BEZPIECZEŃSTWO
W ŚWIECIE CYFROWYM

Program szkoleniowy z warsztatami, scenariuszami i materiałami dla nauczycieli na temat cyberbezpieczeństwa seniorów

SPIS TREŚCI

1. Wprowadzenie

„Cyber Safe Senior" to finansowany przez Unię Europejską projekt mający na celu poprawę umiejętności cyfrowych, bezpieczeństwa w Internecie i ogólnego wzmocnienia pozycji osób starszych w wieku 65 lat i powyżej w zakresie technologii cyfrowych. W dzisiejszym coraz bardziej cyfrowym świecie seniorzy napotykają szczególne przeszkody podczas poruszania się po środowiskach internetowych, ponieważ często nie znają nowych technologii, zagrożeń internetowych i bezpiecznych zachowań cyfrowych. Mając tego świadomość, inicjatywa Cyber Safe Senior ma na celu wypełnienie istotnych luk w wiedzy i kompetencjach cyfrowych poprzez zorganizowane, dostępne i wieloaspektowe podejście.

Projekt obejmuje stworzenie informacyjnego e-booka zawierającego rzeczywiste studia przypadków przestępstw internetowych, praktyczne porady dotyczące bezpieczeństwa oraz szczegółowe instrukcje dotyczące bezpiecznego zachowania w Internecie. Ponadto inicjatywa oferuje wirtualne wykłady, interaktywne ćwiczenia oparte na scenariuszach oraz pilotażowe sesje szkoleniowe, które są specjalnie dostosowane do celów edukacyjnych i preferencji starszych uczestników. Cyber Safe Senior ma na celu wyeliminowanie wykluczenia cyfrowego, zwiększenie zaufania do korzystania z technologii oraz umożliwienie osobom starszym samodzielnego i bezpiecznego uczestnictwa w środowiskach cyfrowych, koncentrując się na seniorach, którzy mają podstawowe doświadczenie cyfrowe, ale brakuje im świadomości w zakresie bezpieczeństwa w Internecie.

Program szkoleniowy projektu dla nauczycieli i trenerów zapewnia im informacje, metodologię i praktyczne narzędzia potrzebne do prowadzenia wysokiej jakości edukacji seniorów w zakresie bezpieczeństwa w Internecie. Trenerzy są przygotowani nie tylko do nauczania podstawowych pojęć z zakresu cyberbezpieczeństwa, ale także do angażowania uczniów w interaktywne zajęcia, scenariusze z życia wzięte i ćwiczenia, które podkreślają specyficzne problemy, z jakimi osoby starsze mogą się spotkać w świecie cyfrowym. Gwarantuje to, że szkolenie jest zarówno praktyczne, jak i bezpośrednio związane z codziennym życiem uczestników.

Projekt jest realizowany przez konsorcjum partnerów z Polski, Słowenii, Turcji i Grecji, którzy łączą wiedzę instytucji edukacyjnych, organizacji społecznych, bibliotek, ośrodków kultury i społeczności seniorów. Korzystając z tych lokalnych sieci, Cyber Safe Senior może dotrzeć do seniorów zarówno w miastach, jak i na obszarach wiejskich, zapewniając równy dostęp do materiałów i wsparcia w zakresie umiejętności cyfrowych.

Poprzez edukowanie seniorów w zakresie pewnego korzystania z platform internetowych, ochrony danych osobowych, rozpoznawania zagrożeń internetowych i aktywnego uczestnictwa w społeczeństwie cyfrowym, projekt ma na celu stworzenie bezpieczniejszego i bardziej przyjaznego środowiska cyfrowego. Ostatecznie Cyber Safe Senior łączy materiały instruktażowe, praktyczne zajęcia i zaangażowanie społeczności, aby stworzyć środowisko, w którym seniorzy mają dostęp do informacji, umiejętności i pewności siebie potrzebnych do bezpiecznego, niezależnego i produktywnego korzystania z narzędzi cyfrowych.

Kluczowym elementem uzupełniającym program szkoleniowy Cyber Safe Senior jest zestaw interaktywnych studiów przypadków Improve opracowanych przy użyciu Genially. Te oparte na scenariuszach przypadki są w pełni dostosowane do tematów poszczególnych modułów szkoleniowych i mają na celu symulowanie rzeczywistych sytuacji cyfrowych, z którymi często spotykają się seniorzy. Dzięki kierowanemu podejmowaniu decyzji, praktycznym zadaniom i interakcji wizualnej studia przypadków Improve wzmacniają wiedzę teoretyczną i wspierają uczenie się przez doświadczenie, sprawiając, że złożone pojęcia związane z bezpieczeństwem w Internecie stają się bardziej przystępne i angażujące dla starszych uczniów.

Każdy moduł szkoleniowy ma ustrukturyzowany format zgodny z interfejsem modułu, obejmujący cele nauczania, planowanie sesji, dodatkowe zasoby, autorefleksję trenera i elementy oceny. Na początku i na końcu każdego modułu przeprowadzane są testy wstępne i końcowe w celu zmierzenia poziomu przyswojonej wiedzy i postępów w nauce. Ponadto stosowane są ankiety oceniające, które służą do zbierania opinii od uczestników i trenerów, wspierając zapewnienie jakości i ciągłe doskonalenie programu szkoleniowego.

1.1 Cel programu szkoleniowego

Program szkoleniowy Cyber Safe Senior został opracowany w celu zaspokojenia rosnącego zapotrzebowania na umiejętności cyfrowe i bezpieczeństwo w Internecie wśród osób starszych w wieku 65 lat i powyżej. Osoby starsze mają trudności z poruszaniem się po środowisku internetowym w dzisiejszym cyfrowym świecie, ponieważ zazwyczaj mają niewielką wiedzę na temat potencjalnych zagrożeń, środków bezpieczeństwa w Internecie i bezpiecznych nawyków cyfrowych. Celem tego programu szkoleniowego jest wypełnienie tych luk poprzez zapewnienie osobom starszym narzędzi potrzebnych do bezpiecznego i pewnego korzystania z technologii cyfrowych w skutecznym, praktycznym i interesującym środowisku edukacyjnym.

Jego celem jest poszerzenie wiedzy seniorów na temat bezpieczeństwa w Internecie, wyposażenie ich w niezbędne umiejętności oraz wzmocnienie ich pewności siebie w zakresie bezpiecznego korzystania z technologii cyfrowych. Oprócz praktycznych środków ochrony danych osobowych i prywatności, program szkoleniowy oferuje jasną świadomość powszechnych zagrożeń internetowych i sposobów ich rozpoznawania, porady dotyczące bezpiecznych zachowań w Internecie oraz wgląd w rzeczywiste scenariusze ilustrujące potencjalne zagrożenia i sposoby ich eliminowania. Program składa się z pięciu obszernych kursów trwających po cztery godziny oraz dziesięciu interaktywnych przypadków IMPROVE, które symulują doraźne reakcje na zagrożenia internetowe. Kładzie on duży nacisk na praktyczną naukę poprzez analizę rzeczywistych przykładów zagrożeń związanych z cyberbezpieczeństwem. Każda sesja zawiera treści, szczegółowe ćwiczenia wraz z instrukcjami oraz narzędzia i zasoby niezbędne do przeprowadzenia programu szkoleniowego.

Zasoby te zapewniają nauczycielom przydatne ćwiczenia, materiały i metody, dzięki którym osoby starsze mogą zainteresować się interaktywną nauką i zaangażować się w nią. Nauczyciele, którzy pomyślnie ukończą ten program, będą przygotowani do pomocy osobom starszym w rozwijaniu ich umiejętności cyfrowych i pewności siebie.

1.2.1 Główne cele programu

Podnoszenie świadomości seniorów na temat zagrożeń internetowych
Uczestnicy zdobędą kompleksową wiedzę na temat najczęstszych zagrożeń internetowych, takich jak złośliwe oprogramowanie, phishing, oszustwa, kradzież tożsamości i niebezpieczne strony internetowe. Program uczy uczestników, jak rozpoznawać sygnały ostrzegawcze, i ilustruje potencjalne zagrożenia na podstawie rzeczywistych przykładów.

Rozwój praktycznych umiejętności cyfrowych
Uczestnicy zdobędą kompleksową wiedzę na temat prawidłowego wykonywania typowych czynności w Internecie, takich jak korzystanie z mediów społecznościowych, bankowości internetowej, zakupów i przeglądania stron internetowych. Nacisk kładziony jest na bezpieczne zarządzanie danymi, uwierzytelnianie dwuskładnikowe i silne hasła.

Promowanie bezpiecznego zachowania w Internecie
Program kładzie nacisk na stosowanie najlepszych praktyk w zakresie ochrony prywatności, bezpiecznej komunikacji i etycznego korzystania z technologii cyfrowych. Seniorzy dowiedzą się, jak zarządzać danymi osobowymi, rozpoznawać fałszywe wiadomości i odpowiednio reagować na podejrzane działania.

Wyposażenie trenerów w wiedzę specjalistyczną
Szkolenie nauczycieli i moderatorów jest podstawową częścią programu. Trenerzy zdobędą umiejętności, zasoby i techniki niezbędne do prowadzenia szkoleń z zakresu bezpieczeństwa w Internecie skierowanych do seniorów. Obejmuje to porady dotyczące zarządzania dynamiką grupy, nauczania opartego na scenariuszach oraz interaktywnych technik nauczania.

Ograniczanie wykluczenia cyfrowego
Program ma na celu zmniejszenie izolacji społecznej i technologicznej osób starszych, zwłaszcza tych mieszkających poza obszarami miejskimi, poprzez zwiększenie umiejętności cyfrowych i wiedzy na temat bezpieczeństwa w Internecie. W dzisiejszym cyfrowym świecie uczestnicy będą czuli się bardziej komfortowo, korzystając samodzielnie z urządzeń cyfrowych, co sprzyja większej integracji społecznej.

1.2.2 Oczekiwane wyniki

- Seniorzy zdobędą wiedzę i praktyczne umiejętności niezbędne do bezpiecznego poruszania się w środowisku internetowym.
- Trenerzy będą dobrze przygotowani do przekazywania seniorom interesujących i przydatnych informacji na temat cyberbezpieczeństwa.
- Seniorzy posiadający umiejętności cyfrowe, którzy mogą bezpiecznie korzystać z usług i aktywności online, przyniosą korzyści swoim społecznościom.

Program szkoleniowy łączy teorię z interaktywnymi ćwiczeniami opartymi na scenariuszach, studiami przypadków i zajęciami grupowymi, aby zapewnić, że uczniowie uczą się poprzez praktykę. Każdy moduł zawiera uporządkowane informacje, praktyczne zadania i możliwości dyskusji, co pozwala seniorom natychmiast wykorzystać swoją wiedzę i nabrać pewności siebie w rzeczywistych sytuacjach. Program zawiera również elementy oceny i refleksji, które zapewniają osiągnięcie wyników nauczania, a jednocześnie oferują informacje zwrotne zarówno dla trenerów, jak i uczestników, aby mogli się stale rozwijać.

1.2.3 Analiza przypadków

Przypadki to interaktywne ćwiczenia oparte na scenariuszach, które mają na celu uzupełnienie modułów szkoleniowych Cyber Safe Senior. Scenariusze te są bezpośrednio związane z modułami I-V i przedstawiają rzeczywiste sytuacje online, z którymi seniorzy mogą spotkać się w codziennych interakcjach cyfrowych, takie jak wiadomości phishingowe, oszustwa związane z zakupami online, niebezpieczne korzystanie z publicznych sieci Wi-Fi i oszukańcze inwestycje. Scenariusze, dostarczane za pośrednictwem interaktywnych treści Genially, pozwalają uczestnikom zidentyfikować potencjalne zagrożenia, podejmować świadome decyzje i zrozumieć skutki ryzykownych działań w Internecie. Przypadki zachęcają do praktycznej nauki poprzez odtworzenie rzeczywistych zagrożeń cyfrowych, umożliwiając seniorom nabycie praktycznych umiejętności bezpiecznego korzystania z Internetu.

Przypadki są dostosowane do modułów szkoleniowych zgodnie z ich tematyką i celami nauczania określonymi w programie.

- **Moduł I – Podstawy cyberbezpieczeństwa: ochrona komputera, poczty elektronicznej i danych osobowych:** smishing; dylemat publicznego Wi-Fi.
- **Moduł II – Typowe oszustwa internetowe wymierzone w seniorów:** Oszustwo na wnuczka; Pułapka oszustwa charytatywnego.
- **Moduł III – Bezpieczeństwo bankowości internetowej i zakupów** online**:** Oszustwa związane z zakupami online; Oszustwa phishingowe w wiadomościach e-mail; Krypto-miraż: iluzja natychmiastowego wzbogacenia się; Złote zyski – cena zaufania.
- **Moduł IV – Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych przez seniorów:** Oszustwa typu deepfake; Oszustwa związane z usługami online.
- **Moduł V – Bezpieczna cyfryzacja seniorów:** omówiona przekrojowo w ramach ogólnej treści szkolenia i ćwiczeń.

Dostęp do przypadków:

- Kryptowalutowy miraż: iluzja natychmiastowego wzbogacenia się
- Oszustwa związane z zakupami online
- Pułapka oszustw charytatywnych
- Smishing
- Dylemat publicznego Wi-Fi
- Oszustwa phishingowe za pośrednictwem poczty elektronicznej
- Oszustwo na wnuczka
- Oszustwo związane z usługami online
- Oszustwo typu deepfake
- Złote zyski – cena zaufania: przypadek oszustwa inwestycyjnego

MODUŁ I

Podstawy cyberbezpieczeństwa ochrona komputerów, poczty elektronicznej i danych osobowych

2. Moduł I – Podstawy cyberbezpieczeństwa – ochrona komputerów, poczty elektronicznej i danych osobowych

Moduł „Podstawy cyberbezpieczeństwa" oferuje kompletny przegląd bezpieczeństwa cyfrowego, łącząc wiedzę teoretyczną z praktycznymi zastosowaniami. Uczestnicy uzyskają dogłębną wiedzę na temat podstawowych zasad bezpieczeństwa komputerowego, prywatności poczty elektronicznej i ochrony danych osobowych. Moduł obejmuje ważne podtematy, takie jak bezpieczeństwo komputerowe i zarządzanie pocztą elektroniczną, w ramach których uczestnicy dowiedzą się, jak konserwować system operacyjny i oprogramowanie, korzystać z programów antywirusowych i zapór sieciowych oraz identyfikować potencjalne zagrożenia cybernetyczne. Skupia się również na bezpieczeństwie i zarządzaniu hasłami, ucząc użytkowników, jak tworzyć silne hasła i skutecznie korzystać z menedżerów haseł.

Uczestnicy programu przechodzą praktyczne ćwiczenia z zakresu bezpieczeństwa poczty elektronicznej, podczas których uczą się rozpoznawać próby phishingu, identyfikować podejrzane linki lub pliki oraz monitorować swoje skrzynki pocztowe pod kątem nieautoryzowanych działań, w tym korzystać z uwierzytelniania dwuskładnikowego w celu zwiększenia bezpieczeństwa. Program obejmuje również omówienie sposobów zabezpieczania urządzeń osobistych, takich jak komputery, telefony komórkowe i tablety, w tym taktyk blokowania ekranu, monitorowania zgubionych urządzeń, unikania nieautoryzowanego dostępu fizycznego oraz aktualizowania oprogramowania w celu ochrony przed pojawiającymi się zagrożeniami. Wreszcie, program koncentruje się na zarządzaniu danymi osobowymi i prywatnością w Internecie, ucząc studentów, jak zmieniać ustawienia prywatności w mediach społecznościowych, chronić krytyczne informacje i bezpiecznie korzystać z publicznych sieci Wi-Fi za pomocą VPN.

Łącząc te podtematy, szkolenie zapewnia seniorom nie tylko zrozumienie potencjalnych zagrożeń w środowisku cyfrowym, ale także naukę praktycznych metod ochrony przed nimi. Uczestnicy opuszczą moduł z większą świadomością, pewnością siebie w radzeniu sobie z problemami związanymi z cyberbezpieczeństwem oraz umiejętnością wdrażania nabytych rozwiązań w rzeczywistych sytuacjach.

2.1 Cele nauczania

Głównym celem tego modułu jest wyposażenie uczestników w praktyczną wiedzę i umiejętności niezbędne do skutecznej ochrony komputerów, kont e-mail i danych osobowych przed zagrożeniami w cyberprzestrzeni. Uczestnicy dowiedzą się, jak rozpoznawać potencjalne zagrożenia, minimalizować ryzyko i wdrażać strategie zwiększające bezpieczeństwo cyfrowe zarówno w życiu osobistym, jak i zawodowym.

- Zrozumienie podstawowych zasad cyberbezpieczeństwa, które pomagają zapobiegać atakom i chronić dane przed nieuprawnionym dostępem.
- Rozwinięcie umiejętności tworzenia silnych haseł i bezpiecznego ich przechowywania, zwiększając odporność na naruszenia.
- Rozpoznawanie i unikanie ataków phishingowych, które są jedną z najczęstszych metod oszustw internetowych.
- Skuteczne zabezpieczanie urządzeń osobistych i przechowywanych na nich danych za pomocą narzędzi takich jak szyfrowanie, blokady ekranu i funkcje śledzenia lokalizacji.
- Świadome zarządzanie ustawieniami prywatności na platformach społecznościowych w celu zmniejszenia ryzyka wycieku danych osobowych.
- Zdobycie wiedzy i umiejętności dotyczących bezpiecznego korzystania z publicznych sieci Wi-Fi poprzez stosowanie sieci VPN i innych narzędzi ochronnych.

2.2 Struktura, treść i efekty uczenia się

Po pomyślnym ukończeniu tego modułu uczestnicy zdobędą wiedzę i umiejętności w zakresie następujących obszarów:

- **Wprowadzenie do podstaw bezpieczeństwa komputerowego:** jak aktualizować system operacyjny i oprogramowanie, korzystać z programów antywirusowych i zapór sieciowych, jak rozpoznawać oznaki potencjalnych ataków na komputer i jak zminimalizować ryzyko ich wystąpienia.
- **Tworzenie bezpiecznych haseł i ich przechowywanie:** jak tworzyć silne hasła składające się z unikalnych kombinacji liter, cyfr i symboli, jak korzystać z menedżerów haseł, aby uniknąć przechowywania haseł w niebezpieczny sposób, np. na papierze.
- **Praktyczne scenariusze wykrywania phishingu w wiadomościach e-mail**: analiza przykładowych wiadomości phishingowych i nauka rozpoznawania podejrzanych linków, załączników lub błędów językowych, jak zgłaszać podejrzane wiadomości e-mail do odpowiednich służb.
- **Monitorowanie i zabezpieczanie skrzynki pocztowej przed nieautoryzowanym dostępem:** jak skonfigurować weryfikację dwuetapową, monitorować nietypową aktywność w skrzynce pocztowej i reagować na próby włamania.
- **Ochrona urządzeń osobistych (komputerów, smartfonów, tabletów**): jak zablokować ekran i korzystać z aplikacji umożliwiających lokalizację zgubionych urządzeń, jak chronić urządzenia przed fizycznym dostępem osób nieuprawnionych.
- **Ochrona urządzeń osobistych (komputerów, smartfonów, tabletów):** jak zablokować ekran i korzystać z aplikacji umożliwiających lokalizację zgubionych urządzeń, jak chronić urządzenia przed fizycznym dostępem osób nieuprawnionych.
- **Regularne aktualizacje oprogramowania w celu zwiększenia bezpieczeństwa:** dlaczego regularne aktualizacje są niezbędne do ochrony urządzeń przed nowymi zagrożeniami i jak skonfigurować system do automatycznych aktualizacji.
- **Ochrona prywatności w mediach społecznościowych:** jak dostosować ustawienia prywatności na popularnych platformach społecznościowych, jakie informacje należy zachować w tajemnicy i jak uniknąć udostępniania danych, które mogłyby zostać wykorzystane w niepożądany sposób.
- **Zasady bezpiecznego korzystania z publicznych sieci Wi-Fi:** ryzyko związane z korzystaniem z otwartych sieci Wi-Fi oraz jak korzystać z VPN w celu ochrony danych podczas łączenia się z Internetem w miejscach publicznych.

2.3 Program | Szczegółowy plan sesji

MODUŁ I
Podstawy cyberbezpieczeństwa | Ochrona komputerów, poczty elektronicznej i danych osobowych

1 sesja

Powitanie
Czas trwania *5 min*

Cele

- Stworzenie otwartej i angażującej atmosfery sprzyjającej aktywnemu uczestnictwu.

Treść/metoda

- Powitanie uczestników i krótkie przedstawienie trenera.
- Przedstawienie programu szkolenia i zasad pracy.
- Zachęcenie uczestników do przedstawienia się (imię i nazwisko oraz jedno słowo związane z cyberzagrożeniami).

Materiały
Brak dodatkowych materiałów.

Uwagi
Pomocne może być przedstawienie celu warsztatów prostym językiem.

2 sesja

Ćwiczenie integracyjne: „Podstawy cyberbezpieczeństwa”
Czas trwania *15 min*

Cele

- Nauka i zrozumienie podstawowych pojęć związanych z cyberbezpieczeństwem.
- Wzmocnienie wiedzy na temat cyberbezpieczeństwa.

Treść/metoda

- Przeprowadzenie ćwiczenia polegającego na dopasowaniu pojęć do definicji.
- Uczestnicy otrzymują arkusz roboczy (załącznik 1). Zadaniem uczestników jest prawidłowe dopasowanie każdego pojęcia do odpowiadającej mu definicji. Ćwiczenie ma charakter indywidualny lub zespołowy, w zależności od decyzji prowadzącego. Po wykonaniu zadania trener moderuje krótką dyskusję, podczas której omawiane są odpowiedzi, wyjaśniane są wszelkie niejasności i poruszane są kwestie związane z tematem ćwiczenia. Zachęcanie uczestników do przedstawienia się (imię i jedno słowo związane z cyberzagrożeniami).

Materiały

- Arkusz roboczy, ćwiczenie integracyjne: „Podstawy cyberbezpieczeństwa” (załącznik 1)

Uwagi

Zadanie to wprowadza temat i pozwala ocenić początkowy poziom wiedzy uczestników.

3 sesja

Wykład 1: Bezpieczeństwo komputerowe i poczta elektroniczna
Czas trwania *20 min*

Cele

- Zrozumienie znaczenia aktualizowania systemu i oprogramowania.
- Rozpoznawanie różnych rodzajów zagrożeń cybernetycznych, w tym złośliwego oprogramowania, oprogramowania szpiegującego i oprogramowania ransomware.
- Zrozumienie roli oprogramowania antywirusowego w zapewnianiu bezpieczeństwa.
- Zdobycie wiedzy i umiejętności niezbędnych do bezpiecznego korzystania z publicznych sieci Wi-Fi przy użyciu sieci VPN i innych narzędzi zabezpieczających.

Treść/metoda

- Wykład wyjaśniający podstawowe pojęcia: dlaczego regularne aktualizacje systemu są tak ważne, w jaki sposób złośliwe oprogramowanie przenika do systemów, jaka jest rola oprogramowania antywirusowego i jak rozpoznać bezpieczną sieć Wi-Fi.
- Wykorzystanie przykładów z życia wziętych (np. znanych ataków ransomware) w celu zilustrowania zagrożeń związanych z przestarzałymi systemami i niezabezpieczonymi urządzeniami.
- Podkreślenie najlepszych praktyk, takich jak włączenie automatycznych aktualizacji i unikanie podejrzanych plików do pobrania. Aby zrealizować wykład, trener ma do dyspozycji propozycje tematów zawarte w załączniku 2.

Materiały

- Propozycja tematów do omówienia (załącznik 2)

Uwagi

Warto zachęcić uczestników do aktywnego udziału w wykładzie, umożliwiając im zadawanie pytań.

Ćwiczenie 1 „Quiz: prawda/fałsz”
Czas trwania *20 min*

Cele

- Utrwalenie wiedzy zdobytej podczas wykładu, rozwijanie świadomości zagrożeń.

Treść/metoda

- Kurs obejmuje ćwiczenie w formie quizu „Prawda czy fałsz?”, przeprowadzane na podstawie arkusza roboczego (załącznik 3), który uczestnicy otrzymują od prowadzącego.

- Uczestnicy mają 5 minut na samodzielne zaznaczenie odpowiedzi. Po zakończeniu tego etapu trener moderuje krótką dyskusję, podczas której omawiane są z grupą prawidłowe odpowiedzi, wyjaśniane są ważne kwestie i korygowane są wszelkie nieporozumienia. Na koniec trener podsumowuje kluczowe treści omówione w quizie, utrwalając zrozumienie i konsolidując dobre praktyki związane z bezpieczeństwem cyfrowym.

Materiały

- Arkusz roboczy Quiz: Prawda/Fałsz (załącznik 3)

Uwagi

Podsumuj kluczowe punkty po quizie, aby utrwalić zrozumienie podstawowych praktyk bezpieczeństwa przez uczestników.

Przerwa | Czas trwania *5 minut*

- **Daj uczestnikom czas na odpoczynek i refleksję.**
- **Krótka przerwa na odświeżenie umysłu.**
- **Zachęć uczestników do rozciągnięcia się lub napicia się czegoś, aby nabrać energii przed kolejnym wykładem.**

4 sesja

Wykład 2: Praktyczne ćwiczenia związane z bezpieczeństwem poczty elektronicznej

Czas trwania *30 min*

Cele

- Poznanie najlepszych praktyk dotyczących tworzenia silnych, bezpiecznych haseł (np. używanie wielkich i małych liter, znaków specjalnych i cyfr).
- Zrozumienie zagrożeń związanych z nieprawidłowym przechowywaniem haseł i poznanie menedżerów haseł.

Treść/metoda

- Wyjaśnienie „zasady trzech elementów” (długość, złożoność, unikalność) tworzenia silnych haseł. Zademonstrowanie działania menedżerów haseł i omówienie ich zalet (np. zwiększone bezpieczeństwo, wygoda). Zwrócenie uwagi na typowe błędy, takie jak ponowne używanie haseł lub przechowywanie ich w niezabezpieczonych plikach.

Materiały

- Propozycja tematów do omówienia (załącznik 4)

Uwagi

Podaj praktyczne wskazówki, z którymi uczniowie mogą się utożsamić, np. tworzenie hasła na podstawie łatwej do zapamiętania, ale unikalnej frazy.

Ćwiczenie 2: Tworzenie silnych haseł

Czas trwania *20 min*

Cele

- Ćwicz tworzenie silnych, unikalnych haseł zgodnie z omówionymi wytycznymi.

Treść/metoda

- Ćwiczenie przeprowadza się w dwóch etapach – najpierw indywidualnie, a następnie w parach. Do ćwiczenia przygotowano arkusz roboczy (załącznik 5).
- Uczestnicy samodzielnie tworzą co najmniej trzy silne hasła zgodnie z zasadami bezpieczeństwa, zapisując je na kartach. Następnie pokazują je partnerowi z pary, który ocenia ich długość, złożoność i unikalność, udzielając informacji zwrotnej i ewentualnych sugestii dotyczących ulepszeń. Na koniec trener omawia cechy bezpiecznego hasła i inicjuje dyskusję z całą grupą, umożliwiając wymianę refleksji i dobrych praktyk.

Materiały

- Arkusz roboczy Tworzenie silnych haseł (załącznik 5)

Uwagi

Warto zachęcić uczestników, aby zwrócili uwagę na to, czy hasła, których obecnie używają, są bezpieczne zgodnie z instrukcjami instruktora.

Przerwa | Czas trwania *5 min*

- **Zapewnij czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**
- **Krótka przerwa na odświeżenie się i relaks.**

5 sesja

Wykład 3: Zabezpieczanie urządzeń osobistych i informacji

Czas trwania *30 min*

Cele

- Zdobycie wiedzy na temat rozpoznawania wiadomości phishingowych.
- Zrozumienie, jak skonfigurować podstawowe ustawienia zabezpieczeń poczty elektronicznej.

Treść/metoda

- Wyjaśnienie charakterystycznych oznak phishingu, takich jak błędy ortograficzne, nieznane adresy nadawców i pilne wiadomości. Pokazanie, jak dostosować ustawienia zabezpieczeń poczty elektronicznej na platformach takich jak Gmail i Outlook. Pokazanie przykładów wiadomości phishingowych i omówienie sposobów rozpoznawania sygnałów ostrzegawczych.

Materiały

Nie są potrzebne żadne dodatkowe materiały.

Uwagi
Przedstawienie prawdziwych przypadków phishingu z popularnych serwisów (np. PayPal, Amazon) w celu uatrakcyjnienia treści.

Ćwiczenie 3: Analiza wiadomości e-mailowych dotyczących phishingu

Czas trwania *20 min*

Cele

- Praktyczna analiza wiadomości e-mail – wykrywanie nieprawidłowości.

Treść/metoda

- Trener dysponuje zestawem szablonów wiadomości e-mail (załącznik 6), które przed rozdaniem uczestnikom należy uzupełnić o szczegóły, takie jak przykładowe linki, nazwy znanych firm (np. banków, firm kurierskich lub platform handlowych).
- Ćwiczenie przeprowadza się w parach lub małych grupach. Uczestnicy analizują przygotowane wiadomości e-mail z arkusza roboczego (załącznik 6), identyfikując i zaznaczając podejrzane elementy. Po zakończeniu analizy odbywa się wspólna dyskusja moderowana przez prowadzącego.

  Sugerowane pytania do dyskusji:
  - Jakie sygnały ostrzegawcze można znaleźć w tej wiadomości e-mail?
  - Jak można się chronić przed takim atakiem?
  - Co należy zrobić, jeśli otrzymasz podejrzaną wiadomość e-mail tego typu?
  - Przygotuj się do omówienia odpowiedzi z grupą.

Materiały

- Arkusz roboczy, Analiza wiadomości e-mail typu phishing (załącznik 6)

Uwagi
Podsumowanie wyników analizy grupowej, podkreślające kluczowe różnice między prawdziwymi a fałszywymi wiadomościami e-mail.

Przerwa

Czas trwania 5 min

- **Czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**
- **Krótka przerwa na odświeżenie się i relaks.**

6 sesja

Wykład 4: Zarządzanie danymi osobowymi i prywatnością w Internecie
Czas trwania *30 min*

Cele

- Przekazywanie informacji na temat polityki prywatności, ustawień prywatności, blokad i aktualizacji. Przekazywanie informacji na temat podstawowych ustawień zabezpieczeń służących ochronie urządzeń (np. włączanie blokad ekranu i automatycznych aktualizacji).
- Zrozumienie, jak skutecznie zarządzać ustawieniami prywatności w Internecie.

Treść/metoda

- Omówienie sposobów ochrony danych w mediach społecznościowych (Instagram, Facebook), ustawień prywatności w smartfonach oraz ograniczeń dotyczących udostępniania aplikacji.
- Trener omawia kluczowe ustawienia zabezpieczeń w smartfonach i komputerach, takie jak blokady ekranu, szyfrowanie danych, zarządzanie aplikacjami i ustawienia uprawnień w systemach Android i iOS.
- Omów zarządzanie prywatnością w Internecie – jak skonfigurować ustawienia prywatności na platformach społecznościowych, kontrolować, kto może wyświetlać posty, dane osobowe oraz które aplikacje mają dostęp do Twoich danych.
- Omów zasady sprawdzania bezpieczeństwa sieci Wi-Fi – jak rozpoznać niezabezpieczone połączenia, dlaczego należy unikać niezabezpieczonych sieci publicznych i jak zwiększyć bezpieczeństwo domowej sieci internetowej.
- Podkreśl znaczenie regularnego sprawdzania ustawień prywatności – znaczenie okresowego sprawdzania i aktualizowania ustawień prywatności w celu dostosowania się do zmieniających się potrzeb i nowych zagrożeń internetowych.

