



KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



# ZAGROŻENIA W CYBERŚWIECIE

BEATA GĘDŻBA – KACZMAREK

PSYCHOLOG, DORADCA ZAWODOWY, EKSPERT DS. EDUKACJI

PROJEKT A.3.1.1.: WSPARCIE ROZWOJU NOWOCZESNEGO KSZTAŁCENIA ZAWODOWEGO,  
SZKOLNICTWA WYŻSZEGO ORAZ UCZENIA SIĘ PRZEZ CAŁE ŻYCIE

ŁUBNIAŃ 14.03.2025 R.



WOJEWÓDZKI  
URZĄD PRACY  
W OPOLU



- Manipulacje w sieci stanowią poważne zagrożenie, zwłaszcza dla seniorów, którzy są często celem różnych oszustw z powodu braku doświadczenia i obeznania z nowoczesną technologią.
- Seniorzy mogą też być bardziej podatni na manipulację również z uwagi na różne psychologiczne czynniki, np. samotność czy większe zaufanie do innych ludzi.
- Ochrona seniorów przed manipulacjami w sieci wymaga wieloaspektowego podejścia, łączącego edukację, technologię oraz wsparcie społeczne.





# INŻYNIERIA SPOŁECZNA

- To metoda wykorzystywana przez cyberprzestępców, której celem jest manipulacja ludźmi w celu uzyskania poufnych informacji, takich jak hasła, numery kont bankowych czy dane osobowe lub w celu ukierunkowania ich na pożądane przez siebie zachowanie.
- Jest to jedna z najbardziej skutecznych i niebezpiecznych technik stosowanych w cyberprzestępczości, ponieważ atakuje bezpośrednio człowieka, a nie jego systemy informatyczne czy programy antywirusowe.

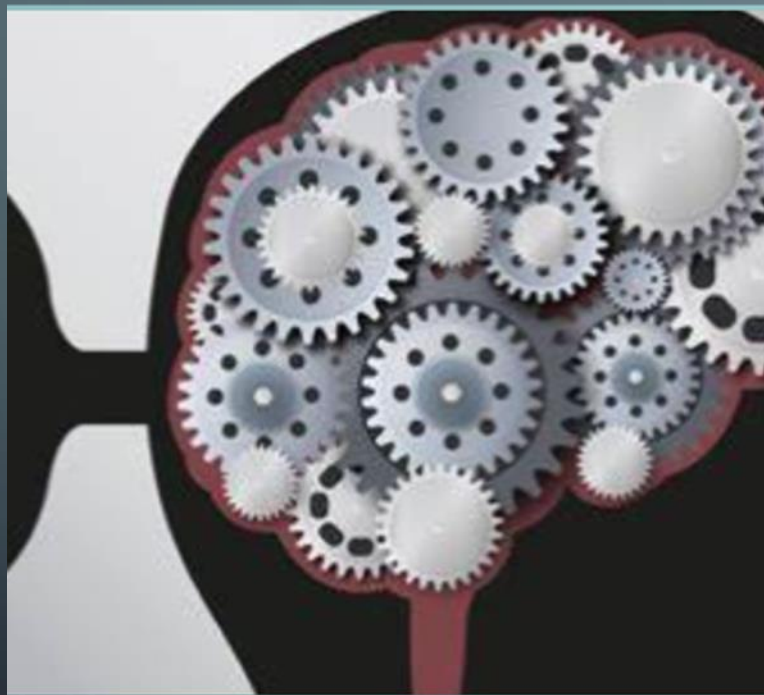


- Inżynieria społeczna opiera się na zrozumieniu ludzkich emocji, zachowań i słabych stron, co sprawia, że jest trudna do zwalczania za pomocą tradycyjnych środków technicznych.
- Dlatego też edukacja, świadomość i ostrożność w działaniu są kluczowe dla zapobiegania tego rodzaju atakom.
- Osoby korzystające z sieci powinny być świadome zagrożeń związanych z inżynierią społeczną i zawsze zachowywać ostrożność w udzielaniu poufnych informacji, szczególnie w odpowiedzi na niespodziewane e-maile, wiadomości czy telefonowanie.





