**Program mentorski dla osób w wieku 50+**

# MODUŁ 6

# Bezpieczne korzystanie z technologii cyfrowych

**Wzmocnienie możliwości wspierania aktywnego starzenia się w warunkach XXI wieku - program mentoringu rówieśniczego dla osób 50+**

**PEER-TRAIN**



50+ PEER TRAIN

Co-funded by the European Union

# SPIS TREŚCI

# 6. Bezpieczne korzystanie z technologii cyfrowych

## 6.1 Wprowadzenie


Bezpieczne korzystanie z technologii cyfrowych odnosi się do odpowiedzialnego i bezpiecznego korzystania z urządzeń elektronicznych, aplikacji i usług online. Ponieważ technologia staje się coraz bardziej wszechobecna w naszym codziennym życiu, ważne jest, aby korzystać z technologii cyfrowych bezpiecznie i skutecznie, szczególnie w przypadku starszych użytkowników, którzy mogą być bardziej podatni na zagrożenia cyfrowe.

Statystyki wskazują, że korzystanie z Internetu przez starszych użytkowników stale rośnie w ostatnich latach. Według Pew Research Center, od 2021 roku 73% dorosłych w wieku 65 lat i starszych korzysta z Internetu. Jednak wielu starszych użytkowników może nie być świadomych zagrożeń związanych z korzystaniem z technologii cyfrowych, takich jak oszustwa phishingowe, kradzież tożsamości i cyberprzemoc.

Aby zapewnić bezpieczne korzystanie z technologii cyfrowych, ważne jest, aby podjąć kroki w celu ochrony danych osobowych i urządzeń. Może to obejmować używanie silnych haseł, unikanie klikania podejrzanych linków lub wiadomości e-mail, regularne aktualizowanie

oprogramowania i ustawień zabezpieczeń oraz ostrożność podczas udostępniania danych osobowych online.

Ponadto pomocne dla starszych użytkowników może być edukacja i szkolenie w zakresie bezpiecznego korzystania z technologii, zwłaszcza jeśli nie są zaznajomieni z najnowszymi środkami bezpieczeństwa i najlepszymi praktykami. Może to obejmować poszukiwanie wskazówek od członków rodziny lub przyjaciół, lub uczestnictwo w warsztatach lub zajęciach zaprojektowanych specjalnie dla seniorów.

Ogólnie rzecz biorąc, bezpieczne korzystanie z technologii cyfrowych jest niezbędne, aby starsi użytkownicy mogli w pełni uczestniczyć w dzisiejszym cyfrowym świecie, jednocześnie chroniąc się przed potencjalnymi zagrożeniami.

Oto 10 ważnych kwestii, które należy wziąć pod uwagę w celu bezpiecznego korzystania z technologii cyfrowych przez starszych użytkowników:

Oszustwa i wyłudzenia internetowe: Starsi użytkownicy mogą być celem oszustw internetowych, takich jak wiadomości phishingowe, fałszywe strony internetowe i kradzież tożsamości. Powinni oni zachować ostrożność podczas udostępniania danych osobowych i finansowych online.

Cyberprzemoc: Starsi użytkownicy mogą być narażeni na cyberprzemoc i nękanie online, zwłaszcza na platformach mediów społecznościowych. Powinni oni być świadomi zagrożeń i podejmować odpowiednie środki, aby się chronić.

Prywatność online: Starsi użytkownicy powinni być świadomi swojej prywatności w Internecie i podejmować kroki w celu ochrony swoich danych osobowych. Obejmuje to używanie silnych haseł, unikanie publicznych sieci Wi-Fi i ostrożność w udostępnianiu danych osobowych online.

Umiejętność korzystania z technologii: Starszym użytkownikom może brakować umiejętności i wiedzy niezbędnych do bezpiecznego i skutecznego korzystania z technologii cyfrowych. Powinni oni otrzymać szkolenie i wsparcie w celu poprawy ich umiejętności korzystania z technologii.

Bezpieczeństwo fizyczne: Starsi użytkownicy powinni być świadomi ryzyka związanego z korzystaniem z technologii, takiego jak zmęczenie oczu, ból pleców i upadki, oraz podejmować kroki w celu zapobiegania tym zagrożeniom.