Materiały

Nie są potrzebne żadne dodatkowe materiały.

Uwagi

Skoncentruj się na praktycznych, łatwych do wdrożenia krokach mających na celu zwiększenie bezpieczeństwa i prywatności urządzeń.

Ćwiczenie 4: Bezpieczna konfiguracja urządzenia
Czas trwania *20 min*

Cele

- Zastosowanie wiedzy poprzez konfigurację ustawień bezpieczeństwa na urządzeniach osobistych.

Treść/metoda

- Uczestnicy ćwiczą konfigurację blokady ekranu, włączanie weryfikacji dwuetapowej i dostosowywanie ustawień prywatności. Trener zapewnia indywidualne wsparcie w razie potrzeby.

Materiały

- Smartfony i/lub komputery.

Uwagi

Zachęcaj uczestników do rozwiązywania problemów i zadawania pytań podczas konfigurowania urządzeń.

7 sesja

Dyskusja
Czas trwania *10 min*

Cele

- Zastanów się nad najważniejszymi wnioskami.
- Zachęć uczestników do podzielenia się najcenniejszymi wnioskami i pozostałymi pytaniami.

Treść/metoda

- Moderowana dyskusja, podczas której uczestnicy dzielą się swoimi spostrzeżeniami, doświadczeniami i pytaniami wymagającymi wyjaśnienia. Trener podsumowuje kluczowe punkty i odpowiada na pytania.

Materiały

Nie są potrzebne żadne dodatkowe materiały.

Uwagi

Zachęć uczestników do powiązania poznanych pojęć z ich codziennymi zachowaniami w Internecie.

Podsumowanie
Czas trwania *5 min*

Cele

- Podsumuj kluczowe punkty programu i zapewnij materiały do dalszej nauki.
- Podziękuj uczestnikom i zakończ sesję.

Treść/metoda

- Podsumowanie kluczowych wniosków z szkolenia.
- Udostępnienie dodatkowych zasobów (np. stron internetowych poświęconych cyberbezpieczeństwu, artykułów).
- Podziękowanie uczestnikom za zaangażowanie i zachęcenie ich do dalszego doskonalenia praktyk w zakresie cyberbezpieczeństwa.

Materiały

- Zalecenia dotyczące dalszej lektury i nauki dla uczestników (załącznik 7)
- Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem

Uwagi

Na koniec warto przeprowadzić krótką ankietę ewaluacyjną.

2.4 Dodatkowe informacje

2.4.1 Samoorefleksja trenerów

- Czy w jasny i skuteczny sposób przekazałem uczestnikom znaczenie bezpieczeństwa w Internecie i świadomego korzystania z mediów społecznościowych?
- Czy wykorzystałem praktyczne przykłady, które pomogły lepiej zrozumieć zagrożenia cyfrowe?
- Czy upewniłem się, że uczestnicy zrozumieli techniczne aspekty ustawień prywatności i rozpoznawania oszustw?
- Czy upewniłem się, że uczestnicy zrozumieli techniczne aspekty ustawień prywatności i byli w stanie rozpoznać oszustwa, takie jak phishing?
- Czy dostosowałem przekazywane informacje do poziomu zaawansowania uczestników?
- W jaki sposób zaangażowałem uczestników podczas zajęć i dyskusji?
- Czy zachęcałem do aktywnego udziału, dzielenia się doświadczeniami i zadawania pytań?
- Czy wykorzystane materiały i zasoby (np. prezentacje, quizy, ćwiczenia praktyczne) były pomocne i odpowiednie dla uczestników?
- Czy przygotowane materiały były jasne i łatwe do zrozumienia?

2.4.2 Ocena programu przez trenerów

- Czy treść szkolenia była dostosowana do potrzeb seniorów i odpowiednio dostosowana do ich poziomu wiedzy i doświadczenia?
- Czy uczestnicy mieli możliwość zrozumienia podstawowych zasad cyberbezpieczeństwa i prywatności w Internecie?
- Czy działania takie jak quizy, ćwiczenia praktyczne i analiza przykładów phishingu wspierały proces uczenia się uczestników?
- Czy dyskusje pozwoliły na pogłębienie wiedzy i zachęciły do refleksji na temat bezpieczeństwa cyfrowego?
- Czy osiągnięte wyniki (np. zrozumienie zagrożeń cyfrowych, umiejętność konfiguracji ustawień zabezpieczeń) są zgodne z zamierzonymi celami edukacyjnymi modułu?
- Czy uczestnicy opanowali kluczowe umiejętności, takie jak tworzenie silnych haseł, rozpoznawanie oszustw i zarządzanie prywatnością w Internecie?

2.4.3 Materiały, dodatkowe zasoby

Załącznik 1 | Arkusz ćwiczeń Ćwiczenie na przełamanie lodów: „Podstawy cyberbezpieczeństwa”

Dopasuj pojęcie do prawidłowej definicji:

Phishing	**nieuczciwa metoda podszywania się pod zaufane podmioty w celu kradzieży poufnych danych.**
Oprogramowanie ransomware	**złośliwe oprogramowanie, które szyfruje dane i żąda okupu za ich odblokowanie.**
Uwierzytelnianie dwuskładnikowe (2FA)	**dodatkowa warstwa zabezpieczeń wymagająca drugiego czynnika uwierzytelniającego.**
Hasła i Menedżerowie haseł	**Strategie zarządzania silnymi i unikalnymi hasłami dla różnych usług.**
Zapora	**system bezpieczeństwa chroniący przed nieautoryzowanym dostępem do sieci.**
Szyfrowanie danych	**metoda ochrony danych przed nieautoryzowanym dostępem poprzez przekształcenie ich w nieczytelny kod.**
VPN (wirtualna sieć prywatna)	**technologia zapewniająca bezpieczne i prywatne połączenia internetowe.**
Bezpieczna poczta elektroniczna	**praktyki służące ochronie wiadomości e-mail przed atakami, takie jak filtrowanie spamu i szyfrowanie.**
SOC (Centrum Operacji Bezpieczeństwa)	**centrum operacyjne odpowiedzialne za monitorowanie zagrożeń cyberbezpieczeństwa i reagowanie na nie.**

Załącznik 1 | Arkusz ćwiczeń Ćwiczenie na przełamanie lodów: „Podstawy cyberbezpieczeństwa”

Prawidłowe odpowiedzi

---

1. **Phishing** – nieuczciwa metoda podszywania się pod zaufane podmioty w celu kradzieży poufnych danych.
2. **Oprogramowanie ransomware** – złośliwe oprogramowanie, które szyfruje dane i żąda okupu za ich odblokowanie.
3. **Uwierzytelnianie dwuskładnikowe (2FA)** – dodatkowa warstwa zabezpieczeń wymagająca drugiego czynnika uwierzytelniającego.
4. **Hasła i menedżery haseł** – strategie zarządzania silnymi i unikalnymi hasłami dla różnych usług.
5. **Zapora sieciowa** – system bezpieczeństwa chroniący przed nieautoryzowanym dostępem do sieci.
6. **Szyfrowanie danych** – metoda ochrony danych przed nieautoryzowanym dostępem poprzez przekształcenie ich w nieczytelny kod.
7. **Złośliwe oprogramowanie** – oprogramowanie zaprojektowane w celu wyrządzenia szkody użytkownikom lub systemom komputerowym.
8. **VPN (wirtualna sieć prywatna)** – technologia zapewniająca bezpieczne i prywatne połączenia internetowe.
9. **Bezpieczna poczta elektroniczna** – praktyki służące ochronie wiadomości e-mail przed atakami, takie jak filtrowanie spamu i szyfrowanie.
10. **SOC (centrum operacji bezpieczeństwa)** – centrum operacyjne odpowiedzialne za monitorowanie zagrożeń cyberbezpieczeństwa i reagowanie na nie.

Załącznik 2 | Sugerowane tematy do omówienia Wykład 1 | Bezpieczeństwo komputerów i poczty elektronicznej

- Znaczenie regularnych aktualizacji systemów operacyjnych i aplikacji.
- Ryzyko związane z przestarzałymi systemami i niezabezpieczonymi urządzeniami.
- Rodzaje złośliwego oprogramowania: wirusy, konie trojańskie, oprogramowanie ransomware i sposób ich działania.
- Mechanizmy umożliwiające złośliwemu oprogramowaniu infiltrację systemów.
- Rola oprogramowania antywirusowego w ochronie przed cyberzagrożeniami.
- Wykorzystanie zapór sieciowych do ochrony przed atakami.
- Praktyki zarządzania hasłami, w tym korzystanie z menedżerów haseł.
- Zasady pozwalające uniknąć niebezpiecznych załączników i podejrzanych linków w wiadomościach e-mail.
- Znaczenie szyfrowania danych w ochronie prywatności i bezpieczeństwa.
- Automatyczne aktualizacje jako najlepsza praktyka zapewniająca bezpieczeństwo.
- Sieci VPN i ich rola w ochronie prywatności w Internecie.
- Dlaczego nie każda bezpłatna sieć Wi-Fi jest bezpieczna?
- Podstawowa ochrona poczty elektronicznej przed phishingiem i spamem.
- Najlepsze praktyki dotyczące tworzenia silnych haseł i ich wpływ na bezpieczeństwo.
- Bezpieczeństwo urządzeń mobilnych i aplikacji.
- Znaczenie edukacji i świadomości użytkowników w zapobieganiu cyberatakom.

Załącznik 3 | Arkusz ćwiczeń Quiz: Prawda/Fałsz

Zaznacz, które stwierdzenia są prawdziwe, a które fałszywe.

- Regularne aktualizacje systemu operacyjnego i aplikacji są konieczne tylko w przypadku nowych urządzeń. **Prawda/Fałsz**
- Złośliwe oprogramowanie, takie jak wirusy lub trojany, może przenikać do systemów poprzez przestarzałe oprogramowanie i luki w zabezpieczeniach. **Prawda/Fałsz**
- Oprogramowanie antywirusowe nie jest konieczne, jeśli system jest regularnie aktualizowany. **Prawda/Fałsz**
- Zapora sieciowa służy wyłącznie do ochrony przed fizycznymi atakami na urządzenia. **Prawda/Fałsz**
- Zarządzanie hasłami i korzystanie z menedżerów haseł ma kluczowe znaczenie dla utrzymania silnych, unikalnych haseł do różnych usług. **Prawda/Fałsz**
- Unikanie podejrzanych załączników w wiadomościach e-mail nie jest ważne, jeśli zainstalowano oprogramowanie antywirusowe. **Prawda/Fałsz**
- Szyfrowanie danych pomaga chronić prywatność i bezpieczeństwo przed nieautoryzowanym dostępem. **Prawda/Fałsz**
- Automatyczne aktualizacje są opcjonalne, ponieważ ręczna aktualizacja systemu zawsze wystarcza do zapewnienia bezpieczeństwa. **Prawda/Fałsz**
- VPN (wirtualna sieć prywatna) umożliwia bezpieczne połączenie z Internetem, ukrywając naszą aktywność online. **Prawda/Fałsz**
- Phishing to technika ataku polegająca na kradzieży haseł za pomocą pozornie wiarygodnych wiadomości e-mail. **Prawda/Fałsz**
- Silne hasło powinno składać się wyłącznie z liter i być łatwe do zapamiętania, aby nie było trudne w użyciu. Urządzenia mobilne wymagają mniej środków bezpieczeństwa niż komputery stacjonarne, ponieważ są mniej podatne na ataki. **Prawda/Fałsz**
- Urządzenia mobilne wymagają mniej środków bezpieczeństwa niż komputery stacjonarne, ponieważ są mniej podatne na ataki. **Prawda/Fałsz**
- Wiedza użytkowników na temat zagrożeń internetowych ma zasadnicze znaczenie dla zapobiegania cyberatakom. **Prawda/Fałsz**
- Oprogramowanie ransomware to oprogramowanie, które blokuje dostęp do systemu lub plików i żąda okupu za ich odblokowanie. **Prawda/Fałsz**
- Nieaktualny system operacyjny jest bezpieczny, ponieważ starsze wersje oprogramowania rzadko są celem ataków. **Prawda/Fałsz**

Załącznik 3 | Arkusz ćwiczeń Quiz: Prawda/Fałsz
Prawidłowe odpowiedzi

1. Regularne aktualizacje systemu operacyjnego i aplikacji są konieczne tylko w przypadku nowych urządzeń. - Fałsz
2. Złośliwe oprogramowanie, takie jak wirusy lub trojany, może przeniknąć do systemów poprzez nieaktualne oprogramowanie i luki w zabezpieczeniach. - Prawda
3. Oprogramowanie antywirusowe nie jest konieczne, jeśli system jest regularnie aktualizowany. - Fałsz
4. Zapora sieciowa służy wyłącznie do ochrony przed fizycznymi atakami na urządzenia. - Fałsz
5. Zarządzanie hasłami i korzystanie z menedżerów haseł ma kluczowe znaczenie dla utrzymania silnych, unikalnych haseł do różnych usług. - Prawda
6. Unikanie podejrzanych załączników w wiadomościach e-mail nie jest ważne, jeśli zainstalowano oprogramowanie antywirusowe. - Fałsz
7. Szyfrowanie danych pomaga chronić prywatność i bezpieczeństwo przed nieautoryzowanym dostępem. - Prawda
8. Automatyczne aktualizacje są opcjonalne, ponieważ ręczna aktualizacja systemu zawsze wystarcza do zapewnienia bezpieczeństwa. - Fałsz
9. VPN (wirtualna sieć prywatna) umożliwia bezpieczne połączenie z Internetem, ukrywając naszą aktywność online. - Prawda
10. Phishing to technika ataku polegająca na kradzieży haseł za pomocą pozornie wiarygodnych wiadomości e-mail. - Prawda
11. Silne hasło powinno składać się wyłącznie z liter i być łatwe do zapamiętania, aby nie było trudne w użyciu. - Fałsz
12. Urządzenia mobilne wymagają mniej środków bezpieczeństwa niż komputery stacjonarne, ponieważ są mniej podatne na ataki. - Fałsz
13. Wiedza użytkowników na temat zagrożeń internetowych ma zasadnicze znaczenie dla zapobiegania cyberatakom. - Prawda
14. Oprogramowanie ransomware to oprogramowanie, które blokuje dostęp do systemu lub plików i żąda okupu za ich odblokowanie. - Fałsz
15. Nieaktualny system operacyjny jest bezpieczny, ponieważ starsze wersje oprogramowania rzadko są celem ataków. - Fałsz

Załącznik 4 | Sugerowane tematy do wykładu 2 „Praktyczne ćwiczenia dotyczące bezpieczeństwa poczty elektronicznej”

- Tworzenie bezpiecznych haseł – zasady tworzenia silnych haseł, które są trudne do złamania, w tym używanie różnych rodzajów znaków (wielkie litery, małe litery, cyfry, znaki specjalne).
- Zarządzanie hasłami – jak unikać przechowywania haseł w niebezpiecznych miejscach, takich jak notatki na papierze, i jak korzystać z menedżerów haseł w celu bezpiecznego przechowywania.
- Zasada trzech elementów – wyjaśnienie, dlaczego hasło powinno mieć odpowiednią długość, złożoność i unikalność, aby zapewnić wysokie bezpieczeństwo.
- Rola menedżerów haseł – omówienie działania menedżerów haseł i korzyści, jakie oferują, takich jak bezpieczeństwo i wygoda w zarządzaniu wieloma hasłami.
- Typowe błędy w zarządzaniu hasłami – jak niebezpieczne jest ponowne używanie tych samych haseł w różnych usługach lub przechowywanie ich w niezabezpieczonych plikach.
- Praktyki dotyczące bezpieczeństwa poczty elektronicznej – jak unikać podejrzanych linków i załączników oraz jak korzystać z dodatkowych metod ochrony, takich jak szyfrowanie.

Załącznik 5 | Arkusz roboczy „Tworzenie silnych haseł”
Twórz silne i bezpieczne hasła w oparciu o następujące zasady:

· Odpowiednia długość (minimum 12 znaków),
· Złożoność (wielkie i małe litery, cyfry, znaki specjalne),
· Wyjątkowość (brak oczywistych wzorców, takich jak data urodzenia).

Praca indywidualna: Zapisz co najmniej trzy różne hasła:

Dodatek 5 | Arkusz roboczy | Tworzenie silnych haseł

Pracujcie w parach:

· Po zakończeniu pracy indywidualnej połączcie się w pary z innym uczestnikiem.
· Pokażcie sobie nawzajem swoje hasła.
· Poproście go, aby zaznaczył (np. znakiem plus), czy hasła spełniają wszystkie kryteria.
· Trener może przedstawić uwagi i sugestie dotyczące ewentualnych ulepszeń.

Hasło 1

Długość	**Uwagi**
Złożoność	
Uniwersalność	

Hasło 2

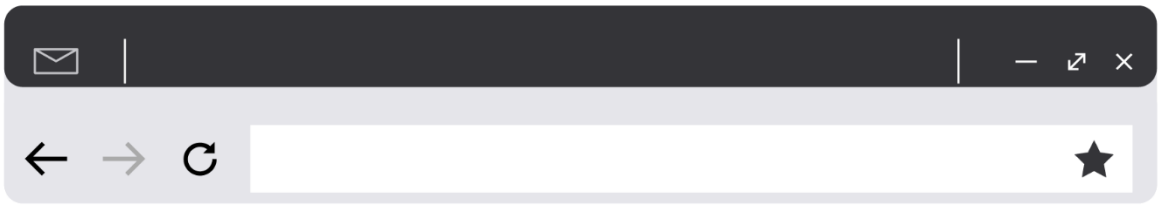
Długość	**Uwagi**
Złożoność	
Wszechstronność	

Hasło 3

Długość	**Uwagi**
Złożoność	
Wszechstronność	

Dodatek 6 | Arkusz roboczy | Analiza wiadomości phishingowych

Przeczytaj uważnie poniższe wiadomości e-mail. Zidentyfikuj elementy wskazujące, że są to wiadomości phishingowe.



Subject : **Pilne! Twoje konto zostało zablokowane!**

Szanowny użytkowniku

W związku z podejrzaną aktywnością na Twoim koncie, zostało ono tymczasowo zablokowane w celu ochrony Twoich danych osobowych. Aby uniknąć trwałego zablokowania, prosimy o natychmiastowe zweryfikowanie konta.

Kliknij tutaj, aby zweryfikować swoje dane i odblokować konto: [link phishingowy]

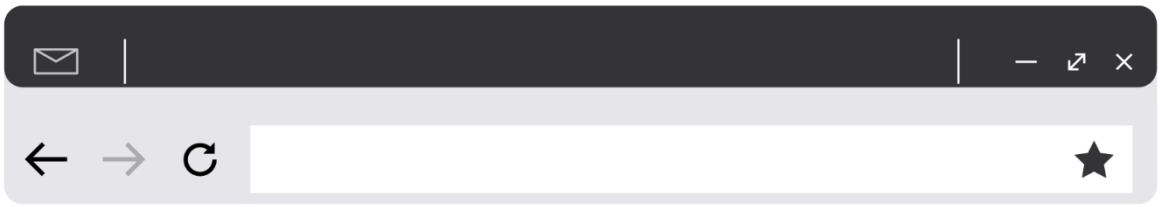
Jeśli nie wykonasz tej czynności w ciągu 24 godzin, Twoje konto zostanie trwale zablokowane. Prosimy o podjęcie szybkich działań, aby uniknąć niedogodności.

W razie jakichkolwiek pytań prosimy o kontakt z naszym zespołem pomocy technicznej.

Z poważaniem
Zespół ds. bezpieczeństwa
[Fałszywa firma]

Załącznik 6 | Arkusz roboczy | Analiza wiadomości phishingowych

Przeczytaj uważnie poniższe wiadomości e-mail. Zidentyfikuj elementy wskazujące, że są to wiadomości phishingowe.



Subject : **Zaktualizuj swoje dane! Twoje konto wymaga weryfikacji**

Witaj [Imię],

Twoje konto w [Fałszywa firma] wymaga natychmiastowej aktualizacji danych osobowych. W związku z rutynową kontrolą bezpieczeństwa musimy upewnić się, że Twoje dane są aktualne, aby zapewnić Ci pełny dostęp do naszych usług. Aby zaktualizować swoje dane, kliknij poniższy link i zaloguj się na swoje konto:

[Link phishingowy – kliknij tutaj, aby zaktualizować swoje dane]

Po kliknięciu linku zostaniesz przekierowany na stronę, na której będziesz musiał podać swoje dane logowania, numer karty kredytowej i inne poufne informacje.

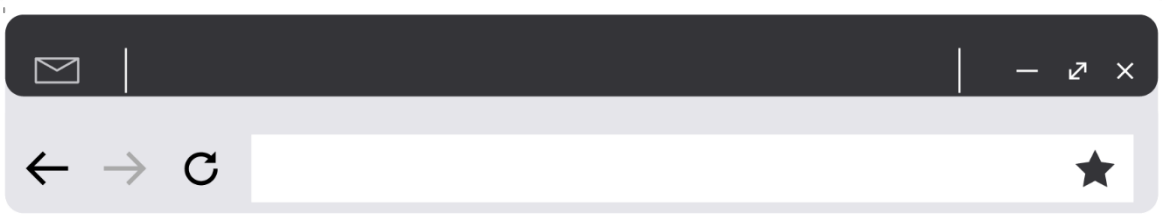
OSTRZEŻENIE: Jeśli nie zaktualizujesz swoich danych w ciągu 48 godzin, Twoje konto zostanie trwale zawieszone.

Dziękujemy za zrozumienie i współpracę.

Z poważaniem
[Fałszywa firma]
Zespół obsługi klienta

Załącznik 6 | Arkusz roboczy | Analiza wiadomości phishingowych

Przeczytaj uważnie poniższe wiadomości e-mail. Zidentyfikuj elementy wskazujące, że są to wiadomości phishingowe.



Subject : **Potwierdzenie wysyłki – paczka nie mogła zostać dostarczona**

Dzień dobry,

Twoja paczka nie mogła zostać dostarczona z powodu nieprawidłowych danych adresowych. Prosimy o natychmiastowe sprawdzenie danych, abyśmy mogli ponownie podjąć próbę dostawy.

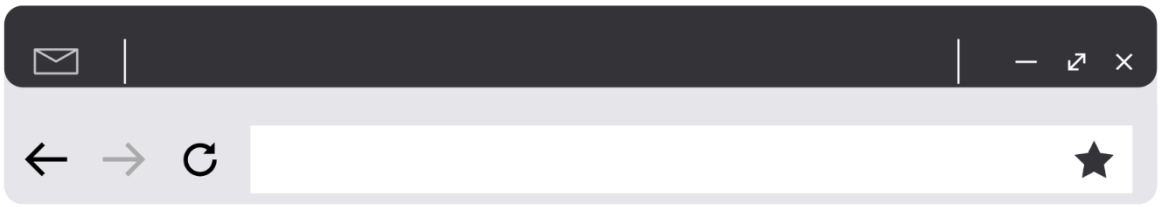
Kliknij tutaj, aby zaktualizować dane dostawy: [link phishingowy]

Jeśli nie potwierdzisz adresu w ciągu 24 godzin, paczka zostanie zwrócona do nadawcy, a Ty poniesiesz dodatkowe koszty.

Dziękujemy za szybką odpowiedź.
Zespół wysyłkowy
[Fałszywa firma kurierska]

Załącznik 6 | Arkusz roboczy | Analiza wiadomości phishingowych

Przeczytaj uważnie poniższe wiadomości e-mail. Zidentyfikuj elementy wskazujące, że są to wiadomości phishingowe.



Subject : **Otrzymałeś e-kartę podarunkową! Odbierz ją teraz!**

Gratulacje!

Zostałeś wybrany jako zwycięzca naszej losowej promocji. Otrzymujesz e-kartę podarunkową o wartości 500 PLN do wykorzystania w [popularnej sieci handlowej].

Aby odebrać nagrodę, kliknij poniższy link i potwierdź swoje dane:
[link phishingowy – odbierz kartę e-podarunkową]

Oferta ważna tylko przez 12 godzin.
Nie przegap tej okazji!

Miłego dnia!
Dział promocji
[Fałszywa firma lub sieć detaliczna]

Załącznik 7 | Zalecenia dotyczące dalszej lektury i nauki dla uczestników

Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem:

1) **ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa)**
   Strona internetowa: https://www.enisa.europa.eu/
   ENISA to agencja UE zajmująca się cyberbezpieczeństwem, która publikuje raporty, przewodniki i ostrzeżenia dotyczące cyberzagrożeń.

2) **CERT-EU (Zespół reagowania na incydenty komputerowe dla instytucji UE)**
   Strona internetowa: https://cert.europa.eu/
   Organizacja monitoruje cyberzagrożenia i reaguje na cyberataki na instytucje europejskie.

3) **EC3 – Centrum ds. Cyberprzestępczości Europolu**
   Strona internetowa: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
   Europol udostępnia informacje na temat cyberprzestępczości i bezpieczeństwa danych.

4) **NCSC UK (Krajowe Centrum Cyberbezpieczeństwa)**
   Strona internetowa: https://www.ncsc.gov.uk/
   Portal rządowy Wielkiej Brytanii poświęcony cyberbezpieczeństwu, zawierający przewodniki, alerty i kursy online dla obywateli, przedsiębiorstw i instytucji publicznych.

2.5 Moduł I – Test wstępny/końcowy

1. Które z poniższych stwierdzeń najlepiej opisuje „phishing”?

A) Instalowanie aktualizacji w celu poprawy wydajności komputera
B) Metoda nakłaniania ludzi do ujawnienia danych osobowych za pomocą fałszywych wiadomości e-mail
C) Rodzaj programu antywirusowego
D) Proces szyfrowania danych

2. Dlaczego regularne aktualizacje oprogramowania są ważne?

A) Spowalniają działanie komputera
B) Zmieniają konstrukcję komputera
C) Naprawiają luki w zabezpieczeniach i chronią przed nowymi zagrożeniami
D) Usuwają oprogramowanie antywirusowe

3. Jaka jest główna funkcja zapory sieciowej?

A) Przyspieszenie połączenia internetowego
B) Ochrona przed nieautoryzowanym dostępem do sieci
C) Bezpieczne przechowywanie haseł
D) Automatyczne usuwanie wiadomości spamowych

4. Które z poniższych haseł jest najbezpieczniejsze?

A) hasło123
B) 12345678
C) MójPiesJestSłodki
D) M@rK_82!x

5. Co należy zrobić, jeśli otrzymasz wiadomość e-mail od nieznanego nadawcy z prośbą o podanie danych osobowych?

A) Natychmiast odpowiedzieć, podając swoje dane
B) Kliknąć link, aby sprawdzić, o co chodzi
C) Usunąć wiadomość lub zgłosić ją jako phishing
D) Przekaż go znajomym, aby ich ostrzec

6. Do czego służy „uwierzytelnianie dwuskładnikowe (2FA)”?

A) Pozwala na użycie dwóch haseł jednocześnie
B) Dodaje dodatkową warstwę bezpieczeństwa, wymagając dwóch form weryfikacji
C) Automatycznie szyfruje wiadomości e-mail
D) Przechowuje dane logowania

7. Które z poniższych stwierdzeń dotyczących publicznych sieci Wi-Fi jest PRAWDZIWE?

A) Są one zawsze bezpieczne, jeśli połączenie jest bezpłatne
B) Podczas korzystania z publicznej sieci Wi-Fi należy unikać wprowadzania poufnych danych
C) Można z nich bezpiecznie korzystać bez hasła
D) Automatycznie szyfrują dane

8. Jaki jest cel sieci VPN (wirtualnej sieci prywatnej)?

A) Zwiększenie prędkości Internetu
B) Blokowanie wyskakujących reklam
C) Zapewnienie bezpiecznego i prywatnego połączenia z Internetem
D) Zarządzanie hasłami

9. Które z poniższych jest przykładem oprogramowania ransomware?

A) Oprogramowanie, które szyfruje pliki i żąda zapłaty za ich odblokowanie
B) Program antywirusowy, który skanuje system
C) Narzędzie do blokowania wiadomości spamowych
D) Aplikacja typu firewall

10. Jaka jest jedna z dobrych praktyk ochrony prywatności w mediach społecznościowych?

A) Podawanie pełnego adresu i numeru telefonu
B) Ustawienie wszystkich postów jako „publiczne”
C) Regularne sprawdzanie i dostosowywanie ustawień prywatności
D) Używanie tego samego hasła do wszystkich kont

Podsumowanie odpowiedzi

1	**B**
2	**C**
3	**B**
4	**D**
5	**C**
6	**B**
7	**B**
8	**C**
9	**A**
10	**C**

MODUŁ II

Typowe oszustwa internetowe wymierzone w seniorów

3. Moduł II – Typowe oszustwa internetowe wymierzone w seniorów

Ten czterogodzinny moduł umożliwia seniorom rozpoznawanie, zrozumienie i ochronę przed oszustwami internetowymi oraz zagrożeniami dla cyberbezpieczeństwa. Odnosi się on do ich szczególnych słabości poprzez praktyczne strategie i środki zapobiegawcze, budując zaufanie do bezpiecznego korzystania z technologii cyfrowych. Uczestnicy dowiedzą się, jak działają oszustwa, nauczą się rozpoznawać sygnały ostrzegawcze w komunikacji cyfrowej i zrozumieją taktyki manipulacyjne, takie jak inżynieria społeczna. Moduł obejmuje typowe oszustwa (phishing, smishing, vishing) i zagrożenia techniczne (złośliwe oprogramowanie, oprogramowanie ransomware, oprogramowanie szpiegujące), oferując strategie ochrony. Ponadto kładzie nacisk na bezpieczeństwo danych osobowych, ucząc seniorów, jak bezpiecznie przechowywać, udostępniać i tworzyć kopie zapasowe poufnych informacji.

3.1 Cele nauczania

Celem tego modułu jest poszerzenie wiedzy seniorów na temat popularnych oszustw internetowych, taktyk stosowanych przez oszustów oraz znaczenia rozpoznawania i unikania zagrożeń cyfrowych. Wyposażenie uczestników w praktyczne umiejętności i środki zapobiegawcze, które pozwolą im chronić się przed zagrożeniami dla cyberbezpieczeństwa, w tym phishingiem, smishingiem, vishingiem i złośliwym oprogramowaniem. Budowanie pewności siebie i umiejętności cyfrowych wśród seniorów poprzez nauczanie ich, jak chronić dane osobowe, rozpoznawać taktyki manipulacyjne i bezpiecznie korzystać z technologii cyfrowych.

- Zrozumienie, jak działają oszustwa, oraz rozpoznawanie metod psychologicznych i technologicznych stosowanych przez oszustów.
- Rozpoznawanie podejrzanych treści i odróżnianie legalnej komunikacji od fałszywej.
- Zdobycie wiedzy na temat popularnych rodzajów oszustw i poznanie strategii ochrony przed zagrożeniami cybernetycznymi.
- Budowanie pewności siebie w zakresie ochrony danych osobowych, tworzenia kopii zapasowych i bezpiecznego korzystania z narzędzi cyfrowych.

