SILWERS

SENIORS ARTIFICIAL INTELLIGENCE LEARNING – WELL EDUCATED AND RISK SECURE

Co-funded by the European Union

Expert fora report

Erasmus+ KA220-ADU – Cooperation partnerships in adult education, Project No: ***2024-1-IS01-KA220-ADU-000256952***

Co-funded by the
European Union

Cele panelu

1. Omówienie trudności i obaw, z jakimi boryka się ta grupa w kontekście nowych technologii, a także identyfikacja obszarów zastosowań sztucznej inteligencji i związanych z nimi zagrożeń.
2. Identyfikacja obecnych i przyszłych zagrożeń w Internecie dla osób 55+.
3. Obecnyprezentacja rzeczywistych przykładów incydentów i korzyści wynikających z wykorzystania sztucznej inteligencji.
4. Definicja kluczowych kompetencji cyfrowych dla osób 55+.

Co-funded by the European Union

Wyniki - Polska

Co-funded by the European Union

Najczęściej cytowane zagrożenia online dla osób powyżej 55. roku życia

Osoby w wieku 55 lat i starsze mierzą się ze szczególnymi wyzwaniami w świecie cyfrowym, co sprawia, że są podatne na różnorodne zagrożenia online.

Zrozumienie najczęstszych i najpoważniejszych zagrożeń jest kluczowe dla poprawy świadomości cyberbezpieczeństwa i ochrony.

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Oszustwa typu phishing – wiadomości e-mail, SMS, linki, połączenia głosowe
- Deepfake atakuje fałszywe materiały audio/wideo, podszywając się pod rodzinę
- Fałszywe sklepy internetowe i oszustwa, podrobione strony internetowe
- Manipulacja emocjonalna i taktyka zastraszania socjotechnicznego
- Kradzież tożsamości z wykorzystaniem skradzionych danych osobowych

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Oszustwo na wnukach – podszywający się pod rodzinę w tarapatach
- Fałszywe prośby o pomoc za pośrednictwem WhatsApp lub Messenger
- Oszustwa matrymonialne i oszustwa oparte na związkach nawiązanych w Internecie
- Oszustwa inwestycyjne – fałszywe reklamy z udziałem celebrytów
- Pliki i załączniki zainfekowane złośliwym oprogramowaniem i oprogramowaniem wymuszającym okup

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Niezweryfikowane aplikacje i pobieranie niebezpiecznego oprogramowania
- Udostępnianie nieznajomym wrażliwych danych, zdjęć i informacji
- Korzystanie ze starych urządzeń lub oprogramowania
- Masowe, spersonalizowane ataki wykorzystujące sztuczną inteligencję, mające na celu profile użytkowników
- Dezinformacja zdrowotna lub niebezpieczne porady medyczne pochodzące z narzędzi AI

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Oszustwa wykorzystujące wykluczenie cyfrowe w usługach obywatelskich i bankowych
- Brak praktyk uwierzytelniania wieloskładnikowego upraszcza hasła i umożliwia ich ponowne wykorzystanie
- Utrata dostępu do kluczowych usług z powodu zmian technologicznych – dostęp tylko za pośrednictwem aplikacji, ograniczone alternatywy
- Zautomatyzowana manipulacja kanałami mediów społecznościowych, powodująca dezinformację i stres
- Hasło, identyfikacja, biometria, 2FA

Co-funded by the
European Union

10 największych obaw według ekspertów

Eksperci podkreślili główne obawy, które najbardziej dotyczą osób w wieku 55 lat i starszych, gdy wchodzą w interakcje z technologiami cyfrowymi.

Rozpatrzenie tych obaw jest kluczowe dla zwiększenia pewności siebie i bezpieczeństwa dzieci w codziennych czynnościach online.

Motywacja

Opracowywanie ukierunkowanych programów wsparcia i szkoleń.

Co-funded by the
European Union

10 największych obaw według ekspertów

- **Zmiana technologiczna**i złożoność: Szybkie tempo rozwoju technologii utrudnia osobom starszym adaptację, szczególnie w przypadku aktualizacji i nowych urządzeń.
- Strach i**manipulacja emocjonalna**:Oszustwa często wykorzystują emocje, takie jak strach czy pilna potrzeba, przez co osoby starsze są bardziej narażone.
- **Wykluczenie społeczne**i samotność: Ograniczony kontakt z rodziną i przyjaciółmi, często nasilony przez komunikację cyfrową zastępującą interakcje bezpośrednie.
- **Wahanie przed proszeniem o pomoc:**Osoby starsze często odczuwają wstyd lub zażenowanie, gdy proszą młodsze osoby o pomoc w kwestiach technologicznych.
- **Ograniczenia finansowe**:Opór lub niemożność wydawania pieniędzy na nowe urządzenia lub oprogramowanie, skutkująca przestarzałą, niebezpieczną technologią.

Co-funded by the
European Union

10 największych obaw według ekspertów

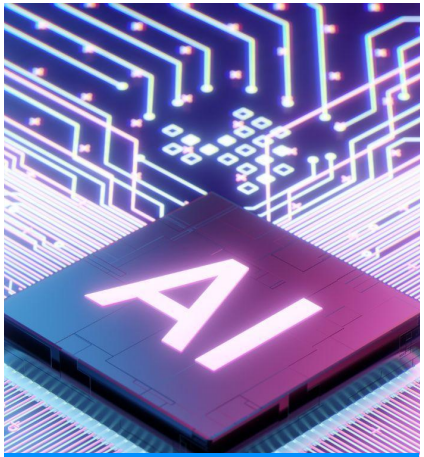
- **Wykluczenie cyfrowe**w usługach: Codzienne czynności (takie jak kupowanie biletów, bankowość, wizyty u lekarza) coraz częściej przenoszą się do Internetu, pozostawiając seniorów bez alternatyw.
- Niski**kompetencje cyfrowe**:Brak podstawowych umiejętności i doświadczenia, czasami pogłębiony przez brak edukacji komputerowej na wcześniejszym etapie życia.
- Impulsywność i**ryzykowne decyzje**:Skłonność do szybkiego działania w obliczu problemów technologicznych, czasami prowadząca do popełniania błędów lub padania ofiarą oszustw.
- **Wrażliwość**do dezinformacji: Problemy z odróżnieniem prawdziwych informacji od manipulacji cyfrowej, szczególnie w Internecie.
- Urządzenie i**problemy z konserwacją oprogramowania**:Problemy z aktualizacją urządzeń, zarządzaniem hasłami i zrozumieniem najlepszych praktyk bezpieczeństwa cyfrowego, rosnące ryzyko.

Co-funded by the European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

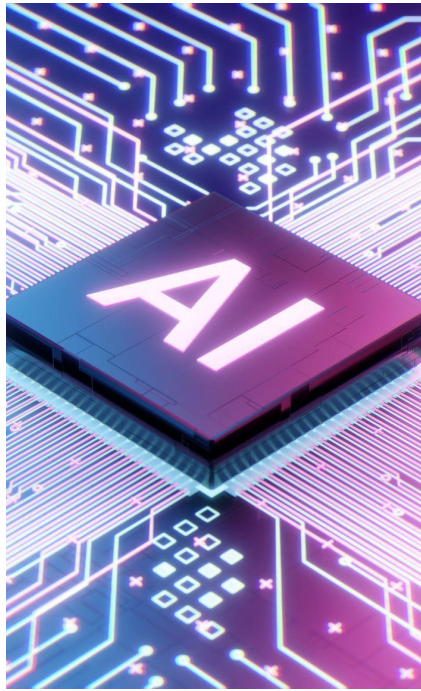
Sztuczna inteligencja jest coraz częściej wykorzystywana w wielu aspektach codziennego życia, oferując znaczące korzyści, ale także wprowadzając nowe zagrożenia dla cyberbezpieczeństwa.

Zrozumienie głównych obszarów zastosowań sztucznej inteligencji i związanych z nimi zagrożeń jest niezbędne do ochrony grup narażonych, takich jak osoby w wieku 55 lat i starsze.



Wsparcie

Aby zapewnić skuteczne wsparcie, konieczne jest podniesienie świadomości zagrożeń związanych ze sztuczną inteligencją.