# JAKIE PSYCHOLOGICZNE MECHANIZMY WYKORZYSTUJĄ OSZUŚCI?:



Manipulacja zaufaniem

Manipulacja emocjami

Zaangażowanie i konsekwencja

Poczucie pilnej konieczności

Efekt odpowiedzi społecznej/  
Społeczny dowód słuszności

# MANIPULACJA ZAUFANIEM:

- Atakujący mogą próbować zbudować zaufanie poprzez fałszywe sytuacje, stosując chwytliwe nagłówki, logo lub inne elementy sugerujące autentyczność.
- Mogą podszywać się pod zaufane instytucje, takie jak banki, firmy IT lub organizacje rządowe, aby zyskać zaufanie ofiary.



zaufanie do autorytetu „lekarz”, „profesor”, „urzędnik państwowy”



„leki” (suplementy) reklamowane przez lekarza







KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



## MANIPULACJA EMOCJAMI:

- Atakujący często stosują techniki inżynierii społecznej, manipulując ludzkim zachowaniem i emocjami.
- Często wykorzystywane są emocje, takie jak między innymi ciekawość, strach, chęć pomocy, sympatia lub chęć zysku.
- Próby wywołania silnych emocji mogą sprawić, że osoba stanie się mniej podejrzliwa i bardziej skłonna do podjęcia ryzyka.

# STRACH / ZARZĄDZANIE STRACHEM



KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



- Atakujący mogą wywoływać strach u ofiar poprzez wysyłanie e – maili lub wiadomości tekstowych zawierających fałszywe alarmy bezpieczeństwa, **groźby** lub **ostrzeżenia** dotyczące bezpieczeństwa sieciowego, na przykład o możliwych konsekwencjach, takich jak utrata danych, naruszenie prywatności czy finansowe straty.
- Mogą wykorzystać strach ofiary, grożąc konsekwencjami w przypadku nieprzestrzegania ich instrukcji, na przykład informując o blokadzie konta bankowego lub możliwym działaniu ze strony organów ścigania.
- Osoba pod wpływem strachu może być skłonna podjąć pochopne decyzje i udzielić wymaganych przez atakującego informacji.

...JEŚLI TEGO  
NIE ZROBISZ  
- POŻAŁUJESZ

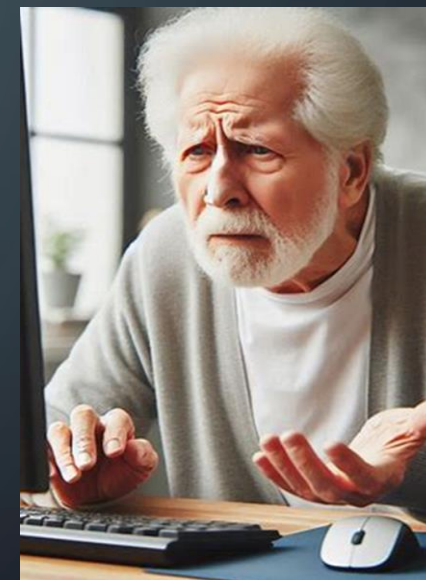


# NIEPEWNOŚĆ:

- Tworzenie niejasnych, niepokojących sytuacji może spowodować u ofiary poczucie dezorientacji i zagubienia, co czyni ją bardziej podatną na manipulację.
- Atakujący mogą wykorzystać brak pewności co do rzeczywistych konsekwencji ich działań, aby wprowadzić ofiarę w stan lęku i niepokoju.

## WSTYD I POCZUCIE WINY

- Atakujący mogą próbować wywołać u ofiary uczucia wstydu lub winy, sugerując, że nieudzielenie odpowiedzi na ich prośby lub pytania może mieć negatywne konsekwencje dla innych osób lub dla samej ofiary. Takie manipulacje mogą sprawić, że osoba zdecyduje się udzielić informacji, aby uniknąć poczucia winy lub wstydu.



KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



# EMPATIA I WSPÓŁCZUCIE, CHĘĆ POMOCY:

- Atakujący mogą próbować zyskać zaufanie ofiary, wywołując u niej uczucia współczucia lub empatii.
- Mogą to robić poprzez przedstawienie fałszywego scenariusza potrzebującej pomocy osoby lub organizacji, która rzekomo cierpi na skutek braku informacji lub wsparcia.
- Atakujący mogą wykorzystać chęć pomocy ofiary, prezentując sytuację, w której ta musi natychmiastowo udzielić wsparcia, np. poprzez przesłanie informacji uwierzytelniających.