3.2 Struktura, treść i efekty uczenia się

Po pomyślnym ukończeniu tego modułu uczestnicy będą potrafili:

- Rozpoznawać typowe techniki, technologie i cele stosowane w oszustwach oraz wyjaśniać, w jaki sposób oszuści zwabiają swoje ofiary.
- Rozpoznawać sygnały ostrzegawcze w treściach cyfrowych, takich jak wiadomości e-mail, SMS-y, strony internetowe i reklamy, oraz odróżniać legalną komunikację od podejrzanej.
- Zdefiniować socjotechnikę, zidentyfikować typowe taktyki stosowane przez oszustów, zrozumieć, dlaczego osoby starsze są często wybierane jako ofiary, oraz stosować środki zapobiegawcze w celu ochrony przed atakami socjotechnicznymi.
- Wyjaśnić, w jaki sposób oszuści wykorzystują emocje i typowe wzorce zachowań osób starszych, oraz stosować strategie pozwalające zachować spokój i ostrożność w sytuacjach stresowych.
- Rozpoznawać najczęstsze rodzaje oszustw, w tym phishing, smishing, vishing oraz oszustwa związane z fałszywą tożsamością lub finansami, oraz opisywać techniki manipulacyjne stosowane w każdym z nich.

- Rozpoznawać różne rodzaje złośliwego oprogramowania, takie jak malware, ransomware, spyware, wirusy i trojany, opisywać metody ochrony przed nimi, rozpoznawać niebezpieczne wyskakujące okienka, bezpiecznie je zamykać oraz stosować narzędzia do blokowania wyskakujących okienek i weryfikowania bezpieczeństwa stron internetowych.
- Zdefiniować dane osobowe, zidentyfikować, które typy są cenne dla oszustów i w jaki sposób są wykorzystywane, oraz stosować najlepsze praktyki w zakresie bezpiecznego przechowywania i udostępniania danych osobowych.
- Wyjaśnienie znaczenia tworzenia kopii zapasowych danych, wdrożenie wskazówek dotyczących zmniejszenia podatności na utratę danych oraz budowanie zaufania do bezpiecznego z technologii.

3.3 Program I Szczegółowy plan sesji

MODUŁ II
Typowe oszustwa internetowe wymierzone w seniorów

1 sesja

Powitanie
Czas trwania *5 min*

Cele

- Przedstawienie tematu i stworzenie przyjaznej atmosfery.

Treść/metoda

- Krótkie wprowadzenie do sesji, nakreślenie celów i ustalenie oczekiwań
- Przygotowanie uczestników do szkolenia poprzez omówienie modułu i jego znaczenia.

Materiały

- Tablica lub flipchart do zapisania celów sesji.
- Markery.
- Wydrukowany plan lub slajdy prezentacji przedstawiające zarys sesji.

2 sesja

Ćwiczenie na przełamanie lodów: „Dwie prawdy i oszustwo”
Czas trwania: *10 min*

Cele

- Po zakończeniu tego ćwiczenia uczestnicy będą potrafili odróżnić prawidłowe praktyki bezpieczeństwa w Internecie od powszechnych błędnych przekonań wykorzystywanych w oszustwach.

Treść/metoda

- Interaktywne ćwiczenie grupowe w formie gry o nazwie „Dwie prawdy i jedno oszustwo", mające na celu przedstawienie kluczowych pojęć związanych z oszustwami i bezpieczeństwem w Internecie. Uczestnicy analizują krótkie stwierdzenia, omawiają je w parach lub małych grupach i identyfikują, które z nich jest fałszywe (kłamstwo lub mit). Trener udziela szybkiej informacji zwrotnej i wyjaśnia wszelkie wątpliwości.
- Uczestnik otrzymuje kartę z trzema stwierdzeniami i musi zdecydować, które z nich jest oszustwem. Następnie uczestnik przedstawia się i po podaniu swojego imienia musi przeczytać swoje stwierdzenia i powiedzieć, które z nich uważa za oszustwo. Pozostali uczestnicy słuchają i wskazują, czy się zgadzają, czy nie. Jeśli ktoś się nie zgadza, wstaje i wyjaśnia, które stwierdzenie uważa za prawdziwe oszustwo. Na koniec trener pyta uczestników, czy ktokolwiek z nich spotkał się z którymś z tych oszustw lub słyszał o nich.

Materiały

- Wydrukowana lub cyfrowa lista zestawów stwierdzeń (załącznik 1, 2).
- Długopis i papier (opcjonalnie, do robienia notatek lub zgadywania w grupie)
- Tablica lub ekran (opcjonalnie, do wyświetlania odpowiedzi i wyjaśnień)

3 sesja

Wykład 1: Rozpoznawanie oszustw

Czas trwania *30 min*

Cele nauczania

- Pomóż uczestnikom zrozumieć kluczowe mechanizmy oszustw, jakie są sztuczki i cele oszustów.

Treść/metoda

- Trener wykorzystuje slajdy, aby przedstawić najczęstsze oszustwa wymierzone w osoby starsze oraz wyjaśnia cele i mechanizmy tych oszustw. Na koniec trener pyta uczestników, który mechanizm przeraża ich najbardziej.

Materiały

- Slajdy prezentacji przedstawiające różne możliwe oszustwa internetowe wymierzone w osoby starsze.
- Projektor i laptop do wyświetlania prezentacji.
- Materiały informacyjne podsumowujące różne mechanizmy oszustw oraz sztuczki stosowane w celu osiągnięcia tych celów (załącznik 3).

Ćwiczenie 1: Rozpoznawanie podejrzanych treści
Czas trwania *15 min*

Cele

- Zapoznanie uczestników z sygnałami ostrzegawczymi w wiadomościach e-mail, SMS-ach, witrynach internetowych i reklamach.

Treść/metoda

- Uczestnikom zostaną pokazane rzeczywiste zrzuty ekranu z prawdziwymi wiadomościami SMS, e-mailami, stronami internetowymi i niebezpiecznymi wyskakującymi okienkami. Zostaną poproszeni o zidentyfikowanie rozbieżności i określenie, które przykłady są prawdziwe, a które stanowią oszustwo. Po każdej decyzji nastąpi wyjaśnienie, dlaczego coś jest oszustwem, a coś innym.
- Trener pokazuje dwa zrzuty ekranu obok siebie i prosi grupę o wskazanie różnic między oszustwem a prawdziwym przykładem oraz określenie, który z nich jest oszustwem. Trener kontynuuje w ten sam sposób z wszystkimi przykładami, utrzymując lekki i angażujący ton, aby utrzymać uwagę i zaangażowanie grupy. Trener wyjaśnia każdą parę przykładów po tym, jak uczestnicy podzielą się swoimi przemyśleniami. Zapytaj ich, który przykład był najtrudniejszy do zidentyfikowania jako oszustwo? Następnie trener rozdaje materiały informacyjne.

Materiały

- Slajdy prezentacji z wizualnymi przykładami prawdziwych i fałszywych zrzutów ekranu wiadomości SMS, e-maili, stron internetowych i wyskakujących okienek.
- Projektor i laptop do wyświetlania prezentacji.
- Arkusze robocze dla uczestników do zaznaczania odpowiedzi lub robienia notatek.
- Materiały informacyjne z wytycznymi dotyczącymi rozpoznawania fałszywych przykładów spośród prawdziwych (załącznik 4).

Przerwa | Czas trwania *5 min*

- **Czas na odpoczynek i refleksję dla uczestników.**
- **Krótka przerwa na odświeżenie się.**

4 sesja

Wykład 2: Zrozumienie manipulacji
Czas trwania *30 min*

Cele

- Pomoc uczestnikom w zrozumieniu socjotechniki.

Treść/metoda

- Przekazanie uczestnikom wiedzy na temat socjotechniki – przegląd najczęściej stosowanych taktyk, powody, dla których oszuści atakują osoby starsze oraz sposoby ochrony przed tego rodzaju oszustwami. Zdefiniowanie sytuacji w taki sposób, aby każdy, kto znajdzie się w sytuacji oszustwa socjotechnicznego, zachował spokój i opanowanie oraz nie uległ presji.

- Trener przedstawia przykłady wiadomości phishingowych i smishingowych, które wywołują strach i niepokój, a następnie pokazuje, jak często sugerują one łatwe i szybkie rozwiązanie – np. kliknięcie linku i podanie danych bankowych lub osobowych, a nawet wykonanie serii poleceń, aby „oni" mogli rozwiązać problem za Ciebie. Trener pyta uczestników, co zrobiliby w przypadku ataku socjotechnicznego. Trener rozdaje materiały drukowane zawierające dodatkowe informacje na temat taktyk socjotechnicznych i sposobów ich rozpoznawania.

Materiały

- Slajdy prezentacji wyjaśniające socjotechnikę.
- Projektor i laptop do przeprowadzenia demonstracji ustawień prywatności na żywo.
- Drukowane materiały informacyjne z opisem socjotechniki oraz wskazówkami dotyczącymi sygnałów ostrzegawczych i środków zapobiegawczych na wypadek, gdyby ktoś stał się ofiarą tego rodzaju oszustwa (załącznik 5).

Ćwiczenie 2: Socjotechnika na żywo
Czas trwania *20 min*

Cele

- Zapewnienie uczestnikom możliwości zapoznania się z różnymi metodami socjotechniki w bezpiecznym środowisku.

Treść/metoda

- Uczestnicy zapoznają się z różnymi scenariuszami, z których część stanowi formę inżynierii społecznej, a część nie. Scenariusze inżynierii społecznej będą ukierunkowane na emocje i zachowania uczestników.
- Trener poprosi uczestników o utworzenie pięciu trzyosobowych grup. Rozdzieli im arkusze robocze i przekaże instrukcje. Zadaniem uczestników będzie określenie, które scenariusze są oszustwami, a które są prawdziwe, oraz zapisanie powodów swoich wniosków. Gdy grupy przeanalizują wszystkie scenariusze i podejmą decyzje, trener poprosi ich o podzielenie się wynikami z pozostałymi uczestnikami. Trener moderuje dyskusję na temat scenariuszy i pyta uczestników, dlaczego uważają, że niektóre z nich są prawdziwe, a inne oszustwami, który scenariusz wywołałby u nich największy strach, gdyby znaleźli się w takiej sytuacji, i dlaczego.

Materiały

- Wydrukowane materiały z różnymi scenariuszami.
- Arkusz roboczy, w którym uczestnicy zaznaczają, które scenariusze są oszustwem, a które nie (załącznik 6).

Przerwa | Czas trwania *5 min*

- **Czas na odpoczynek i przygotowanie się do kolejnej sesji.**
- **Krótka przerwa na odświeżenie się.**

5 sesja

Wykład 3: Najczęstsze rodzaje oszustw
Czas trwania *30 min*

Cele

- Aby odświeżyć informacje na temat oszustw, które zostały już omówione, krótkie podsumowanie najczęstszych oszustw, takich jak smishing, vishing i phishing.
- Uzupełnienie wiedzy przekazanej podczas poprzednich wykładów o informacje dotyczące złośliwego oprogramowania.

Treść/metoda

- Krótki przegląd najczęstszych oszustw. Phishing, smishing, vishing, fałszywe tożsamości i oszustwa finansowe. Dodatkowo poinformowanie uczestników o złośliwym oprogramowaniu, czym jest i jak je wykrywać.
- Trener wyjaśnia najważniejsze informacje na temat najczęstszych oszustw i złośliwego oprogramowania, korzystając z slajdów. Następnie rozdaje materiały opisujące te zagadnienia i omawia je z uczestnikami szkolenia, aby upewnić się, że wszyscy rozumieją wszystko tak jasno, jak to tylko możliwe. Na koniec pyta uczestników, czy wiedzą, na jakie oznaki należy zwracać uwagę w Internecie.

Materiały

- Slajdy prezentacji przedstawiające przykłady oszustw phishingowych, vishingowych i smishingowych.
- Projektor i laptop do pokazania przykładów najczęstszych oszustw.
- Wydrukowane materiały informacyjne zawierające szczegółowe informacje na temat najczęstszych oszustw i złośliwego oprogramowania, czym one są, jak mogą zaszkodzić ofierze i jak je rozpoznać (załącznik 7).

Ćwiczenie 3: Wykryj złośliwe oprogramowanie
Czas trwania *20 min*

Cele

- Rozwinięcie umiejętności rozpoznawania różnych rodzajów złośliwego oprogramowania.

Treść/metoda

- Zajęcia grupowe, podczas których uczestnicy identyfikują i omawiają różne rodzaje złośliwego oprogramowania na podstawie materiałów informacyjnych.
- Trener wyjaśnia, że uczestnicy będą sprawdzać swoją wiedzę na temat złośliwego oprogramowania w grupach trzyosobowych. Trener rozdaje scenariusze i prosi uczestników o ich przeczytanie. Zadaniem uczestników jest określenie, jaki rodzaj oprogramowania został użyty (trojan, wirus, adware, ransomware lub spyware) i udzielenie odpowiedzi na pytania zawarte w każdym scenariuszu. Każda grupa dzieli się swoimi odpowiedziami z pozostałymi grupami. Następnie trener rozdaje arkusze odpowiedzi i prosi uczestników o przejrzenie odpowiedzi oraz przeanalizowanie kluczowych aspektów rozpoznawania użytego

oprogramowania i sposobów ochrony przed takim atakiem. Na koniec trener pyta, który rodzaj oprogramowania uważają za najbardziej i najmniej szkodliwy.

Materiały

- Materiały informacyjne z opisami złośliwego oprogramowania.
- Arkusze robocze dla uczestników, na których zapisują, jakie oprogramowanie wykorzystano w podanym przykładzie, jaki ma ono wpływ na urządzenie i jakie są środki zapobiegawcze w danym przypadku.
- Materiały dla uczestników – Rozpoznaj złośliwe oprogramowanie – załącznik 8

Przerwa | Czas trwania 5 minut

- **Czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**

6 sesja

Wykład 4: Podstawy ochrony danych i tworzenia kopii zapasowych danych
Czas trwania *30 min*

Cele

- Uczestnicy będą potrafili zdefiniować dane osobowe oraz określić, które dane są cenne dla oszustów. Będą również świadomi znaczenia tworzenia kopii zapasowych danych.

Treść/metoda

- Prezentacja z wyjaśnieniem pojęcia danych osobowych. Uczestnicy zostaną poinformowani o tym, gdzie można bezpiecznie udostępniać dane, a gdzie nie, oraz o znaczeniu identyfikacji danych, które mogą zostać wykorzystane przeciwko nim. Uczestnicy zostaną również poinformowani o tym, które dane należy archiwizować i dlaczego.
- Trener rozdaje materiały drukowane i prowadzi uczestników przez treść prezentacji, wyjaśniając: kategorie danych osobowych, jakie dane mogą być szkodliwe w niepowołanych rękach i dlaczego, gdzie możemy udostępniać dane osobowe w Internecie, czego nigdy nie powinniśmy udostępniać w Internecie, czym jest tworzenie kopii zapasowych, w jaki sposób kopie zapasowe mogą chronić przed atakami złośliwego oprogramowania, najlepsze praktyki dotyczące bezpiecznego tworzenia kopii zapasowych oraz wskazówki dotyczące bezpieczeństwa danych.
- Trener zachęca do dyskusji i pyta uczestników, czy kiedykolwiek byli świadkami próby cyberataku z wykorzystaniem oprogramowania lub brali udział w takim ataku. Na koniec trener pyta, czy będą teraz tworzyć kopie zapasowe ważnych danych.

Materiały

- Prezentacja dotycząca danych osobowych, gdzie i jakie informacje możemy udostępniać w Internecie, w połączeniu z informacjami niezbędnymi do tworzenia kopii zapasowych danych.
- Materiały informacyjne zawierające wytyczne dotyczące danych osobowych, gdzie można je udostępniać, a gdzie nie, oraz dlaczego ważne jest tworzenie kopii zapasowych ważnych informacji (załącznik 9).

Ćwiczenie 4: Tworzenie kopii zapasowych plików w usłudze w chmurze i na zewnętrznej pamięci masowej.
Czas trwania *20 min*

Cele

- Ta wiedza pomoże uczestnikom w bezpiecznym tworzeniu kopii zapasowych plików przy użyciu sprawdzonych usług w chmurze i zewnętrznych dysków twardych.

Treść/metoda

- Uczestnicy utworzą kopię zapasową fikcyjnych plików w znanej im usłudze w chmurze (Google Drive, Dropbox, iCloud, OneDrive). Utworzą również kopię zapasową tych samych fikcyjnych plików na dysku USB.
- Trener rozdaje materiały zawierające informacje na temat tworzenia kopii zapasowych plików na dysku zewnętrznym i w usłudze w chmurze. Trener demonstruje na ekranie lub projektorze, a uczestnicy śledzą proces kopiowania plików z komputera na dysk zewnętrzny i przesyłania plików do usługi w chmurze. Trener pomaga osobom, które potrzebują pomocy. Pytania do refleksji na koniec: „Czy uważacie, że potraficie samodzielnie wykonać kopię zapasową swoich plików, czy ktoś potrzebuje dodatkowych informacji?", „Czy jest coś, o co chcielibyście zapytać lub podzielić się swoją opinią na temat dzisiejszego tematu dotyczącego oszustw internetowych?".

Materiały

- Pliki testowe, które można skopiować.
- Komputery i pamięci USB.
- Laptop i projektor, aby nauczyciel mógł pokazać przykładowy proces.
- Materiały informacyjne z instrukcjami dotyczącymi tworzenia kopii zapasowych plików na dysku zewnętrznym i w usłudze w chmurze – instrukcje dostosowane do wszystkich głównych dostawców usług w chmurze – Jak tworzyć kopie zapasowe plików (załącznik 10).

7 sesja

Dyskusja | Czas trwania *10* min

Cele

- Zachęcanie do proaktywnego podejścia i świadomości w zakresie oszustw internetowych.
- Podsumowanie szkolenia i upewnienie się, że uczestnicy rozumieją, jak chronić się przed oszustwami internetowymi.

Treść/metoda

- Omówienie kluczowych punktów dotyczących najczęstszych oszustw internetowych. Uświadomienie uczestnikom, że jeśli coś jest komunikowane w sposób wymagający natychmiastowej reakcji, należy zawsze mieć świadomość, że może to być oszustwo.
- Dyskusja w grupie na temat tego, jak postępować w sytuacji, w której można paść ofiarą oszustwa internetowego. Jakie są kluczowe oznaki podejrzanych działań, z którymi możemy się spotkać, i co należy zrobić w takich sytuacjach.

- Trener podsumowuje najważniejsze informacje na temat tego, co należy zrobić, jeśli padnie się ofiarą oszustwa internetowego, i wymienia kluczowe oznaki podejrzanej aktywności. Trener dziękuje uczestnikom i rozdaje materiały pomocnicze, a następnie rozdaje listę kontrolną dotyczącą rozpoznawania oszustw internetowych i postępowania w takich sytuacjach. Trener zadaje uczestnikom pytania otwarte: „Jaka jest najważniejsza rzecz, której dowiedzieliście się dzisiaj na temat oszustw internetowych i sposobów ochrony przed nimi?" „Czy czujecie się teraz pewniej w rozpoznawaniu i unikaniu oszustw?" „Czy jest jakiś temat lub pytanie z dzisiejszej sesji, o którym chcielibyście uzyskać więcej informacji?"

Materiały

- Tablica i markery do burzy mózgów na temat sposobów rozpoznawania oszustw.
- Materiały informacyjne: lista kontrolna dotycząca oszustw internetowych (załącznik 11). Materiały informacyjne Lista kontrolna dotycząca bezpieczeństwa w Internecie.

Podsumowanie
Czas trwania 5 minut

Cele

- Podsumowanie sesji i zachęcenie uczestników do dalszego bezpiecznego korzystania z Internetu.

Treść/metoda

- Ostateczne podsumowanie kluczowych punktów, zapewnienie dodatkowych zasobów do dalszej nauki.

Materiały

- Materiały informacyjne zawierające kluczowe punkty i zasoby.

3.4 Dodatkowe informacje

3.4.1 Samoorefleksja trenerów

- Czy skutecznie przekazałem uczestnikom informacje na temat zagrożeń związanych z korzystaniem z Internetu?
- Czy upewniłem się, że uczestnicy zrozumieli środki zapobiegawcze?
- W jaki sposób zaangażowałem uczestników w ćwiczenia i dyskusje?
- Czy zasoby i materiały były pomocne dla uczestników?

3.4.2 Ocena programu przez trenerów

- Czy treść szkolenia jest odpowiednia i zrozumiała dla seniorów?
- Czy zajęcia i dyskusje skutecznie pomogły uczestnikom w przyswojeniu materiału?
- Czy wyniki są zgodne z celami edukacyjnymi modułu?

3.4.3 Materiały, dodatkowe zasoby

Załącznik 1 | Dwie prawdy i oszustwo

Zestaw 1

Oszuści często podszywają się pod osoby, którym ufasz.

Legalne firmy nigdy nie wysyłają wiadomości e-mail.

Wiadomości phishingowe często wywołują poczucie pilności.

Zestaw 2

Nigdy nie należy udostępniać nikomu swojego kodu PIN do bankowości.

Wszystkie strony internetowe, których adres zaczyna się od „https”, są w 100%

Oszuści mogą wykorzystywać logo wyglądające na oficjalne, aby Cię oszukać.

Zestaw 3

Oprogramowanie ransomware może zablokować dostęp do komputera.

Kliknięcie nieznanych wyskakujących okienek może spowodować zainstalowanie

Otwieranie załączników od znajomych bez sprawdzania jest bezpieczne.

Zestaw 4

Inżynieria społeczna często wiąże się z manipulacją emocjonalną.

Agencje rządowe zawsze najpierw kontaktują się z Tobą telefonicznie.

Osoby starsze są często celem ataków ze względu na postrzegane jako słabość.

Zestaw 5

Można używać tego samego hasła do wielu kont.

Silne hasło zawiera litery, cyfry i symbole.

Używanie uwierzytelniania dwuskładnikowego zapewnia dodatkową ochronę.

Zestaw 6

Oszuści mogą sfałszować identyfikator dzwoniącego, aby wyglądał jak prawdziwy

Podanie pełnego adresu w internetowym konkursie jest bezpieczne.

Zawsze zachowuj ostrożność w przypadku niechcianych ofert.

Zestaw 7

Smishing to oszustwo realizowane za pośrednictwem wiadomości tekstowych.

Złośliwe oprogramowanie atakuje tylko stare komputery.

Oprogramowanie antywirusowe pomaga chronić przed złośliwymi atakami.

Zestaw 8

Oszuści mogą podszywać się pod pracowników pomocy technicznej.

Należy kliknąć nieznane linki, aby sprawdzić, czy działają.

Zawsze sprawdzaj adresy URL przed wprowadzeniem danych osobowych.

Zestaw 9

Fałszywe oferty pracy mogą służyć do kradzieży danych osobowych.

Oszustwa dotyczą wyłącznie osób, które nie znają się na technologii.

Reklamy internetowe mogą czasami prowadzić do fałszywych stron inter-

Zestaw 10

Niektóre oszustwa wymagają płatności kartami podarunkowymi.

Pobieranie aplikacji z zaufanych sklepów z aplikacjami jest bezpieczne.

Powinieneś udostępniać swoje dane logowania bliskim znajomym.

Zestaw 11

Oszuści czasami wykorzystują strach, aby wywrzeć presję na użytkowniku.

Każde wyskakujące okienko z ostrzeżeniem jest prawdziwym alertem o wirusie.

Ważne jest, aby zweryfikować wiadomości przed podjęciem działania.

Zestaw 12

Legalne firmy nie proszą o podawanie danych osobowych za pośrednictwem poczty e-mail

Publiczne sieci Wi-Fi są zawsze bezpieczne i można z nich korzystać bez obaw.

Aktualizacja urządzenia pomaga naprawić luki w zabezpieczeniach.

Zestaw 13

Oszustwa mogą mieć miejsce na platformach społecznościowych.

Kliknięcie „zrezygnuj z subskrypcji” w oszukańczej wiadomości e-mail jest nieszkodliwe.

Należy zgłaszać podejrzane działania platformie.

Zestaw 14

Można publicznie publikować swoje plany podróży w Internecie.

Oszuści mogą monitorować Twoje posty w mediach społecznościowych.

Zachowaj ostrożność w przypadku zaproszeń do grona znajomych od nieznajomych.

Zestaw 15

Kopie zapasowe chronią dane w przypadku ataków.

Należy ignorować przypomnienia o aktualizacjach oprogramowania.

Używaj silnych, unikalnych haseł dla każdego konta.

Dodatek 2 | Prawidłowe odpowiedzi

Zestaw 1

- Prawda – Oszuści często podszywają się pod osoby, którym ufasz.
- Fałsz – Legalne firmy nigdy nie wysyłają wiadomości e-mail. (To mit. Legalne firmy mogą kontaktować się z użytkownikami za pośrednictwem poczty elektronicznej, ale nie proszą o podawanie poufnych danych osobowych ani finansowych).
- Prawda – wiadomości phishingowe często wywołują poczucie pilności.

Zestaw 2

- Prawda – Nigdy nie należy nikomu ujawniać swojego kodu PIN do bankowości.
- Fałsz – Wszystkie strony internetowe, których adres zaczyna się od „https", są całkowicie bezpieczne. (To mit. „https" oznacza szyfrowanie, a nie legalność).
- Prawda – Oszuści mogą wykorzystywać oficjalnie wyglądające logo, aby oszukać użytkowników.

Zestaw 3

- Prawda – oprogramowanie ransomware może zablokować użytkownikom dostęp do ich komputerów.
- Prawda – Kliknięcie nieznanych wyskakujących okienek może spowodować zainstalowanie złośliwego oprogramowania.
- Fałsz – Otwieranie załączników od znajomych bez sprawdzania jest bezpieczne. (To mit. Załączniki od zaufanych kontaktów również mogą być zainfekowane).

Zestaw 4

- Prawda – Socjotechnika często opiera się na manipulacji emocjonalnej.
- Fałsz – Agencje rządowe zawsze najpierw kontaktują się z osobami fizycznymi telefonicznie. (To mit. Oficjalna komunikacja często odbywa się za pośrednictwem poczty).
- Prawda – Osoby starsze są często celem ataków ze względu na postrzegane jako słabe punkty.

Zestaw 5

- Fałsz – Dopuszczalne jest ponowne użycie tego samego hasła do wielu kont. (To mit. Ponowne użycie hasła zwiększa ryzyko związane z bezpieczeństwem).
- Prawda – Silne hasła zawierają kombinację liter, cyfr i symboli.
- Prawda – Uwierzytelnianie dwuskładnikowe zapewnia dodatkową warstwę bezpieczeństwa.

Zestaw 6

- Prawda – Oszuści mogą sfałszować informacje o numerze dzwoniącego.
- Fałsz – Podawanie pełnego adresu w internetowych konkursach z nagrodami jest bezpieczne. (To mit. Dane osobowe mogą zostać wykorzystane do oszustw).
- Prawda – Niezamówione oferty należy zawsze traktować z ostrożnością.

Zestaw 7

- Prawda – Smishing odnosi się do oszustw wysyłanych za pośrednictwem wiadomości tekstowych.
- Fałsz – Złośliwe oprogramowanie atakuje tylko stare komputery. (To mit. Może ono zaatakować każde urządzenie).
- Prawda – Oprogramowanie antywirusowe pomaga chronić przed złośliwymi zagrożeniami.

Zestaw 8

- Prawda – Oszuści mogą podszywać się pod pracowników pomocy technicznej.
- Fałsz – Należy klikać nieznane linki, aby sprawdzić, czy są one legalne. (To mit. Klikanie nieznanych linków może być niebezpieczne).
- Prawda – przed wprowadzeniem danych osobowych należy zawsze sprawdzić adresy URL.

Zestaw 9

- Prawda – Fałszywe oferty pracy mogą służyć do kradzieży danych osobowych.
- Fałsz – Oszuści atakują wyłącznie osoby o niskich umiejętnościach cyfrowych. (To mit. Ofiarą oszustwa może paść każdy).
- Prawda – Reklamy internetowe mogą czasami przekierowywać użytkowników do oszukańczych stron internetowych.

Zestaw 10

- Prawda – Niektóre oszustwa wymagają płatności kartami podarunkowymi.
- Prawda – Pobieranie aplikacji z zaufanych sklepów z aplikacjami jest zazwyczaj bezpieczniejsze.
- Fałsz – Dane logowania należy udostępniać bliskim znajomym. (To mit. Nigdy nie należy udostępniać danych logowania).

Zestaw 11

- Prawda – Oszuści często wykorzystują strach, aby wywrzeć presję na ofiarach.
- Fałsz – Każde wyskakujące okienko z ostrzeżeniem oznacza rzeczywiste zagrożenie wirusem. (To mit. Wiele alertów jest fałszywych).
- Prawda – Przed podjęciem działania należy zawsze zweryfikować wiadomości.

Zestaw 12

- Prawda – Legalne firmy nie proszą o podanie danych osobowych za pośrednictwem poczty elektronicznej.
- Fałsz – Publiczne sieci Wi-Fi są zawsze bezpieczne. (To mit. Sieci publiczne mogą narazić dane osobowe na niebezpieczeństwo).
- Prawda – Regularne aktualizacje oprogramowania pomagają naprawić luki w zabezpieczeniach.

Zestaw 13

- Prawda – Oszustwa mogą mieć miejsce na platformach społecznościowych.
- Fałsz – Kliknięcie „zrezygnuj z subskrypcji” w oszukańczych wiadomościach e-mail jest nieszkodliwe. (To mit. Może to potwierdzić, że użytkownik jest aktywnym celem ataku).
- Prawda – Podejrzane działania należy zgłaszać odpowiedniej platformie.

Zestaw 14

- Fałsz – Publiczne udostępnianie planów podróży w Internecie jest bezpieczne. (To mit. Takie informacje mogą zostać wykorzystane przez oszustów).
- Prawda – Oszuści mogą monitorować aktywność w mediach społecznościowych.
- Prawda – Prośby o dodanie do znajomych od nieznanych osób należy traktować z ostrożnością.

Zestaw 15

- Prawda – Kopie zapasowe danych chronią informacje w przypadku cyberataków.
- Fałsz – Przypomnienia o aktualizacjach oprogramowania należy ignorować. (To mit. Aktualizacje mają kluczowe znaczenie dla bezpieczeństwa).
- Prawda – Do każdego konta należy używać silnych i unikalnych haseł.

Załącznik 3 | Mechanizmy stosowane w oszustwach internetowych wymierzonych w osoby starsze

1. Phishing (oszustwa e-mailowe)

Seniorzy otrzymują e-maile, które wydają się pochodzić z zaufanych źródeł (banki, służba zdrowia itp.).

Sztuczka: fałszywe linki lub strony logowania

Cel: kradzież danych osobowych lub finansowych

2. Smishing (oszustwa SMS-owe)

Oszuści wysyłają wiadomości SMS z fałszywymi powiadomieniami o dostawie, informacjami o wygranych lub ostrzeżeniami.

Sztuczka: pilny język + link do złośliwej strony

Cel: zainstalowanie złośliwego oprogramowania lub zebranie prywatnych danych

3. Vishing (oszustwa telefoniczne)

Połączenia telefoniczne od oszustów podających się za pracowników banku, pomocy technicznej lub instytucji rządowej.

Sztuczka: fałszywy identyfikator dzwoniącego + presja emocjonalna

Cel: uzyskanie danych bankowych lub zdalnego dostępu

4. Fałszywe strony internetowe (spoofing)

Osoby starsze są kierowane na fałszywe strony internetowe, które wyglądają jak prawdziwe (banki, sklepy, portale medyczne).