Co-funded by the European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

- **Asystenci osobiści** w telefonach i urządzeniach (np. asystentach głosowych, takich jak Alexa), które wspierają osoby starsze w codziennych czynnościach, ale wymagają znajomości zasad prywatności i bezpieczeństwa.
- Sztuczna inteligencja w **monitorowanie opieki zdrowotnej** (urządzenia noszone, wykrywanie anomalii w tętnie), które zapewniają wczesne ostrzeżenia, ale do ich obsługi potrzebne jest zaufanie i podstawowe umiejętności cyfrowe.
- Oszustwa i oszustwa oparte na sztucznej inteligencji **wykrywanie oszustw** (identyfikacja phishingu, rozpoznawanie deepfake) w celu ochrony seniorów przed ukierunkowanymi atakami, ale wymagająca wiedzy na temat rozpoznawania podejrzanych treści.
- Wygenerowane przez sztuczną inteligencję **ataki spersonalizowane** które dostosowują się do zachowań i emocji poszczególnych seniorów, przez co wykrywanie zagrożeń w sieci staje się trudniejsze.
- **Generowanie treści** oraz dezinformacji za pośrednictwem sztucznej inteligencji (deepfake'i, fałszywe reklamy, fake newsy), wpływającej na decyzje i wywołującej zamieszanie wśród seniorów nieposiadających umiejętności krytycznej oceny.

Co-funded by the
European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

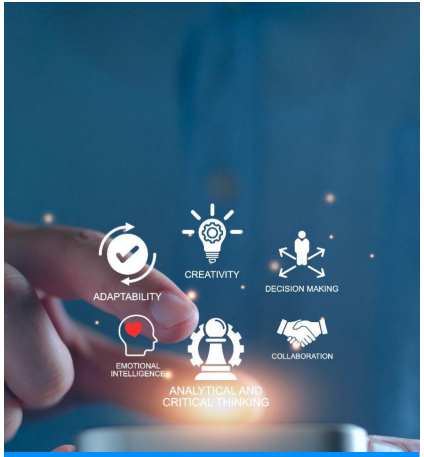
- Sztuczna inteligencja w **inteligentny dom** oraz urządzenia IoT wspomagające codzienne życie, ale stwarzające zagrożenie, jeśli urządzenia są niezabezpieczone lub źle zarządzane.
- Podróże wspomagane sztuczną inteligencją i **planowanie wypoczynku** pomagając w organizacji wycieczek i zajęć, zwiększając komfort, ale wymagając pewnej znajomości technologii cyfrowych w celu bezpiecznego korzystania.
- Zautomatyzowany **interakcje społeczne** boty symulujące ludzką rozmowę, często wykorzystywane w oszustwach lub w celu zmniejszenia izolacji, wymagające czujności, aby uniknąć oszustwa.
- Sztuczna inteligencja w świecie cyfrowym **usługi finansowe** automatyzacja transakcji i bankowości, która może poprawić dostępność, ale wymaga znajomości praktyk bezpieczeństwa i zapobiegania oszustwom.
- Narzędzia AI w **komunikacja** z rodziną i opiekunami (monitoring w czasie rzeczywistym, systemy powiadamiania o sytuacjach awaryjnych), co zwiększa bezpieczeństwo, ale wymaga kompetencji w zakresie konfiguracji i interpretacji.

Co-funded by the
European Union

Kluczowe kompetencje dla seniorów

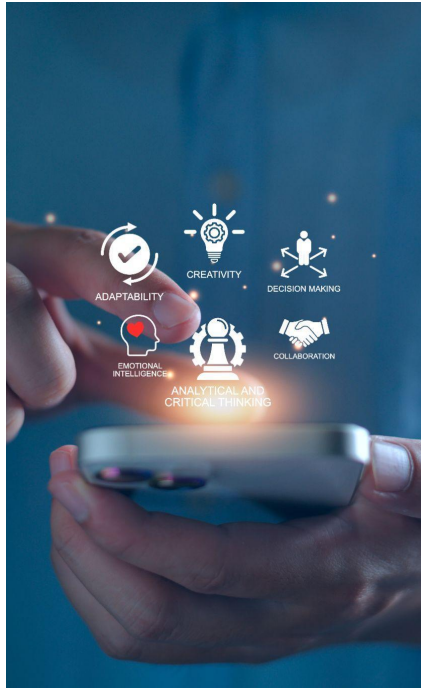
Rozwijanie podstawowych kompetencji cyfrowych jest kluczowe, aby umożliwić seniorom bezpieczne i pewne poruszanie się w świecie online.

Umiejętności te pomagają im skutecznie wykorzystywać technologię w celu usprawnienia codziennego życia i zwiększenia odporności na zagrożenia cybernetyczne.



Kompetencje

Pomóż seniorom lepiej się chronić i pewniej korzystać z nowoczesnych technologii.



Co-funded by the
European Union

Kluczowe kompetencje dla seniorów

- **Zrozumienie**podstawowa obsługa urządzeń cyfrowych i ustawienia zabezpieczeń.
- **Uznanie**manipulacji i fałszywych treści opartych na sztucznej inteligencji.
- **Umiejętności cyfrowe**aby bezpiecznie korzystać z asystentów AI i inteligentnych urządzeń.
- **Świadomość**prywatności danych i środków ochrony w aplikacjach AI.
- **Umiejętność**aby szukać wiarygodnych informacji i weryfikować treści generowane przez sztuczną inteligencję.

Co-funded by the
European Union

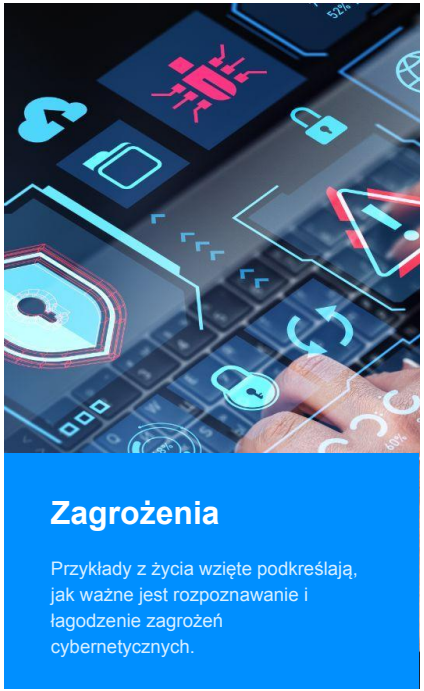
Kluczowe kompetencje dla seniorów

- Emocjonalny**odporność**aby nie dać się zmanipulować oszustwom wykorzystującym sztuczną inteligencję.
- **Komfort**z podstawowym rozwiązywaniem problemów i konserwacją narzędzi cyfrowych.
- **Wiedza**bezpiecznych praktyk zarządzania hasłami i uwierzytelniania.
- Kompetencje do**używać**Narzędzia AI dla ochrony zdrowia, bezpieczeństwa i komunikacji.
- **Otwartość**do ciągłego uczenia się dzięki szybkiemu rozwojowi technologii AI.

Co-funded by the European Union

Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat powszechnych zagrożeń cybernetycznych, jakie sztuczna inteligencja stwarza dla codziennego życia seniorów.



Co-funded by the
European Union

Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

- Użycie**deepfake**Technologia podszywania się pod członka rodziny: Senior odbiera telefon, w którym dzwoniący, używając przekonującego głosu imitującego głos wnuka lub dziecka, twierdzi, że potrzebuje natychmiastowych pieniędzy (np. na wypadek). Senior, przekonany emocjonalną manipulacją i znajomością głosu, przelewa pieniądze, często za pomocą BLIKA lub przelewu bankowego.
- Romans**oszustwa**z udziałem sztucznej inteligencji: Seniorzy padają ofiarą ataków w sieci ze strony osób (czasem chatbotów lub zautomatyzowanych profili), które nawiązują „relacje” emocjonalne, a następnie pod fałszywymi pretekstami proszą o pieniądze, wykorzystując samotność i zaufanie.
- Podróbka**loteria**lub wygrana: Senior zostaje poinformowany, często telefonicznie lub e-mailem z wykorzystaniem treści generowanych przez sztuczną inteligencję, o wygranej dużej sumy pieniędzy. Aby ją odebrać, proszony jest o wpłatę depozytu lub podanie danych osobowych, co skutkuje stratą finansową, a czasem kradzieżą tożsamości.

