instrukcje przelała na wskazane konto wszystkie oszczędności.

2. Przykład oszustwa na tzw. legendę



Seniorka została oszukana metodą „na wnuczka”, 86-latka przekazała oszustom 86 tysięcy złotych. Kobieta spakowała pieniądze do reklamówki i przekazała młodemu mężczyźnie, którego nie знаła

Seniorka odebrała dzwoniący telefon stacjonarny od mężczyzny, który podał się za jej wnuczka i poinformował, że miał wypadek i w konsekwencji grozi mu więzienie. Zaniepokojona całą sytuacją kobieta zapytała co dokładnie się wydarzyło, jednak połączenie w tym momencie zostało zerwane. Za chwilę telefon zadzwonił ponownie, wówczas po drugiej stronie odezwała się kobieta, która poinformowała, że osoba, która została potrącona przez wnuczka znajduje się w ciężkim stanie a prokurator za umorzenie sprawy żąda zapłaty 120 000 zł. Seniorka wierząc w całą historię odparła, że ma tylko 86 000 zł. Więc całą tą kwotę włożyła do foliowej reklamówki i przekazała obcemu mężczyźnie.



3. Przykład oszustwa na tzw. legendę

Seniorka została oszukana metodą „na pracownika banku”, 66-lątka przelała na konto bankowe wskazane przez oszusta 50 tysięcy złotych

Z 66 letnią kobietą skontaktował się telefonicznie mężczyzna, który przedstawił się jako pracownik banku. W toku rozmowy poinformował swoją rozmówczynię, że ktoś przy wykorzystaniu jej danych personalnych chciał zaciągnąć kredyt. Po tym połączeniu nastąpiło kolejne, podczas którego rzekomy pracownik banku przekazał informację seniorce, że aby uchronić oszczędności zgromadzone na koncie należy przelać je na inne konto, wskazane przez rozmówcę. Seniorka postępowała zgodnie z przekazywanymi przez fałszywego bankowca instrukcjami i na tzw. bezpieczne konto przelała łącznie 50 000 złotych.



O czym należy pamiętać odbierając taki telefon

- ✓ nie sugeruj się nazwą widoczną na ekranie telefonu
- ✓ nie podejmuj żadnych pochopnych decyzji
- ✓ zakończ połączenie i zweryfikuj rozmówcę
- ✓ nigdy nie podawaj nikomu wrażliwych danych
- ✓ nie pobieraj ani nie instaluj aplikacji lub oprogramowania
- ✓ poinformuj bliskich
- ✓ ustal z najbliższymi hasło - klucz

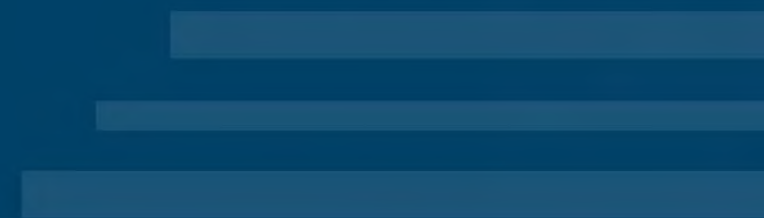




Oszustwa na fałszywe sms i wiadomości e-mail

najpopularniejsze tematy fałszywych wiadomości

- ✓ nieopłacona faktura np. za prąd lub gaz
- ✓ problemy z kontem bankowym
- ✓ wygrane na loterii, zniżki i kupony do popularnych sklepów
- ✓ problemy z wypłaceniem świadczeń
- ✓ konieczność dopłacenia do przesyłki kurierskiej



Przykład oszustwa na fałszywą wiadomość sms



Twoja paczka została wstrzymana z tytułu niedopłaty 2.50 PLN Przepraszamy za utrudnienia. Prosimy uregulować należność:
<https://tiny.one/Ja0t8f>

Twoja przesyłka pod wskazany adres jest droższa, prosimy o dopłatę (1.00 PLN). Brak wpłaty oznacza anulowanie zamówienia:
<https://bit.ly./2RcN9hq>

PGE: Na dzień 05.02 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności 3,81zł:
<https://pge.auction/ce154a>



Przykład oszustwa na fałszywą wiadomość e-mail

Pani Krystyna dostała wiadomość e-mail z prośbą o zaktualizowanie danych logowania do internetowego Konta Pacjenta. Wiadomość nie wzbudziła żadnych podejrzeń, tym bardziej, że przyszła od banku – właśnie taką formę logowania do IKP wybrała seniorka. Kliknęła link i trafiła na fałszywą stronę internetową, dzięki czemu oszuści zdobyli poufne dane