Sztuczka: Nieznacznie zmienione adresy URL (np. paypa1.com)

Cel: przechwycenie danych logowania lub informacji dotyczących płatności

5. Oszustwa związane z pomocą techniczną (oszustwa e-mailowe)

Wyskakujące okienka lub telefony ostrzegają o „wirusie" lub problemie z komputerem, nakłaniając seniorów do skorzystania z pomocy.

Sztuczka: fałszywe komunikaty o błędach + prośby o zdalny dostęp

Cel: przejęcie kontroli nad urządzeniem lub kradzież danych karty kredytowej

6. Oszustwa matrymonialne

W mediach społecznościowych lub na portalach randkowych oszuści tworzą więzi emocjonalne, aby manipulować ofiarami.

Sztuczka: Fałszywe zdjęcia, historie i uczucia

Cel: Przekonanie seniorów do wysłania pieniędzy

7. Oszustwa inwestycyjne lub loteryjne

Obietnice ogromnych zysków lub wiadomości typu „wygrałeś", które wymagają przedpłaty.

Sztuczka: fałszywe dokumenty, pilność lub oficjalnie brzmiące nazwy

Cel: Uzyskanie przelewów bankowych, kryptowalut lub kart podarunkowych

Załącznik 4 | Rozpoznaj oszustwo: krótki przewodnik

Skorzystaj z poniższej listy kontrolnej, aby zdecydować, czy wiadomość, e-mail, strona internetowa lub reklama są prawdziwe, czy fałszywe.

1. Sprawdź nadawcę lub źródło

- *Adres e-mail / numer telefonu: Czy dane nadawcy wyglądają podejrzanie lub są nieznane?*

✗ ***Fałszywe:*** *support@paypal-secure123.com*
✓ ***Prawdziwe:*** *support@paypal.com*

- *Błędnie napisane nazwy marek lub dziwne adresy URL:*

✗ *netfflix-billing.com*
✓ *netflix.com*

2. Zwróć uwagę na poczucie pilności lub presję

- Czy wiadomość próbuje Cię przestraszyć lub zmusić do pośpiechu?

  „Zareaguj natychmiast, bo Twoje konto zostanie zablokowane!”
  „Ostatnie ostrzeżenie przed podjęciem kroków prawnych!”

Prawdziwe firmy nie grożą ani nie wywierają presji w ten sposób.

3. Zwróć uwagę na język i ton

- Zwróć uwagę na błędy ortograficzne i gramatyczne
- Czy ton jest zbyt swobodny lub zbyt agresywny?
- Czy brzmi nienaturalnie lub jakby był tłumaczeniem?

  ✗ **Fałszywe:** „Szanowny Kliencie, Twoje konto zostało pilnie zablokowane, prosimy o podjęcie natychmiastowych działań”.

  ✓ **Prawdziwe:** „Zauważyliśmy nietypową aktywność na Twoim koncie. Prosimy o sprawdzenie”.

4. Sprawdź link przed kliknięciem

- Najedź kursorem na linki, aby sprawdzić, dokąd faktycznie prowadzą

- Czy adres URL pasuje do prawdziwej strony internetowej firmy?
  - ✗ **Fałszywy:** http://paypal.verify-now-support.com
  - ✓ **Prawdziwy:** https://www.paypal.com

5. Uważaj na prośby o podanie danych osobowych

Prawdziwe firmy nigdy nie proszą o:

- Hasła
- Kodów PIN
- Numerów kont bankowych lub kart
- Numerów ubezpieczenia społecznego
  - ✗ „Proszę przesłać swoje dane logowania w celu weryfikacji konta".
  - ✓ „Nigdy nie prosimy o podanie hasła w wiadomości e-mail".

6. Zwróć uwagę na logo i wygląd

- Czy logo są rozmyte, rozciągnięte lub mają nieprawidłowy kolor?
- Czy układ strony jest dziwny lub niespójny?

Prawdziwe firmy stosują przejrzysty, profesjonalny i spójny projekt.

7. Zbyt piękne, aby mogło być prawdziwe? Prawdopodobnie tak jest.

„Wygrałeś nowy iPhone!"

„Zostałeś wybrany do otrzymania karty podarunkowej o wartości 1000 dolarów!"

Prawdziwe nagrody nie wymagają wcześniejszej płatności ani podania poufnych informacji.

✔ **Prawdziwe czy ✗ Fałszywe?**

Zadaj sobie pytanie:

- **Czy ufam źródłu?**
- **Czy ktoś mnie popędza lub straszy, żebym podjął działanie?**
- **Czy coś wydaje się nie tak lub niezwykłe?**

W razie wątpliwości nie klikaj, nie odpowiadaj i zgłoś to!

Dodatek 5 | Oszustwa socjotechniczne – co należy wiedzieć

Czym jest socjotechnika?

Socjotechnika polega na wykorzystywaniu przez oszustów manipulacji, presji i emocji w celu nakłonienia Cię do ujawnienia danych osobowych, przekazania pieniędzy lub uzyskania dostępu do Twoich kont.

Niebezpieczeństwa związane z socjotechniką

Oszuści mogą podszywać się pod zaufane źródła, takie jak:

- Banki (np. „Twoje konto zostało zablokowane!")
- Firmy kurierskie (np. „Nie odebrałeś paczki. Zapłać teraz!")
- Agencje rządowe (np. „Masz zaległości podatkowe")
- Policja lub Ministerstwo Sprawiedliwości (np. „Jesteś objęty dochodzeniem")
- Pomoc techniczna (np. „Wykryliśmy wirusa na Twoim komputerze")
- Rodzina lub przyjaciele (np. „Mam kłopoty, proszę, wyślij pieniądze!")

Często wywołują poczucie pilności lub strachu, aby skłonić Cię do podjęcia szybkich działań bez zastanowienia.

Sygnały ostrzegawcze, na które należy zwrócić uwagę

- Zostajesz poinformowany, że musisz działać **natychmiast,** bo w przeciwnym razie poniesiesz konsekwencje
- Proszą Cię o podanie **danych osobowych**, haseł lub danych bankowych
- Proszą Cię o **dokonanie płatności za pomocą kart podarunkowych**, **kryptowalut lub przelewów bankowych**
- Wiadomości zawierają **dziwne błędy gramatyczne lub ortograficzne.**
- Nagle kontaktuje się z Tobą ktoś, kogo nie znasz

Środki zapobiegawcze

Zawsze postępuj w następujący sposób:

1. Zachowaj spokój. Weź głęboki oddech i nie działaj pochopnie.
2. Nigdy nie podawaj danych osobowych przez telefon, e-mail lub SMS.
3. Jeśli coś wydaje Ci się podejrzane, rozłącz się lub usuń wiadomość.
4. Samodzielnie zweryfikuj prośbę:

Jeśli ktoś twierdzi, że jest z banku, firmy kurierskiej, urzędu państwowego lub pomocy technicznej — zawsze kontaktuj się bezpośrednio z tą organizacją.
Skorzystaj z oficjalnej strony internetowej lub numeru telefonu, a nie tych podanych w wiadomości lub e-mailu.

Przykład:

- Zadzwoń do swojego banku, korzystając z numeru podanego na karcie bankowej lub oficjalnej stronie internetowej.
- Jeśli nie masz pewności co do wiadomości dotyczących podatków, odwiedź oficjalną stronę rządową
- Skontaktuj się z oficjalnym działem pomocy firmy kurierskiej, aby sprawdzić, czy paczka jest prawdziwa.

Pamiętaj:

- Prawdziwe firmy nie grożą ani nie wywierają presji
- Prawdziwe instytucje nigdy nie proszą o podanie haseł ani kodów PIN
- Prawdziwe wiadomości są profesjonalne i pełne szacunku.
- Oszuści wykorzystują strach, zamieszanie i pośpiech

Jeśli coś wydaje się „nie tak”, zatrzymaj się i zapytaj kogoś, komu ufasz. Zawsze lepiej jest sprawdzić dwa razy, niż wpaść w pułapkę.

Załącznik 6 | Scenariusze: Rozpoznaj oszustwo

Scenariusz 1: Pilna wiadomość od banku

Otrzymujesz wiadomość e-mail, która wygląda na pochodzącą z Twojego banku. Temat wiadomości brzmi: „PILNE: Problem z dostępem do konta". W wiadomości znajduje się informacja, że na Twoim koncie wykryto podejrzaną aktywność i musisz natychmiast zweryfikować swoje dane osobowe i bankowe. Wiadomość zawiera link i ostrzeżenie, że jeśli nie odpowiesz w ciągu 24 godzin, Twoje konto zostanie trwale zawieszone.

Scenariusz 2: Alert o zapełnieniu pamięci telefonu

Podczas przeglądania Internetu lub korzystania z aplikacji pojawia się wyskakujące okienko z komunikatem: „Ostrzeżenie! Pamięć telefonu jest pełna. Naciśnij tutaj, aby wyczyścić urządzenie i uniknąć utraty danych". Komunikat wygląda na pilny, naśladuje styl systemu telefonu, a po naciśnięciu przekierowuje do pobrania aplikacji innej firmy, która obiecuje zoptymalizować urządzenie.

Scenariusz 3: Telefon od pomocy technicznej

Otrzymujesz telefon od osoby podającej się za technika firmy Microsoft. Twierdzi ona, że Twój komputer został zainfekowany niebezpiecznym wirusem i wysyła komunikaty o błędach. Oferuje zdalne naprawienie problemu i pomaga w pobraniu oprogramowania, które umożliwi jej dostęp do Twojego komputera. Po nawiązaniu połączenia „skanuje" komputer, a następnie żąda zapłaty za usunięcie wirusa, często prosząc o podanie danych karty kredytowej lub dostępu do bankowości internetowej.

Scenariusz 4: Oszustwo związane z płatnością rachunków za media

Otrzymujesz wiadomość e-mail lub SMS, która wygląda, jakby pochodziła od dostawcy energii elektrycznej. Twierdzi ona, że ostatnia płatność nie doszła do skutku i jeśli nie uregulujesz zaległej kwoty w ciągu 12 godzin, zostanie odcięty dopływ energii elektrycznej. Wiadomość zawiera link do strony płatności, która wygląda bardzo podobnie do prawdziwej strony internetowej dostawcy mediów, ale wymaga podania danych karty kredytowej i danych osobowych.

Scenariusz 5: Powiadomienie o transakcji bankowej

Otrzymujesz wiadomość e-mail od swojego banku z tematem: „Potwierdzenie transakcji – 74,60 € w MERKUR". Wiadomość potwierdza transakcję dokonaną dzisiaj o godz. 13:45. Jeśli nie rozpoznajesz tej opłaty, otrzymujesz instrukcję, aby skontaktować się z działem ds. oszustw bankowych pod oficjalnym numerem podanym na stronie internetowej banku. Wiadomość e-mail nie zawiera żadnych linków, które można kliknąć, a jej ton jest spokojny i profesjonalny.

Scenariusz 6: Ostrzeżenie dotyczące pamięci Google

Otrzymujesz wiadomość e-mail od Google o treści: „Pamięć Twojego konta Google jest zapełniona w 98%. Obecnie wykorzystujesz 14,8 GB z 15 GB przydzielonej pamięci. Aby nadal otrzymywać wiadomości e-mail i korzystać z Dysku Google, zarządzaj pamięcią lub zwiększ jej pojemność". Wiadomość zawiera dwa przyciski: jeden do zarządzania pamięcią, a drugi do zwiększenia jej pojemności. Oba prowadzą do oficjalnych stron internetowych Google.

Dodatek 7 | Typowe oszustwa internetowe i sposoby ochrony przed nimi

1. Smishing (phishing SMS)
Otrzymujesz wiadomość tekstową, która wygląda na pochodzącą z Twojego banku, firmy kurierskiej lub instytucji rządowej. Może ona zawierać informację o problemie z Twoim kontem lub paczką oraz link.

Sygnały ostrzegawcze:
- Pilny język („Twoje konto zostanie zamknięte")
- Podejrzane linki
- Prośba o podanie danych osobowych lub bankowych

Co należy zrobić:
- Nigdy nie klikaj linków z nieznanych numerów.
- Skontaktuj się bezpośrednio z firmą, korzystając z oficjalnego numeru telefonu lub strony internetowej.
- Zablokuj i zgłoś nadawcę.

2. Vishing (phishing głosowy)
Otrzymujesz telefon od osoby podającej się za pracownika banku, policji lub pomocy technicznej. Prosi ona o podanie danych osobowych lub twierdzi, że wykryto podejrzaną aktywność.

Odmiana: fałszywy głos wykorzystujący sztuczną inteligencję
Oszuści mogą teraz naśladować głos bliskiej osoby za pomocą sztucznej inteligencji. Mogą zadzwonić, podając się za Twoje dziecko lub wnuka, prosząc o pilną pomoc lub pieniądze.

Sygnały ostrzegawcze:
- Dzwoniący naciska, abyś działał szybko
- Manipulacja emocjonalna („Mam kłopoty!")
- Prosi o pieniądze lub informacje

Co należy zrobić:
- Odłóż słuchawkę i oddzwonij bezpośrednio pod znany numer.
- Skontaktuj się z innym członkiem rodziny, aby zweryfikować tę historię.
- Nigdy nie podawaj danych osobowych ani bankowych przez telefon.

3. Phishing (oszustwo e-mailowe)
Otrzymujesz wiadomość e-mail, która wygląda na oficjalną (od banku, serwisu PayPal, urzędu skarbowego itp.), z prośbą o potwierdzenie danych, zresetowanie hasła lub kliknięcie linku.

Sygnały ostrzegawcze:
- E-mail zawiera błędy gramatyczne
- Wykorzystuje strach („wykryto nieautoryzowane logowanie")
- Prośba o podanie danych osobowych

Co należy zrobić:
- Nie klikaj podejrzanych linków.
- Dokładnie sprawdź adres e-mail nadawcy.
- Skontaktuj się z firmą za pośrednictwem jej oficjalnej strony internetowej.

4. Oszustwa finansowe

Oszuści podszywają się pod doradców inwestycyjnych, fałszywe organizacje charytatywne, a nawet osoby zainteresowane romansem. Budują zaufanie, a następnie proszą o pieniądze, darowizny lub pomoc.

Sygnały ostrzegawcze:

- Zbyt wysokie zyski z inwestycji, aby mogły być prawdziwe
- Manipulacja emocjonalna
- Niezweryfikowane organizacje charytatywne lub cele

Co należy zrobić:

- Nigdy nie wysyłaj pieniędzy osobom, których nie znasz osobiście.
- Zawsze sprawdzaj firmę lub osobę.
- Przed podjęciem decyzji finansowych skonsultuj się z zaufanym członkiem rodziny lub doradcą.

5. Fałszywe tożsamości i podszywanie się

Oszuści mogą podawać się za kogoś, kim nie są — na przykład urzędnika państwowego, pracownika banku, a nawet członka rodziny. Wykorzystują fałszywe dokumenty, e-maile lub głosy generowane przez sztuczną inteligencję, aby nakłonić ludzi do ujawnienia poufnych informacji lub wysłania pieniędzy.

Sygnały ostrzegawcze:

- Nieoczekiwane prośby o podanie danych osobowych lub pieniędzy
- Poczucie pilności lub presja emocjonalna
- Kontakt nawiązany za pośrednictwem nieoficjalnych lub podejrzanych kanałów

Co należy zrobić:

- Zawsze weryfikuj tożsamość, dzwoniąc do prawdziwej osoby lub instytucji, korzystając z oficjalnych danych kontaktowych.
- Nie bój się rozłączyć i najpierw sprawdzić.
- W razie wątpliwości poproś zaufaną osobę o pomoc w ocenie sytuacji.

6. Złośliwe oprogramowanie lub malware

To każde oprogramowanie zaprojektowane w celu wyrządzenia szkody komputerowi lub kradzieży danych osobowych. Oszuści często nakłaniają użytkowników do pobrania go za pomocą fałszywych wiadomości e-mail, linków lub wyskakujących reklam. Po zainstalowaniu złośliwe oprogramowanie może wykraść hasła, zablokować pliki, a nawet przejąć kontrolę nad urządzeniem. Zawsze zachowuj ostrożność w przypadku nieznanych linków lub załączników i upewnij się, że Twój komputer ma aktualne oprogramowanie antywirusowe, które zapewni Ci ochronę.

Załącznik 8 | Materiały dla uczestników – Wykrywanie złośliwego oprogramowania

Cel

Zapoznaj się z popularnymi rodzajami złośliwego oprogramowania (wirusy, trojany, oprogramowanie szpiegujące, oprogramowanie ransomware, oprogramowanie reklamowe), czytając i analizując poniższe realistyczne scenariusze.
Dla każdego oszustwa zapisz, jakie to oszustwo (trojan, wirus, adware, ransomware, spyware) i odpowiedz na pytanie.

Scenariusz 1

„Otrzymujesz wiadomość e-mail od zaufanego znajomego z załącznikiem zatytułowanym „Ważny dokument". Po otwarciu załącznika komputer zaczyna działać wolniej i pojawiają się dziwne wyskakujące okienka".

Pytanie: Jakiego rodzaju złośliwe oprogramowanie to Twoim zdaniem jest? Jak się przed nim zabezpieczysz?

Scenariusz 2

„Podczas przeglądania stron internetowych pojawia się wyskakujące okienko z komunikatem: „Twoje urządzenie jest przestarzałe! Kliknij tutaj, aby pobrać aktualizację". Klikasz link i nieświadomie pobierasz złośliwe oprogramowanie podszywające się pod aktualizację".

Pytanie: Jakie niebezpieczeństwo się z tym wiąże? Co należy zrobić w takiej sytuacji?

Scenariusz 3

„Pobierasz bezpłatną aplikację do edycji zdjęć z nieznanej strony internetowej. Z czasem zauważasz, że w przeglądarce pojawiają się reklamy i zaczynasz otrzymywać niechciane wiadomości e-mail o charakterze marketingowym".

Pytanie: Jak myślisz, co się stało? Co należy zrobić w takiej sytuacji?

Scenariusz 4

„Po kliknięciu linku w wiadomości e-mail z informacją „Twoja subskrypcja Netflix wkrótce wygaśnie, kliknij tutaj, aby potwierdzić płatność" pojawia się komunikat z żądaniem zapłaty okupu za odblokowanie plików".

Pytanie: Jak rozpoznać, że jest to oszustwo? Co należy zrobić w takiej sytuacji?

Scenariusz 5

„Po kliknięciu linku w wiadomości e-mail z informacją „Twoja subskrypcja Netflix wkrótce wygaśnie, kliknij tutaj, aby potwierdzić płatność" pojawia się komunikat z żądaniem zapłaty okupu w celu odblokowania plików".

Pytanie: Czy jest to niebezpieczny rodzaj oprogramowania? Jak można się go pozbyć?

Załącznik 9 | Ochrona danych osobowych

1. Czym są dane osobowe?

Dane osobowe to wszelkie informacje, które mogą posłużyć do bezpośredniej lub pośredniej identyfikacji użytkownika. Obejmują one:

- **Dane podstawowe:** imię, nazwisko, data urodzenia, adres
- **Dane kontaktowe:** adres e-mail, numer telefonu
- **Numery identyfikacyjne:** numer dowodu osobistego, numer podatkowy, numer paszportu
- **Dane finansowe:** numery kont bankowych, numery kart kredytowych
- **Dane logowania:** nazwy użytkownika, hasła
- **Dane dotyczące zdrowia:** dokumentacja medyczna, recepty
- **Dane biometryczne:** odciski palców, rozpoznawanie twarzy, głos
- **Dane dotyczące lokalizacji:** śledzenie GPS, adres IP
- **Preferencje osobiste:** historia wyszukiwania, aktywność w mediach społecznościowych

2. Jakie dane mogą być szkodliwe w niepowołanych rękach (i dlaczego)?

Oszuści i cyberprzestępcy atakują konkretne dane, które mogą wykorzystać do:

- **Kradzieży tożsamości**
- **uzyskania dostępu do kont bankowych**
- **Popełnienia oszustwa w Twoim imieniu**
- **Manipulowanie Tobą emocjonalnie lub finansowo**

Najcenniejsze dane dla oszustów:

- **Dane osobowe (paszport itp.) –** wykorzystywane do kradzieży tożsamości lub otwierania fałszywych kont.
- **Dane logowania –** umożliwiają dostęp do poczty elektronicznej, mediów społecznościowych, bankowości internetowej.
- **Dane bankowe i karty kredytowe –** wykorzystywane do nieautoryzowanych zakupów lub przelewów środków.
- **Numery telefonów i adresy e-mail –** wykorzystywane do phishingu, smishingu, spamu i podszywania się pod inne osoby.
- **Treści w mediach społecznościowych –** wykorzystywane do tworzenia fałszywych profili lub manipulowania użytkownikami.

3. Gdzie możemy udostępniać nasze dane osobowe w Internecie?

Ważne jest, aby wiedzieć, gdzie i kiedy można bezpiecznie udostępniać dane osobowe. Niektóre platformy są godne zaufania, podczas gdy inne wiążą się z większym ryzykiem.

Miejsca, w których udostępnianie danych osobowych jest ogólnie bezpieczne (z zachowaniem ostrożności):

- Zweryfikowane sklepy internetowe (np. Amazon, Zalando, Mimovrste): w przypadku zakupów, tylko wtedy, gdy strona internetowa posiada szyfrowanie HTTPS i bezpieczne metody płatności.
- Oficjalne strony rządowe (np. IRS, portale ubezpieczeń społecznych, portale e-administracji): w celu składania dokumentów, podatków, wniosków.
- Renomowani dostawcy usług (np. bank, placówka służby zdrowia): wyłącznie za pośrednictwem ich oficjalnych stron internetowych lub aplikacji.
- Zaufani dostawcy poczty elektronicznej i usług w chmurze (np. Gmail, Outlook, Dropbox): podczas zakładania kont, tworzenia kopii zapasowych danych.

Przed przesłaniem jakichkolwiek informacji zawsze upewnij się, że strona jest oficjalna, posiada protokół HTTPS i jest dobrze znana.

Miejsca, w których należy zachować szczególną ostrożność lub unikać udostępniania danych osobowych:

- Niezweryfikowane sklepy internetowe lub reklamy (często spotykane w wyskakujących okienkach lub mediach społecznościowych)
- Nieznane ankiety, quizy online lub konkursy z nagrodami
- Niebezpieczne publiczne sieci Wi-Fi
- Linki w niechcianych wiadomościach e-mail lub SMS-ach
- Platformy społecznościowe, zwłaszcza w komentarzach lub wiadomościach bezpośrednich

Wskazówka: Nawet jeśli platforma wydaje się znajoma, zawsze sprawdzaj adres internetowy i unikaj udostępniania poufnych danych, takich jak numery identyfikacyjne lub informacje finansowe, chyba że jest to absolutnie konieczne i bezpieczne.

4. Jakie informacje możemy udostępniać, a jakich nigdy nie powinniśmy udostępniać w Internecie?

- **Można udostępniać (z zachowaniem ostrożności):** imię, miasto i ogólną lokalizację, ogólne zainteresowania lub hobby, informacje zawodowe (np. stanowisko), publiczny adres e-mail (służbowy), zdjęcia profilowe
- **Nigdy nie należy udostępniać w Internecie:** hasła i kody PIN, pełny adres (z wyjątkiem zweryfikowanych serwisów rządowych i sklepów internetowych), numery identyfikacyjne, numery podatkowe, dane bankowe lub karty kredytowej, dokumentacja medyczna lub informacje dotyczące zdrowia, poufne informacje dotyczące rodziny lub planów podróży

Ogólna zasada: jeśli informacje mogą zostać wykorzystane do uzyskania dostępu do Twoich pieniędzy, tożsamości lub życia prywatnego, nie udostępniaj ich w Internecie, niezależnie od tego, kto o nie prosi.

5. Tworzenie kopii zapasowej danych oznacza wykonanie kopii ważnych plików, dokumentów, zdjęć i ustawień w bezpiecznej i oddzielnej lokalizacji. Może to być zewnętrzny dysk twardy, pamięć USB lub bezpieczna usługa przechowywania danych w chmurze.

Dlaczego tworzenie kopii zapasowych jest ważne:

Twoje dane mogą zostać nagle utracone lub naruszone z powodu:

- Awaria urządzenia (np. awaria komputera, uszkodzenie telefonu)
- Kradzieży lub utraty telefonu lub komputera
- ataków ransomware lub złośliwego oprogramowania, które blokują lub niszczą pliki
- Przypadkowego usunięcia lub sformatowania
- klęsk żywiołowych (pożar, powódź itp.)

Jak kopia zapasowa chroni przed atakami złośliwego oprogramowania:

Złośliwe oprogramowanie, takie jak oprogramowanie ransomware, może zaszyfrować pliki i zażądać zapłaty za ich odblokowanie. Jeśli masz bezpieczną kopię zapasową, nie musisz płacić okupu — możesz zresetować urządzenie i bezpiecznie przywrócić pliki z kopii zapasowej.

Podobnie wirusy i trojany mogą uszkodzić pliki lub system operacyjny. Jeśli pliki są zarchiwizowane, można ponownie zainstalować system i przywrócić ważne dane bez utraty czegokolwiek.

Najlepsze praktyki dotyczące bezpiecznych kopii zapasowych:

- Korzystaj zarówno z lokalnej kopii zapasowej, jak i kopii w chmurze: przechowuj kopię na zewnętrznym dysku twardym i w zaufanej usłudze w chmurze (takiej jak Google Drive, Dropbox, iCloud, OneDrive).
- Szyfruj wrażliwe kopie zapasowe: używaj ochrony hasłem lub szyfrowania dla wrażliwych danych.
- Twórz kopie zapasowe regularnie: Ustal harmonogram tygodniowy lub miesięczny w zależności od częstotliwości aktualizacji plików.
- Odłączaj dyski zewnętrzne, gdy nie są używane: w przypadku ataku ransomware może on również zaatakować podłączone dyski.
- Testuj kopie zapasowe: upewnij się, że system tworzenia kopii zapasowych działa, próbując od czasu do czasu przywrócić pliki.

6. Wskazówki dotyczące bezpieczeństwa danych

- Używaj silnych, unikalnych haseł (i regularnie je zmieniaj)
- Włącz uwierzytelnianie dwuskładnikowe (2FA)
- Aktualizuj oprogramowanie i programy antywirusowe
- Unikaj klikania podejrzanych linków lub załączników
- Nie udostępniaj danych osobowych przez telefon lub e-mail, chyba że zostały one zweryfikowane
- Regularnie twórz kopie zapasowe danych (w chmurze lub na zewnętrznym dysku twardym)
- Zachowaj ostrożność podczas korzystania z publicznych sieci Wi-Fi – unikaj logowania się do kont zawierających poufne informacje
- Sprawdź ustawienia prywatności w mediach społecznościowych
- Zastanów się przed opublikowaniem – raz umieszczone w Internecie informacje mogą zostać skopiowane lub wykorzystane w niewłaściwy sposób

Załącznik 10 | Jak tworzyć kopie zapasowe plików

1. Tworzenie kopii zapasowych plików na dysku zewnętrznym

Krok 1: Podłącz dysk zewnętrzny

- Podłącz zewnętrzny dysk twardy lub pamięć USB do komputera za pomocą odpowiedniego kabla lub portu.
- Upewnij się, że urządzenie zostało rozpoznane przez komputer (sprawdź folder „Ten komputer" lub „Mój komputer" w systemie Windows lub Finder w systemie Mac).

Krok 2: Wybierz pliki, które chcesz zarchiwizować

- Otwórz folder zawierający pliki, które chcesz zarchiwizować.
- Możesz wybrać konkretne pliki lub całe foldery. Aby wybrać wiele plików lub folderów, przytrzymaj klawisz Ctrl (Windows) lub Cmd (Mac) podczas klikania elementów.

Krok 3: Skopiuj pliki

- Kliknij prawym przyciskiem myszy wybrane pliki i wybierz opcję Kopiuj (lub użyj skrótu klawiaturowego **Ctrl+C** w systemie Windows lub **Cmd+C** w systemie Mac).
- Przejdź do dysku zewnętrznego w „Ten komputer" (Windows) lub Finder (Mac).
- Kliknij prawym przyciskiem myszy dysk zewnętrzny i wybierz opcję Wklej (lub użyj skrótu klawiszowego **Ctrl+V** w systemie Windows lub **Cmd+V** w systemie Mac), aby skopiować pliki.

Krok 4: Bezpieczne wyjęcie dysku zewnętrznego

- Po skopiowaniu plików należy bezpiecznie odłączyć dysk zewnętrzny, aby uniknąć uszkodzenia plików.
- W systemie Windows kliknij prawym przyciskiem myszy dysk zewnętrzny w „Ten komputer" i wybierz opcję Wyjmij.
- W systemie Mac przeciągnij ikonę dysku zewnętrznego do Kosza lub kliknij przycisk wysuwania obok dysku w Finderze.
- Na urządzeniu Apple (Mac lub iPhone) przejdź do **Ustawień** i zaloguj się przy użyciu swojego Apple ID.
- Na komputerze Mac dostęp do usługi iCloud można uzyskać, wybierając kolejno opcje **Preferencje systemowe** > **Apple ID** > **iCloud**.
- W telefonie iPhone przejdź do **Ustawienia** > [Twoje imię] > **iCloud**.

2. Tworzenie kopii zapasowych plików w usłudze w chmurze

Korzystanie z Dysku Google

Krok 1: Zaloguj się na swoje konto Google

- Otwórz przeglądarkę internetową i przejdź do Google Drive.
- Zaloguj się przy użyciu danych logowania do konta Google (lub utwórz nowe konto, jeśli jeszcze go nie masz).

Krok 2: Prześlij pliki do Google Drive

- Kliknij przycisk Nowy na lewym pasku bocznym.
- Wybierz opcję Prześlij plik lub Prześlij folder, w zależności od tego, co chcesz zarchiwizować.
- Wyszukaj pliki lub foldery, które chcesz przesłać, i kliknij Otwórz.

Krok 3: Uporządkuj swoje pliki (opcjonalnie)

- Możesz tworzyć foldery w Dysku Google, aby uporządkować kopię zapasową. Kliknij opcję Nowy > Folder, nadaj nazwę folderowi i przenieś do niego pliki, przeciągając je i upuszczając.

Krok 4: Sprawdź przesyłanie

- Upewnij się, że przesyłanie plików zostało zakończone. Podczas przesyłania w Google Drive wyświetlany jest pasek stanu.

Korzystanie z Dropbox

Krok 1: Zaloguj się na swoje konto Dropbox

- Otwórz przeglądarkę i przejdź do serwisu Dropbox.
- Zaloguj się lub utwórz nowe konto Dropbox, jeśli jeszcze go nie masz.

Krok 2: Prześlij pliki do Dropbox

- Po zalogowaniu kliknij przycisk Prześlij pliki.
- Wybierz pliki lub foldery, które chcesz zarchiwizować z komputera, i kliknij Otwórz.
- Możesz również przeciągnąć i upuścić pliki bezpośrednio na stronę Dropbox.
- Na telefonie iPhone sprawdź wykorzystanie pamięci iCloud, przechodząc do Ustawienia > [Twoje imię] > iCloud

Ważne wskazówki dotyczące tworzenia kopii zapasowych:

- Twórz kopie zapasowe regularnie: Wyrób sobie nawyk tworzenia kopii zapasowych danych co najmniej raz w tygodniu, aby mieć pewność, że nie stracisz ważnych plików.
- Korzystaj zarówno z kopii zapasowych lokalnych, jak i w chmurze: dla dodatkowego bezpieczeństwa przechowuj kopię swoich danych zarówno na zewnętrznym dysku twardym, jak i w chmurze.
- Szyfruj poufne pliki: podczas przechowywania poufnych danych (np. dokumentacji finansowej, dokumentów osobistych) rozważ ich szyfrowanie przed przesłaniem do chmury lub zapisaniem na dysku zewnętrznym.
- Testuj kopię zapasową: od czasu do czasu testuj kopię zapasową, przywracając niektóre pliki, aby upewnić się, że wszystko działa poprawnie.