Co-funded by the
European Union

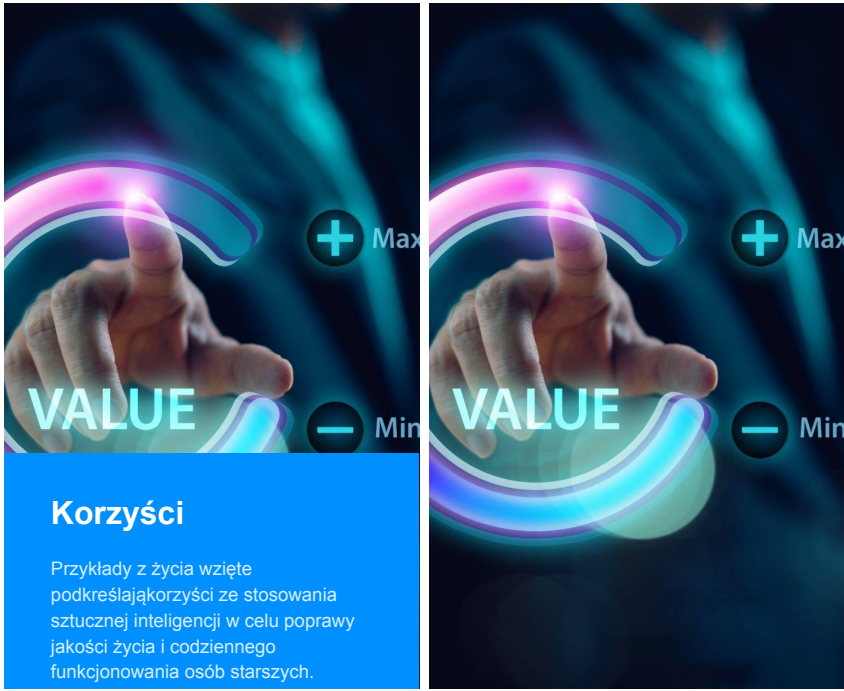
Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

- **Manipulacja**za pośrednictwem fałszywych sklepów internetowych: Seniorzy nieświadomie kupują towary na stronach internetowych, które są niemal identyczne z witrynami legalnych sklepów (z niewielką zmianą w adresie lub nazwie). Płacą za towary, które nigdy nie docierają, padając ofiarą wyrafinowanych witryn phishingowych opartych na sztucznej inteligencji.
- Medycyna wspomagana sztuczną inteligencją**mylna informacja**Seniorzy korzystają z chatbotów AI lub narzędzi online w celu uzyskania porad zdrowotnych. Czasami porady te są mylące, przez co pomijają wizytę u lekarza lub nawet przyjmują niewłaściwe leki, co może być niebezpieczne dla zdrowia.

Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat korzyści
wpływu sztucznej inteligencji na codzienne życie seniorów.



Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

- Starszy mężczyzna korzystał z funkcji podróży wspomaganej sztuczną inteligencją**planowanie**narzędzie do organizowania podróży, określania dat i zainteresowań (np. muzea czy zajęcia na świeżym powietrzu), otrzymywania szczegółowego, spersonalizowanego planu podróży, dzięki czemu podróż staje się łatwiejsza i przyjemniejsza.
- Medycyna oparta na sztucznej inteligencji**diagnostyczny**Narzędzia te umożliwiły identyfikację wczesnych sygnałów ostrzegawczych problemów zdrowotnych (takich jak nieregularne bicie serca u pacjentów z rozrusznikiem serca lub cukrzycą), co pozwoliło na podjęcie wczesnej interwencji medycznej i poprawę samopoczucia.
- Seniorzy wykorzystują sztuczną inteligencję w swojej pracy**asystenci**(jak Alexa) do codziennych przypomnień (np. o porach przyjmowania leków i wizyt), zarządzania gospodarstwem domowym i podtrzymywania kontaktów społecznych, zmniejszania samotności i zwiększania niezależności.

Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

- Przykład dotyczył inteligentnego**zdatny do noszenia**urządzenia (opaski na rękę z obsługą sztucznej inteligencji), które stale monitorują najważniejsze wskaźniki zdrowia seniorów mieszkających samotnie i automatycznie powiadamiają opiekunów lub służby ratunkowe w przypadku nieprawidłowości lub sytuacji awaryjnych.
- Obraz AI**uznanie**i wyszukiwanie pomogło starszej osobie zidentyfikować nieznaną roślinę w jej ogrodzie, zapewniając natychmiastowe wskazówki dotyczące jej pielęgnacji, a tym samym rozwijając umiejętności ogrodnicze i pewność siebie.

Co-funded by the European Union

Wyniki - Czechy

Co-funded by the European Union

Najczęściej cytowane zagrożenia online dla osób powyżej 55. roku życia

Osoby w wieku 55 lat i starsze mierzą się ze szczególnymi wyzwaniami w świecie cyfrowym, co sprawia, że są podatne na różnorodne zagrożenia online.

Zrozumienie najczęstszych i najpoważniejszych zagrożeń jest kluczowe dla poprawy świadomości cyberbezpieczeństwa i ochrony.

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Ataki phishingowe obejmują wiadomości e-mail, SMS-y i połączenia telefoniczne, w których atakujący podszywają się pod banki lub zaufane instytucje w celu kradzieży poufnych danych.
- Fałszywe sklepy internetowe i oszustwa mające na celu zaoferowanie osobom starszym fałszywych ofert i stron internetowych.
- Kradzież tożsamości, w której dane osobowe są wykorzystywane w celu uzyskania pieniędzy lub podszywania się pod ofiarę.
- Manipulacja za pomocą krótkich filmów i dezinformacji, w tym zmyślonych wiadomości i podprogowych przekazów.

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- Niedostateczna konserwacja IT, np. przestarzałe oprogramowanie sprzętowe i ignorowanie aktualizacji zabezpieczeń, skutkujące podatnością systemów na ataki.
- Oszustwa wykorzystujące samotność — oszuści nawiązują fałszywe przyjaźnie lub związki romantyczne.
- Niebezpieczna synchronizacja między urządzeniami i niebezpieczne przechowywanie haseł w przeglądarkach.
- Rosnące zagrożenie oszustwami z wykorzystaniem sztucznej inteligencji, w tym klonowanych głosów podszywających się pod krewnych w celu uzyskania pilnej pomocy finansowej.
- Rosnące ryzyko związane ze sztuczną inteligencją w programach antywirusowych sprawia, że konfiguracja i bezpieczne użytkowanie mają kluczowe znaczenie dla seniorów.

Co-funded by the
European Union

10 największych obaw według ekspertów

Eksperci podkreślili główne obawy, które najbardziej dotyczą osób w wieku 55 lat i starszych, gdy wchodzą w interakcje z technologiami cyfrowymi.

Rozpatrzenie tych obaw jest kluczowe dla zwiększenia pewności siebie i bezpieczeństwa dzieci w codziennych czynnościach online.

Motywacja

Opracowywanie ukierunkowanych programów wsparcia i szkoleń.

Co-funded by the
European Union

10 największych obaw według ekspertów

- **Trudności z nadążaniem**ze złożonością i szybkim rozwojem technologii.
- **Strach przed utratą dostępu**do danych osobowych i finansowych oraz paść ofiarą oszustw.
- **Zakłopotanie**lub utrata pewności siebie, gdy nie można korzystać z technologii w obecności rodziny.
- **Zależność**na innych (krewnych lub techników), co utrudnia budowanie niezależności.
- Bezpieczeństwo publicznych sieci Wi-Fi, z których często korzystają seniorzy bez**świadomość bezpieczeństwa.**

Co-funded by the
European Union

10 największych obaw według ekspertów

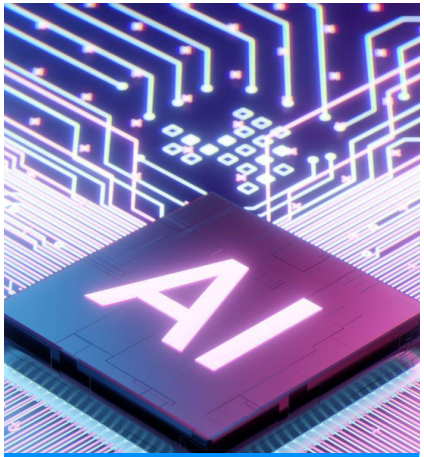
- **Niebezpieczne hasło**przechowywania, np. korzystanie z przeglądarek zamiast menedżerów haseł.
- **Komunikacja cyfrowa**zastąpienie cennego kontaktu twarzą w twarz, co prowadzi do izolacji społecznej.
- Wyłączanie aktualizacji lub funkcji bezpieczeństwa ze względu na**brak zrozumienia**, narażając urządzenia na ataki.
- **Walka ze zmieniającym się systemem**układów, ikon lub nieoczekiwanych nowych funkcji.
- Niezdolność do rozpoznania**podejrzana lub zmanipulowana treść**, co sprawia, że seniorzy są bardziej podatni na oszustwa.