# POCZUCIE PILNEJ KONIECZNOŚCI/ BRAK CZASU NA PRZEMYŚLENIE:

- Atakujący często wywołują uczucie pilnej konieczności lub tworzą sytuacje, które sugerują nagłą potrzebę podjęcia działań lub szybkich decyzji bez zastanowienia. Na przykład, mogą twierdzić, że konto bankowe jest zagrożone lub że istnieje pilna potrzeba aktualizacji hasła lub przestania skanu podpisu.
- Mogą sugerować, że konto zostało zhakowane lub twierdzić, że zostało zablokowane, a jedynym sposobem na jego ponowne odblokowanie jest natychmiastowe przekazanie poufnych informacji, podanie swoich danych osobowych lub finansowych.
- Atakujący mogą podkreślać, że ofiara musi działać szybko i bez zastanowienia się, aby uniknąć szkód lub niebezpieczeństwa lub obiecywać, że szybkie działanie ofiary pomoże uniknąć negatywnych konsekwencji. Mogą to robić poprzez tworzenie fałszywych limitów czasowych lub stresujących scenariuszy.



# EFEKT ODPOWIEDZI SPOŁECZNEJ / SPOŁECZNY DOWÓD SŁUSZNOŚCI

- Atakujący mogą wykorzystać zjawisko społecznego oddziaływania, sugerując, że wielu ludzi już podjęło daną akcję (np. udzieliło informacji lub pomocy), co może wpłynąć na decyzję ofiary.
- Społeczny dowód słuszności to psychologiczny fenomen, w którym ludzie patrzą na działania innych jako wsparcie dla swoich własnych decyzji lub zachowań. W praktyce oznacza to, że jeśli inni ludzie robią coś lub wyrażają określone przekonania, to istnieje większa tendencja do tego, aby inni również przyjęli te same działania czy przekonania.



# PRZYKŁADY OSZUSTW W SIECI:

- Fałszywe sklepy internetowe;
- Fałszywe zbiórki, oszustwa charytatywne;
- Fałszywe spadki, oferty lub loterie;
- Fałszywe ofert pracy (np. praca z domu);
- Fałszywe romantyczne relacje (np. na portalach randkowych);
- Oszuści podający się za rodzinę lub znajomych;



- Wyłudzenia danych = Phishing
- Złośliwe oprogramowanie;
- Oszustwa inwestycyjne.



# FAŁSZYWE SKLEPY INTERNETOWE

- Seniorzy mogą natknąć się na fałszywe sklepy internetowe, które oferują atrakcyjne ceny na nieistniejące produkty (atrakcyjne produkty po niskich cenach). Po dokonaniu płatności produkty nigdy nie zostają dostarczone, a oszuści znikają z pieniędzmi.
- Kradzież Danych Kart Płatniczych: Strony, które wyłudzą dane kart płatniczych pod pretekstem dokonania zakupu.



## OSZUSTWA CHARYTATYWNE / FAŁSZYWE ZBIÓRKI CHARYTATYWNE

- Oszustwa polegające na fałszywych zbiórkach charytatywnych, zwłaszcza po katastrofach naturalnych lub innych sytuacjach kryzysowych czy wydarzeniach wywołujących empatię.
- Seniorzy są proszeni o darowizny na wymyślone cele charytatywne i wpłaty na fałszywe konta bankowe.





## FAŁSZYWE SPADKI, OFERTY I LOTERIE

- Oszustwa, w których seniorzy otrzymują wiadomości o wygranej w loterii, konkursie lub otrzymaniu nagrody.
- Aby odebrać nagrodę, muszą zapłacić „opłatę” lub podać dane osobowe.
- Te oszustwa często prowadzą do strat finansowych i kradzieży tożsamości.





KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



## FAŁSZYWE OFERTY PRACY

- Seniorzy są kuszeni ofertą pracy, którą mogą wykonywać w domu.
- Oszuści wymagają wpłaty na materiały startowe lub szkolenia, które nigdy nie są dostarczane.