Tworzenie kopii zapasowych plików ma kluczowe znaczenie dla zapewnienia bezpieczeństwa danych i możliwości ich odzyskania w przypadku awarii urządzenia, cyberataku lub przypadkowego usunięcia. Zarówno dyski zewnętrzne, jak i usługi w chmurze oferują niezawodne sposoby bezpiecznego przechowywania danych. Jeśli masz jakieś pytania, nie wahaj się poprosić o pomoc lub wsparcie w konfiguracji systemu kopii zapasowych!

Załącznik 11 | Lista kontrolna bezpieczeństwa w Internecie

1. Ochrona danych osobowych

- **Sprawdź dane osobowe, które udostępniasz w Internecie** – zawsze zachowuj ostrożność w przypadku publikowania treści w mediach społecznościowych i na innych platformach. Udostępniaj tylko niezbędne informacje.

- **Zachowaj poufność wrażliwych informacji** – nigdy nie udostępniaj haseł, kodów PIN, numerów kont bankowych ani numerów identyfikacyjnych w Internecie.

- **Używaj silnych, unikalnych haseł** do swoich kont i regularnie je zmieniaj.

  W miarę możliwości **włącz uwierzytelnianie dwuskładnikowe** na kontach, zwłaszcza bankowych, e-mailowych i w mediach społecznościowych.

2. Rozpoznawanie oszustw

- **Bądź świadomy popularnych oszustw internetowych** – naucz się rozpoznawać oszustwa, takie jak phishing, smishing, vishing i oszustwa finansowe.

- **Sygnały ostrzegawcze wskazujące na oszustwa**:

  - Pilny język (np. „Wymagane natychmiastowe działanie!”)
  - Prośby o podanie danych osobowych, bankowych lub loginów
  - Podejrzane linki lub numery telefonów
  - Manipulacja emocjonalna lub groźby (np. „Twoje konto zostanie zamknięte”)

- **Poznaj różnicę między uzasadnionymi a fałszywymi prośbami** – przed udzieleniem odpowiedzi sprawdź autentyczność każdego otrzymanego połączenia telefonicznego, wiadomości e-mail lub wiadomości.

- **W razie wątpliwości zawsze kontaktuj się bezpośrednio z organizacją,** korzystając z jej oficjalnych danych kontaktowych, aby zweryfikować zgłoszenie.

3. Postępowanie w przypadku oszustw i złośliwych treści

- **Nie klikaj podejrzanych linków ani nie otwieraj załączników** od nieznanych nadawców. Mogą to być próby phishingu lub zawierać złośliwe oprogramowanie.

- **Zgłaszaj wszelkie podejrzane wiadomości e-mail, wiadomości lub połączenia telefoniczne** odpowiednim organom (np. SI-CERT w Słowenii).

- **Zawsze dokładnie sprawdzaj wszelkie prośby finansowe** (przelewy pieniężne, dane karty kredytowej), dzwoniąc bezpośrednio do danej osoby lub organizacji.

- **Zachowaj ostrożność w przypadku niechcianych połączeń telefonicznych**, zwłaszcza jeśli rozmówca naciska na Ciebie, abyś podał dane dotyczące pieniędzy lub dane osobowe. Odłóż słuchawkę i oddzwonij, korzystając ze znanego numeru.

4. Ochrona urządzeń przed złośliwym oprogramowaniem

- **Zainstaluj i aktualizuj oprogramowanie antywirusowe,** aby chronić swoje urządzenie przed wirusami, złośliwym oprogramowaniem i oprogramowaniem szpiegującym typu „ ”.
- **Unikaj pobierania aplikacji lub oprogramowania** z niezweryfikowanych źródeł. Korzystaj wyłącznie z oficjalnych sklepów z aplikacjami (Google Play Store, Apple App Store).
- **Regularnie twórz kopie zapasowe danych** na dysku zewnętrznym lub w usłudze w chmurze, aby zapobiec utracie danych w wyniku potencjalnego ataku.
- **Aktualizuj oprogramowanie i urządzenia**, instalując najnowsze poprawki zabezpieczeń.
- **Zachowaj ostrożność podczas korzystania z publicznych sieci Wi-Fi** – unikaj logowania się do wrażliwych kont podczas połączenia z sieciami publicznymi.

5. Bezpieczne zakupy online

- **Kupuj wyłącznie w sprawdzonych, zaufanych witrynach internetowych** – szukaj symbolu kłódki w pasku przeglądarki i „https” w adresie URL.
- **Korzystaj z bezpiecznych metod płatności**, takich jak karty kredytowe, podczas zakupów online, ponieważ zapewniają one ochronę przed oszustwami .
- Przed dokonaniem zakupu w nowym sklepie internetowym **sprawdź opinie i oceny**.

6. Twórz kopie zapasowe danych

- Regularnie **twórz kopie zapasowe ważnych plików** (dokumentów, zdjęć, kontaktów) na dysku zewnętrznym lub w usłudze w chmurze. Dzięki temu Twoje dane będą chronione przed awarią urządzenia lub atakami ransomware.
- Aby zwiększyć bezpieczeństwo, **korzystaj z niezawodnej usługi tworzenia kopii zapasowych w chmurze** (Google Drive, Dropbox, OneDrive).
- **Utwórz harmonogram tworzenia kopii zapasowych**, aby mieć pewność, że Twoje dane są zawsze aktualne i bezpieczne.

7. Bezpieczeństwo w mediach społecznościowych

- **Zachowaj ostrożność w zakresie treści udostępnianych** na platformach społecznościowych (Facebook, Instagram itp.). Unikaj udostępniania poufnych informacji, takich jak pełny adres, numer telefonu i dane finansowe .
- **Dostosuj ustawienia prywatności,** aby kontrolować, kto może zobaczyć Twoje posty i dane osobowe.
- **Nie akceptuj zaproszeń do grona znajomych** ani wiadomości od nieznajomych. Jeśli nie znasz danej osoby, bezpieczniej jest zignorować jej zaproszenie.

8. Jak radzić sobie z atakiem socjotechnicznym

- **Zachowaj spokój i nie działaj pochopnie,** jeśli otrzymasz podejrzaną wiadomość lub telefon.
- **Nigdy nie podawaj danych osobowych przez telefon, e-mail** lub **SMS-em, chyba że masz pewność co** do **tożsamości** osoby, z którą rozmawiasz.
- **Zweryfikuj tożsamość rozmówcy**, oddzwaniając pod oficjalny numer kontaktowy (np. oficjalny numer banku lub numer podany na stronie internetowej firmy).
- **Nie daj się naciskać** – oszuści często wywołują poczucie pilności, aby skłonić Cię do szybkiego działania. Nie spiesz się i zweryfikuj prośbę.

9. Reagowanie w sytuacjach awaryjnych

- **Jeśli podejrzewasz oszustwo lub Twoje dane osobowe zostały naruszone**, natychmiast skontaktuj się z bankiem lub wystawcą karty kredytowej, aby zablokować swoje konta.
- **Zgłoś oszustwo organom** takim jak SI-CERT w Słowenii lub lokalnej policji, jeśli to konieczne.
- Jeśli nie masz pewności co do sytuacji, **poproś o radę zaufanego przyjaciela lub** członka **rodziny**.

10. Bądź na bieżąco

- Bądź na bieżąco z najnowszymi oszustwami – zapisz się do newsletterów lub alertów z zaufanych źródeł, takich jak SI-CERT lub inne platformy bezpieczeństwa.
- Regularnie zdobywaj wiedzę na temat zagrożeń internetowych i sposobów ochrony przed nimi.

Pamiętaj:
Internet może być świetnym narzędziem, ale ważne jest, aby zachować czujność i być świadomym potencjalnych zagrożeń. Postępując zgodnie z tą listą kontrolną, możesz znacznie zmniejszyć swoją podatność na zagrożenia i zapewnić bezpieczeństwo swoich danych osobowych i urządzeń. Jeśli masz wątpliwości, zawsze poproś o pomoc lub radę kogoś, komu ufasz. Twoje bezpieczeństwo i spokój ducha są najważniejsze!

Załącznik 12 | Zalecenia dotyczące dalszej lektury i nauki dla uczestników

Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem:

1) **OLAF – EUROPEJSKI URZĄD DS. ZWALCZANIA NADUŻYĆ FINANSOWYCH**
   Strona internetowa: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
   OLAF jest organem UE, który zajmuje się badaniem nadużyć finansowych, korupcji i poważnych uchybień w instytucjach i funduszach UE.

2) **Victim Support Europe**
   Strona internetowa: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/
   Victim Support Europe to europejska organizacja parasolowa, która działa na rzecz praw wszystkich ofiar przestępstw i zapewnia wsparcie poprzez sieć krajowych organizacji członkowskich.

3) **EC3 – Centrum ds. Cyberprzestępczości Europolu**
   Strona internetowa: https://www.europol.europa.eu/crime-areas/cybercrime
   Europol oferuje informacje na temat cyberprzestępczości i bezpieczeństwa danych.

4) **CERT-EU (Zespół reagowania na zagrożenia komputerowe dla instytucji UE)**
   Strona internetowa: https://cert.europa.eu/
   Organizacja monitoruje zagrożenia cybernetyczne i reaguje na cyberataki na instytucje europejskie.

3.5 Moduł II – Test przed/po

1. Które z poniższych zachowań jest przykładem bezpiecznego korzystania z internetu?

A) Udostępnianie swojego adresu osobistego w mediach społecznościowych
B) Używanie silnych i unikalnych haseł do każdego konta
C) Akceptowanie zaproszeń do grona znajomych od nieznanych osób
D) Kliknięcie każdego linku, który wygląda interesująco

2. Jakie jest typowe ryzyko związane z korzystaniem z mediów społecznościowych?

A) Poznawanie nowych przyjaciół
B) Nadmiar informacji
C) Udostępnianie zbyt wielu informacji osobistych, które mogą zostać wykorzystane w niewłaściwy sposób
D) Regularne aktualizowanie ustawień prywatności

3. Dlaczego przed udostępnieniem informacji w Internecie należy zweryfikować jej źródło?

A) Aby uniknąć rozpowszechniania fałszywych informacji lub oszustw
B) Aby zwiększyć liczbę polubień i obserwujących
C) Aby poprawić wydajność komputera
D) Aby zmienić poziom bezpieczeństwa swojego profilu

4. Które z poniższych haseł jest najsilniejsze?

A) 123456
B) qwerty
C) Sunflower2025!#
D) hasło

5. Co należy zrobić, jeśli otrzymasz podejrzaną wiadomość z zhakowanego konta znajomego?

A) Kliknąć link, aby sprawdzić, co to jest
B) Zgłoś lub zablokuj konto i poinformuj znajomego
C) Odpowiedzieć, prosząc o więcej informacji
D) Całkowicie zignorować

6. Co oznacza termin „cyfrowy ślad”?

A) Całkowita ilość danych przechowywanych na komputerze
B) Zapis Twojej aktywności online i udostępnionych informacji
C) Hasło używane do logowania się na konta
D) Oprogramowanie chroniące komputer

7. Dlaczego używanie tego samego hasła do wszystkich kont jest ryzykowne?

A) Może to spowolnić logowanie
B) Jeśli jedno konto zostanie zhakowane, inne mogą zostać łatwo przejęte
C) Pozwala zaoszczędzić zbyt dużo czasu
D) Wymaga używania menedżerów haseł

8. Jaki jest najlepszy sposób ochrony prywatności w mediach społecznościowych?

A) Ustaw profil jako „publiczny”
B) Udostępnienie wszystkich danych osobowych
C) Regularnie sprawdzaj i dostosowuj ustawienia prywatności
D) Podawać prawdziwą datę urodzenia i adres w każdym poście

9. Jak rozpoznać fałszywą lub oszukańczą stronę internetową?

A) Adres zaczyna się od „https://”
B) Zawiera błędy ortograficzne i nierealne oferty
C) W przeglądarce wyświetla się symbol kłódki
D) Zawiera dane kontaktowe

10. Dlaczego należy wylogowywać się ze swoich kont na komputerach współdzielonych lub publicznych?

A) Aby zwolnić miejsce dla następnego użytkownika
B) Aby zapobiec nieautoryzowanemu dostępowi do danych
C) Aby oszczędzać energię baterii
D) Aby automatycznie zaktualizować hasło

Podsumowanie odpowiedzi

1	**B**
2	**C**
3	**A**
4	**C**
5	**B**
6	**B**
7	**B**
8	**C**
9	**B**
10	**B**

MODUŁ III

Bezpieczeństwo bankowości internetowej i zakupów online

4. Moduł III – Bezpieczeństwo bankowości internetowej i zakupów online

Celem tego modułu jest umożliwienie seniorom pewnego korzystania z bankowości internetowej i platform zakupowych poprzez przekazanie im niezbędnej wiedzy i praktycznych umiejętności w zakresie zarządzania cyfrowymi operacjami finansowymi. Moduł ten pogłębia zrozumienie uczestników na temat funkcjonowania bankowości internetowej i usług e-commerce, kładąc jednocześnie nacisk na bezpieczne i odpowiedzialne praktyki chroniące przed oszustwami, wyłudzeniami i cyberzagrożeniami.

Dzięki praktycznym wskazówkom i przykładom z życia codziennego moduł wspiera rozwój umiejętności cyfrowych i zachęca seniorów do przyjmowania bezpiecznych nawyków podczas dokonywania płatności online, zarządzania kontami i udostępniania danych osobowych. Po ukończeniu modułu uczestnicy są lepiej przygotowani do zachowania niezależności finansowej, korzystania z usług cyfrowych oraz bezpiecznego i samodzielnego korzystania z bankowości internetowej i zakupów online.

Ponadto moduł porusza kwestie typowych obaw i niepewności, których mogą doświadczać seniorzy podczas korzystania z cyfrowych usług finansowych, mając na celu zmniejszenie niepokoju związanego z transakcjami internetowymi. Uczestnicy są uczeni rozpoznawania wiarygodnych platform, stosowania podstawowych środków bezpieczeństwa i odpowiedniego reagowania na podejrzane działania. Wzmacniając pewność siebie poprzez praktykę i jasne wyjaśnienia, moduł pomaga seniorom poczuć większą kontrolę nad swoimi cyfrowymi decyzjami finansowymi i wspiera ich długoterminowe zaangażowanie w bankowość internetową i zakupy online w bezpieczny i świadomy sposób.

4.1 Cele nauczania

Głównym celem tego modułu jest wyposażenie seniorów w praktyczną wiedzę i umiejętności niezbędne do bezpiecznego korzystania z bankowości internetowej i platform handlu elektronicznego. Moduł koncentruje się na budowaniu zaufania do technologii cyfrowych przy jednoczesnym zmniejszeniu obaw i niepokoju związanych z technologią, umożliwiając uczestnikom bezpieczne i niezależne zarządzanie transakcjami finansowymi. Uczestnicy dowiedzą się, jak chronić swoje dane osobowe i finansowe, rozpoznawać zagrożenia internetowe oraz stosować skuteczne praktyki bezpieczeństwa w codziennych cyfrowych działaniach finansowych.

- Zrozumienie podstaw bankowości internetowej i handlu elektronicznego, które wspierają bezpieczną nawigację, zarządzanie kontem i transakcje cyfrowe.
- Rozwijanie umiejętności tworzenia silnych haseł i aktywowania uwierzytelniania dwuskładnikowego (2FA) w celu zwiększenia bezpieczeństwa kont internetowych.
- Rozpoznawanie wiarygodnych platform zakupowych i sprzedawców internetowych poprzez rozpoznawanie wskaźników bezpieczeństwa, takich jak HTTPS, ikony kłódki, recenzje klientów i zaufane metody płatności.
- Rozpoznawanie i unikanie oszustw internetowych i finansowych, w tym fałszywych stron internetowych, prób phishingu i zwodniczych ofert.
- Ochrona danych osobowych i finansowych, korzystając z oprogramowania antywirusowego, monitorując transakcje i ustawiając alerty dotyczące podejrzanych działań.

- Stosowanie bezpiecznych praktyk internetowych podczas korzystania z sieci publicznych, w tym zrozumienie zagrożeń związanych z publicznymi sieciami Wi-Fi i korzystanie z VPN w celu zabezpieczenia połączeń.

- Budowanie pewności siebie w zakresie technologii cyfrowych i niezależność finansową, stosując nabyte umiejętności w rzeczywistych sytuacjach związanych z bankowością internetową i zakupami online, zmniejszając niepokój i zwiększając zaufanie do narzędzi cyfrowych.

4.2 Struktura, treść i efekty uczenia się

Po pomyślnym ukończeniu tego modułu uczestnicy będą potrafili:

- Zrozumieć, jak działa bankowość internetowa, poznać zalety zarządzania kontami online i uzyskać przegląd popularnych platform bankowych.
- Poruszać się po stronach internetowych sklepów internetowych, poznać zalety zakupów online i popularnych platform.
- Ustawić silne hasła i uwierzytelnianie dwuskładnikowe (2FA): wskazówki dotyczące tworzenia silnych haseł i korzystania z 2FA w celu zwiększenia bezpieczeństwa.
- Korzystać z aplikacji i stron internetowych banków w bezpieczny sposób: korzystać wyłącznie z oficjalnych aplikacji/stron internetowych, sprawdzać, czy połączenie jest bezpieczne (https).
- Robić zakupy w zaufanych witrynach internetowych: weryfikować autentyczność witryny internetowej oraz rozumieć recenzje i oceny.
- Rozpoznawać bezpieczne opcje płatności: identyfikowanie bezpiecznych metod płatności (karty kredytowe) i unikanie niezabezpieczonych płatności (przelewy bankowe).
- Zabezpieczać urządzenia: jak korzystać z oprogramowania antywirusowego i aktualizować oprogramowanie.
- Bezpiecznie korzystać z publicznych sieci Wi-Fi do transakcji finansowych: ryzyko związane z sieciami publicznymi i korzystanie z VPN w celu zapewnienia bezpieczeństwa.

4.3 Program I Szczegółowy plan sesji

MODUŁ III
Bezpieczeństwo bankowości internetowej i zakupów online

1 sesja

Powitanie
Czas trwania 5 minut

Cele

- Przedstawienie tematu i stworzenie przyjaznej atmosfery.

Treść/metoda

- Krótkie wprowadzenie do sesji, przedstawienie celów i oczekiwań. Przygotowanie uczestników do szkolenia poprzez przedstawienie modułu i jego znaczenia.

Materiały

- Tablica lub flipchart do zapisania celów sesji.
- Markery.
- Wydrukowany plan lub slajdy prezentacji przedstawiające zarys sesji.

2 sesja

Ćwiczenie na przełamanie lodów: „Moje pierwsze doświadczenie z bankowością internetową”
Czas trwania: 10 minut

Cele

- Buduj relacje poprzez wspólne doświadczenia i wprowadź temat.

Treść/metoda

- Trener prosi uczestników o krótkie opowiedzenie o swoich pierwszych doświadczeniach z bankowością internetową, w tym o tym, co zrobili i jak się czuli. Podczas gdy uczestnicy dzielą się swoimi doświadczeniami, trener aktywnie słucha i zapisuje kluczowe uczucia i myśli na tablicy flipchart lub tablicy suchościeralnej (np. zdenerwowanie, podekscytowanie, dezorientacja), wizualnie uchwycając wspólne doświadczenia i emocje grupy. Na koniec trener krótko podsumowuje emocje i doświadczenia, którymi podzielili się uczestnicy.

Materiały

- Flipchart lub tablica do zapisywania słów kluczowych (np. zdenerwowanie, podekscytowanie), markery.

3 sesja

Wykład 1: Podstawy bankowości internetowej i zakupów online
Czas trwania 30

Cele

- Pomoc uczestnikom w zrozumieniu, jak działają bankowość internetowa i zakupy online, oraz rozróżnienie bezpiecznych i niebezpiecznych platform.

Treść/metoda

- Trener omawia przyjazne dla użytkownika przykłady, takie jak Monzo lub Revolut (bankowość) oraz Zalando lub Coolblue (zakupy), podkreślając kluczowe cechy, takie jak bezpieczeństwo, nawigacja i użyteczność. Aby utrwalić zdobytą wiedzę, uczestnicy porównują prawdziwą stronę internetową z fałszywą, wykorzystując swoją wiedzę do wykrywania oznak wiarygodności i oszustwa.
- Trener przedstawia podstawy bankowości internetowej i zakupów online, korzystając ze zrzutów ekranu i pokazów na żywo. Trener prowadzi uczestników przez prostą platformę bankową, wyjaśniając, jak działa bankowość internetowa, i pokazując im, jak sprawdzić saldo,

przelać pieniądze i korzystać z innych podstawowych funkcji. Następnie trener robi to samo w przypadku strony zakupowej, pokazując uczestnikom, jak poruszać się po platformie, wybierać produkty i kontynuować proces zakupu. Trener wyświetla dwie strony internetowe – jedną bezpieczną, a drugą fałszywą – i prosi uczestników o wskazanie, która z nich jest bezpieczna, oraz wyjaśnienie dlaczego, zachęcając ich do zastosowania swojej wiedzy na temat bezpieczeństwa stron internetowych. Na koniec trener omawia kluczowe wnioski z sesji: znaczenie sprawdzania bezpiecznych połączeń (HTTPS), rozpoznawania legalnych platform oraz sposobów unikania oszustw.

Materiały

- Prezentacja PowerPoint, materiały wizualne,
- laptop, projektor.

Ćwiczenie 1: Poznawanie platformy
Czas trwania 20 minut

Cele

- Ćwiczenie korzystania z platform internetowych i identyfikowanie kluczowych funkcji.

Treść/metoda

- Trener dzieli uczestników na pary i rozdaje każdej z nich jedną kartę z zadaniem, informując, że każda karta zawiera instrukcje dotyczące tego, na co należy zwrócić uwagę podczas ćwiczenia, np. rozpoznawanie zabezpieczeń na stronie internetowej banku lub sklepu internetowego. Po rozpoczęciu ćwiczenia trener krąży po sali, obserwując uczestników, udzielając wskazówek i odpowiadając na pytania. Trener pomaga również uczestnikom skupić się na kluczowych elementach bezpieczeństwa, takich jak ikony kłódki, ustawienia 2FA, adresy „https” lub symbole bezpiecznych płatności, aby upewnić się, że rozumieją, jak rozpoznawać funkcje bezpieczeństwa. Po zakończeniu ćwiczenia trener poprosi każdą parę o krótkie podzielenie się tym, co odkryli podczas badania. Trener zachęca do krótkiej dyskusji, zadając pytania takie jak: „Co było łatwe, a co trudne w tym zadaniu?” oraz „Co sprawiło, że uznaliście stronę internetową lub aplikację za bezpieczną lub niebezpieczną?”. Pomoże to uczestnikom zastanowić się nad swoimi doświadczeniami i pogłębić zrozumienie tego, co sprawia, że platforma internetowa jest bezpieczna.
- Na koniec trener udostępnia dodatkowe zasoby, udostępniając linki do krótkich artykułów lub filmów na temat bezpieczeństwa platform internetowych. Rozdane zostaną również materiały drukowane zawierające przykłady bezpiecznych i niebezpiecznych elementów stron internetowych/aplikacji, które posłużą jako materiały referencyjne i utrwalą wiedzę zdobytą podczas ćwiczenia.

Materiały

- Drukowane przewodniki z zadaniami dla uczestników.
- Tablety, laptopy lub duże wydrukowane zrzuty ekranu z wersjami demonstracyjnymi platform bankowych lub zakupowych.

Przerwa | Czas trwania *5 minut*

- **Daj uczestnikom czas na odpoczynek i refleksję.**
- **Krótka przerwa na odświeżenie się.**

4 sesja

Wykład 2: Bezpieczne praktyki bankowości internetowej
Czas trwania 30 minut

Cele

- Pomoc uczestnikom w tworzeniu silnych haseł i monitorowaniu kont.

Treść/metoda

- Trener rozpoczyna od prezentacji obejmującej kluczowe praktyki bezpieczeństwa w bankowości internetowej. Tematy do omówienia obejmują tworzenie silnych haseł, włączanie uwierzytelniania dwuskładnikowego (2FA) oraz konfigurowanie alertów dotyczących konta. Podczas wykładu trener przedstawi rzeczywiste przykłady lub krótkie historie dotyczące oszustw w bankowości internetowej. Korzystając z rzeczywistych przypadków oszustw, trener zwraca uwagę na typowe zagrożenia i dzieli się praktycznymi wskazówkami dotyczącymi bezpieczeństwa. Jednym z takich przypadków jest oszustwo „Safe Account" zgłoszone w Irlandii, które pomaga zilustrować, jak oszustwa działają w praktyce. Uczestnicy są zachęcani do zastosowania tych kroków na swoich urządzeniach, dzięki czemu sesja jest praktyczna, użyteczna i można od razu wprowadzić w życie.
- Trener wyjaśnia uczestnikom, dlaczego bezpieczna bankowość internetowa jest niezbędna i jak często dochodzi do naruszeń bezpieczeństwa . Podkreśla potencjalne zagrożenia i pokazuje, jak proste środki ostrożności mogą chronić uczestników przed oszustwami. Korzystając z narzędzia do sprawdzania siły hasła, trener demonstruje w czasie rzeczywistym różnicę między słabymi a silnymi hasłami. Trener prosi uczestników o podanie przykładowych haseł i testuje je na żywo, aby podkreślić znaczenie tworzenia silnych, unikalnych haseł. Następnie demonstruje, jak włączyć 2FA, korzystając ze zrzutów ekranu lub symulacji na żywo. Trener wyjaśnia rolę 2FA w zapobieganiu nieautoryzowanemu dostępowi i prowadzi uczestników przez proces jej włączania. Następnie trener wyjaśni, jak monitorować aktywność bankową i konfigurować alerty dotyczące podejrzanych transakcji. Korzystając ze zrzutów ekranu lub przykładowej aplikacji bankowej, trener przeprowadzi uczestników przez kolejne etapy konfiguracji tych alertów, podkreślając znaczenie zachowania czujności w zakresie aktywności na koncie. Podczas sesji pytań i odpowiedzi trener poprosi uczestników o podzielenie się swoimi doświadczeniami lub obawami dotyczącymi bezpieczeństwa bankowości internetowej. Na koniec trener rozda uczestnikom wydrukowane listy kontrolne podsumowujące bezpieczne nawyki związane z bankowością internetową, które będą dla nich przydatnym źródłem informacji.

Materiały

- Prezentacja, narzędzie do sprawdzania siły hasła.
- Wydrukowana lista kontrolna.

Ćwiczenie 2: Zabezpiecz swoją bankowość internetową
Czas trwania 20 minut

Cele

- Uczestnicy ćwiczą konfigurację uwierzytelniania dwuskładnikowego (2FA) i monitorowanie transakcji w symulowanym środowisku bankowym.

Treść/metoda

- Trener dzieli uczestników na pary lub małe grupy. Każda grupa będzie pracować na laptopach lub smartfonach z zainstalowanymi aplikacjami demonstracyjnymi lub platformami bankowymi, takimi jak Revolut lub Monzo. Trener prowadzi uczestników przez proces włączania 2FA: korzystając z przewodnika krok po kroku, pomaga uczestnikom zakończyć proces konfiguracji 2FA na platformie demonstracyjnej. Chodzi po sali, oferując pomoc i upewniając się, że wszyscy prawidłowo wykonują kolejne kroki. Następnie trener prosi uczestników o sprawdzenie, czy nie ma żadnych nieautoryzowanych transakcji, i pomaga im skonfigurować powiadomienia o podejrzanych działaniach. Upewnia się, że uczestnicy rozumieją proces i wykonują te czynności na platformie demonstracyjnej.
- Po zakończeniu ćwiczenia poproś każdą grupę o podzielenie się swoimi doświadczeniami: „Jakie wyzwania napotkaliście podczas konfiguracji 2FA?" „Czy udało wam się znaleźć i skonfigurować alerty transakcyjne? Które kroki były pomocne, a które trudne?" Przekazuje informacje zwrotne: Podkreśla znaczenie włączenia 2FA i monitorowania transakcji dla bezpieczeństwa bankowości internetowej.

Materiały

- Laptopy lub smartfony.
- Demo aplikacji bankowej.
- Przewodnik krok po kroku dotyczący konfiguracji 2FA i przeglądania transakcji.

Przerwa | Czas trwania *5 minut*

- **Czas na odpoczynek i przygotowanie**
- **Krótka przerwa na odświeżenie się.**

5 sesja

Wykład 3: Bezpieczne zakupy online
Czas trwania 30

Cele

- Pomoc seniorom w zrozumieniu, jak oceniać strony internetowe, identyfikować bezpieczne opcje płatności i rozpoznawać nieuczciwych sprzedawców.

Treść/metoda

- Podczas wykładu trener wyjaśnia, jak rozpoznać bezpieczne strony internetowe do zakupów online i zweryfikować autentyczność sprzedawców. Trener wyjaśnia, jak rozpoznać bezpieczne strony internetowe, skupiając się na protokole HTTPS, ikonach kłódki i innych symbolach

bezpieczeństwa. Przedstawia przykłady dobrych i złych stron internetowych, aby pokazać, jak oceniać ich wiarygodność. Trener pokazuje również, jak czytać recenzje i sprawdzać, czy sprzedawcy są autentyczni. Na koniec wykładu trener zadaje uczestnikom pytania, takie jak „Co protokół HTTPS mówi o bezpieczeństwie stron internetowych?" i „Jak sprawdzić, czy sprzedawca internetowy jest godny zaufania?", aby utrwalić kluczowe pojęcia i zaangażować uczestników.

- Na koniec trener zachęca uczestników do podzielenia się swoimi doświadczeniami związanymi z zakupami online lub obawami dotyczącymi bezpiecznych zakupów w Internecie. Omówione zostaną wszelkie wyzwania, z jakimi uczestnicy mogli się spotkać podczas zakupów online, a trener odpowie na wszelkie pytania.

Materiały

- Wydrukowane przykłady zakupów, zrzuty ekranu ze stron internetowych.

Ćwiczenie 3: Zakupy w zaufanych witrynach internetowych
Czas trwania 20 minut

Cele

- Uczestnicy uczą się, jak oceniać bezpieczeństwo sklepów internetowych i weryfikować metody płatności.

Treść/metoda

- W grupach uczestnicy najpierw zapoznają się z legalną stroną internetową sklepu, aby zidentyfikować kluczowe funkcje bezpieczeństwa (np. HTTPS, pieczęcie zaufania, bezpieczne opcje płatności). Następnie, korzystając z prezentacji lub wcześniej nagranego filmu, pokazane są im przykłady fałszywych stron internetowych lub podejrzanych działań online. Ćwiczenie koncentruje się na pomocy w rozpoznawaniu typowych znaków ostrzegawczych oraz porównywaniu bezpiecznych i niebezpiecznych stron internetowych.
- Trener dzieli uczestników na małe grupy i przekazuje im listę stron internetowych do sprawdzenia. Każda grupa ocenia strony internetowe pod kątem bezpieczeństwa, koncentrując się na takich wskaźnikach, jak protokół HTTPS, bezpieczne metody płatności i wiarygodne recenzje. Trener krąży między grupami, udzielając pomocy w razie potrzeby i oferując wskazówki, jeśli grupy potrzebują pomocy w rozpoznaniu sygnałów ostrzegawczych, takich jak podejrzane recenzje lub niebezpieczne elementy strony internetowej. Na koniec grupy dzielą się informacjami na temat stron internetowych, które zostały uznane za bezpieczne, i uzasadniają swoją ocenę.