Izolacja społeczna: Starsi użytkownicy mogą doświadczać izolacji społecznej z powodu korzystania z technologii cyfrowych, takich jak platformy mediów społecznościowych. Należy ich zachęcać do korzystania z technologii jako sposobu na pozostanie w kontakcie z rodziną i przyjaciółmi.

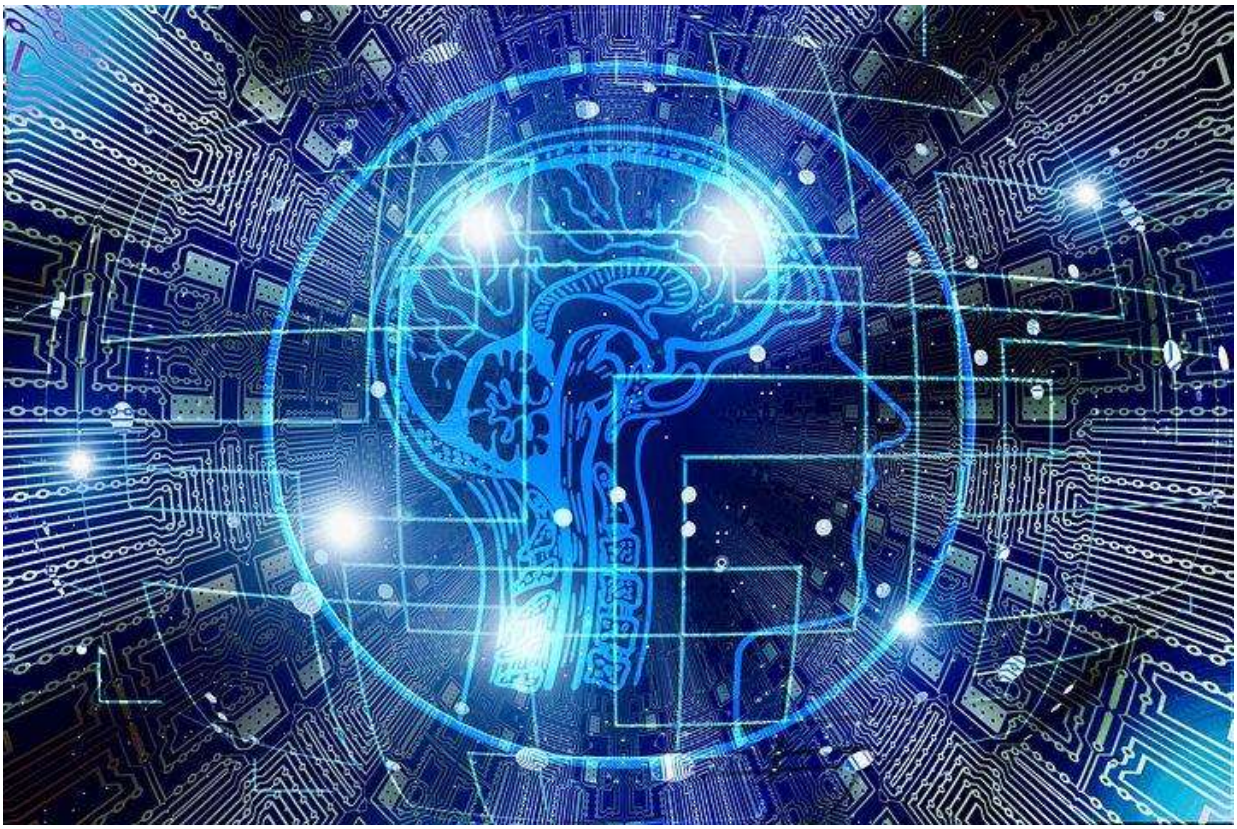
Dostępność: Starsi użytkownicy mogą mieć upośledzenia fizyczne i poznawcze, które wpływają na ich zdolność do korzystania z technologii cyfrowych. Powinni oni mieć dostęp do technologii wspomagających i udogodnień wspierających korzystanie z nich.

Cyberbezpieczeństwo: Starsi użytkownicy mogą być bardziej narażeni na cyberataki ze względu na brak znajomości technologii cyfrowych. Powinni oni korzystać z oprogramowania antywirusowego i zachować ostrożność przy pobieraniu załączników i klikaniu linków.