# FAŁSZYWE ROMANTYCZNE RELACJE:

- Oszustwa polegające na nawiązywaniu relacji romantycznych online (np. na portalach randkowych), podszywaniu się pod osoby szukające miłości, a następnie proszeniu o pieniądze na rzekome różne nagłe, "pilne" potrzeby.
- Ofiary często nieświadomie przekazują duże sumy pieniędzy oszustom.







## OSZUSTWA „NA BLISKĄ OSOBĘ”

- Przestępcy podają się często za bliskich znajomych lub członków rodziny seniora, zazwyczaj za wnuki i proszą o pilne wsparcie finansowe.
- Mogą twierdzić, że są w trudnej sytuacji, np. ulegli wypadkowi samochodowemu i potrzebują natychmiastowej pomocy.

# E – MAILE PHISHINGOWE

## lub SMS PHISHING (SMISHING)

- Phishing = wyłudzenie danych - fałszywe wiadomości z prośbą o potwierdzenie danych konta lub informacji osobistych.
- Polega na wysyłaniu fałszywych wiadomości e-mail, SMS-ów lub wiadomości na mediach społecznościowych, które wyglądają jak oficjalne komunikaty pochodzące od zaufanych instytucji (np. banków, urzędów, firm, instytucji).
- Oszuści chcąc wyłudzić dane w mailach lub wiadomościach podszywają się pod pracowników w/w instytucji i proszą o aktualizację danych, potwierdzenie tożsamości, podanie haseł, danych osobowych czy finansowych (np. numery kart kredytowych) lub proszą o kliknięcie w link, który prowadzi do fałszywej strony.