Materiały

- Komputery z dostępem do Internetu.
- Lista stron internetowych sklepów.

Przerwa | Czas trwania 5 minut

- **Czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**

6 sesja

Wykład 4: Ochrona danych osobowych i finansowych
Czas trwania 30

Cele

- Przekazanie seniorom wiedzy na temat zabezpieczania urządzeń, korzystania z oprogramowania antywirusowego i zabezpieczania połączeń Wi-Fi.

Treść/metoda

- Trener prowadzi wykład wyjaśniający pojęcia oprogramowania antywirusowego, sieci VPN i bezpiecznego przeglądania stron internetowych. Prezentacja będzie zawierała slajdy z kluczowymi informacjami i przykładami dla każdego tematu, podkreślając najlepsze praktyki w zakresie bezpieczeństwa urządzeń. Trener pokazuje, jak aktualizować urządzenia, instalować oprogramowanie antywirusowe i zarządzać ustawieniami prywatności w celu poprawy bezpieczeństwa. Pokazuje krótki film instruktażowy demonstrujący prawidłowe korzystanie z sieci VPN w celu bezpiecznego przeglądania stron internetowych. Podczas wykładu trener zachęca uczestników do aktywnego udziału i sprawia, że sesja ma charakter interaktywny, zadając pytania i podając rzeczywiste przykłady tego, jak zachować bezpieczeństwo w Internecie. Po wykładzie uczestnicy mają możliwość zadawania pytań i wyjaśnienia wszelkich wątpliwości dotyczących bezpieczeństwa urządzeń i ochrony w Internecie.
- Na koniec trener podzieli się prostymi, codziennymi praktykami dotyczącymi ochrony danych osobowych, takimi jak unikanie podejrzanych linków, nieudostępnianie zbyt wielu informacji na stronach internetowych oraz rozpoznawanie typowych pułapek internetowych. Kroki te pomogą uczestnikom wyrobić bezpieczniejsze nawyki cyfrowe.

Materiały

- Slajdy prezentacji, film instruktażowy na temat sieci VPN.

Ćwiczenie 4: Zabezpieczanie urządzeń
Czas trwania 20 minut

Cele

- Uczestnicy ćwiczą instalowanie oprogramowania antywirusowego, korzystanie z sieci VPN i zarządzanie ustawieniami prywatności.

Treść/metoda

- Uczestnicy pracują w grupach, aby zainstalować oprogramowanie antywirusowe, włączyć VPN w celu bezpiecznego przeglądania stron internetowych oraz sprawdzić ustawienia prywatności w aplikacjach i mediach społecznościowych. To praktyczne ćwiczenie pomaga im zastosować praktyczne kroki w celu ochrony swoich urządzeń i danych osobowych w Internecie.
- Trener dzieli uczestników na małe grupy lub pary i zapewnia im laptopy, oprogramowanie antywirusowe oraz aplikacje VPN do wykorzystania podczas ćwiczenia. Każda grupa postępuje zgodnie z instrukcjami krok po kroku przekazanymi przez trenera, aby zainstalować oprogramowanie antywirusowe, włączyć VPN w celu bezpiecznego przeglądania stron

internetowych oraz sprawdzić ustawienia prywatności w aplikacjach i na kontach w mediach społecznościowych. Trener krąży między grupami, oferując pomoc w razie potrzeby i upewniając się, że wszyscy uczestnicy mogą pomyślnie wykonać zadania. Trener prowadzi również grupy przez proces identyfikacji kluczowych ustawień prywatności na ich urządzeniach i profilach w mediach społecznościowych, które zwiększają bezpieczeństwo. Po zakończeniu ćwiczenia trener prosi uczestników o podzielenie się swoimi doświadczeniami związanymi z zabezpieczaniem urządzeń i ustawieniami prywatności.

Materiały

- Laptopy, oprogramowanie antywirusowe, aplikacja VPN

7 sesja

Dyskusja | Czas trwania 10 minut

Cele

- Zastanów się nad najważniejszymi wnioskami z sesji i wyjaśnij wszelkie wątpliwości.

Treść/metoda

- Dyskusja grupowa, podczas której uczestnicy dzielą się swoimi doświadczeniami i wnioskami. Trener odpowiada na wszelkie pozostałe pytania. Zachęca uczestników do dalszego ćwiczenia umiejętności nabytych podczas sesji.

Podsumowanie
Czas trwania 5

Cele

- Podsumowanie sesji i zachęcenie uczestników do dalszego bezpiecznego ćwiczenia.

Treść/metoda

- Trener podsumowuje sesję, podkreślając najważniejsze omówione kwestie. Uczestnicy zostaną zachęceni do dalszego ćwiczenia umiejętności nabytych podczas osobistych działań online. Trener dziękuje uczestnikom za udział i zachęca ich do wykorzystania zdobytej wiedzy w celu zapewnienia sobie bezpieczeństwa w Internecie.

Materiały

- Materiały informacyjne zawierające kluczowe punkty i zasoby.

4.4 Dodatkowe informacje

4.4.1 Samoorefleksja trenerów

- Które aspekty szkolenia przebiegły szczególnie dobrze?
- Które części sesji były dla mnie największym wyzwaniem?
- Jak bardzo uczestnicy byli zaangażowani i reagowali podczas zajęć?
- Czy uczestnicy osiągnęli cele szkoleniowe? Jeśli nie, to dlaczego?
- Jakie zmiany mogłyby poprawić jakość sesji w przyszłości?

4.4.2 Ocena programu przez trenerów

- Czy treść szkolenia była dostosowana do potrzeb seniorów oraz ich poziomu wiedzy i doświadczenia w zakresie technologii cyfrowych?
- Czy uczestnicy zrozumieli podstawowe zasady bankowości internetowej, handlu elektronicznego, cyberbezpieczeństwa i prywatności w Internecie?
- Czy praktyczne ćwiczenia, quizy i pokazy były skuteczne w utrwalaniu wiedzy i budowaniu pewności w zakresie korzystania z technologii cyfrowych?
- Czy dyskusje i refleksje pozwoliły uczestnikom pogłębić zrozumienie bezpiecznych praktyk online?
- Czy osiągnięto zamierzone efekty kształcenia, takie jak umiejętność tworzenia silnych haseł, rozpoznawania fałszywych stron internetowych, monitorowania transakcji i konfigurowania ustawień bezpieczeństwa?
- Czy uczestnicy wykazali się większą pewnością siebie i niezależnością w wykonywaniu zadań związanych z bankowością internetową i zakupami online?
- Które aspekty szkolenia okazały się najbardziej skuteczne, a które obszary można by poprawić w przyszłych sesjach?

4.4.3 Materiały, dodatkowe zasoby

Załącznik 1 | Cechy silnych haseł

Aby zapewnić bezpieczeństwo kont internetowych, hasło powinno mieć następujące cechy:

- Co najmniej 8 znaków – im dłuższe, tym lepsze
- Mieszanka wielkich i małych liter
- Kombinacja liter i cyfr
- Co najmniej jeden znak specjalny, np. !, @, #, ?,]
- Uwaga: nie używaj znaków < lub > w haśle, ponieważ mogą one powodować problemy w przeglądarkach internetowych
- Szczegółowe informacje znajdują się poniżej!

Bezpieczeństwo bankowości internetowej i zakupów online
Cechy silnych haseł
Dlaczego silne hasła są ważne

Tworzenie silnych haseł jest kluczowym krokiem w ochronie danych osobowych i zawodowych. Słabe hasła ułatwiają hakerom dostęp do kont.

Aby stworzyć bezpieczne hasła, należy stosować się do poniższych wytycznych:

<u>Cechy silnych haseł</u>

- Co najmniej 8 znaków – im dłuższe, tym lepsze.
- Kombinacja wielkich i małych liter.
- Mieszanka liter i cyfr.
- Co najmniej jeden znak specjalny, taki jak: !, @, #, ?,].
- Unikaj używania znaków < lub > w haśle, ponieważ mogą one powodować problemy w niektórych przeglądarkach internetowych.
- Dodatkowe wskazówki
- Nie używaj danych osobowych (takich jak imię i nazwisko lub data urodzenia).
- Używaj unikalnego hasła dla każdego konta.
- Rozważ użycie zaufanego menedżera haseł.
- Regularnie zmieniaj hasła i unikaj ponownego używania starych.

Sekcja ćwiczeniowa (opcjonalna)
Utwórz silne hasło przykładowe, korzystając z powyższych wskazówek:

Oceń siłę swojego hasła:

SŁABE	PRZYZWOITE	MOCNE

Załącznik 2 | Instrukcje krok po kroku dotyczące uwierzytelniania dwuskładnikowego (2FA) i alertów

Część I: *Konfiguracja uwierzytelniania dwuskładnikowego (2FA)*

Cel: *2FA zapewnia dodatkowe bezpieczeństwo, wymagając zarówno hasła, jak i drugiej metody weryfikacji (np. kodu wysłanego na telefon).*

Kroki:

1. *Otwórz demonstracyjną aplikację lub platformę bankową na swoim urządzeniu.*
2. *Przejdź do Ustawienia → Ustawienia zabezpieczeń.*
3. *Naciśnij Włącz uwierzytelnianie dwuskładnikowe (2FA).*
4. *Wybierz metodę weryfikacji:*
   - *Kod SMS*
   - *Aplikacja uwierzytelniająca (np. Google Authenticator)*
5. *Postępuj zgodnie z instrukcjami (wprowadź otrzymany kod weryfikacyjny).*
6. *Sprawdź, czy 2FA działa.*

Część 2*: Przeglądaj transakcje i konfiguruj powiadomienia*

Cel: *Monitorowanie transakcji i konfigurowanie alertów pomaga wcześnie wykrywać podejrzane działania.*

Kroki:

7. *Przejdź do historii transakcji w aplikacji.*
8. *Przejrzyj ostatnie transakcje.*
9. *Zidentyfikuj i oznacz wszystkie nieznane transakcje.*
10. *Przejdź do ustawień powiadomień lub alertów.*
11. *Włącz alerty dla:*
    - *Duże lub nietypowe transakcje*
    - *Logowania z nowych urządzeń*
    - *Zmiany w ustawieniach konta*

Najważniejsze przypomnienia

- *Włącz 2FA we wszystkich aplikacjach finansowych.*
- *Regularnie sprawdzaj historię transakcji.*
- *Korzystaj z alertów, aby otrzymywać powiadomienia o nietypowej aktywności.*

Załącznik 3 | Rozpoznawanie elementów bezpieczeństwa na platformach bankowych i platformach zakupów online

Zadanie 1. Znajdź saldo konta

Spróbuj znaleźć miejsce, w którym można sprawdzić saldo konta.

- Gdzie się znajduje? .....
- Jak jest oznaczone (np. „Saldo", „Przegląd konta", „Dostępne środki")? .....

Zadanie 2. Znajdź opcję płatności

Spróbuj znaleźć miejsce, w którym można dokonać płatności lub sfinalizować zakup.

- Jak nazywa się ta opcja?
  ☐ Przelew
  ☐ Zapłać
  ☐ Koszyk / Realizacja zamówienia
  ☐ Inne: .....
- Czy łatwo było ją znaleźć?
  ☐ Tak
  ☐ Nie
  Dlaczego? .....

Zadanie 3. Zidentyfikuj zabezpieczenia strony internetowej

Przyjrzyj się uważnie stronie internetowej i zaznacz elementy, które wskazują, że jest ona bezpieczna.

☐ Ikona kłódki w pasku adresu przeglądarki
☐ adres zaczyna się od **https**
☐ rozpoznawalne logo systemów płatności (np. Visa, Mastercard, PayPal, BLIK)
☐ dodatkowe potwierdzenie płatności (kod SMS, aplikacja bankowa)
☐ informacje o polityce prywatności

Czy zauważyłeś coś jeszcze? .....

Zadanie 4. Poszukaj potencjalnych sygnałów ostrzegawczych

Czy zauważyłeś coś, co mogłoby wskazywać, że strona internetowa może być niebezpieczna?

☐ brak ikony kłódki
☐ podejrzany adres strony internetowej
☐ zbyt wiele wyskakujących okienek
☐ prośby o podanie zbyt wielu danych osobowych
☐ inne: .....

Zadanie 5. Sprawdź dodatkowe ustawienia zabezpieczeń

Poszukaj informacji o dodatkowej ochronie konta lub płatności.

Czy znalazłeś:
☐ uwierzytelnianie dwuskładnikowe (2FA)
☐ weryfikację SMS
☐ potwierdzenie za pośrednictwem aplikacji bankowej

Gdzie znajduje się ta opcja? .....

Podsumowanie ćwiczenia:
Co było najłatwiejszą częścią zadania? .....
Co było najtrudniejsze? .....
Co pomaga Ci rozpoznać, że strona internetowa lub aplikacja jest bezpieczna?
.....

Wniosek: Aby bezpiecznie korzystać z bankowości internetowej i platform zakupowych, należy zwracać uwagę na wskaźniki bezpieczeństwa strony internetowej, adres internetowy oraz sposób potwierdzania płatności.

Pamiętaj: Jeśli coś na stronie internetowej budzi Twoje wątpliwości lub podejrzenia, **nie wprowadzaj swoich danych osobowych i przerwij proces.**

Załącznik 4 | Zalecenia dotyczące dalszej lektury i nauki dla uczestników

Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem:

1) **Jak skonfigurować uwierzytelnianie dwuskładnikowe na wszystkich kontach internetowych**
   Strona internetowa: https://www.loginradius.com/blog/identity/how-to-setup-2fa-in-online-accounts/
   Ten kompleksowy przewodnik wyjaśnia znaczenie uwierzytelniania dwuskładnikowego (2FA) i zawiera szczegółowe instrukcje dotyczące jego konfiguracji na różnych kontach internetowych, w tym na platformach poczty elektronicznej, mediów społecznościowych i bankowości. Obejmuje on metody takie jak kody SMS, aplikacje uwierzytelniające i sprzętowe klucze bezpieczeństwa, które zwiększają bezpieczeństwo konta.
2) **Konfiguracja uwierzytelniania dwuskładnikowego | Usługi wsparcia technicznego**
   Strona internetowa: https://it.nmu.edu/docs/setting-2-factor-authentication
   Ten zasób udostępniony przez dział IT Uniwersytetu Północnego Michigan opisuje proces włączania uwierzytelniania dwuskładnikowego (2FA) w usługach NMU, takich jak MyNMU i MyUser. Oferuje wiele opcji weryfikacji, w tym aplikacje uwierzytelniające, klucze bezpieczeństwa USB i kody zapasowe, aby zapewnić bezpieczny dostęp do systemów uniwersyteckich.

3) **Bank of Ireland ostrzega przed wzrostem liczby oszustw związanych z „bezpiecznymi kontami"**
Artykuł: https://www.rte.ie/news/business/2025/0606/1517043-spike-in-safe-account-scam-warning-boi/
W tym artykule informacyjnym opisano znaczny wzrost liczby zgłoszeń dotyczących oszustw związanych z „bezpiecznymi kontami" w Irlandii, które w ciągu ostatniego tygodnia wzrosły dziesięciokrotnie. Bank of Ireland ostrzega konsumentów przed tego typu oszustwami, w których oszuści pod fałszywym pretekstem nakłaniają osoby fizyczne do przelania pieniędzy na „bezpieczne" konta, podkreślając znaczenie czujności i bezpiecznych praktyk bankowych.

4) **Krajowe Centrum Cyberbezpieczeństwa – Bezpieczne zakupy online**
Strona internetowa: https://www.ncsc.gov.uk/guidance/shopping-online-securely
Te oficjalne wytyczne rządu Wielkiej Brytanii zawierają praktyczne wskazówki dla konsumentów dotyczące bezpiecznych zakupów online. Obejmują one takie obszary, jak weryfikacja legalności sklepów internetowych, korzystanie z bezpiecznych metod płatności, ochrona danych osobowych i zgłaszanie podejrzanych działań. Najważniejsze zalecenia obejmują korzystanie z kart kredytowych do zakupów online, włączenie weryfikacji dwuetapowej oraz ostrożność w przypadku niechcianych ofert i linków.
5) **Jak stworzyć silne hasło**
Film: https://www.youtube.com/watch?v=_wQTRMBAvzg
Ten film zawiera praktyczne wskazówki dotyczące tworzenia silnych i łatwych do zapamiętania haseł. Podkreśla znaczenie stosowania kombinacji liter, cyfr i symboli, unikania typowych błędów oraz rozważenia haseł jako bezpiecznej alternatywy.
6) **TechRadar – Wirtualne sieci prywatne (VPN)**
Strona internetowa: https://www.techradar.com/vpn/virtual-private-networks
Ten kompleksowy przewodnik TechRadar omawia koncepcję wirtualnych sieci prywatnych (VPN). Wyjaśnia, jak działają sieci VPN, jakie korzyści zapewniają one w zakresie prywatności i bezpieczeństwa w Internecie, a także zawiera rekomendacje najlepszych usług VPN oparte na testach przeprowadzonych przez ekspertów.

4.5 Moduł III – Test przed/po

1. Co oznacza „HTTPS” w adresie strony internetowej?

A) Strona internetowa jest hostowana w innym kraju
B) Witryna jest bezpieczna, a dane są szyfrowane
C) Witryna oferuje zniżki
D) Witryna wymaga logowania

2. Dlaczego ważne jest stosowanie uwierzytelniania dwuskładnikowego (2FA) w bankowości internetowej?

A) Przyspiesza transakcje internetowe
B) Pozwala na logowanie się z wielu urządzeń jednocześnie
C) Zapewnia dodatkową warstwę bezpieczeństwa, wymagając dwóch etapów weryfikacji
D) Zastępuje konieczność podawania hasła

3. Jaka jest główna zaleta korzystania z oprogramowania antywirusowego?

A) Przyspiesza działanie komputera
B) Chroni przed złośliwym oprogramowaniem i atakami phishingowymi
C) Pomaga zarządzać hasłami online
D) Blokuje dostęp do wszystkich stron internetowych sklepów

4. Które z poniższych haseł jest najbezpieczniejsze?

A) Zakupy2024
B) 12345678
C) Mybankpassword
D) H@ppy$hopper92!

5. Co należy zrobić, jeśli natrafisz na ofertę internetową, która wydaje się „zbyt piękna, aby była prawdziwa”?

A) Natychmiast podzielić się nią ze znajomymi
B) Kliknąć link, aby sprawdzić szczegóły
C) Unikaj jej i sprawdź stronę internetową przed podjęciem jakichkolwiek działań
D) Podaj swoje dane, aby szybko skorzystać z oferty

6. Jaka metoda płatności jest bezpieczna podczas zakupów online?

A) Płatność kartą kredytową na bezpiecznej stronie internetowej
B) Przesłanie pieniędzy bezpośrednim przelewem bankowym
C) Podanie numeru karty w wiadomości e-mail
D) Korzystanie z dowolnej metody, jeśli strona internetowa wygląda profesjonalnie

7. Dlaczego należy unikać korzystania z publicznych sieci Wi-Fi do transakcji finansowych?

A) Jest zbyt wolna do obsługi bankowości internetowej
B) Może być niezaszyfrowana i umożliwić hakerom kradzież danych
C) Nie obsługuje bezpiecznych stron internetowych
D) Blokuje dostęp do aplikacji bankowych

8. Co oznacza ikona kłódki w pasku adresu przeglądarki?

A) Strona internetowa jest w trakcie konserwacji
B) Połączenie między Twoim urządzeniem a stroną internetową jest bezpieczne
C) Witryna wymaga plików cookie
D) Witryna nie jest godna zaufania

9. Jak rozpoznać godną zaufania stronę internetową do zakupów online?

A) Prosi o podanie hasła w wiadomości e-mail
B) Zawiera błędy ortograficzne i niejasne dane kontaktowe
C) Posiada protokół HTTPS, ikonę kłódki i zweryfikowane opinie klientów
D) Oferuje bezpłatne produkty bez konieczności dokonywania płatności

10. Co należy zrobić, aby chronić swoje urządzenie i dane finansowe?

A) Wyłączyć oprogramowanie antywirusowe, aby przyspieszyć działanie komputera
B) Aktualizować oprogramowanie i korzystać z VPN w sieciach publicznych
C) Unikać sprawdzania historii transakcji
D) Używać tego samego hasła do wszystkich kont

Podsumowanie odpowiedzi

1	**B**
2	**C**
3	**B**
4	**D**
5	**C**
6	**A**
7	**B**
8	**B**
9	**C**
10	**B**

MODUŁ IV

Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych przez seniorów

5. Moduł IV – Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych przez seniorów

Moduł „Bezpieczne korzystanie z mediów społecznościowych" wprowadza seniorów w odpowiedzialne i bezpieczne korzystanie z platform mediów społecznościowych, łącząc niezbędną wiedzę z praktycznymi wskazówkami. Uczestnicy dowiadują się, jak zakładać konta i zarządzać nimi, dostosowywać ustawienia prywatności, rozpoznawać typowe oszustwa internetowe i bezpiecznie komunikować się, co pozwala im uczestniczyć w cyfrowych przestrzeniach społecznościowych z większą pewnością siebie i kontrolą.

Moduł obejmuje praktyczne ćwiczenia, które pomagają uczestnikom rozpoznawać podejrzane wiadomości, fałszywe profile i wprowadzające w błąd linki, które często pojawiają się w mediach społecznościowych. Koncentruje się również na ochronie danych osobowych i tożsamości cyfrowej poprzez skuteczne zarządzanie prywatnością, ograniczone udostępnianie danych oraz bezpieczne praktyki związane z kontami, takie jak silne hasła i uwierzytelnianie dwuskładnikowe. Zawiera również wskazówki dotyczące bezpieczeństwa urządzeń, aktualizacji oprogramowania i bezpiecznych połączeń internetowych.

Dzięki połączeniu tych elementów moduł zapewnia seniorom nie tylko zrozumienie zagrożeń związanych z mediami społecznościowymi, ale także pozwala im rozwinąć praktyczne umiejętności skutecznego zarządzania nimi. Po ukończeniu modułu uczestnicy mają większą świadomość cyfrową, pewność siebie i umiejętność stosowania bezpiecznych praktyk w mediach społecznościowych podczas codziennych interakcji online.

5.1 Cele nauczania

Celem tego modułu jest poszerzenie wiedzy i umiejętności seniorów w zakresie bezpiecznego, odpowiedzialnego i sensownego korzystania z mediów społecznościowych. Dzięki temu szkoleniu osoby w wieku 65 lat i starsze:

- Zyskają pewność siebie w poruszaniu się po popularnych platformach mediów społecznościowych.
- Zrozumieją znaczenie ustawień prywatności i nauczą się, jak skutecznie je dostosowywać.
- Rozpoznawać i unikać typowych oszustw internetowych i zagrożeń w mediach społecznościowych.
- wyrobią sobie nawyki bezpiecznego i odpowiedzialnego udostępniania danych osobowych w Internecie
- Będą odpowiedzialnie korzystać z treści w mediach społecznościowych, dbając jednocześnie o swoje bezpieczeństwo i dobre samopoczucie.

5.2 Struktura, treść i efekty uczenia się

Po pomyślnym ukończeniu tego modułu uczestnicy będą potrafili:

- Rozpoznawać kluczowe cechy i zastosowania popularnych platform, takich jak Facebook, Instagram i LinkedIn.
- Wykazać się umiejętnością tworzenia kont w mediach społecznościowych przy użyciu bezpiecznych metod, takich jak wybór silnych haseł i włączenie uwierzytelniania dwuskładnikowego.

- Dostosowywać ustawienia prywatności w celu kontrolowania widoczności danych osobowych i postów.
- Zarządzać ustawieniami kontaktów w celu ograniczenia niechcianych wiadomości i zaproszeń do nawiązania kontaktu.
- Rozpoznawać sygnały ostrzegawcze oszustw, takich jak phishing, fałszywe profile i fałszywe linki.
- Wdrażać strategie ochrony wrażliwych danych osobowych przed złośliwymi podmiotami.
- Mosyfikować wcześniej udostępnione treści, aby dostosować je do najlepszych praktyk w zakresie bezpieczeństwa w Internecie.
- Wykształcić nawyki bezpiecznego udostępniania informacji, w tym unikaj nadmiernego udostępniania lub udostępniania wrażliwych treści.

5.3 Program I Szczegółowy plan sesji

MODUŁ IV
Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych przez seniorów

1 sesja

Powitanie
Czas trwania 5

Cele

- Przedstawienie tematu i stworzenie przyjaznej atmosfery.

Treść/metoda

- Krótkie wprowadzenie do sesji, nakreślenie celów i ustalenie oczekiwań
- Przygotowanie uczestników do szkolenia poprzez przedstawienie modułu i jego znaczenia.

Materiały

- Tablica lub flipchart do zapisania celów sesji.
- Markery.
- Wydrukowany plan lub slajdy prezentacji przedstawiające zarys sesji.

2 sesja

Ćwiczenie integracyjne: Bingo w mediach społecznościowych
Czas trwania: 5 minut

Cele

- Zachęcenie uczestników do interakcji i rozpoczęcie refleksji nad ich cyfrowymi nawykami.

Treść/metoda

- Podczas przedstawiania się uczestnicy zaznaczają terminy, które są im znane. Pierwszy uczestnik, który wypełni rząd na swojej karcie bingo, otrzyma niewielką nagrodę. Zachęci to uczestników do podzielenia się swoimi doświadczeniami z mediami społecznościowymi i zainicjuje rozmowę na temat ich cyfrowych nawyków.

Materiały

- Wydrukuj karty z popularnymi terminami związanymi z mediami społecznościowymi, takimi jak „Facebook", „Instagram", „Lubię to", „Hashtag", „Komentarz", „Obserwuj", „Profil" itp.
- Długopisy i ołówki, zakreślacze i/lub naklejki

3 sesja

Wykład 1: Przegląd mediów społecznościowych

Czas trwania *30 minut*

Cele

- Pomoc uczestnikom w zrozumieniu kluczowych funkcji i rodzajów platform mediów społecznościowych.

Treść/metoda

- Przedstawienie przeglądu popularnych platform (Facebook, Instagram, Twitter itp.) wraz z wyjaśnieniem ich podstawowych cech i funkcji. Wyjaśnienie ich cech, zalet i potencjalnych zagrożeń oraz sposobu bezpiecznego zakładania konta.

Materiały

- Slajdy prezentacji obejmujące popularne platformy mediów społecznościowych, ich cechy i zagrożenia dla bezpieczeństwa.
- Projektor i laptop do wyświetlania prezentacji.
- Materiały informacyjne podsumowujące funkcje i wskazówki dotyczące bezpieczeństwa na Facebooku, Instagramie i Twitterze.
- Połączenie internetowe do przeprowadzenia demonstracji funkcji platform na żywo.

Ćwiczenie 1: Zapoznanie się z platformą

Czas trwania: 20 minut

Cele

- Zapoznanie uczestników z nawigacją po platformach mediów społecznościowych.

Treść/metoda

- Praktyczne zapoznanie się z platformami (np. Facebook, Instagram, Twitter). Uczestnicy przećwiczą zakładanie konta w mediach społecznościowych, kładąc nacisk na bezpieczeństwo (np. wybór silnych haseł, włączenie uwierzytelniania dwuskładnikowego).

Materiały

- Komputery, tablety lub smartfony dla uczestników do zapoznania się z platformami.
- Wydrukowane przewodniki dotyczące bezpiecznego zakładania kont, w tym: *instrukcje tworzenia silnych haseł. Kroki umożliwiające włączenie uwierzytelniania dwuskładnikowego.*

Przerwa | Czas trwania *5 minut*

- **Czas na odpoczynek i refleksję dla uczestników.**
- **Krótka przerwa na odświeżenie się.**

4 sesja

Wykład 2: Ustawienia prywatności

Czas trwania *30 minut*

Cele

- Wyposażenie uczestników w umiejętności dostosowywania ustawień prywatności i ochrony danych osobowych.

Treść/metoda

- Nauczanie, jak dostosować ustawienia prywatności na platformach społecznościowych w celu ochrony danych osobowych.

Materiały

- Prezentacja slajdów wyjaśniająca ustawienia prywatności dla popularnych platform.
- Wydrukowane instrukcje krok po kroku dotyczące dostosowywania ustawień prywatności na Facebooku, Instagramie i Twitterze.
- Projektor i laptop do przeprowadzenia pokazów na żywo dotyczących ustawień prywatności.

Ćwiczenie 2: Dostosowywanie ustawień prywatności

Czas trwania *20 minut*

Cele

- Przeprowadzenie uczestników przez proces konfiguracji ustawień prywatności na platformach społecznościowych.

Treść/metoda

- Interaktywne ćwiczenie, podczas którego uczestnicy dostosowują ustawienia prywatności na swoich kontach w mediach społecznościowych.

Materiały

- Komputery, tablety lub smartfony do ćwiczeń praktycznych.
- Wstępnie utworzone konta testowe (opcjonalnie) dla uczestników nieposiadających kont osobistych.
- Wydrukowane arkusze robocze z miejscem na zapisanie wprowadzonych zmian w ustawieniach prywatności.

Przerwa | Czas trwania *5 minut*

- **Czas na odpoczynek i przygotowanie się do kolejnej sesji.**
- **Krótka przerwa na odświeżenie się.**

5 sesja

Wykład 3: Rozpoznawanie oszustw i zagrożeń internetowych w mediach społecznościowych
Czas trwania *30 minut*

Cele

- Pomoc uczestnikom w rozpoznawaniu oszustw i zagrożeń charakterystycznych dla mediów społecznościowych.

Treść/metoda

- Omówienie typowych oszustw w mediach społecznościowych, w tym phishingu, fałszywych reklam, fałszywych profili i kradzieży tożsamości.

Materiały

- Slajdy prezentacji przedstawiające przykłady oszustw, takich jak wiadomości phishingowe i fałszywe zaproszenia do grona znajomych.
- Wydrukowane materiały informacyjne zawierające szczegółowe informacje na temat typowych oszustw i sygnałów ostrzegawczych, na które należy zwrócić uwagę.
- Projektor i laptop do wyświetlania przykładów lub filmów dotyczących oszustw w mediach społecznościowych.

Ćwiczenie 3: Ćwiczenie rozpoznawania oszustw
Czas trwania 20 minut

Cele

- Rozwinięcie umiejętności rozpoznawania oszustw w mediach społecznościowych i nauczenie się, jak uniknąć padnięcia ofiarą nieuczciwych praktyk.

Treść/metoda

- Ćwiczenie grupowe, podczas którego uczestnicy identyfikują i omawiają przykłady oszustw w mediach społecznościowych, takich jak fałszywe zaproszenia do grona znajomych lub wiadomości phishingowe.

Materiały

- Karty scenariuszy z przykładami oszustw do omówienia w grupie.
- Flipchart lub tablica do zapisywania wniosków grupy.
- Markery do zapisywania odpowiedzi uczestników.

Przerwa | Czas trwania 5 minut

- **Zapewnij czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**

6 sesja

Wykład 4: Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych
Czas trwania *30 minut*

Cele

- Wyjaśnienie znaczenia bezpiecznego i odpowiedzialnego korzystania z mediów społecznościowych
- Nauczyć uczniów, jak rozwijać bezpieczne nawyki związane z udostępnianiem treści.