Oszustwa telefoniczne: Starsi użytkownicy mogą otrzymywać oszukańcze połączenia, które próbują wyłudzić od nich pieniądze lub informacje. Powinni być świadomi takich połączeń i podjąć niezbędne środki ostrożności.

Ageizm: Starsi użytkownicy mogą być narażeni na ageizm w świecie cyfrowym, np. poprzez wykluczenie ze społeczności lub usług online. Powinni oni mieć możliwość kwestionowania takich praktyk i obrony swoich praw.

## 6.2. Światło na sztuczną inteligencję



Sztuczna inteligencja (AI) odnosi się do rozwoju systemów komputerowych, które mogą wykonywać zadania zwykle wymagające ludzkiej inteligencji, takie jak percepcja wzrokowa, rozpoznawanie mowy, podejmowanie decyzji i tłumaczenie języka. Sztuczna inteligencja staje się coraz ważniejsza w wielu branżach, w tym w opiece zdrowotnej, finansach i transporcie, ze względu na jej zdolność do analizowania dużych ilości danych i przewidywania na ich podstawie.

Jednym z najlepszych przykładów zastosowania sztucznej inteligencji jest opieka zdrowotna. Sztuczna inteligencja może być wykorzystywana do analizowania danych pacjentów, identyfikowania wzorców i przewidywania potencjalnych zagrożeń dla zdrowia. Algorytmy AI mogą na przykład analizować obrazy medyczne, takie jak zdjęcia rentgenowskie lub rezonans magnetyczny, w celu zidentyfikowania nieprawidłowości, które mogą być trudne do wykrycia przez lekarzy. Sztuczna inteligencja może być również wykorzystywana do personalizacji planów leczenia w oparciu o indywidualne dane pacjenta, co może poprawić wyniki leczenia i obniżyć koszty opieki zdrowotnej.

Innym przykładem zastosowania sztucznej inteligencji jest dziedzina finansów. Sztuczna inteligencja może być wykorzystywana do analizy dużych ilości danych finansowych, takich jak

ceny akcji i wskaźniki ekonomiczne, oraz do przewidywania przyszłych trendów rynkowych. Może to pomóc instytucjom finansowym w podejmowaniu bardziej świadomych decyzji inwestycyjnych i zmniejszeniu ryzyka związanego ze zmiennością rynku.

W transporcie sztuczna inteligencja jest wykorzystywana do opracowywania autonomicznych samochodów i ulepszania systemów zarządzania ruchem. Samojezdne samochody wykorzystują algorytmy sztucznej inteligencji do interpretowania danych o ruchu drogowym w czasie rzeczywistym, nawigowania po drogach oraz podejmowania decyzji dotyczących prędkości i kierunku jazdy. Sztuczna inteligencja może być również wykorzystywana do optymalizacji przepływu ruchu poprzez analizę danych z czujników i kamer na drogach i autostradach.

Ogólnie rzecz biorąc, sztuczna inteligencja ma potencjał, aby przekształcić wiele branż i poprawić nasze codzienne życie na niezliczone sposoby. Ważne jest jednak, aby wziąć pod uwagę etyczne implikacje rozwoju sztucznej inteligencji i upewnić się, że jest ona wykorzystywana w sposób odpowiedzialny i z korzyścią dla całego społeczeństwa.

## 6.3. Korzyści i zagrożenia związane z technologiami cyfrowymi

Technologie cyfrowe zrewolucjonizowały sposób, w jaki żyjemy i pracujemy, zapewniając wiele korzyści, takich jak zwiększona wydajność, wygoda i łączność. Jednak wraz z tymi korzyściami istnieją również zagrożenia związane z wykorzystaniem technologii cyfrowych, których musimy być świadomi.

Jedną z głównych zalet technologii cyfrowych jest zwiększona wydajność. Zadania, które kiedyś zajmowały godziny, a nawet dni, można teraz wykonać w ciągu kilku minut dzięki narzędziom cyfrowym i automatyzacji. Ta zwiększona wydajność może pomóc osobom i organizacjom zaoszczędzić czas i pieniądze, a także pozwolić im skupić się na bardziej kreatywnych lub strategicznych zadaniach.