Co-funded by the European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

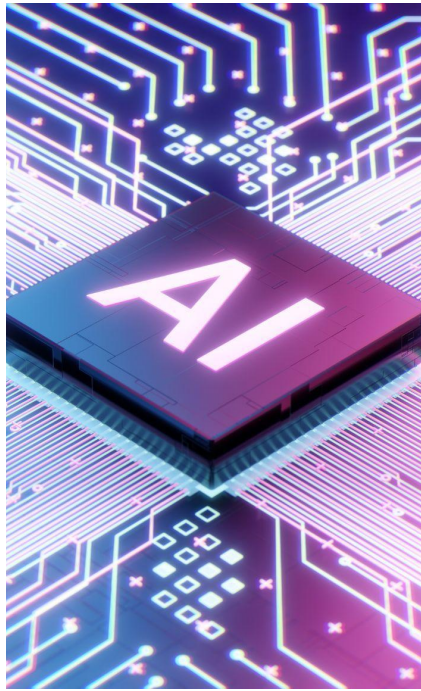
Sztuczna inteligencja jest coraz częściej wykorzystywana w wielu aspektach codziennego życia, oferując znaczące korzyści, ale także wprowadzając nowe zagrożenia dla cyberbezpieczeństwa.

Zrozumienie głównych obszarów zastosowań sztucznej inteligencji i związanych z nimi zagrożeń jest niezbędne do ochrony grup narażonych, takich jak osoby w wieku 55 lat i starsze.



Wsparcie

Aby zapewnić skuteczne wsparcie, konieczne jest podniesienie świadomości zagrożeń związanych ze sztuczną inteligencją.



Co-funded by the
European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

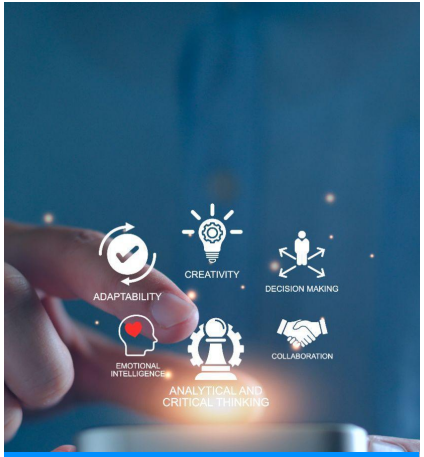
- **Sztuczna inteligencja w opiece zdrowotnej:**telemedycyna, monitorowanie stanu zdrowia i tłumaczenia umożliwiające komunikację z rodziną.
- **Codzienne wsparcie:**Asystenci głosowi AI, inteligentne urządzenia domowe, narzędzia antywirusowe.
- Ryzyko**manipulacja danymi**, ataki deepfake i rozprzestrzenianie dezinformacji.
- Z obsługą sztucznej inteligencji**klonowanie głosu**podszywanie się pod krewnych, co prowadzi do oszustw finansowych.
- **Nadmierne poleganie na narzędziach AI**bez zrozumienia ich ograniczeń — sztuczną inteligencję należy postrzegać jako narzędzie, a nie nieomylny autorytet.

Co-funded by the
European Union

Kluczowe kompetencje dla seniorów

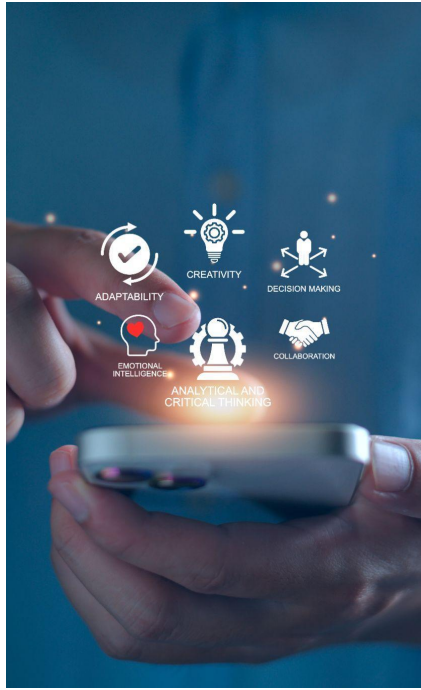
Rozwijanie podstawowych kompetencji cyfrowych jest kluczowe, aby umożliwić seniorom bezpieczne i pewne poruszanie się w świecie online.

Umiejętności te pomagają im skutecznie wykorzystywać technologię w celu usprawnienia codziennego życia i zwiększenia odporności na zagrożenia cybernetyczne.



Kompetencje

Pomóż seniorom lepiej się chronić i pewniej korzystać z nowoczesnych technologii.



Co-funded by the
European Union

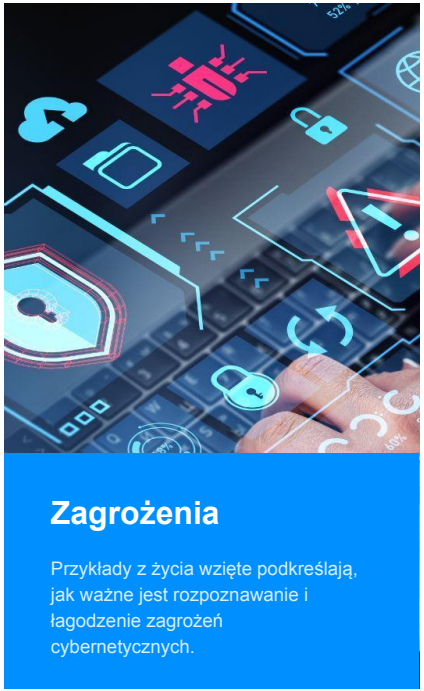
Kluczowe kompetencje dla seniorów

- Ustanawianie silnych, unikalnych haseł i**zarządzanie bezpieczeństwem**(unikaj przechowywania danych w przeglądarce, korzystaj z menedżera haseł).
- Włączanie**uwierzytelnianie dwuskładnikowe**w celu zabezpieczenia kont.
- Zrozumienie i**konfigurowanie programów antywirusowych**, zwłaszcza narzędzi opartych na sztucznej inteligencji.
- **Rozpoznawanie**podejrzany, zmanipulowany lub**oszukańcze treści online**.
- **Korzystanie z asystentów AI**praktycznie, ale pozostając krytycznym wobec wyników.
- Podstawowy**umiejętności cyfrowe**: aktualizacja urządzeń, bezpieczne przeglądanie stron internetowych, bezpieczne korzystanie z sieci Wi-Fi.
- **Budowanie pewności siebie**w celu zmniejszenia zależności od innych i wspierania ciągłej edukacji cyfrowej.

Co-funded by the European Union

Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat powszechnych zagrożeń cybernetycznych, jakie sztuczna inteligencja stwarza dla codziennego życia seniorów.



Co-funded by the
European Union

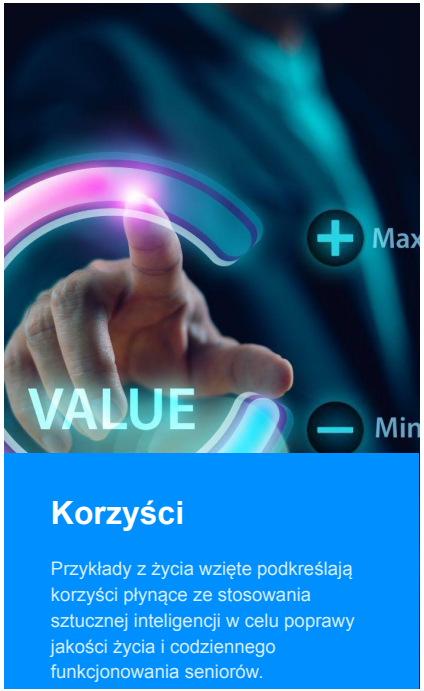
Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

- Przykład: Starsza kobieta padła ofiarą oszustwa, gdy dzwoniący wykorzystał technologię deepfake, aby sklonować głos jej wnuka i pilnie zażądał gotówki, którą kobieta dostarczyła kurierowi.
- Oszustwa mające na celu nawiązanie romansu lub przyjaźni, wykorzystujące przywiązanie emocjonalne, często za pośrednictwem wiadomości tekstowych lub połączeń telefonicznych.
- Dezinformacja rozprzestrzenia się za pośrednictwem filmów i krótkich wiadomości, przez co osobom starszym trudno jest zweryfikować jej autentyczność.
- Niewłaściwa konserwacja systemów informatycznych lub korzystanie z niezabezpieczonych sieci może prowadzić do rzeczywistych naruszeń bezpieczeństwa.

Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat korzyści
wpływu sztucznej inteligencji na codzienne życie seniorów.



Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

- 72-letnia kobieta skorzystała z asystenta głosowego AI do tłumaczenia, dzięki czemu mogła uczestniczyć w rodzinnych rozmowach wideo, rozumieć ich treść i czuć się częścią międzynarodowych konwersacji.
- Seniorzy korzystają ze sztucznej inteligencji do planowania (np. porady dotyczące systemu Windows, majsterkowanie w domu) lub z chatbotów w ośrodkach opieki nad osobą z chorobą Alzheimera.
- Sztuczna inteligencja oferuje spersonalizowane porady i wspiera codzienną niezależność, ale działa najlepiej w połączeniu z solidnymi umiejętnościami podstawowymi.

Co-funded by the European Union

Wyniki – Islandia

Co-funded by the European Union

Najczęściej cytowane zagrożenia online dla osób powyżej 55. roku życia

Osoby w wieku 55 lat i starsze mierzą się ze szczególnymi wyzwaniami w świecie cyfrowym, co sprawia, że są podatne na różnorodne zagrożenia online.

Zrozumienie najczęstszych i najpoważniejszych zagrożeń jest kluczowe dla poprawy świadomości cyberbezpieczeństwa i ochrony.

Co-funded by the
European Union

Zagrożenia online dla osób powyżej 55. roku życia

- **Oszustwa typu deepfake**prezentowanie fałszywych zdjęć i filmów, zwłaszcza na WhatsAppie, na których przestępcy podszywają się pod członków rodziny i twierdzą, że pilnie potrzebują pieniędzy.
- Wyrafinowany**phishing**przekształciła się w inżynierię społeczną za pośrednictwem aplikacji do przesyłania wiadomości z przekonującymi fałszywymi połączeniami telefonicznymi i wiadomościami.
- **Oszustwa miłosne**na platformach randkowych skierowanych do samotnych seniorów na całym świecie, w tym w Islandii, co prowadzi do szkód finansowych i emocjonalnych.
- Fizyczny**podszywanie się pod kogoś innego przez przestępców**podszywając się pod przedstawicieli pomocy technicznej lub banku odwiedzających domy seniorów.

Co-funded by the
European Union

10 największych obaw według ekspertów

Eksperci podkreślili główne obawy, które najbardziej dotyczą osób w wieku 55 lat i starszych, gdy wchodzą w interakcje z technologiami cyfrowymi.

Rozpatrzenie tych obaw jest kluczowe dla zwiększenia pewności siebie i bezpieczeństwa dzieci w codziennych czynnościach online.

Motywacja

Opracowywanie ukierunkowanych programów wsparcia i szkoleń.

Co-funded by the
European Union

10 największych obaw według ekspertów

- Trudności ze złożonymi**procesy logowania**w tym wymagania dotyczące hasła i częstego resetowania.
- Zamieszanie i**odporność na uwierzytelnianie dwuskładnikowe**wśród starszych użytkowników.
- **Słaba znajomość poczty e-mail**utrudniając odzyskiwanie hasła.
- **Mały rozmiar tekstu**i starsze telefony ograniczające funkcjonalność i funkcje bezpieczeństwa.
- **Brak jasnych instrukcji**z usług wymagających elektronicznego identyfikatora lub podobnego uwierzytelnienia.

Co-funded by the
European Union

10 największych obaw według ekspertów

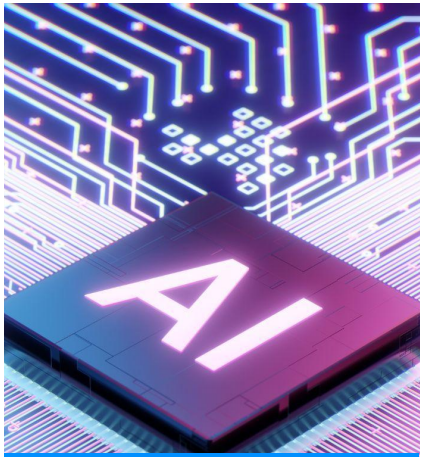
- Seniorzy**ponowne używanie haseł**w obrębie kluczowych witryn, co wiąże się z ryzykiem naruszenia bezpieczeństwa wielu kont.
- **Podszywanie się pod domenę**tworzenie przekonujących fałszywych stron internetowych w celu kradzieży poufnych danych.
- Ciągły niezauważony**kompromisy dotyczące poświadczeń**z monitoringu dark webu.
- **Ogólna nieufność**lub niezrozumienie zagrożeń cyberbezpieczeństwa mających wpływ na reakcje seniorów.
- Bariery stworzone przez**złożoność technologiczna**zmniejszając pewność siebie i niezależność.

Co-funded by the European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

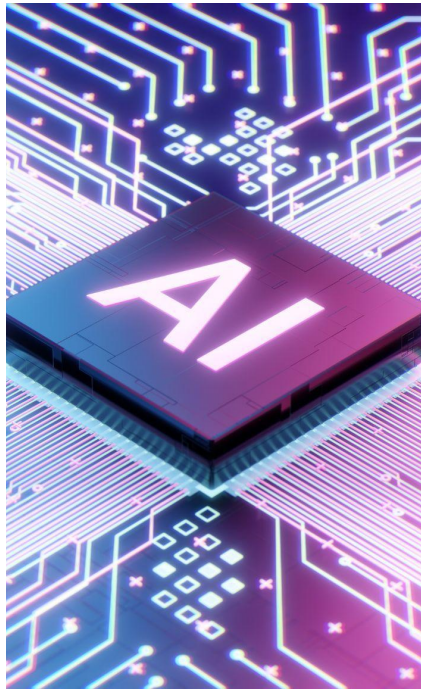
Sztuczna inteligencja jest coraz częściej wykorzystywana w wielu aspektach codziennego życia, oferując znaczące korzyści, ale także wprowadzając nowe zagrożenia dla cyberbezpieczeństwa.

Zrozumienie głównych obszarów zastosowań sztucznej inteligencji i związanych z nimi zagrożeń jest niezbędne do ochrony grup narażonych, takich jak osoby w wieku 55 lat i starsze.



Wsparcie

Aby zapewnić skuteczne wsparcie, konieczne jest podniesienie świadomości zagrożeń związanych ze sztuczną inteligencją.



Co-funded by the
European Union

Kluczowe obszary wykorzystania sztucznej inteligencji i zagrożenia cybernetyczne

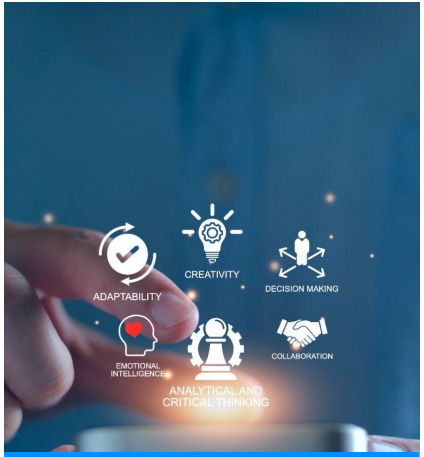
- **Edukacja**na temat ryzyka związanego z fałszywymi treściami generowanymi przez sztuczną inteligencję w Internecie, w szczególności filmami rzekomo dotyczącymi sytuacji kryzysowych w rodzinie.
- **Doradztwo**seniorzy weryfikowali pilne wiadomości, dzwoniąc bezpośrednio do rodziny, podkreślając, że prawdziwe sytuacje awaryjne zwykle wiążą się z rozmowami telefonicznymi, a nie wiadomościami tekstowymi.
- **Świadomość**że sztuczna inteligencja może imitować dowolne dane, w tym filmy i obrazy, co wymaga sceptycyzmu i alternatywnej weryfikacji.
- Ryzyko z**nadmierne udostępnianie informacji osobistych**w chatbotach AI i narzędziach takich jak ChatGPT, w których przechowywane są dane.
- Nacisk na**utrzymywanie krytycznego myślenia**i weryfikowanie informacji za pośrednictwem innych kanałów komunikacji.