Treść/metoda

- Prezentacja *„Dlaczego bezpieczeństwo w Internecie jest ważne dla osób prywatnych i profesjonalistów?”*. Przykłady potencjalnych zagrożeń wynikających z niebezpiecznych praktyk związanych z udostępnianiem informacji (np. kradzież tożsamości, utrata reputacji). Przedstawienie uczniom hipotetycznych scenariuszy (np. udostępnianie planów wakacyjnych lub osiągnięć zawodowych). Pytanie: *„Co byście udostępnili? Jak udostępnilibyście to w bezpieczny sposób?*”. Dyskusja grupowa na temat odpowiedzi.

Materiały

- Slajdy ze statystykami dotyczącymi zagrożeń w Internecie.
- Infografika podsumowująca kluczowe zagrożenia i konsekwencje niebezpiecznych praktyk.

Ćwiczenie 4: Przeglądanie poprzednich postów i informacji
Czas trwania *20 minut*

Cele

- Umożliwienie uczniom oceny i modyfikacji swoich profili i postów w mediach społecznościowych pod kątem bezpieczeństwa.

Treść/metoda

- Przeprowadzenie audytu przykładowego profilu w mediach społecznościowych (fikcyjny lub anonimowy przykład). Zidentyfikowanie niebezpiecznych lub zbyt osobistych treści (np. numery telefonów, lokalizacje, wrażliwe zdjęcia). Pokazanie, jak usuwać lub modyfikować posty oraz dostosowywać ustawienia prywatności.

Materiały

- Przykładowy profil w mediach społecznościowych (w wersji drukowanej lub na ekranie).
- Przewodnik krok po kroku dotyczący dostosowywania ustawień prywatności (PDF lub materiały informacyjne).

7 sesja

Dyskusja | Czas trwania 10 minut

Cele

- Zachęcanie do proaktywnego podejścia w rozpoznawaniu i zgłaszaniu podejrzanych działań w mediach społecznościowych.

Treść/metoda

- Dyskusja grupowa na temat postępowania w przypadku podejrzanych działań w mediach społecznościowych, np. zgłaszania oszustw i rozpoznawania fałszywych kont.

Materiały

- Tablica i markery do burzy mózgów na temat sposobów zgłaszania oszustw i postępowania w przypadku podejrzanych kont.
- Wydrukowane materiały z danymi kontaktowymi do zgłaszania oszustw (np. linki do centrów pomocy platform).

Podsumowanie | Czas trwania 5 minut

Cele szkolenia

- Podsumowanie szkolenia i upewnienie się, że uczestnicy rozumieją, jak chronić się przed zagrożeniami związanymi z mediami społecznościowymi.

Treść/metoda

- Przejrzyj kluczowe punkty dotyczące oszustw i zagrożeń w mediach społecznościowych, odpowiedz na pozostałe pytania i zapewnij zasoby do dalszej nauki.

Materiały

- Materiały informacyjne podsumowujące kluczowe punkty omówione podczas sesji: ***Lista kontrolna bezpieczeństwa w mediach społecznościowych***

5.4 Dodatkowe informacje

5.4.1 Samorefleksja trenerów

- Czy skutecznie przekazałem uczestnikom informacje na temat znaczenia bezpieczeństwa w Internecie i korzystania z mediów społecznościowych?
- Czy upewniłem się, że uczestnicy zrozumieli techniczne aspekty ustawień prywatności i rozpoznawania oszustw?
- W jaki sposób zaangażowałem uczestników w ćwiczenia i dyskusje?
- Czy zasoby i materiały były pomocne dla uczestników?

5.4.2 Ocena programu przez trenerów

- Czy treść szkolenia jest odpowiednia i zrozumiała dla seniorów?
- Czy zajęcia i dyskusje skutecznie pomogły uczestnikom w przyswojeniu materiału?
- Czy wyniki są zgodne z celami edukacyjnymi modułu?

5.4.3 Materiały, dodatkowe zasoby

Załącznik 1 | Ćwiczenie integracyjne: Bingo w mediach społecznościowych

Karta bingo mediów społecznościowych – A

Lubię	Komentarz	Facebook	Historia	Hashtag
Selfie	Wiadomość	Instagram	Tag	Profil
Emoji	Obserwujący	BEZPŁATNE	Tweet	Udostępnij
Wideo	Prywatność	LinkedIn	Status	Post
Oś czasu	Powiadomienie	Twitter	Grupa	Reels

Karta bingo mediów społecznościowych – B

Tag	Post	Instagram	Relacja	Prywatność
Wiadomość	Facebook	Oś czasu	Lubię	Grupa
Reels	Hashtag	BEZPŁATNE	Status	Komentarz
Tweet	Udostępnij	LinkedIn	Wideo	Selfie
Obserwujący	Powiadomienie	Profil	Emoji	Blokuj

Karta bingo mediów społecznościowych – C

Status	Lubię	LinkedIn	Selfie	Udostępnij
Facebook	Emoji	Instagram	Tweet	Reels
Wiadomość	Prywatność	BEZPŁATNE	Grupa	Historia
Kalendarium	Tagi	Powiadomienie	Post	Hashtag
Blok	Obserwujący	Wideo	Komentarz	Profil

Załącznik 2 I Wykład 1: Przegląd mediów społecznościowych

Prezentacja slajdów:

- **Facebook:** „Jest to najczęściej używana platforma do utrzymywania kontaktu z przyjaciółmi i rodziną. Można na niej udostępniać zdjęcia, komentować aktualizacje, dołączać do grup zainteresowań i nie tylko".
- **Instagram:** „Ta platforma skupia się na zdjęciach i filmach. Świetnie nadaje się do dzielenia się chwilami w formie wizualnej, korzystając z funkcji takich jak „Relacje", które znikają po 24 godzinach".
- **LinkedIn:** „Potraktuj tę platformę jako swoje profesjonalne CV online. Jest przydatna do poszukiwania pracy i nawiązywania kontaktów, choć nie jest powszechnie używana przez osoby starsze, chyba że nadal są aktywne zawodowo".
- **Twitter:** „Użytkownicy publikują tutaj krótkie wiadomości tekstowe zwane tweetami. Jest używany głównie do śledzenia wiadomości i osób publicznych".

Porównanie platform społecznościowych

Kategoria	Facebook	Instagram	LinkedIn	Twitter	Twitter (duplikowana kolumna)
Cel	Kontaktowanie się z przyjaciółmi i rodziną	Udostępnianie zdjęć i krótkich filmów	Nawiązywanie kontaktów zawodowych	Udostępnianie krótkich aktualności	Udostępnianie krótkich aktualizacji
Rodzaje postów	Tekst, zdjęcia, filmy, linki, relacje	Zdjęcia, filmy, relacje, historie	Aktualizacje dotyczące pracy, artykuły, CV	Tweety (tekst), zdjęcia, filmy	Publiczne, obserwujący
Komentarze i reakcje	Znajomi, grupy, publiczne	Obserwujący, publiczność	Kontakty zawodowe	Polubienia, komentarze	Polubienia, komentarze
Wiadomości	Aplikacja komunikacyjna	Lajki, komentarze	Lajki, komentarze	Lajki, komentarze, retweety	Polubienia, retweety
Ustawienia prywatności	Możliwość dostosowania: publiczne, znajomi, grupy	Ograniczone, głównie publiczne, chyba że prywatne	Domyślnie bardziej publiczne	Głównie publiczne, ograniczona kontrola	Domyślnie publiczna nazwa i posty
Widoczność profilu	Możliwość dostosowania: imię i nazwisko, zdjęcia, biografia	Ograniczona kontrola, chyba że konto prywatne	Publiczne, chyba że dostosowane domyślnie	Publiczna nazwa i dostosowane	Publiczne imię i nazwisko oraz posty domyślnie
Typowe zagrożenia	Fałszywe konta, nadmierne udostępnianie informacji, oszustwa	Oszustwa w wiadomościach prywatnych, podszywanie się pod inne osoby	Wiadomości phishingowe, podszywanie się pod inne osoby	Nękanie, fałszywe linki, podszywanie się pod inne osoby	Nękanie, fałszywe linki, podszywanie się pod inne osoby
Dobre dla	✓	✓	✓	✓	✓

Załącznik 3 | Ćwiczenie 1: Zapoznanie się z platformą

Trener prowadzi grupę krok po kroku:

„Otwórz przeglądarkę internetową i przejdź do strony www.facebook.com lub www.instagram.com".
„Kliknijcie „Utwórz nowe konto" i wprowadźcie swoje dane — imię i nazwisko, datę urodzenia itp."
„Kiedy pojawi się prośba o wybranie hasła, upewnij się, że jest ono silne. Dobre hasło ma co najmniej 8 znaków, zawiera kombinację liter i cyfr oraz symbol".

Trener dodaje:

„Na przykład zamiast „maria123" można użyć „Maria!74books".
„Teraz włączmy uwierzytelnianie dwuskładnikowe — uwierzytelnianie dwuskładnikowe (2FA) zapewnia dodatkową warstwę bezpieczeństwa. Po wprowadzeniu hasła zostaniesz poproszony o podanie kodu wysłanego na telefon komórkowy lub adres e-mail".

Załącznik 4 | Lista kontrolna konfiguracji konta, Lista kontrolna konfiguracji konta

1. Wybierz platformę (Facebook, Instagram itp.)
2. Wejdź na oficjalną stronę internetową lub pobierz oficjalną aplikację.
3. Kliknij „Utwórz nowe konto".
4. Wprowadź swoje prawdziwe imię i nazwisko oraz datę urodzenia.
5. Użyj silnego i unikalnego hasła (patrz materiał informacyjny nr 2).
6. Podaj numer telefonu komórkowego lub adres e-mail.
7. Włącz uwierzytelnianie dwuskładnikowe.
8. Pomiń niepotrzebne dane osobowe (takie jak adres).
9. Sprawdź ustawienia prywatności zaraz po utworzeniu konta.
10. Wyloguj się po zakończeniu korzystania z urządzenia publicznego lub współdzielonego.

Lista kontrolna konfiguracji konta

Silne hasło powinno:

- Mieć co najmniej 8 znaków.
- Zawierać kombinację wielkich i małych liter.
- Zawierać co najmniej jedną cyfrę i jeden znak specjalny (np. !, @, #, $).
- Unikać popularnych słów lub łatwych do odgadnięcia informacji (takich jak imię lub data urodzenia).
- Być unikalne dla każdego utworzonego konta.

Przykład słabego hasła: maria123
Przykład silnego hasła: M@r!a74Books

Załącznik 5 | Wykład 2: Ustawienia prywatności

Lista kontrolna prywatności w mediach społecznościowych

[ ] Czy sprawdziłeś ustawienia widoczności swojego profilu?

[ ] Czy Twoje posty są widoczne tylko dla „znajomych" lub „obserwujących"?

[ ] Czy włączyłeś uwierzytelnianie dwuskładnikowe na wszystkich platformach?

[ ] Czy unikasz podawania swojego numeru telefonu, adresu domowego lub pełnej daty urodzin?

[ ] Czy sprawdziłeś, kto może wysyłać Ci wiadomości lub zaproszenia do grona znajomych?

[ ] Czy sprawdzasz oznaczone zdjęcia i posty, zanim pojawią się one na Twoim profilu?

[ ] Czy zachowujesz ostrożność przy akceptowaniu nowych zaproszeń do grona znajomych lub obserwujących?

[ ] Czy usunąłeś stare posty zawierające poufne informacje?

[ ] Czy regularnie sprawdzasz swoje ustawienia prywatności?

[ ] Czy wiesz, gdzie zgłaszać oszustwa i nadużycia na każdej platformie?

Przewodnik po ustawieniach prywatności

Linki i instrukcje dotyczące dostosowania ustawień prywatności na popularnych platformach:

1. Facebook:

- Przejdź do narzędzia sprawdzającego ustawienia prywatności: https://www.facebook.com/privacy/checkup
- Centrum prywatności: https://www.facebook.com/privacy/center
- Dostosuj, kto może widzieć Twoje posty, kto może wysyłać Ci zaproszenia do grona znajomych i kto może Cię wyszukiwać.

2. Instagram:

- Przejdź do Centrum bezpieczeństwa: https://help.instagram.com/196883487377501
- Jak ustawić swoje konto na Instagramie jako prywatne: https://help.instagram.com/448523408565555
- Ustaw swoje konto jako prywatne, zarządzaj komentarzami i kontroluj tagi.

3. LinkedIn:

- Przejdź do przeglądu ustawień prywatności: https://www.linkedin.com/help/linkedin/answer/66
- Zarządzaj ustawieniami publicznego profilu LinkedIn: https://www.linkedin.com/help/linkedin/answer/83
- Wybierz, kto może zobaczyć Twoje kontakty, szczegóły profilu i aktywność.

4. Twitter (X):

- Przejdź do ustawień bezpieczeństwa: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Bezpieczeństwo i dostęp do konta: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data
- Chroń swoje tweety, ograniczaj krąg osób, które mogą wysyłać Ci wiadomości lub Cię wspominać, oraz kontroluj swoją widoczność.

Załącznik 6 | Zadanie 2: Dostosowywanie ustawień prywatności

Arkusz roboczy dotyczący dostosowania prywatności

Skorzystaj z tego arkusza, aby śledzić zmiany wprowadzane w ustawieniach prywatności w mediach społecznościowych. Po przejrzeniu swojego konta podaj poniżej szczegóły wprowadzonych zmian i powody ich wprowadzenia.

1.

Dostosowane ustawienie _____

Nowa wartość/opcja _____

Powód zmiany _____

2.

Dostosowane ustawienie _____

Nowa wartość/opcja _____

Powód zmiany _____

3.

Dostosowane ustawienie _____

Nowa wartość/opcja _____

Powód zmiany _____

4.

Dostosowane ustawienie _____

Nowa wartość/opcja _____

Powód zmiany _____

5.

Dostosowane ustawienie _____

Nowa wartość/opcja _____

Powód zmiany _____

Załącznik 7| Wykład 3: Rozpoznawanie oszustw i zagrożeń internetowych w mediach społecznościowych

Najważniejsze informacje dotyczące najczęstszych oszustw:

- **Phishing:** *„Są to fałszywe wiadomości, które mają na celu wyłudzenie danych osobowych. Na przykład wiadomość o treści: „Wygrałeś nagrodę! Kliknij tutaj, aby ją odebrać”.*
- **Fałszywe zaproszenia do grona znajomych:** *„Możesz otrzymać zaproszenie od osoby podającej się za Twojego kuzyna lub sąsiada — zawsze sprawdzaj takie wiadomości”.*
- **Podejrzane linki:** *„Mogą one zainfekować Twoje urządzenie lub wykraść hasła. Jeśli link wygląda dziwnie lub nie spodziewałeś się go — nie klikaj”.*
- **Oszustwa związane z podszywaniem się i romansami:** *„Niektóre osoby mogą nawiązać przyjaźń lub romantyczną rozmowę tylko po to, aby później poprosić o pieniądze”.*
- **Fałszywe tożsamości***: „Oszuści tworzą fałszywe profile online, aby zbudować zaufanie i manipulować ofiarami, aby te przekazały im pieniądze lub dane osobowe”.*

Załącznik 8 | Przewodnik po rozpoznawaniu oszustw

Dowiedz się, jak rozpoznać typowe oszustwa w mediach społecznościowych:

1. Wiadomości phishingowe:

- Zwróć uwagę na pilne prośby, takie jak „Twoje konto zostanie zablokowane!”.
- Sprawdź adres e-mail lub nazwę użytkownika nadawcy — czy wygląda podejrzanie?

2. Fałszywe zaproszenia do grona znajomych:

- Zachowaj ostrożność w stosunku do osób, których nie znasz.
- Zwracaj uwagę na zduplikowane profile udające osoby, które znasz.

3. Oszustwa związane z nagrodami lub loteriami:

- Wiadomości typu „Wygrałeś!” są prawie zawsze oszustwem.
- Nigdy nie podawaj swoich danych bankowych ani nie płacisz za odbiór nagrody.

4. Oszustwa związane z romansami lub przyjaźnią:

- Oszuści mogą najpierw zdobyć zaufanie, a następnie poprosić o pieniądze.
- Zachowaj ostrożność, jeśli ktoś zbyt szybko staje się zbyt osobisty.

5. Podejrzane linki:

- Nie klikaj nieznanych linków, zwłaszcza tych wysłanych w prywatnych wiadomościach.
- Zawsze sprawdzaj dokładnie i zgłaszaj podejrzane działania.

Załącznik 9 | Wskazówki dotyczące bezpieczeństwa w mediach społecznościowych

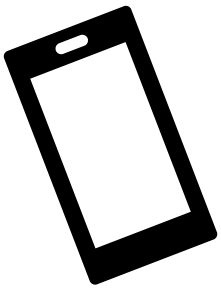
Aby zachować bezpieczeństwo w mediach społecznościowych, postępuj zgodnie z poniższymi wskazówkami:

- Ustaw swój profil jako prywatny i kontroluj, kto może widzieć Twoje posty.
- Używaj silnych, unikalnych haseł do każdego konta.
- Włącz uwierzytelnianie dwuskładnikowe, aby zapewnić dodatkowe bezpieczeństwo.
- Nie akceptuj zaproszeń do grona znajomych od nieznajomych.
- Zwracaj uwagę na to, co publikujesz – unikaj udostępniania planów podróży lub danych osobowych.
- Wyloguj się po zakończeniu korzystania z urządzeń publicznych lub współdzielonych.
- Zgłaszaj wszelkie podejrzane działania, w tym oszustwa i fałszywe konta.
- Aktualizuj aplikacje, aby chronić się przed nowymi zagrożeniami.
- Zastanów się, zanim klikniesz link lub pobierzesz plik.
- W razie wątpliwości poproś o pomoc zaufaną osobę lub zgłoś problem.

Bądź na bieżąco. Dbaj o bezpieczeństwo.

Załącznik 10 | Ćwiczenie 3: Rozpoznawanie oszustw

Scenariusz 1: Wygrałeś!



Otrzymujesz wiadomość z nieznanego konta o treści:
„Gratulacje! Wygrałeś nowy smartfon! Kliknij poniższy link, aby odebrać nagrodę”.
Wiadomość zawiera link i prośbę o podanie danych osobowych.

Scenariusz 2: Przyjaciel w tarapatach

Otrzymujesz wiadomość na Facebooku Messenger od znajomego, z którym nie rozmawiałeś od dłuższego czasu. Pisze on, że utknął za granicą i potrzebuje natychmiastowego przelewu 500 EUR.

Prosi Cię o podanie numeru telefonu i danych bankowych.

Scenariusz 3: Powiadomienie bankowe

Konto podające się za Twój bank wysyła bezpośrednią wiadomość na Instagramie:
„Wykryliśmy podejrzaną aktywność na Twoim koncie. Prosimy o natychmiastowe potwierdzenie danych logowania, odpowiadając tutaj”.
Profil konta ma jako zdjęcie logo banku.

Scenariusz 4: Oferta pracy

Otrzymujesz zaproszenie do nawiązania kontaktu na LinkedIn od osoby podającej się za rekrutera. Oferuje Ci pracę zdalną z wysokim wynagrodzeniem i elastycznymi godzinami pracy.
Po zaakceptowaniu prośby osoba ta prosi Cię o przesłanie CV, zdjęcia do dowodu osobistego i numeru ubezpieczenia społecznego.

Scenariusz 5: Lokalna grupa społecznościowa

Otrzymujesz zaproszenie do lokalnej grupy dla seniorów na Facebooku. Grupa dzieli się poradami zdrowotnymi, aktualnościami dotyczącymi wydarzeń i wiadomościami społecznościowymi. Członkowie są przyjaźni i nikt nie prosi o podanie danych osobowych.

Załącznik 11 | Wykład 4: Bezpieczne i odpowiedzialne korzystanie z mediów społecznościowych

Wytyczne dotyczące bezpiecznego udostępniania treści

Aby odpowiedzialnie udostępniać treści w mediach społecznościowych, stosuj się do poniższych wytycznych:

- Zastanów się przed opublikowaniem: czy nie miałbyś nic przeciwko, gdyby zobaczyła to osoba nieznajoma?
- Unikaj udostępniania swojej dokładnej lokalizacji, zwłaszcza w czasie rzeczywistym.
- Nie ogłaszaj długich podróży ani tego, kiedy Twój dom będzie pusty.
- Nigdy nie publikuj dokumentów osobistych, takich jak dowody tożsamości, bilety lub dane bankowe.
- Zachowaj ostrożność przy udostępnianiu zdjęć dzieci – w razie potrzeby uzyskaj zgodę.
- Korzystaj z ustawień prywatności, aby kontrolować, kto widzi Twoje posty.
- Unikaj dzielenia się wrażliwymi tematami w publicznych postach.
- Nie udostępniaj treści, gdy jesteś pod wpływem emocji – najpierw zatrzymaj się i zastanów.
- Do prywatnych rozmów używaj prywatnych wiadomości zamiast publicznych komentarzy.
- Regularnie przeglądaj swoje poprzednie posty i usuwaj wszystko, co wydaje Ci się niebezpieczne.

Pamiętaj: gdy coś trafi do sieci, trudno to cofnąć.

Załącznik 12 | Ćwiczenie 4: Przeglądanie poprzednich postów i informacji

Trener mówi:

„Teraz przejdziemy do Twoich kont w mediach społecznościowych i przejrzymy poprzednie posty lub zdjęcia. Jest to ćwiczenie zwane „cyfrowym sprzątaniem”.

Trener prowadzi uczestników przez kolejne kroki:

- *„Przejdź do swojego profilu lub osi czasu”.*
- *„Przejrzyj 3–5 starszych postów. Zadaj sobie pytanie: czy podzieliłbym się tym dzisiaj? Czy ujawnia to prywatne informacje?”.*
- *„Jeśli tak – usuńmy lub edytujmy to. Pokażę wam, jak to zrobić”.*

Trener demonstruje na ekranie lub projektorze:

- *Jak usunąć post na Facebooku*
- *Jak usunąć swoje oznaczenie ze zdjęć*
- *Jak zmienić widoczność z „Publiczna” na „Znajomi”*

Załącznik 13 | Lista kontrolna bezpieczeństwa profilu

Skorzystaj z tej listy kontrolnej, aby sprawdzić bezpieczeństwo swojego profilu w mediach społecznościowych:

[ ] Czy Twoje zdjęcie profilowe jest odpowiednie i nie pozwala na identyfikację (nie zawiera danych osobowych, takich jak adres domowy w tle)?

[ ] Czy usunąłeś lub ukryłeś datę urodzenia, numer telefonu lub adres domowy ze swojego profilu?

[ ] Czy Twoje posty są ustawione jako „Tylko znajomi" lub „Prywatne", a nie „Publiczne"?

[ ] Czy sprawdziłeś, kto może komentować lub udostępniać Twoje posty?

[ ] Czy sprawdziłeś, kto może wysyłać Ci zaproszenia do grona znajomych/obserwowania?

[ ] Czy używasz silnego, unikalnego hasła do swojego konta?

[ ] Czy masz włączone uwierzytelnianie dwuskładnikowe?

[ ] Czy regularnie przeglądasz posty i usuwasz te, które są nieaktualne lub niebezpieczne?

[ ] Czy wyłączyłeś udostępnianie lokalizacji w swoich postach?

[ ] Czy przeglądasz posty, w których zostałeś oznaczony, zanim pojawią się one na Twojej osi czasu?

Wypełniaj tę listę kontrolną co kilka miesięcy, aby zapewnić bezpieczeństwo swojego profilu.

Załącznik 14 | Lista kontrolna bezpieczeństwa w mediach społecznościowych

[ ] Używaj silnych, unikalnych haseł dla każdego konta

[ ] Włącz uwierzytelnianie dwuskładnikowe

[ ] Regularnie sprawdzaj i dostosowuj ustawienia prywatności

[ ] Zwracaj uwagę na informacje osobiste, które udostępniasz publicznie

[ ] Zastanów się przed zaakceptowaniem zaproszeń do grona znajomych lub obserwowania

[ ] Uważaj na oszustwa, phishing i podejrzane wiadomości

[ ] Zachowaj ostrożność podczas klikania linków lub pobierania treści

[ ] Zgłaszaj i blokuj podejrzanych lub obraźliwych użytkowników

[ ] Ogranicz udostępnianie lokalizacji i geotagowanie

[ ] Aktualizuj aplikacje i urządzenia

Załącznik 15 | Zalecenia dotyczące dalszej lektury i nauki dla uczestników

Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem:

1) **ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa)**
   Strona internetowa: https://www.enisa.europa.eu/
2) **CERT-EU (Zespół reagowania na incydenty komputerowe dla instytucji UE)**
   Strona internetowa: https://cert.europa.eu/
3) **EC3 – Centrum ds. Cyberprzestępczości Europolu**
   Strona internetowa: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
4) **Stay Safe Online – National Cybersecurity Alliance (USA)**
   Strona internetowa: https://staysafeonline.org/
5) **Sieć AARP Fraud Watch**
   Strona internetowa: https://www.aarp.org/money/scams-fraud/
6) **NCSC UK – Wytyczne dotyczące mediów społecznościowych**
   Strona internetowa: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/social-media
7) **NCSC UK – Wytyczne dotyczące haseł**
   Strona internetowa: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/passwords
8) **Pomoc LinkedIn – ustawienia prywatności**

   Strona internetowa: https://www.linkedin.com/help/linkedin/answer/66

5.5 Moduł IV – Test przed/po

1. Co obejmuje pojęcie „dane osobowe”?

A) Tylko Twoje posty w mediach społecznościowych
B) Wszelkie informacje, które mogą zidentyfikować użytkownika, takie jak imię i nazwisko lub numer identyfikacyjny
C) Wyłącznie dane dotyczące konta bankowego
D) Tylko hasła internetowe

2. Dlaczego warto zapoznać się z polityką prywatności?

A) Zawierają żarty na temat bezpieczeństwa danych
B) Wyjaśniają, w jaki sposób dane użytkownika będą gromadzone i wykorzystywane
C) Pomagają one w szybszym działaniu urządzenia
D) Są wymagane przez prawo, ale nie mają znaczenia

3. Które z poniższych stanowi przykład wrażliwych danych osobowych?

A) Ulubiony kolor
B) Adres zamieszkania
C) Historia medyczna lub dane biometryczne
D) Preferencje zakupowe

4. Jakie są najlepsze praktyki dotyczące udostępniania zdjęć lub informacji w Internecie?

A) Udostępniać wszystkie dane osobowe, aby być otwartym i towarzyskim
B) Przed opublikowaniem sprawdź, kto może zobaczyć te informacje
C) Często publikować posty, aby pozostać widocznym
D) Zawsze podawaj swoją lokalizację

5. Co oznacza „szyfrowanie danych”?

A) Ukrywanie plików w tajnym folderze
B) Zmiana informacji na kod w celu ochrony przed nieautoryzowanym dostępem
C) Zapisywanie plików na pendrive'ie
D) Usunięcie wszystkich starych danych

6. Dlaczego należy ograniczać ilość informacji udostępnianych w mediach społecznościowych?

A) Oszczędza dane internetowe
B) Zmniejsza ryzyko kradzieży tożsamości i oszustw
C) Zwiększa liczbę obserwujących
D) Zapobiega komentowaniu przez inne osoby

7. Co należy zrobić przed udzieleniem aplikacji dostępu do swoich danych osobowych?

A) Natychmiast wyrazić zgodę, aby szybciej korzystać z aplikacji
B) Przeczytaj uważnie uprawnienia i zezwól tylko na te niezbędne
C) Zezwolić na wszystkie uprawnienia, aby uniknąć błędów aplikacji
D) Natychmiast odinstalować aplikację

8. Jaki jest cel ogólnego rozporządzenia o ochronie danych (RODO)?

A) Pomoc firmom w gromadzeniu większej ilości danych
B) Ochrona danych osobowych i praw do prywatności osób fizycznych
C) Zapobieganie korzystaniu z mediów społecznościowych
D) Kontrolowanie aktywności zakupowej w Internecie

9. Które z poniższych działań pomaga chronić dane na wspólnym komputerze?

A) Pozostawanie zalogowanym dla wygody
B) Wylogowanie się i wyczyszczenie historii przeglądarki po zakończeniu korzystania
C) Zezwolenie przeglądarkom na zapisywanie haseł
D) Udostępnianie danych logowania członkom rodziny

10. Co należy zrobić, jeśli podejrzewasz, że Twoje dane osobowe zostały skradzione?

A) Zignorować to i mieć nadzieję, że problem sam się rozwiąże
B) Opublikować informację o tym w mediach społecznościowych
C) Zgłoś to odpowiednim organom i natychmiast zmień hasła
D) Nie robić nic, chyba że skradziono pieniądze

Podsumowanie odpowiedzi: 1-B, 2-B, 3-C, 4-B, 5-B, 6-B 7-B, 8-B, 9-B, 10-C

MODUŁ V

Bezpieczna cyfryzacja seniorów

6. Moduł V – Bezpieczna cyfryzacja seniorów

Moduł 5 koncentruje się na wyposażeniu nauczycieli w wiedzę, narzędzia i metody pracy niezbędne do skutecznego wspierania seniorów w bezpiecznym korzystaniu z technologii cyfrowych. Moduł ten zapoznaje uczestników z konkretnymi cechami i potrzebami edukacyjnymi osób starszych, szczególnie w odniesieniu do korzystania z aplikacji internetowych, usług poczty elektronicznej, platform mediów społecznościowych i narzędzi bankowości internetowej.

Duży nacisk kładzie się na cyberbezpieczeństwo, ze szczególnym uwzględnieniem minimalizacji ryzyka oszustw, wyłudzeń i dezinformacji. Uczestnicy poznają typowe zagrożenia internetowe, na jakie narażeni są seniorzy, i uczą się, jak radzić sobie z tymi zagrożeniami poprzez strategie zapobiegawcze, jasną komunikację i praktyczne wskazówki dostosowane do tej grupy wiekowej.

Ponadto moduł 5 zapewnia kompleksowe wsparcie edukacyjne w zakresie cyfryzacji seniorów, łącząc narzędzia dydaktyczne z praktycznymi ćwiczeniami. Uczestnicy rozwijają umiejętności skutecznego i empatycznego przekazywania wiedzy, reagowania na wyzwania związane z cyberbezpieczeństwem oraz projektowania dostępnych i sprzyjających środowisk edukacyjnych zarówno dla indywidualnych sesji coachingowych, jak i grupowych działań szkoleniowych.

6.1 Cele nauczania

Celem tego modułu jest umożliwienie uczestnikom nabycie umiejętności edukacyjnych i praktycznych niezbędnych do skutecznego nauczania seniorów bezpiecznego korzystania z technologii cyfrowych oraz wspierania ich w radzeniu sobie z wyzwaniami związanymi z cyberbezpieczeństwem.

- Zrozumienie specyficznych potrzeb osób starszych w zakresie cyfryzacji.
- Nauka metod nauczania dostosowanych do potrzeb seniorów.
- Nabycie umiejętności rozpoznawania typowych cyberzagrożeń skierowanych przeciwko seniorom i reagowania na nie.