Kolejną zaletą technologii cyfrowych jest wygoda. Zakupy online, bankowość mobilna i wideokonferencje to tylko kilka przykładów tego, jak technologie cyfrowe uczyniły nasze życie wygodniejszym. Możemy teraz uzyskać dostęp do informacji i usług z dowolnego miejsca i w dowolnym czasie, dzięki czemu nasze życie jest bardziej elastyczne i elastyczne.

Technologie cyfrowe zwiększyły również łączność, pozwalając nam komunikować się z ludźmi na całym świecie w czasie rzeczywistym. Media społecznościowe, aplikacje do przesyłania wiadomości i społeczności internetowe ułatwiły nawiązywanie kontaktów z osobami o podobnych poglądach i budowanie relacji, niezależnie od położenia geograficznego. Ta zwiększona łączność może pomóc we wspieraniu współpracy i innowacji, prowadząc do nowych pomysłów i rozwiązań.

Jednak wraz z tymi korzyściami pojawiają się zagrożenia, których musimy być świadomi. Zagrożenia dla cyberbezpieczeństwa, takie jak hakowanie, phishing i kradzież tożsamości, stają się coraz bardziej powszechne i wyrafinowane, narażając na ryzyko osoby fizyczne i organizacje. Technologie cyfrowe mogą również prowadzić do obaw o prywatność, ponieważ nasze dane osobowe są często przechowywane i udostępniane online bez naszej zgody lub wiedzy. Ponadto nadmierne poleganie na technologiach cyfrowych może prowadzić do braku interakcji społecznych i zmniejszenia aktywności fizycznej, co może mieć negatywny wpływ na nasze zdrowie psychiczne i fizyczne.

Podsumowując, technologie cyfrowe przynoszą wiele korzyści, które zmieniły nasz sposób życia i pracy. Musimy jednak być również świadomi zagrożeń związanych z ich użytkowaniem i podjąć kroki w celu złagodzenia tego ryzyka. Obejmuje to czujność w zakresie cyberbezpieczeństwa, ochronę naszych danych osobowych i znalezienie równowagi między łącznością cyfrową a interakcjami w świecie rzeczywistym. W ten sposób możemy nadal czerpać korzyści z technologii cyfrowych, zachowując jednocześnie bezpieczeństwo w coraz bardziej cyfrowym świecie.

## 6.4. Podsumowanie i często zadawane pytania


Poniższe zasoby mogą być pomocne dla osób fizycznych, rodziców, nauczycieli i firm, którzy chcą dowiedzieć się więcej o bezpiecznym korzystaniu z technologii cyfrowych oraz o tym, jak chronić siebie i swoje dane osobowe w Internecie:

- StaySafeOnline.org - Ta strona internetowa jest prowadzona przez National Cyber Security Alliance i zawiera zasoby i wskazówki dotyczące zachowania bezpieczeństwa w Internecie, w tym informacje o tym, jak chronić swoje urządzenia i dane osobowe.
- Cybersecurity & Infrastructure Security Agency (CISA) - CISA to agencja rządowa, która zapewnia zasoby i wytyczne dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa, w tym wskazówki dla osób fizycznych i firm dotyczące ochrony przed zagrożeniami cybernetycznymi.
- Common Sense Media - Ta strona internetowa zawiera zasoby i porady dla rodziców, nauczycieli i dzieci dotyczące bezpiecznego i odpowiedzialnego korzystania z

technologii cyfrowych, w tym informacje na temat prywatności, cyberprzemocy i czasu spędzanego przed ekranem.

- NetSmartz - NetSmartz to interaktywna strona internetowa, która zapewnia zasoby i działania dla dzieci i nastolatków, aby dowiedzieć się o bezpieczeństwie w Internecie i cyberprzemocy.
- Federalna Komisja Handlu (FTC) - FTC zapewnia informacje na temat ochrony konsumentów, w tym zasoby dotyczące bezpieczeństwa w Internecie, kradzieży tożsamości i oszustw.
- Online Safety Foundation - ta organizacja non-profit zapewnia zasoby i narzędzia do bezpiecznego zachowania w Internecie, w tym wskazówki dla rodziców, nauczycieli i seniorów, jak zachować bezpieczeństwo w Internecie.
- Privacy Rights Clearinghouse - ta organizacja zapewnia zasoby i porady dotyczące ochrony danych osobowych i prywatności, w tym informacje na temat naruszeń danych, kradzieży tożsamości i śledzenia online.