Co-funded by the
European Union

Kluczowe kompetencje dla seniorów

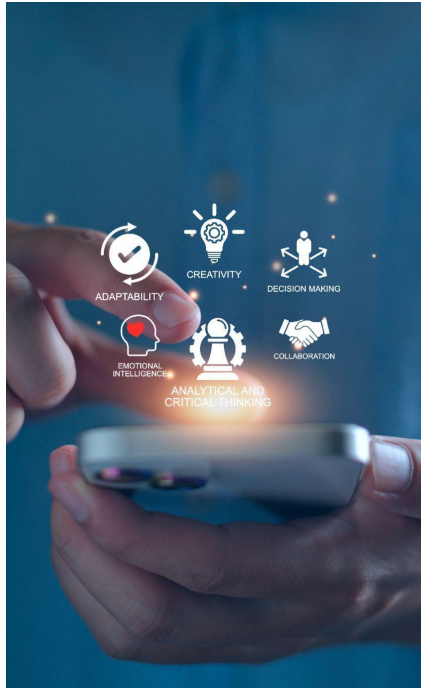
Rozwijanie podstawowych kompetencji cyfrowych jest kluczowe, aby umożliwić seniorom bezpieczne i pewne poruszanie się w świecie online.

Umiejętności te pomagają im skutecznie wykorzystywać technologię w celu usprawnienia codziennego życia i zwiększenia odporności na zagrożenia cybernetyczne.



Kompetencje

Pomóż seniorom lepiej się chronić i pewniej korzystać z nowoczesnych technologii.



Co-funded by the
European Union

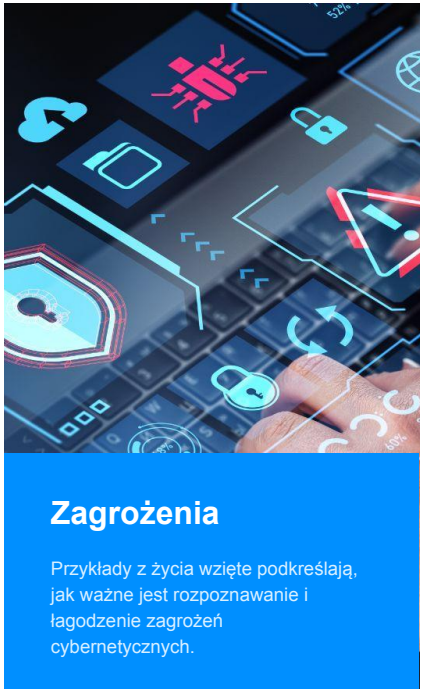
Kluczowe kompetencje dla seniorów

- Zrozumienie**znaczenie weryfikacji**przed udzieleniem odpowiedzi na pilne prośby za pośrednictwem mediów cyfrowych.
- Podstawowy**umiejętności cyfrowe**w tym bezpieczne zarządzanie hasłami i świadomość ryzyka związanego ze sztuczną inteligencją.
- **Umiejętność zadawania pytań**i weryfikować nieoczekiwane lub emocjonalne wiadomości, zwłaszcza te, które wydają się pilne lub niepokojące.
- **Sceptycyzm**w kierunku autentyczności treści online, zwłaszcza mediów generowanych przez sztuczną inteligencję.
- Wzmacnianie zaufania do członków rodziny**komunikacja bezpośrednia**i pomoc.

Co-funded by the European Union

Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat powszechnych zagrożeń cybernetycznych, jakie sztuczna inteligencja stwarza dla codziennego życia seniorów.



Co-funded by the
European Union

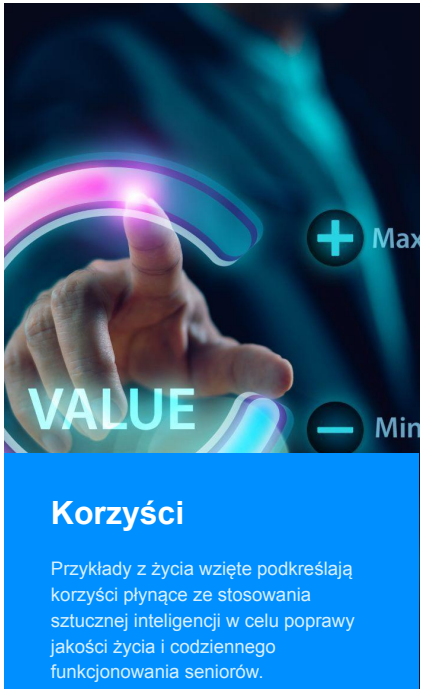
Rzeczywiste zagrożenia zidentyfikowane przez ekspertów

- Przykłady ofiar, które straciły oszczędności w wyniku oszustw typu deepfake, wykorzystujących podobizny gwiazd wygenerowane przez sztuczną inteligencję.
- Oszustwa rozsyłane za pośrednictwem WhatsApp polegały na wysyłaniu fałszywych wiadomości o chorych krewnych potrzebujących wpłaty pieniędzy. Oszustwa te czasami powstrzymywała interwencja rodziny.
- Oszustwa w mediach społecznościowych i aplikacjach randkowych są uwielbiane przez seniorów, którzy płacą za fałszywą opiekę zdrowotną lub wyjeżdżają za granicę, by spotykać się z nieistniejącymi partnerami.
- Oszustwa związane z pracą polegają na kradzieży danych kart kredytowych za pomocą fałszywych ofert pracy, klonowanych głosem.
- Przykłady osób, które nieświadomie zamieszczają w Internecie kompromitujące treści, nie zdając sobie sprawy z konsekwencji.

Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

Eksperci podzielili się przykładami z życia wziętymi ilustrującymi zarówno zagrożenia, jak i korzyści, jakie technologie cyfrowe niosą dla osób w wieku 55 lat i starszych.
Przypadki te dostarczają cennych informacji na temat korzyści
wpływu sztucznej inteligencji na codzienne życie seniorów.



Co-funded by the
European Union

Korzyści w życiu realnym zidentyfikowane przez ekspertów

- Sztuczna inteligencja pomaga seniorom w udzielaniu praktycznych porad dotyczących życia codziennego, takich jak sprzątanie, naprawy domowe i szybkie rozwiązywanie problemów.
- Chatboty oparte na sztucznej inteligencji zapewniają wsparcie emocjonalne i towarzystwo, oferując całodobową dostępność w celu łagodzenia lęku i prowadzenia ogólnych rozmów.
- Wykorzystanie narzędzi sztucznej inteligencji, takich jak ChatGPT, do weryfikacji podejrzanych wiadomości e-mail lub wiadomości związanych z cyberbezpieczeństwem.
- Sukces wdrażania sztucznej inteligencji w dużej mierze zależy od indywidualnych umiejętności technicznych osób starszych i ich zaufania do technologii.

Co-funded by the European Union

Zagrożenia online dla osób 55+ – słownik

Co-funded by the
European Union

Phishing (oszukańcze wiadomości e-mail, SMS-y, linki, połączenia głosowe)

Phishing to rodzaj cyberataku, w którym przestępcy wysyłają fałszywe e-maile, SMS-y, połączenia telefoniczne lub linki, podszywając się pod kogoś, komu ufasz, np. bank lub znajomego. Ich celem jest nakłonienie Cię do podania ważnych danych osobowych, takich jak hasła, numery kart kredytowych lub dane konta bankowego. Te fałszywe wiadomości często wyglądają bardzo realistycznie i próbują nakłonić Cię do szybkiego działania, wywołując poczucie pilności lub strachu. Atakujący chcą ukraść Twoje pieniądze lub tożsamość, nakłaniając Cię do kliknięcia w niebezpieczne linki lub udostępnienia poufnych danych. Aby zachować bezpieczeństwo, zawsze dokładnie sprawdzaj, kto jest nadawcą wiadomości, unikaj klikania w podejrzane linki i nigdy nie udostępniaj danych osobowych, jeśli nie masz absolutnej pewności, że są bezpieczne.

Co-funded by the
European Union

Ataki deepfake (fałszywe materiały audio/wideo, podszywanie się pod członków rodziny)

Ataki deepfake polegają na tworzeniu fałszywych nagrań audio lub wideo za pomocą sztucznej inteligencji, które wyglądają i brzmią bardzo realistycznie. W tych atakach przestępcy imitują głos lub twarz znanej osoby, często członka rodziny, aby wmówić rozmówcy, że rozmawiają z bliską osobą. Na przykład, oszust może użyć technologii deepfake, aby wykonać połączenie telefoniczne, które brzmi dokładnie jak wnuczka prosząca o pilne pieniądze. Te fałszywe nagrania są bardzo przekonujące i mogą oszukać nawet ostrożne osoby. Ataki deepfake są niebezpieczne, ponieważ wykorzystują zaufanie i emocje, utrudniając rozpoznanie oszustwa, dopóki nie jest za późno. Aby się chronić, zawsze weryfikuj nietypowe prośby, kontaktując się z daną osobą bezpośrednio za pośrednictwem różnych kanałów komunikacji, zanim podejmiesz jakiekolwiek działania.