# ZŁOŚLIWE OPROGRAMOWANIE

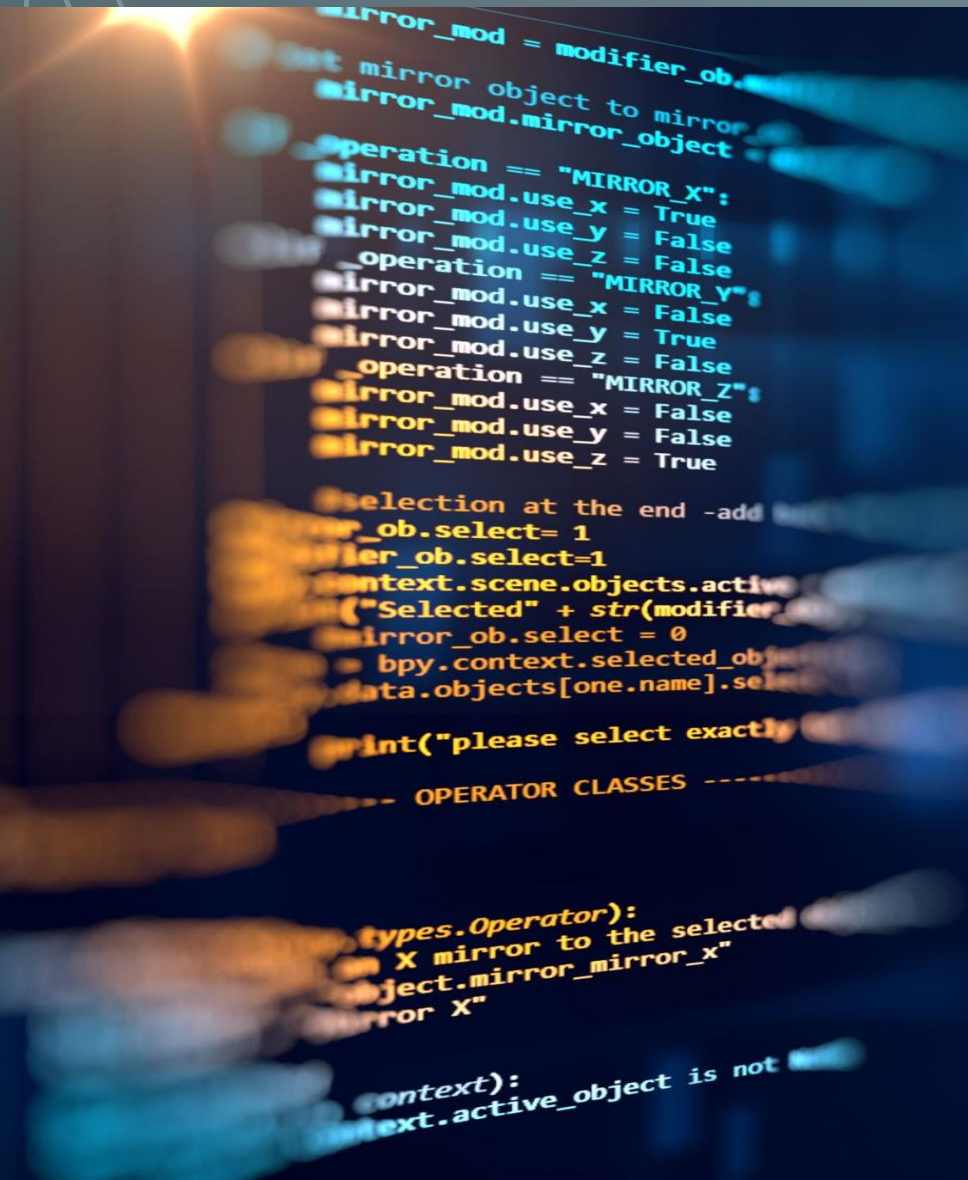


KRAJOWY  
PLAN  
ODBUĐOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



- Oszuści mogą też próbować uzyskać dostęp do komputera, aby ukraść dane lub zainstalować złośliwe oprogramowanie.
- Seniorzy mogą przypadkowo pobrać pliki lub linki do fałszywych stron, które po otwarciu instalują na komputerze złośliwe oprogramowanie, które wykrada dane osobowe lub monitoruje aktywność na komputerze.
- Malware - Złośliwe Oprogramowanie
- Ransomware: Oprogramowanie, które szyfruje pliki na komputerze. Oszuści potem żądają okupu za ich odblokowanie.
- Oszustwa na zdalną pomoc - oszuści przekonują do zainstalowania oprogramowania do zdalnego dostępu, twierdząc, że naprawią komputer. W rzeczywistości uzyskują dostęp do danych osobowych i finansowych.



## OSZUSTWA INWESTYCYJNE / OSZUSTWA NA RYNKACH INWESTYCYJNYCH

- Oszustwa związane z fałszywymi inwestycjami, takie jak np. oferty inwestycji w nieruchomości, fałszywe akcje, obligacje, kryptowaluty czy inne schematy inwestycyjne.
- Oszuści obiecują wysokie zyski przy minimalnym ryzyku, a w rzeczywistości kradną pieniądze.
- Piramidy Finansowe: Schematy, które obiecują duże zyski za werbowanie kolejnych uczestników.

# JAK ROZPOZNAĆ I JAK UCHRONIĆ SIĘ PRZED MANIPULACJĄ W SIECI:



Zasady rozpoznawania oszustw

Sygnaly ostrzegawcze

Jak się chronić?

Podstawowe zasady bezpieczeństwa

Wsparcie (narzędzia) techniczne

Edukacja i świadomość

Wsparcie rodziny, przyjaciół, społeczności

Reagowanie na oszustwa



# ZASADY ROZPOZNAWANIA OSZUSTW:



- Zwracaj uwagę na adres URL, certyfikaty bezpieczeństwa i inne wskaźniki wiarygodności.
- Bądź nieufny/a wobec „Zbyt dobrych ofert”: Pamiętaj, że zbyt atrakcyjne oferty często są oszustwem i że należy zawsze zachować zdrowy rozsądek i sceptycyzm.
- Korzystaj z niezależnych źródeł i recenzji w celu oceny wiarygodności usług i produktów.
- Rób zakupy tylko na renomowanych i znanych stronach internetowych.
- Sprawdzaj opinie innych klientów oraz bezpieczeństwo płatności.

# SYGNAŁY OSTRZEGAWCZE

- Rozpoznanie sygnałów ostrzegawczych związanych z potencjalnym wyłudzeniem danych jest kluczowe dla ochrony przed cyberprzestępczością.

Warto zwrócić uwagę na:

- Nietypowe wiadomości e-mail;
- Błędy gramatyczne i ortograficzne w komunikatach;
- Brak adekwatnych informacji od nadawcy;
- Nieoczekiwane zmiany w rachunkach czy transakcjach finansowych;
- Prośby o kliknięcie w linki lub otwarcie załączników.