Oto przykładowe często zadawane pytania:

P: Jakie są typowe zagrożenia cyberbezpieczeństwa, o których powinienem wiedzieć?

O: Powszechne zagrożenia cyberbezpieczeństwa obejmują oszustwa phishingowe, złośliwe oprogramowanie, kradzież tożsamości i hakowanie. Ważne jest, aby zwracać uwagę na podejrzane wiadomości e-mail, linki i pliki do pobrania, a także używać silnych haseł i oprogramowania zabezpieczającego w celu ochrony urządzeń.

P: Jak mogę chronić swoje dane osobowe online?

O: Aby chronić swoje dane osobowe w Internecie, należy używać silnych i unikalnych haseł do wszystkich swoich kont, unikać udostępniania danych osobowych w mediach społecznościowych lub na innych platformach internetowych oraz zachować ostrożność podczas udostępniania informacji nieznanym stronom. Powinieneś także regularnie aktualizować ustawienia prywatności w mediach społecznościowych i innych platformach internetowych, aby upewnić się, że Twoje informacje nie są udostępniane bez Twojej zgody.

P: Jak mogę zapewnić bezpieczeństwo moich urządzeń?

O: Aby zapewnić bezpieczeństwo urządzeń, należy regularnie aktualizować oprogramowanie i ustawienia zabezpieczeń, korzystać z oprogramowania antywirusowego i chroniącego przed złośliwym oprogramowaniem oraz unikać pobierania lub instalowania oprogramowania z nieznanych źródeł. W miarę możliwości należy również korzystać z uwierzytelniania dwuskładnikowego, które wymaga podania hasła i dodatkowej metody weryfikacji, takiej jak odcisk palca lub wiadomość tekstowa.

P: Jak mogę uniknąć stania się ofiarą cyberprzemocy?

O: Aby nie stać się ofiarą cyberprzemocy, należy uważać na to, co udostępnia się w sieci i unikać kontaktów z osobami, które zachowują się agresywnie lub niewłaściwie w sieci. Powinieneś być również świadomy dostępnych zasobów do zgłaszania cyberprzemocy i szukania wsparcia, takich jak szkoła, miejsce pracy lub lokalne organy ścigania.

P: Jak mogę zapewnić moim dzieciom bezpieczeństwo w Internecie?

O: Aby zapewnić dzieciom bezpieczeństwo w Internecie, należy monitorować ich aktywność online oraz korzystać z kontroli rodzicielskiej i oprogramowania filtrującego w celu ograniczenia dostępu do nieodpowiednich treści. Powinieneś także nauczyć swoje dzieci bezpiecznych zachowań w Internecie, takich jak unikanie udostępniania danych osobowych w Internecie i ostrożność podczas osobistych spotkań z nieznajomymi.

P: Co powinienem zrobić, jeśli podejrzewam, że moje dane osobowe zostały naruszone?

O: Jeśli podejrzewasz, że Twoje dane osobowe zostały naruszone, natychmiast skontaktuj się ze swoją instytucją finansową, firmą obsługującą karty kredytowe lub innymi odpowiednimi organizacjami, aby zgłosić problem i podjąć kroki w celu ochrony swoich kont. Powinieneś także rozważyć umieszczenie ostrzeżenia o oszustwie lub zamrożenia zabezpieczeń w raporcie kredytowym, aby zapobiec dalszym nieautoryzowanym działaniom.

P: Czym jest sztuczna inteligencja?

A: AI, czyli sztuczna inteligencja, odnosi się do zdolności maszyn lub komputerów do wykonywania zadań, które zazwyczaj wymagają ludzkiej inteligencji, takich jak rozpoznawanie wzorców, uczenie się i rozwiązywanie problemów.

P: Jak działa sztuczna inteligencja?

A: Sztuczna inteligencja wykorzystuje algorytmy i dane do uczenia się i przewidywania lub podejmowania decyzji. Wykorzystuje uczenie maszynowe, przetwarzanie języka naturalnego i inne technologie do symulowania ludzkiej inteligencji.

P: Jakie są przykłady zastosowań sztucznej inteligencji?

O: Sztuczna inteligencja jest wykorzystywana w szerokim zakresie zastosowań, w tym w wirtualnych asystentach, rozpoznawaniu obrazu, analizie predykcyjnej, autonomicznych pojazdach i inteligentnych domach.