Co-funded by the
European Union

Fałszywe sklepy internetowe i oszustwa (fałszywe strony internetowe)

Fałszywe sklepy internetowe i oszustwa to fałszywe strony internetowe, które wyglądają jak legalne sklepy, ale w rzeczywistości służą do nakłaniania ludzi do zakupu produktów, które nie istnieją lub są niskiej jakości. Te fałszywe sklepy często kopiują logo, opisy produktów i zdjęcia prawdziwych firm, aby wyglądać przekonująco. Oszuści wykorzystują te strony do kradzieży pieniędzy i danych osobowych niczego niepodejrzewających klientów. Wabią kupujących obietnicami bardzo niskich cen lub ofert specjalnych, które wydają się zbyt piękne, aby mogły być prawdziwe.

Te strony internetowe mogą mieć dziwne adresy internetowe, zawierać błędy ortograficzne lub brakować prawidłowych danych kontaktowych. Po dokonaniu płatności klienci często nie otrzymują zamówienia lub otrzymują podróbki. Aby się chronić, zawsze kupuj w zaufanych sklepach, sprawdzaj opinie o stronach, unikaj ofert, które wydają się nierealistycznie tanie i nigdy nie udostępniaj danych do płatności na podejrzanych stronach. Jeśli coś wydaje Ci się podejrzane, lepiej to sprawdzić przed zakupem.

Co-funded by the
European Union

Manipulacja emocjonalna i inżynieria społeczna (taktyka zastraszania)

Manipulacja emocjonalna i socjotechnika polegają na oszukiwaniu ludzi poprzez grę na ich emocjach, aby skłonić ich do działania w sposób, którego normalnie by nie zrobili. Cyberprzestępcy stosują taktyki takie jak straszenie, natarczywość, udawanie autorytetu lub życzliwości, aby wywołać poczucie strachu, zaufania lub obowiązku. Na przykład mogą udawać pracownika banku ostrzegającego o problemie z kontem, nakłaniając do szybkiego działania, aby bez zastanowienia podać poufne informacje. Taktyki te wykorzystują naturalne ludzkie reakcje – strach, zaufanie, ciekawość lub chęć pomocy – utrudniając im opór. Najlepszą obroną jest świadomość: rozpoznanie tych emocjonalnych sztuczek i zatrzymanie się, aby zweryfikować, kto naprawdę prosi o informacje, zanim odpowie.

Co-funded by the
European Union

Kradzież tożsamości (wykorzystując skradzione dane osobowe)

Kradzież tożsamości oznacza sytuację, gdy ktoś kradnie Twoje dane osobowe bez Twojej zgody i wykorzystuje je, podszywając się pod Ciebie. Może wykorzystać Twoje imię i nazwisko, numer ubezpieczenia społecznego, dane konta bankowego lub inne dane do zakładania kont, zaciągania pożyczek lub dokonywania zakupów w Twoim imieniu. Może to spowodować poważne problemy finansowe i zaszkodzić Twojej reputacji.

Co-funded by the
European Union

Oszustwo „na wnuka” (oszuści podszywający się pod rodzinę w tarapatach)

Oszustwo „na wnuka”, znane również jako „oszustwo na dziadka”, to powszechna metoda stosowana przez przestępców, którzy podszywają się pod członka rodziny – zazwyczaj wnuka lub dziecko – w potrzebie. Zazwyczaj odbywa się to telefonicznie, kiedy oszust dzwoni do osoby starszej i twierdzi, że ma poważne kłopoty, takie jak wypadek, została aresztowana lub potrzebuje pilnej pomocy finansowej. Dzwoniący często prosi o szybkie przesłanie pieniędzy i nalega, aby ofiara zachowała to w tajemnicy, na przykład mówiąc: „Nie mów mamie, bo się zmartwi”.

To oszustwo wykorzystuje emocje, takie jak miłość i troska o członków rodziny, sprawiając, że osoba chce natychmiast pomóc, bez chwili namysłu. Coraz częściej oszuści wykorzystują technologie takie jak sztuczna inteligencja, aby naśladować głos prawdziwego wnuka, dzięki czemu rozmowa brzmi bardzo przekonująco.

Co-funded by the
European Union

Fałszywe prośby o „pomoc” przez WhatsApp lub Messenger

Fałszywe prośby o „pomoc” za pośrednictwem WhatsApp lub Messengera to oszustwa, w których ktoś podszywa się pod znajomego lub członka rodziny w pilnych tarapatach, prosząc o pieniądze lub dane osobowe. Wiadomości te często przychodzą niespodziewanie od nieznanych lub podszywających się osób. Oszust może twierdzić, że zgubił telefon, został zablokowany na koncie lub potrzebuje pilnej pomocy finansowej. Stara się stworzyć poczucie pilności i zaufania, aby skłonić ofiary do szybkiego działania, nie sprawdzając, czy to prawda.

Co-funded by the
European Union

Oszustwa matrymonialne i oszustwa oparte na związkach budowanych w Internecie

Oszustwa matrymonialne to rodzaj oszustwa, w którym przestępcy tworzą fałszywe profile internetowe i udają zainteresowanie daną osobą. Z czasem budują zaufanie i więź emocjonalną, wmawiając ofierze, że jest w prawdziwym związku. Po zdobyciu zaufania, oszuści wymyślają nagłe przypadki lub pilne potrzeby finansowe – takie jak rachunki za leczenie czy koszty podróży – i proszą ofiarę o pieniądze lub prezenty.

Ci oszuści potrafią doskonale udawać troskliwych i godnych zaufania, często unikając spotkań osobistych lub rozmów wideo, podając wymówki. Wykorzystują samotność i emocjonalną wrażliwość ofiar, co zwiększa prawdopodobieństwo, że dadzą im pieniądze.

Co-funded by the
European Union

Oszustwa inwestycyjne (fałszywe reklamy z udziałem gwiazd)

Oszustwa inwestycyjne z wykorzystaniem fałszywych reklam z udziałem celebrytów to rodzaj oszustwa, w którym przestępcy wykorzystują zdjęcia, filmy lub nazwiska znanych osób, aby przedstawić okazję inwestycyjną jako legalną i wiarygodną. Czasami reklamy te zawierają filmy deepfake, na których celebryci rekomendują daną inwestycję, lub podszywają się pod artykuły prasowe, łączące celebrytów z sukcesami finansowymi na określonych platformach.

Oszuści wmawiają ludziom, że mogą szybko i dużo zarobić, często w kryptowalutach lub handlu walutami. Nakłaniają ofiary do zakładania kont, wpłacania pieniędzy, a następnie proszą o dodatkowe środki na pokrycie fałszywych opłat lub podatków. Szybkie zwroty mogą okazać się sposobem na zdobycie zaufania, ale gdy ofiary próbują wypłacić pieniądze, zostają zablokowane i poproszone o dodatkowe, wysokie płatności.

Co-funded by the
European Union

Oprogramowanie złośliwe i ransomware (zainfekowane pliki, załączniki)

Złośliwe oprogramowanie (malware) to złośliwe oprogramowanie, które może zainfekować komputer lub telefon i spowodować szkody, takie jak kradzież danych osobowych, uszkodzenie plików lub przejęcie kontroli nad urządzeniem. Ransomware to specjalny rodzaj złośliwego oprogramowania, który blokuje lub szyfruje pliki, uniemożliwiając dostęp do nich do momentu zapłacenia atakującemu okupu – zazwyczaj w kryptowalucie. Ransomware może przedostać się na urządzenie za pośrednictwem zainfekowanych załączników do wiadomości e-mail, złośliwych stron internetowych lub niebezpiecznych plików do pobrania.

Po zainfekowaniu ransomware uniemożliwia korzystanie z ważnych plików, a czasami żąda pieniędzy za przywrócenie dostępu. Zapłacenie okupu nie gwarantuje uwolnienia danych, a wręcz zachęca przestępców do kontynuowania ataków.

Co-funded by the
European Union

Niezweryfikowane aplikacje i pobieranie niebezpiecznego oprogramowania

Niezweryfikowane aplikacje i niebezpieczne pobieranie oprogramowania to cyberzagrożenia, które polegają na pobieraniu i instalowaniu aplikacji lub plików z nieznanych lub niepewnych źródeł. Te aplikacje lub pliki mogą zawierać ukryte złośliwe oprogramowanie, wirusy lub oprogramowanie szpiegujące, które może uszkodzić urządzenie, wykraść dane osobowe lub umożliwić hakerom nieautoryzowany dostęp.