Co zrobić gdy otrzymasz podejrzanego sms lub wiadomość e-mail

- ✓ zweryfikuj nadawcę
- ✓ nie udostępniaj swoich danych
- ✓ nie loguj się do banku lub na inne konta
- ✓ nie klikaj w linki i załączniki
- ✓ zwracaj uwagę na wszelkie nieścisłości w komunikatach
- ✓ nie pobieraj i nie instaluj oprogramowania lub aplikacji
- ✓ zwróć uwagę na szatę graficzną



Gdy otrzymasz niepokojącą wiadomość – przekaż ją do zespołu CERT Polska, który ją zweryfikuje, a następnie zablokuje fałszywą stronę.



Oszustwa inwestycyjne i deepfake

Oszuści najczęściej umieszczają reklamę fałszywych inwestycji w mediach społecznościowych i na wielu stronach internetowych. Umieszczają na niej kuszące hasła, takie jak „bezpieczna inwestycja”, „zysk bez ryzyka” czy „gwarancja szybkiego zarobku”.

Deepfake to technologia, która wykorzystuje sztuczną inteligencję do tworzenia niezwykle realistycznych, ale nieprawdziwych obrazów, filmów i nagrań dźwiękowych.



Przykład oszustwa na fałszywą inwestycję

77-latka w Internecie zauważyła ofertę inwestycyjną, która miała w szybki i łatwy sposób pomnożyć jej oszczędności. Reklamę miał uwiarygodnić wizerunek popularnego dziennikarza i jednego z rządowych ministrów. Po kliknięciu w reklamę i podanie swoich danych z kobieta skontaktowała się rzekoma konsultantka, która nakłoniła ją do założenia konta na podanej przez nią stronie. Fałszywa doradczyni finansowa przeprowadziła poszkodowaną przez cały proces zakładania wirtualnego portfela inwestycyjnego i następnie przez około miesiąc nakłaniała kobietę do dalszego inwestowania. Przedstawiała też jej sfabrykowane tabelki i wykresy z zyskami z inwestycji. Kiedy kobieta zachciała wybrać część zysków, fałszywa konsultantka posunęła się do gróźb i kontakt z oszustami się urwał . W ten sposób przestępcy wyłudzili od seniorki 270 000 zł.



Oszustwa romantyczne

schemat działania

- ✓ nawiązanie kontaktu – fałszywy profil lub e-mail
- ✓ budowanie relacji
- ✓ prośby o pieniądze
- ✓ zerwanie kontaktu





Przykład oszustwa romantycznego

Kobieta poznała w Internecie mężczyznę podającego się za żołnierza sił zbrojnych Stanów Zjednoczonych. Zaczęła z nim regularnie korespondować. Na pewnym etapie znajomości mężczyzna przekazał, że niebawem przechodzi na emeryturę, chciałby przyjechać do Polski i zamieszkać z nią. Rzekomy żołnierz miał wysłać do Polski swoje rzeczy osobiste i oszczędności. Przekazał jednak, że paczka została zatrzymana przez celników. Z uwagi na to, że wszystkie oszczędności były w przesyłce, nie był w stanie pokryć kosztów. Poprosił o przelew 47 000 zł. Po ich przekazaniu kobieta otrzymała kolejną informację o problemie z przesyłką i konieczności wykonania kolejnego przelewu, czego nie zrobiła, a kontakt z amerykańskim żołnierzem nagle się urwał.



Oszustwa romantyczne c.d.

jak się chronić

- ✓ nie udostępniaj osobistych informacji
- ✓ chroń swoje pieniądze – nie przekazuj nawet drobnych kwot obcym
- ✓ nie ograniczaj się tylko do kontaktu poprzez komunikatory internetowe
- ✓ weryfikuj zdjęcia, które otrzymujesz online
- ✓ porozmawiaj z bliskimi o nowej znajomości



Wspólnie przeciwko oszustwom

co każdy z nas może zrobić, by chronić seniorów

- ✓ rozmawiamy z seniorami – często otwarcie, bez oceniania
- ✓ uczulamy na konkretne scenariusze oszustw
- ✓ reagujemy, gdy coś budzi naszą wątpliwość
- ✓ budujemy społeczną czujność – sąsiedzi, wspólnoty lokalne, organizacje senioralne

„Nie dajmy się oszukać – bądźmy czujni, wspierajmy się nawzajem, informujmy!”