P: Czy sztuczna inteligencja zastępuje miejsca pracy?

O: Sztuczna inteligencja może potencjalnie zautomatyzować niektóre zadania i miejsca pracy, ale może także stworzyć nowe miejsca pracy i możliwości. Podczas gdy niektóre zawody mogą zostać zastąpione przez sztuczną inteligencję, inne będą wymagały ludzkich umiejętności, takich jak kreatywność, rozwiązywanie problemów i inteligencja emocjonalna.

P: Jak regulowana jest sztuczna inteligencja?

O: Sztuczna inteligencja to szybko rozwijająca się dziedzina, a przepisy wciąż są opracowywane w celu uwzględnienia jej etycznych, prawnych i społecznych implikacji. Niektóre kraje ustanowiły polityki i wytyczne dotyczące AI, a organizacje międzynarodowe, takie jak OECD i UE, pracują nad opracowaniem zasad AI.

P: Jakie są obawy etyczne związane ze sztuczną inteligencją?

O: Obawy etyczne związane ze sztuczną inteligencją obejmują kwestie stronniczości, przejrzystości, prywatności, odpowiedzialności i potencjalnego niewłaściwego wykorzystania technologii AI do nadzoru lub wyrządzania szkód.

P: Czy sztuczna inteligencja może być stronnicza?

O: Sztuczna inteligencja może być stronnicza, jeśli jest szkolona na podstawie stronniczych danych lub algorytmów. Może to prowadzić do dyskryminacji w obszarach takich jak zatrudnianie, udzielanie pożyczek i wymiar sprawiedliwości w sprawach karnych.

P: Czy sztuczna inteligencja jest niebezpieczna?

O: Sztuczna inteligencja może być niebezpieczna, jeśli nie jest rozwijana i wykorzystywana w sposób odpowiedzialny. Istnieją obawy dotyczące potencjalnego niewłaściwego wykorzystania technologii AI, takich jak autonomiczna broń lub systemy nadzoru.

P: Jak mogę dowiedzieć się więcej o sztucznej inteligencji?

O: Istnieje wiele dostępnych zasobów, aby dowiedzieć się więcej o sztucznej inteligencji, w tym kursy online, książki i konferencje. Niektóre popularne zasoby to Coursera, Udemy i MIT OpenCourseWare.

Weź plakat!

# 5 wskazówek dotyczących bezpieczeństwa w Internecie

| | |
|---|---|
|  | **Nie podawaj danych osobowych**<br>Zachowaj prywatność swoich danych osobowych i używaj ich tylko w bezpiecznych witrynach. |
|  | **Tworzenie złożonych haseł**<br>Tworzenie haseł składających się z kombinacji liter, cyfr i symboli |
|  | **Aktualizuj swój komputer**<br>Aktualizuj oprogramowanie urządzenia, aby nie było podatne na złośliwe oprogramowanie. |

| | |
|---|---|
|  | **Unikaj podejrzanych linków online**<br><br>Niektóre strony internetowe mogą wykraść Twoje dane osobowe, prosząc Cię o wypełnienie quizu. Bądź ostrożny! |
|  | **Sprawdź niezawodność witryny**<br><br>Przed zakupem czegokolwiek na stronie internetowej upewnij się, że jest ona bezpieczna. |

## 6.5. Pytania

### 6.5.1 Quiz

1. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Kliknięcie dowolnego linku lub pobranie dowolnego załącznika przychodzącego w wiadomości e-mail jest bezpieczne, niezależnie od nadawcy. (Fałsz)

a) Prawda
b) Fałsz

2. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Używanie silnych haseł, częsta ich zmiana i nieudostępnianie ich innym osobom jest ważne dla bezpieczeństwa online. (Prawda)

a) Prawda
b) Fałsz

3. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Podawanie w Internecie danych osobowych, takich jak imię i nazwisko, adres i numer ubezpieczenia społecznego, jest bezpieczne. (Fałsz)

a) Prawda
b) Fałsz

4. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Publiczne sieci Wi-Fi, takie jak te znajdujące się w kawiarniach i na lotniskach, są zazwyczaj bezpieczne. (Fałsz)