Ponieważ te aplikacje nie są sprawdzane ani zatwierdzane przez zaufane platformy, mogą one zakłócać bezpieczeństwo Twojego urządzenia, powodować awarie lub narażać Cię na oszustwa. Fałszywe aplikacje mogą wyglądać jak prawdziwe, ale po zainstalowaniu mogą gromadzić Twoje dane lub rozprzestrzeniać szkodliwe oprogramowanie.

Co-funded by the
European Union

Udostępnianie wrażliwych danych obcym osobom (zdjęć, informacji)

Udostępnianie poufnych danych, takich jak zdjęcia czy dane osobowe, obcym osobom to cyberzagrożenie, polegające na udostępnianiu prywatnych danych nieznanym lub niegodnym zaufania osobom w sieci. Może się to wydawać nieszkodliwe, jak udostępnianie zdjęcia, ale dane te mogą zostać wykorzystane do kradzieży tożsamości, popełnienia oszustwa lub zaszkodzenia reputacji.

Zdjęcia mogą ujawnić Twój dom, lokalizację lub nawyki osobiste, nawet jeśli tego nie zauważysz. Nieznajomi mogą wykorzystać te informacje, aby Cię oszukać lub wykorzystać do oszustw. Aby zachować bezpieczeństwo, udostępniaj dane osobowe i zdjęcia tylko osobom, którym ufasz, zastanów się dobrze, zanim opublikujesz je w internecie, i dostosuj ustawienia prywatności, aby ograniczyć liczbę osób, które mogą zobaczyć Twoje dane.

Co-funded by the
European Union

Wycieki danych z powodu korzystania z przestarzałych urządzenia lub oprogramowanie

Korzystanie z przestarzałych urządzeń lub oprogramowania stanowi cyberzagrożenie, ponieważ stare wersje często nie posiadają najnowszych aktualizacji zabezpieczeń. Brak aktualizacji tworzy słabe punkty, zwane lukami, które hakerzy mogą łatwo wykorzystać do uzyskania dostępu do danych osobowych lub przejęcia kontroli nad urządzeniem. Może to prowadzić do wycieku danych, kradzieży lub infekcji złośliwym oprogramowaniem.

Przestarzałe oprogramowanie również spowalnia działanie urządzenia i może przestać działać z nowszymi programami, utrudniając codzienne czynności. Aby się chronić, ważne jest regularne aktualizowanie urządzenia i oprogramowania najnowszymi poprawkami i poprawkami bezpieczeństwa. Pozwala to wyeliminować luki w zabezpieczeniach, zapewnić bezpieczeństwo danych i płynne działanie urządzenia.

Co-funded by the
European Union

Masowe, spersonalizowane ataki wykorzystujące sztuczną inteligencję, mające na celu profile użytkowników

Masowe ataki personalizowane z wykorzystaniem sztucznej inteligencji to cyberzagrożenia, w których atakujący wykorzystują sztuczną inteligencję do tworzenia wysoce spersonalizowanych i przekonujących komunikatów skierowanych do konkretnych osób w oparciu o ich dane osobowe. Sztuczna inteligencja analizuje informacje z mediów społecznościowych, wiadomości e-mail i źródeł publicznych, aby tworzyć komunikaty, które wydają się znajome i godne zaufania dla ofiary.

Ataki te mogą obejmować spersonalizowane e-maile lub wiadomości phishingowe, które zawierają imię i nazwisko ofiary, jej zawód, ostatnie aktywności lub zainteresowania. Celem jest nakłonienie użytkowników do kliknięcia w złośliwe linki, ujawnienia haseł lub przelania pieniędzy. Ponieważ sztuczna inteligencja stale się uczy i adaptuje, ataki te stają się skuteczniejsze i trudniejsze do wykrycia.

Co-funded by the
European Union

Dezinformacja zdrowotna lub niebezpieczne porady medyczne pochodzące z narzędzi AI

Dezinformacja zdrowotna lub niebezpieczne porady medyczne pochodzące z narzędzi AI to cyberzagrożenie, w którym sztuczna inteligencja generuje nieprawidłowe, wprowadzające w błąd lub szkodliwe informacje zdrowotne. Ludzie mogą ufać chatbotom AI lub narzędziom online w zakresie porad medycznych, ale czasami systemy te stawiają błędne diagnozy, sugerują niebezpieczne metody leczenia lub rozpowszechniają fałszywe informacje na temat chorób.

Ta dezinformacja może prowadzić do opóźniania odpowiedniej opieki medycznej, stosowania nieskutecznych metod leczenia lub podejmowania szkodliwych działań. Treści generowane przez sztuczną inteligencję mogą brzmieć bardzo profesjonalnie i przekonująco, przez co trudno ocenić, czy porady są wiarygodne.

Co-funded by the
European Union

Oszustwa wykorzystujące wykluczenie cyfrowe w służbach obywatelskich i bankowych

Oszustwa wykorzystujące wykluczenie cyfrowe w usługach obywatelskich i bankowych to zagrożenia skierowane do osób z ograniczonym dostępem do technologii cyfrowych lub ich ograniczoną znajomością. Oszustwa te wykorzystują osoby, które mają trudności z korzystaniem z internetowych usług rządowych lub bankowych, czasami z powodu braku urządzeń, dostępu do internetu, umiejętności cyfrowych lub pewności siebie.

Przestępcy oszukują te osoby, oferując fałszywą pomoc w procesach online lub wysyłając fałszywe wiadomości podszywające się pod oficjalne instytucje, licząc na to, że ofiary udostępnią poufne dane lub prześlą pieniądze. Ponieważ osoby te mają mniej zasobów lub wsparcia, aby rozpoznać oszustwa, są bardziej podatne na ataki.

Co-funded by the
European Union

Brak praktyk uwierzytelniania wieloskładnikowego (uproszczone hasła, ponowne wykorzystanie)

Brak uwierzytelniania wieloskładnikowego (MFA) oznacza używanie wyłącznie hasła – często prostego lub powtarzanego na wielu stronach – do ochrony kont online. Jest to ryzykowne, ponieważ jeśli ktoś ukradnie lub odgadnie Twoje hasło, może łatwo uzyskać dostęp do Twoich kont.

Uwierzytelnianie wieloskładnikowe dodaje dodatkową warstwę bezpieczeństwa, wymagając dwóch lub więcej form weryfikacji. Na przykład, po wpisaniu hasła, możesz wpisać kod wysłany na telefon lub skorzystać ze skanu odcisku palca. To znacznie utrudnia hakerom dostęp do Twojego konta, nawet jeśli znają Twoje hasło.

Co-funded by the
European Union

Utrata dostępu do kluczowych usług z powodu zmian technologicznych (dostęp tylko za pośrednictwem aplikacji, ograniczone alternatywy)

Utrata dostępu do kluczowych usług spowodowana zmianami technologicznymi ma miejsce, gdy ważne usługi publiczne lub bankowe przechodzą na formaty wyłącznie cyfrowe, takie jak aplikacje czy portale internetowe, bez łatwych alternatyw dla osób, które nie czują się komfortowo lub nie mają do nich dostępu. Oznacza to, że osoby nieposiadające smartfonów, komputerów ani umiejętności cyfrowych mogą mieć trudności lub wręcz nie mieć dostępu do podstawowych usług, takich jak wizyty u lekarza, świadczenia emerytalne czy transakcje bankowe.

Ta cyfrowa zmiana może powodować wykluczenie wielu osób, zwłaszcza starszych i tych o ograniczonych zasobach, czyniąc je zależnymi od innych lub uniemożliwiając im realizację ważnych zadań.

Co-funded by the
European Union

Zautomatyzowana manipulacja kanałami mediów społecznościowych, powodująca dezinformację i stres

Zautomatyzowana manipulacja kanałami mediów społecznościowych to cyberzagrożenie, w którym programy komputerowe, zwane botami, oraz sztuczna inteligencja kontrolują treści, które widzisz na swoich stronach w mediach społecznościowych. Systemy te analizują, co lubisz, udostępniasz lub komentujesz, a następnie wyświetlają Ci więcej podobnych postów, aby utrzymać Twoje zaangażowanie.

Niestety, może to być wykorzystywane do rozpowszechniania dezinformacji, fałszywych wiadomości lub treści ekstremalnych, wywołujących stres, strach lub gniew. Boty mogą sztucznie zwiększać popularność takich postów poprzez lajkowanie, udostępnianie lub komentowanie, sprawiając wrażenie, że wiele osób się z nimi zgadza.