# JAK SIĘ CHRONIĆ ?



Podstawowe zasady  
bezpieczeństwa,  
ograniczone zaufanie

wyczulenie na wsparcie  
finansowe

nic nie klikaj

nie wchodź w linki/SMS  
(8080)

nie ściągaaj załączników

Wsparcie (narzędzia)  
techniczne, inwestycja  
w programy  
antywirusowe

Edukacja i świadomość,  
aktualizacja wiedzy  
(podcasty, słuchowiska,  
webinaria, YouTube,  
Spotify)

lepiej sprawdzić  
(oddzwoń na numer,  
który dzwoni, zadzwoń  
na oficjalną infolinię)

Wsparcie rodziny,  
przyjaciół  
i społeczności



## PODSTAWOWE ZASADY BEZPIECZEŃSTWA

- Silne Hasła i Menedżery Haseł: Używanie silnych, unikalnych haseł do różnych kont i regularna ich zmiana, korzystanie z menedżerów haseł, które ułatwiają zarządzanie skomplikowanymi hasłami.
- Uwierzytelnianie Dwuskładnikowe (2FA): Aktywacja uwierzytelniania dwuskładnikowego na ważnych kontach, takich jak e-mail, bankowość internetowa i media społecznościowe. Osoba logująca się do serwisu musi potwierdzić swoją tożsamość na dwa sposoby, np. poprzez e-mail i sms.



KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



# WSPARCIE/NARZĘDZIA TECHNICZNE

## Bezpieczeństwo Techniczne:

- Korzystaj z bezpiecznych przeglądarek internetowych z funkcjami blokowania reklam i ochroną przed phishingiem, takich jak Mozilla Firefox lub Google Chrome.
- Używaj i regularnie aktualizuj renomowane oprogramowanie antywirusowe i antyphishingowe, które chroni przed złośliwym oprogramowaniem i próbami wyłudzenia danych.





KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



## EDUKACJA I ŚWIADOMOŚĆ

- Czytaj ostrzeżenia o popularnych oszustwach, zyskaj wiedzę o najnowszych metodach oszustw internetowych, takich jak na przykład fałszywe e-maile od banków, oszustwa związane z wygranymi w konkursach, czy fałszywe oferty sprzedaży.

# WSPARCIE ROZINY/ PRZYJACIÓŁ/ SPOŁECZNOŚCI



- Bliscy powinni regularnie kontaktować się z seniorami, by wspólnie omawiać ich aktywność online, pomóc w razie potrzeby i wspierać w rozwiązywaniu problemów technicznych.
- Warto, by seniorzy dzielili się podejrzanymi wiadomościami i linkami, aby wspólnie ocenić ich autentyczność.
- Pomocne jest organizowanie spotkań i dyskusji w grupie seniorów na temat najnowszych zagrożeń i metod ochrony.





KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU



# REAGOWANIE NA OSZUSTWA

- Natychmiast zgłaszaj podejrzone aktywności/ incydenty, podejrzenia kradzieży tożsamości, oszustwa finansowego lub podejrzone wiadomości, telefony lub strony internetowe odpowiednim służbom i organom, takim jak banki, firmy technologiczne czy Policja.
- CERT Polska **8080**
- Informuj bliskich i społeczności o próbach oszustwa.
- Zmieniaj hasła.



## PODSUMOWANIE

- Dzięki świadomości zagrożeń i metod manipulacji oraz zastosowaniu odpowiednich środków ostrożności, a także dzięki połączeniu edukacji, technologii ochronnych i wsparcia ze strony rodziny i społeczności, seniorzy mogą skuteczniej i lepiej chronić się przed manipulacjami oraz oszustwami w sieci i czuć się bezpieczniej korzystając z Internetu.



# DZIĘKUJĘ ZA UWAGĘ 😊

Beata Gędźba – Kaczmarek  
psycholog, doradca zawodowy,  
ekspert ds. edukacji w powiecie opolskim  
tel. 604703892; [beatagedzba-kaczmarek@outlook.com](mailto:beatagedzba-kaczmarek@outlook.com)