a) Prawda
b) Fałsz

5. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Wyskakujące reklamy, które twierdzą, że wygrałeś nagrodę lub musisz zaktualizować oprogramowanie komputerowe, są zazwyczaj legalne. (Fałsz)

a) Prawda
b) Fałsz

6. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Instalowanie i regularne aktualizowanie oprogramowania antywirusowego na komputerze jest skutecznym sposobem ochrony przed złośliwym oprogramowaniem i innymi zagrożeniami internetowymi. (Prawda)

a) Prawda
b) Fałsz

7. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Bezpiecznie jest ufać każdej recenzji i opinii online podczas dokonywania zakupu. (Fałsz)

a) Prawda
b) Fałsz

8. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Platformy mediów społecznościowych są bezpiecznym miejscem do dzielenia się osobistymi informacjami i zdjęciami z przyjaciółmi i rodziną. (Fałsz)

a) Prawda
b) Fałsz

9. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Oszustwa phishingowe, w których ktoś podszywa się pod legalny podmiot, aby nakłonić użytkownika do przekazania mu poufnych informacji, nie są zbyt powszechne. (Fałsz)

a) Prawda
b) Fałsz

10. **Czy to stwierdzenie jest prawdziwe czy fałszywe?**

Oszustwa i oszustwa internetowe zdarzają się tylko osobom, które nie są obeznane z technologią. (Fałsz)

a) Prawda
b) Fałsz

### 6.5.2. Przygotowanie do sesji grupowej

**Online Scavenger Hunt:** Stwórz listę wskazówek dotyczących bezpieczeństwa w Internecie oraz terminów lub pojęć związanych ze sztuczną inteligencją i poproś seniorów, aby znaleźli i dowiedzieli się więcej na ich temat w Internecie. Mogą na przykład wyszukać "jak utworzyć silne hasło", "czym jest uwierzytelnianie dwuskładnikowe", "czym jest uczenie maszynowe" lub "czym są chatboty".

**Korzystanie z uwierzytelniania dwuskładnikowego:** Wyjaśnij koncepcję uwierzytelniania dwuskładnikowego i sposób, w jaki może ono pomóc w ochronie kont internetowych. Poproś seniorów, aby przećwiczyli konfigurowanie uwierzytelniania dwuskładnikowego na swoich kontach e-mail lub kontach w mediach społecznościowych i wyjaśnij, w jaki sposób ta dodatkowa warstwa zabezpieczeń może pomóc w zapobieganiu próbom włamań.

**Wykrywanie fałszywych wiadomości:** Podziel się kilkoma artykułami z seniorami i poproś ich, aby zidentyfikowali, które z nich są fałszywymi wiadomościami. Wyjaśnij, jak identyfikować wiarygodne źródła, jak sprawdzać fakty i jak rozpoznawać nagłówki typu clickbait. To ćwiczenie pomoże seniorom stać się bardziej krytycznymi konsumentami treści online.

**Identyfikacja wiadomości phishingowych:** Przedstaw seniorom przykładowe wiadomości e-mail i poproś ich o zidentyfikowanie, które z nich są wiadomościami phishingowymi. Wyjaśnij, jakich wskazówek powinni szukać, takich jak podejrzane linki, błędy gramatyczne lub prośby o podanie danych osobowych. To ćwiczenie pomoże seniorom stać się bardziej świadomymi powszechnych taktyk phishingowych i uniknąć stania się ich ofiarą.

**Rozpoznaj oszustwo:** Pokaż seniorom przykłady oszustw internetowych i poproś ich o zidentyfikowanie czerwonych flag, które sugerują, że nie są one legalne. Możesz na przykład pokazać im wiadomość phishingową, wyskakującą reklamę, która twierdzi, że wygrali nagrodę lub wiadomość z prośbą o podanie danych osobowych.

**Burza mózgów na temat zastosowań sztucznej inteligencji:** Poproś seniorów o przeprowadzenie burzy mózgów na temat praktycznych zastosowań sztucznej inteligencji, które mogliby uznać za pomocne lub interesujące w ich codziennym życiu. Mogą na przykład wymyślić osobistego asystenta opartego na sztucznej inteligencji, aplikację wykorzystującą sztuczną inteligencję do pomocy w zakupach spożywczych lub zarządzaniu lekami lub urządzenie wykorzystujące sztuczną inteligencję do monitorowania ich zdrowia.

**Zrozumienie uprzedzeń związanych ze sztuczną** inteligencją: Wyjaśnij, w jaki sposób sztuczna inteligencja może czasami utrwalać uprzedzenia i stereotypy oraz podaj przykłady tego zjawiska. Poproś seniorów o krytyczne zastanowienie się nad tym, w jaki sposób sztuczna inteligencja jest wykorzystywana w ich codziennym życiu oraz w jaki sposób mogą zidentyfikować i rozwiązać przypadki uprzedzeń.

**Ćwiczenie silnych haseł:** Poinstruuj seniorów, aby tworzyli silne hasła przy użyciu kombinacji wielkich i małych liter, cyfr i symboli. Niech przećwiczą tworzenie i zapamiętywanie kilku haseł i wyjaśnią, dlaczego jest to ważne dla bezpieczeństwa w Internecie.

**Zarządzanie hasłami:** Przedstaw seniorom przykłady słabych haseł i poproś ich o stworzenie silnych haseł zgodnych z najlepszymi praktykami. Możesz także pokazać im, jak używać menedżera haseł do bezpiecznego przechowywania haseł i zarządzania nimi.

**Tworzenie quizu na temat bezpieczeństwa w Internecie:** Stwórz quiz na tematy związane z bezpieczeństwem w Internecie i sztuczną inteligencją i poproś seniorów o przygotowanie pytań. Zasugeruj przygotowanie pytań dotyczących bezpiecznych nawyków przeglądania, oszustw phishingowych, ustawień prywatności w mediach społecznościowych i etyki AI. Wspólnie przejrzyjcie odpowiedzi i omówcie obszary, w których mogą potrzebować więcej wskazówek.

## Załącznik: Odpowiedzi do quizu

| Pytanie | Prawidłowa odpowiedź |
|---|---|
| 1. | Fałsz |
| 2. | Prawda |
| 3. | Fałsz |
| 4. | Fałsz |
| 5. | Fałsz |
| 6. | Prawda |
| 7. | Fałsz |
| 8. | Fałsz |
| 9. | Fałsz |
| 10. | Fałsz |

## 6.6. Literatura


1. Wersja ChatGPT z 13 lutego, https://chat.openai.com/chat, ostatnie otwarcie 2023.02.25
2. BLOG Sektor 3.0 https://sektor3-0.pl/blog/chatgpt-jak-korzystac/, ostatnio otwarty 2023.02.25
3. DeepL Translator, https://www.deepl.com/en/translator, ostatnio otwarty 2023.02.25
4. Lista odtwarzania YouTube, Light on AI, Światło na Sztuczną Inteligencję, https://youtube.com/playlist?list=PLeOe3daa0qUxPcl2YaC04pF9ZIjr1IleE, ostatnio otwarta 2023.02.25
5. AI for the Common Good, https://www.semanticscholar.org/about, ostatnie otwarcie 2023.02.25
6. Future IT Professionals Education in Artificial Intelligence (FITPED-AI), https://fitped.eu/fitped-ai/, ostatnie otwarcie 2023.02.25
7. ABC Cyberbezpieczeństwa, https://www.gov.pl/web/baza-wiedzy/abc-cyberbezpieczenstwa---nowy-poradnik-przygotowany-przez-nask-pib, ostatnio otwarty 2023.02.25
8. ABC Cyberbezpieczeństwa, https://www.nask.pl/pl/aktualnosci/5123,ABC-cyberbezpieczenstwa-od-NASK.html, ostatnio otwarty 2023.02.25
9. ACE IT Scotland, Keeping safe on the Internet, https://youtube.com/playlist?list=PLJQ1e8zJE5Gwo3XpT8OFpyK1qJdIUHrB5, ostatnie otwarcie 2023.02.25
10. ACE IT Scotland, Podstawy online, https://youtube.com/playlist?list=PLJQ1e8zJE5GxvegbjgJAAOfVYt95R4Ogm, ostatnio otwarty 2023.02.25
11. Grabowska A., Konferencja MoodleMoot PL 2022, MoodleCloud & PEER-TRAIN na Festiwalu Światła http://utwpg.gda.pl/2023FS/MoodleMoot%202022%20-%20MoodleCloud%20%26%20PEER-TRAIN%20na%20Festiwalu%20%C5%9Awiat%C5%82a.pdf