6.2 Struktura, treść i efekty uczenia się

Po pomyślnym ukończeniu tego modułu uczestnicy będą potrafili:

- Zrozumieć bariery utrudniające seniorom naukę korzystania z technologii (psychologiczne, poznawcze i techniczne) oraz stosować praktyczne i przystępne metody nauczania, takie jak powtarzanie, ćwiczenia w małych krokach i proste wyjaśnienia.
- Stosować metody przekazywania zasad bezpiecznego logowania, rozpoznawania bezpiecznych stron internetowych oraz ochrony danych osobowych, wspierając seniorów w samodzielnym i bezpiecznym korzystaniu z usług online.
- Poznać najczęstsze zagrożenia internetowe, na które seniorzy są szczególnie narażeni, oraz sposoby przekazywania tej wiedzy w prosty i zrozumiały sposób, aby budować czujność seniorów.

- Rozwijać umiejętność wspierania seniorów w rozpoznawaniu zagrożeń internetowych i kształtowaniu bezpiecznych nawyków poprzez ćwiczenia praktyczne i scenariusze sytuacyjne.
- Zrozumieć jakie działania należy podjąć w sytuacji zagrożenia (np. natychmiastowa zmiana hasła, odłączenie urządzenia od sieci) oraz jakie dane i informacje są kluczowe dla ochrony użytkownika w sytuacji incydentu.
- Poznać procedury zgłaszania incydentów związanych z cyberzagrożeniami, takie jak kontakt z bankiem, policją lub specjalistycznymi organizacjami, oraz dostępne źródła wsparcia dla ofiar cyberprzestępstw.
- Zrozumieć zasady bezpieczeństwa w komunikatorach internetowych, wiadomościach e-mail oraz aplikacjach do wideorozmów, a także sposoby prowadzenia ćwiczeń dotyczących rozpoznawania zagrożeń w komunikacji online.
- Poznać podstawowe zasady ochrony urządzeń przed wirusami oraz metody przekazywania seniorom wiedzy na temat aktualizacji systemów i aplikacji w sposób prosty i zrozumiały.

6.3 Program I Szczegółowy plan sesji

MODUŁ V
Bezpieczna cyfryzacja seniorów

1 sesja

Powitanie
Czas trwania 5

Cele

- Stworzenie otwartej i angażującej atmosfery, która zachęca do aktywnego udziału.

Treść/metoda

- Powitanie uczestników, krótka prezentacja trenera. Trener przedstawia plan szkolenia i zasady pracy.

Materiały
Brak dodatkowych materiałów.

Uwagi
Pomocne może być wyjaśnienie celu warsztatów prostym językiem.

2 sesja

Ćwiczenie integracyjne
Czas trwania 15 minut

Cele

- Nawiązanie przyjaznych relacji między uczestnikami, wzajemne poznanie się i aktywizacja grupy przed rozpoczęciem części merytorycznej.

Treść/metoda

- Krótkie ćwiczenie aktywizujące, które rozpoczyna dyskusję: „Jakie wyzwania napotykają podczas nauczania seniorów nowych technologii? Jak sobie z nimi radzą?". Trener może dodać pytania pomocnicze, które będą miały wpływ na przebieg dyskusji: Co było dla Ciebie zaskakujące? Jakie metody okazały się najbardziej skuteczne? Jak można dostosować tempo lub formę zajęć do indywidualnych potrzeb uczestników? Każdy uczestnik może przedstawić jedno wyzwanie.

Materiały

Brak dodatkowych materiałów.

Uwagi

Warto zapisać odpowiedzi uczestników na tablicy lub flipcharcie, aby zidentyfikować najczęstsze trudności.

3 sesja

Wykład 1: Praktyczne wskazówki dotyczące nauczania seniorów o cyberbezpieczeństwie i nowych technologiach

Czas trwania *25 minut*

Cele

- Podniesienie świadomości nauczycieli na temat barier, z jakimi borykają się seniorzy podczas nauki korzystania z nowych technologii, oraz wyposażenie ich w skuteczne narzędzia dydaktyczne wspierające proces uczenia się.
- Przekazanie nauczycielom wiedzy i metod nauczania seniorów zasad bezpiecznego korzystania z aplikacji internetowych, wzmacniających ich poczucie bezpieczeństwa i kompetencje cyfrowe.

Treść/metoda

- Wykład podzielony jest na dwa obszary tematyczne:

Temat 1: Metody skutecznego nauczania seniorów w zakresie cyberbezpieczeństwa i nowych technologii

Treść/metody:

- Identyfikacja barier psychologicznych (np. strach przed technologią, niska pewność siebie), barier poznawczych (np. wolniejsze przetwarzanie informacji, trudności z koncentracją) i barier technicznych (brak doświadczenia w obsłudze urządzeń).
- Omówienie zasad przyjaznej komunikacji z osobami starszymi.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Praktyczne metody nauczania seniorów – materiały ćwiczeniowe dla nauczycieli (załącznik 1)

Temat 2: Przygotowanie nauczycieli do nauczania seniorów zasad bezpiecznego korzystania z aplikacji internetowych (bankowość, zakupy, serwisy społecznościowe)

Treść / Metody:

- Przegląd popularnych aplikacji internetowych używanych przez seniorów.
- Nauka rozpoznawania bezpiecznych stron internetowych i aplikacji (certyfikaty, adresy URL, wygląd formularzy logowania).
- Omówienie zasad tworzenia bezpiecznych haseł i przechowywania danych logowania.
- Ćwiczenia praktyczne na fikcyjnych kontach: logowanie, sprawdzanie bezpieczeństwa strony, symulowane zakupy online.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Ćwiczenia praktyczne – nauczanie nauczycieli zasad cyberbezpieczeństwa dla seniorów (załącznik 2)

Uwagi

Warto zapisywać odpowiedzi uczestników na tablicy lub flipcharcie, aby zidentyfikować najczęstsze trudności.

Ćwiczenie 1: Identyfikacja barier w nauce wśród osób starszych
Czas trwania 15 minut

Cele

- ❖ Zwiększenie świadomości na temat procesu uczenia się osób starszych.
- ❖ Rozpoznawanie barier w nauce wśród seniorów.

Treść/metoda

- ❖ Ćwiczenie przeprowadza się indywidualnie lub w parach – w zależności od preferencji uczestników.
- ❖ Uczestnicy otrzymują arkusze robocze (załącznik 3), które zawierają zadanie polegające na zastanowieniu się nad możliwymi barierami w procesie uczenia się seniorów.
- ❖ Uczestnicy mają za zadanie wskazać przykłady barier psychologicznych, poznawczych i technicznych, które mogą pojawić się u seniorów podczas nauki.
- ❖ Następnie proponują sposoby pokonania każdej z tych barier i opisują, w jaki sposób mogą one wpływać na proces uczenia się seniorów.
- ❖ Ćwiczenie kończy się dyskusją moderowaną przez prowadzącego, podczas której uczestnicy dzielą się swoimi wnioskami i doświadczeniami.

Materiały

- ❖ Arkusz roboczy – Identyfikacja barier w nauce osób starszych (załącznik 3)

Uwagi

Warto zachęcić uczestników do aktywnego udziału w dyskusji.

Przerwa | Czas trwania *5 minut*

- ❖ **Należy dać uczestnikom czas na odpoczynek i refleksję.**
- ❖ **Krótka przerwa na odświeżenie się.**

4 sesja

Wykład 2: Wprowadzenie do cyberbezpieczeństwa dla seniorów
Czas trwania *35 minut*

Cele

- Zapoznanie się z najczęstszymi zagrożeniami, na które szczególnie narażeni są seniorzy, oraz nauka przekazywania tej wiedzy w przystępny i skuteczny sposób, aby zwiększyć czujność seniorów i poprawić ich bezpieczeństwo w Internecie.
- Zdobycie wiedzy na temat tego, jak wspierać seniorów w rozpoznawaniu zagrożeń internetowych i jak kształtować u nich nawyki bezpiecznego korzystania z Internetu, zwiększając w ten sposób ich świadomość cyfrową.

Treść/metoda

- Wykład podzielony jest na dwa obszary tematyczne:

Temat 1: Typowe zagrożenia cyfrowe i potrzeby osób starszych

Treść/metody:

- Omówienie typowych zagrożeń internetowych, takich jak phishing, oszustwa internetowe, kradzież danych, fałszywe wiadomości.
- Identyfikacja konkretnych zagrożeń, na które osoby starsze są bardziej narażone.
- Wskazówki dotyczące skutecznego edukowania seniorów na temat tych zagrożeń bez wywoływania niepotrzebnego strachu.
- Przykłady oszustw internetowych, z którymi mogą spotkać się seniorzy, oraz sposoby ich rozpoznawania.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Bezpieczne korzystanie z Internetu przez seniorów (załącznik 4)

Temat 2: Budowanie świadomości cyfrowej wśród seniorów

Treść/metody:

- Omówienie metod wspierania seniorów w nauce rozpoznawania podejrzanych sytuacji w Internecie.
- Przykłady ćwiczeń, które pomagają seniorom zapamiętać zasady bezpieczeństwa cybernetycznego.
- Symulacje sytuacji online, w których seniorzy mogą popełniać błędy, oraz sposoby skutecznego pomagania im w nauce unikania tych błędów.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Rozpoznawanie zagrożeń w Internecie (załącznik 5)

Komentarze

Zachęć uczestników do podzielenia się doświadczeniami z pracy z seniorami oraz przykładami skutecznych metod wyjaśniania trudnych tematów.

Ćwiczenie 2: Ćwiczenie symulacyjne: rozmowa z seniorem na temat cyberbezpieczeństwa
Czas trwania *15 minut*

Cele

- Umożliwienie edukatorowi rozmowy z seniorem, pomagając mu zrozumieć, jak unikać zagrożeń internetowych.

Treść/metoda

- Zadanie jest wykonywane w parach, w których uczestnicy na zmianę wcielają się w rolę edukatora i seniora. Celem ćwiczenia jest przeprowadzenie symulowanej rozmowy edukacyjnej na temat zagrożeń w Internecie, z uwzględnieniem rzeczywistych sytuacji, z którymi mogą spotkać się seniorzy. Każda para otrzymuje opis przedstawiający konkretne zagrożenie (załącznik 6).
- Rola edukatora polega na spokojnym, zrozumiałym wyjaśnieniu, czym jest dane zagrożenie, jak je rozpoznać i jak na nie reagować. Rola seniora pozwala wcielić się w osobę, która może mieć ograniczoną wiedzę cyfrową i potrzebuje jasnych, przyjaznych instrukcji. Ćwiczenie kończy się wspólną dyskusją moderowaną przez prowadzącego, podczas której uczestnicy dzielą się swoimi odczuciami, wnioskami i refleksjami na temat skutecznej komunikacji edukacyjnej z seniorami.

Materiały

- Ćwiczenie symulacyjne: Rozmowa z seniorem na temat cyberbezpieczeństwa (załącznik 6)

Uwagi

Warto zwrócić uwagę na jasność języka i unikać żargonu technicznego.

Przerwa | Czas trwania *5 minut*

- **Zapewnij czas na odpoczynek i przygotowanie się do następnej sesji.**
- **Krótka przerwa na odświeżenie się.**

5 sesja

Wykład 3: Reagowanie na cyberzagrożenia
Czas trwania *30 minut*

Cele

- Przygotowanie nauczycieli do skutecznego przekazywania seniorom wiedzy na temat zagrożeń cyfrowych i sposobów ich unikania.
- Rozwijanie umiejętności nauczycieli w zakresie prowadzenia zajęć z seniorami na temat reagowania na zagrożenia cybernetyczne.
- Wzmocnienie kompetencji nauczycieli w zakresie stosowania metod aktywizujących i dostosowanych do potrzeb osób starszych.

Treść/metoda

- Wykład podzielony jest na dwa obszary tematyczne:

Temat 1: Kroki, które należy podjąć w przypadku podejrzenia cyberataku
Treść/metody:
Trener omawia:

- najczęstsze objawy potencjalnego cyberataku (np. dziwne zachowanie urządzenia, podejrzane wiadomości e-mail, komunikaty o błędach, nagłe wylogowania);
- podstawowe zasady bezpieczeństwa – jak reagować w przypadku podejrzenia ataku: natychmiastowe odłączenie się od sieci, zmiana haseł, nieotwieranie podejrzanych załączników lub linków;
- znaczenie zachowania spokoju i niepodejmowania pochopnych działań (np. nieoddzwanianie na nieznane numery, nieklikanie na ostrzeżenia dotyczące phishingu);
- sposoby tworzenia bezpiecznych haseł i ich aktualizowania – w tym unikanie dat urodzin i prostych kombinacji.

Temat 2: Jak zgłaszać zagrożenia cyfrowe i gdzie szukać pomocy
Treść/metody:
Trener omawia:

- instytucje i miejsca, w których można zgłaszać cyberzagrożenia (np. CERT Polska, infolinie bankowe, lokalna policja, organizacje wspierające seniorów);
- kiedy i jak skontaktować się z bankiem – np. gdy podejrzewasz przejęcie konta, nieautoryzowaną transakcję;
- jak przygotować się do zgłoszenia – zapisanie daty, godziny, treści wiadomości, zrobienie zrzutu ekranu, zapisanie podejrzanych wiadomości;
- rolę wsparcia emocjonalnego i informacyjnego – jak i gdzie go szukać (infolinie, punkty doradcze, bliscy);
- znaczenie zgłaszania prób oszustwa, nawet jeśli nie doszło do strat – dla dobra innych użytkowników.

Materiały

- Pomoce dydaktyczne dla nauczycieli: symulacje scenariuszy (załącznik 7)

Uwagi
Warto zachęcić uczestników do dyskusji.

Ćwiczenie 3: Ćwiczenie rozpoznawania oszustw
Czas trwania 20 minut

Cele

- Zdobycie wiedzy na temat tego, jak pomóc seniorom zachować spokój i opanowanie w sytuacjach zagrożenia w Internecie (np. próby oszustwa, podejrzane wiadomości e-mail, nieznane połączenia telefoniczne).
- Rozwijanie umiejętności podejmowania racjonalnych decyzji, unikania pochopnych działań i kontaktowania się z odpowiednimi osobami i instytucjami.

Treść/metoda

- Ćwiczenie polega na przeprowadzeniu symulacji rozmowy między seniorem a edukatorem.

- Uczestnicy pracują w parach, odgrywając przypisane role: edukatora i seniora. Uczestnicy mają dostęp do wskazówek i tematów symulacji (załącznik 8), które pomagają im przeprowadzić realistyczną rozmowę na temat cyberzagrożeń. Po zakończeniu symulacji prowadzący moderuje dyskusję. Każda para dzieli się swoimi refleksjami z grupą, omawiając napotkane trudności, emocje i skuteczne strategie komunikacyjne. Dyskusja pomaga lepiej zrozumieć metody wspierania seniorów w rozpoznawaniu zagrożeń i nauce odpowiedniego reagowania na nie.

Materiały

- Ćwiczenie symulacyjne: Przykładowe raporty dotyczące cyberzagrożeń (załącznik 8)

Uwagi

Ważne jest, aby nauczyciele byli dobrze przygotowani do zaangażowania seniorów i motywowania ich do aktywnego udziału w nauce, wykorzystując przykłady z ich codziennego życia.

Przerwa | Czas trwania 5 minut

- **Zapewnij czas na odpoczynek i przygotowanie się.**
- **Krótka przerwa na odświeżenie się.**
- **Krótka przerwa na odświeżenie się i relaks.**

6 sesja

Wykład 4: Edukacja seniorów w zakresie obsługi urządzeń elektronicznych i aplikacji internetowych – przewodnik dla nauczycieli

Czas trwania *20 minut*

Cele

- Wyposażenie nauczycieli w narzędzia i metody umożliwiające skuteczne nauczanie seniorów zasad bezpiecznego korzystania z aplikacji komunikacyjnych, takich jak poczta elektroniczna, komunikatory internetowe (np. Messenger, WhatsApp) i aplikacje do wideorozmów (np. Zoom).
- Przygotowanie nauczycieli do prowadzenia zajęć dotyczących ochrony urządzeń cyfrowych seniorów – od podstawowej obsługi programów antywirusowych po naukę aktualizacji systemu operacyjnego i aplikacji.

Treść/metoda

- Wykład podzielony jest na dwa obszary tematyczne:

Temat 1: Jak nauczyć seniorów bezpiecznego korzystania z aplikacji komunikacyjnych

Treść/metody:

- Sposoby wyjaśniania podstawowych funkcji aplikacji komunikacyjnych prostym, potocznym językiem.
- Przykłady ćwiczeń pomagających rozpoznawać niebezpieczne wiadomości (spam, phishing), np. analiza prawdziwych i fałszywych wiadomości e-mail.

- Praktyczne demonstracje ustawień prywatności i bezpieczeństwa w aplikacjach – blokowanie nieznanych kontaktów, zmiana haseł, ustawienia prywatności.
- Metody aktywizacji: praca z listą kontrolną, symulacje niebezpiecznych sytuacji, wspólne rozwiązywanie scenariuszy.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Jak nauczyć seniorów bezpiecznego korzystania z aplikacji komunikacyjnych (załącznik 9)

Temat 2: Jak nauczyć seniorów korzystania z programów antywirusowych i aktualizacji systemu

Treść / metody:

- Jak w przystępny sposób wyjaśnić seniorom pojęcia: wirus komputerowy, aktualizacja, skanowanie systemu.
- Ćwiczenia grupowe dotyczące instalacji i korzystania z bezpłatnych programów antywirusowych (np. Avast, AVG).
- Krok po kroku: jak pokazać seniorom, jak przeprowadzać aktualizacje systemu i aplikacji.

Materiały:

Pomoce dydaktyczne dla nauczycieli: Jak nauczyć seniorów korzystania z programów antywirusowych i aktualizacji systemu (załącznik 10)

Uwagi

Podczas dyskusji ważne jest zapewnienie wymiany pomysłów między uczestnikami.

Ćwiczenie 4: Praktyczne porady i techniki dla seniorów
Czas trwania *30 minut*

Cele

- Rozwijanie umiejętności udzielania seniorom prostych i skutecznych porad dotyczących bezpiecznego korzystania z Internetu.
- Rozwijanie umiejętności rozpoznawania i stosowania technik nauczania, które są zrozumiałe i dostępne dla seniorów.
- Dzielenie się dobrymi praktykami i prawdziwymi doświadczeniami z pracy z seniorami, które mogą stanowić inspirację dla innych nauczycieli.

Treść/metoda

- Ćwiczenie składa się z dwóch etapów pracy: indywidualnego i grupowego. W pierwszym etapie uczestnicy samodzielnie wypełniają arkusz roboczy (załącznik 11), zapisując własne refleksje, obserwacje i pomysły dotyczące skutecznych metod nauczania seniorów w zakresie cyberbezpieczeństwa. W drugim etapie uczestnicy dzielą się swoimi przemyśleniami na forum całej grupy, co ułatwia wymianę doświadczeń oraz poszukiwanie inspirujących rozwiązań i sprawdzonych praktyk. Wspólna rozmowa pozwala uzupełnić wiedzę, wzbogacić perspektywy i dostrzec różne style pracy edukacyjnej z seniorami. Na zakończenie ćwiczenia prowadzący inicjuje dyskusję mającą na celu pogłębienie tematu.

Materiały

- Arkusz roboczy: Bezpieczne korzystanie z Internetu: praktyczne wskazówki i techniki dla seniorów (załącznik 11)

Uwagi

Warto zachęcać uczestników do zadawania pytań podczas wykonywania ćwiczenia.

7 sesja

Dyskusja | Czas trwania 10 minut

Cele

- Umożliwienie uczestnikom podzielenia się doświadczeniami i spostrzeżeniami po zakończeniu sesji.
- Zidentyfikowanie wyzwań związanych z nauczaniem seniorów.
- Zainicjowanie zbiorowej burzy mózgów w celu poprawy pracy z grupami seniorów.

Treść/metoda

- Trener rozpoczyna otwartą dyskusję, zadając pytania takie jak: „Co było najtrudniejsze?”, „Które obszary wymagają dalszego rozwoju?”, „Jak można uprościć nauczanie osób starszych?”. Uczestnicy dzielą się swoimi refleksjami, praktykami i wnioskami z sesji. Wnioski zapisuje się na tablicy flipchart lub tablicy suchościeralnej, co ułatwia ich podsumowanie i ewentualne wykorzystanie w przyszłości.

Materiały

- Flipchart lub tablica
- Markery

Podsumowanie | Czas trwania 5 minut

Cele nauczania

- Podsumowanie kluczowych informacji, udzielenie odpowiedzi na ostatnie pytania uczestników i wskazanie zasobów do dalszej nauki.

Treść/metoda

- Krótkie przypomnienie najważniejszych tematów poruszonych podczas szkolenia.
- Wskazanie dodatkowych źródeł wiedzy (np. stron internetowych o charakterze edukacyjnym, materiałów wideo).
- Podziękowanie uczestnikom za udział i zakończenie sesji.

Materiały

- Pomoce dydaktyczne dla nauczycieli: strony internetowe poświęcone bezpiecznemu korzystaniu z technologii (załącznik 12).

Uwagi

Na koniec warto przeprowadzić krótką ankietę ewaluacyjną.

6.4 Dodatkowe informacje

6.4.1 Samoorefleksja trenerów

- Co było dla uczestników najtrudniejsze do zrozumienia w kwestii cyberbezpieczeństwa?
- Jakie metody okazały się najbardziej skuteczne podczas szkolenia?
- Jakie zmiany mogłyby poprawić wrażenia uczestników podczas ćwiczeń?
- Czy uczestnicy czuli się swobodnie, dzieląc się swoimi doświadczeniami i obawami dotyczącymi nauki w starszym wieku?

6.4.2 Ocena programu przez trenerów

- Czy cele szkolenia zostały osiągnięte?
- Jakie tematy wymagają rozszerzenia lub modyfikacji w przyszłości?
- Jakie techniki dydaktyczne okazały się najbardziej skuteczne w przypadku tej grupy uczestników?

6.4.3 Materiały, dodatkowe zasoby

Załącznik 1 | Praktyczne metody nauczania seniorów – materiały ćwiczeniowe dla nauczycieli

Wykonaj ćwiczenia dla nauczycieli dla każdej metody (np. stwórz przewodniki, zaproponuj analogie, zaprojektuj materiały wizualne lub opisz odpowiedzi).

Powtarzanie i ćwiczenia krok po kroku

- **Opis metody:** Krótkie, powtarzalne instrukcje, każde zadanie podzielone na proste kroki.
- **Ćwiczenie dla nauczyciela:** Opracuj przewodnik krok po kroku dotyczący logowania się do platformy mediów społecznościowych lub systemu bankowości internetowej (używając prostego i jasnego języka).
- **Cel:** Rozwinięcie umiejętności formułowania zadań w logicznej i łatwej do zrozumienia strukturze.

Wykorzystanie wizualizacji i przykładów z życia codziennego

- **Opis metody:** Łączenie abstrakcyjnych pojęć technologicznych z codziennymi doświadczeniami seniorów (np. porównanie hasła do klucza do domu).
- **Ćwiczenie dla nauczyciela:** Zaproponuj 3 analogie, które pomogą wyjaśnić seniorom następujące pojęcia: hasło, bezpieczna strona internetowa i phishing.
- **Cel:** Pomoc seniorom w zrozumieniu złożonych pojęć poprzez odniesienia do znanych im sytuacji.

Wykorzystanie materiałów drukowanych dużym drukiem

- **Opis metody:** Wykorzystanie powiększonego druku, kontrastowych kolorów, piktogramów i diagramów.
- **Ćwiczenie dla nauczyciela:** Przygotuj przykładową kartę z pomocą wizualną dla seniorów, zawierającą zasady tworzenia bezpiecznego hasła.
- **Cel:** Rozwinięcie umiejętności tworzenia materiałów dostosowanych do potrzeb wizualnych i poznawczych seniorów.

Nauczanie w tempie dostosowanym do grupy

- **Opis metody:** Obserwowanie reakcji uczestników, zadawanie pytań kontrolnych i zachowanie elastyczności w tempie lekcji.
- **Ćwiczenie dla nauczyciela:** Opisz, jak zareagowałbyś, gdyby połowa grupy nie rozumiała funkcji omawianej aplikacji – jakie kroki podjąłbyś?
- **Cel:** Rozwinięcie refleksyjnego podejścia do nauczania i elastyczności podczas pracy z grupą o zróżnicowanym tempie nauki.

  Jak korzystać z załącznika:

  Załącznik może być wykorzystywany podczas warsztatów dla edukatorów jako zestaw ćwiczeń indywidualnych i grupowych, materiał do symulowanych sesji szkoleniowych dla seniorów oraz punkt wyjścia do tworzenia dostosowanych do potrzeb planów lekcji.

Załącznik 2 | Ćwiczenia praktyczne – nauczanie nauczycieli zasad cyberbezpieczeństwa dla seniorów z program

Wykonaj zadania praktyczne dla każdego tematu (np. przejrzyj aplikacje, sprawdź bezpieczeństwo stron internetowych, utwórz bezpieczne hasła i przećwicz na kontach testowych).

Treści i metody pracy z nauczycielami:

1. Przegląd popularnych aplikacji internetowych używanych przez seniorów
   - **Zadanie dla nauczycieli:** Zapoznaj się z interfejsami aplikacji, takich jak serwisy zakupowe (np. Allegro), platformy społecznościowe (np. Facebook) i bankowość mobilna.
   - **Metoda:** Analiza zrzutów ekranu, przegląd interfejsów na urządzeniach mobilnych i komputerach.
   - **Cel:** Rozpoznanie wspólnych elementów i potencjalnych trudności napotykanych przez seniorów.

2. Nauka rozpoznawania bezpiecznych stron internetowych i aplikacji
   - **Zadanie praktyczne:** Przejrzyj 5 przykładowych stron internetowych – określ, które z nich są bezpieczne. Wskaż certyfikat SSL, ocenę adresu URL, podejrzane formularze logowania.
   - **Metoda:** Analiza porównawcza (bezpieczne vs. niebezpieczne strony internetowe), interaktywny quiz.
   - **Cel:** Nauczyć krytycznej analizy bezpieczeństwa stron internetowych.

3. Zasady tworzenia bezpiecznych haseł i przechowywania danych logowania
   - **Ćwiczenie:** Utwórz 3 bezpieczne hasła, stosując zasadę 3C (złożoność, zmienność, łatwość zapamiętania). Zaproponuj bezpieczny sposób przechowywania danych logowania (np. menedżery haseł, notatnik offline).
   - **Metoda:** Burza mózgów, dyskusja + mini-warsztaty dotyczące tworzenia haseł.
   - **Cel:** Zrozumienie i przekazanie zasad bezpieczeństwa w prosty i przekonujący sposób.

4. Ćwiczenia praktyczne z wykorzystaniem fikcyjnych kont
   - **Zadanie:** Zaloguj się do testowego konta bankowego lub sklepu internetowego (symulacja), dokonaj bezpiecznego „zakupu” i sprawdź elementy bezpieczeństwa na stronie.
   - **Metoda:** Praca w parach z komputerami/tabletami, scenariusze sytuacyjne.
   - **Cel:** Przekształcenie wiedzy teoretycznej w praktyczne umiejętności, które nauczyciele mogą przekazać seniorom.

Załącznik 3 | Arkusz roboczy: Rozpoznawanie barier w nauce osób starszych

Wypełnij arkusz roboczy, identyfikując bariery (psychologiczne, poznawcze, techniczne).

Bariery psychologiczne	Przykład	Jak rozwiązać	Wpływ na naukę
Strach przed porażką			
Brak pewności siebie			
Ograniczona motywacja			
Bariery poznawcze	Przykład	Jak rozwiązać	Wpływ na naukę
Wolniejsze zapamiętywanie			
Trudności z koncentracją			
Problemy z pamięcią krótkotrwałą			
Bariery techniczne	Przykład	Jak rozwiązać	Wpływ na naukę
Trudności w korzystaniu z technologii			
Brak doświadczenia w korzystaniu z Internetu			
Problemy z korzystaniem z nowych platform edukacyjnych			

Załącznik 4 | Bezpieczne korzystanie z Internetu przez seniorów

Przedstaw przykłady, omów rzeczywiste zagrożenia i przeprowadź interaktywne ćwiczenia, aby nauczyć seniorów bezpieczeństwa w Internecie.

1. Prezentacje z przykładami oszustw internetowych

- **Opis:** Prezentacje powinny zawierać realistyczne przykłady oszustw internetowych, których ofiarami często padają seniorzy, takich jak phishing, fałszywe aukcje lub oszukańcze wiadomości e-mail. Nauczyciele mogą przygotować slajdy lub materiały wizualne ilustrujące konkretne przypadki, pokazujące, jak rozpoznać niebezpieczne elementy.
- **Cel:** Podniesienie świadomości seniorów na temat najczęstszych zagrożeń internetowych. Nauczanie rozpoznawania oszustw i innych form nadużyć internetowych, na które seniorzy mogą być szczególnie narażeni.
- **Przykłady oszustw do omówienia:**
  Phishing: fałszywe wiadomości e-mail lub strony internetowe próbujące wykraść dane logowania.
  Oszustwa związane z aukcjami internetowymi: fałszywe oferty sprzedaży produktów.
  Fałszywe SMS-y i e-maile: wiadomości udające pochodzące od instytucji, takich jak banki.

2. Dyskusja na temat rzeczywistych zagrożeń w codziennym życiu seniorów

- **Opis:** Po przedstawieniu przykładów oszustw ważne jest, aby prowadzący dyskusję zachęcił uczestników do podzielenia się swoimi doświadczeniami i wiedzą na temat zagrożeń internetowych, z jakimi spotykają się seniorzy. Prowadzący powinni zachęcać seniorów do rozmowy o własnych doświadczeniach i trudnościach, z jakimi borykają się podczas korzystania z technologii.
- **Cel**: Zrozumienie rzeczywistych zagrożeń, na jakie narażeni są seniorzy w życiu codziennym. Zidentyfikowanie barier utrudniających seniorom korzystanie z internetu, takich jak brak umiejętności cyfrowych lub obawy związane z bezpieczeństwem.
- **Przykładowe pytania do dyskusji**
  - Z jakimi rodzajami oszustw internetowych spotkałeś się lub słyszałeś?
  - Jakie są główne obawy seniorów dotyczące bezpieczeństwa w Internecie?
  - Co stanowi największe wyzwanie dla seniorów podczas nauki korzystania z Internetu?

3. Interaktywne ćwiczenia i symulacje służące identyfikacji zagrożeń internetowych

- **Opis:** Ćwiczenia i symulacje pomagają zastosować wiedzę na temat bezpieczeństwa w Internecie w praktyce. Seniorzy mogą uczestniczyć w zajęciach, podczas których muszą zidentyfikować, które strony internetowe lub wiadomości są bezpieczne, a które mogą być niebezpieczne. Nauczyciele mogą wykorzystać przykłady, takie jak fikcyjne konto bankowe, sklep internetowy lub profil w mediach społecznościowych, aby pokazać w czasie rzeczywistym, jak rozpoznać podejrzane elementy.
- **Cel:** Poprawa umiejętności rozpoznawania zagrożeń internetowych poprzez praktyczne ćwiczenia. Rozwijanie umiejętności seniorów w zakresie podejmowania świadomych decyzji dotyczących bezpieczeństwa w Internecie.
- **Przykładowe ćwiczenia**
  - *Ćwiczenie rozpoznawania phishingu:* Uczestnicy otrzymują przykładowe wiadomości e-mail i muszą wskazać, które z nich mogą być próbami phishingu.
  - *Symulacja zakupów online:* analiza grupowa witryny e-commerce, sprawdzanie, jak rozpoznać fałszywe oferty i jakie elementy wskazują, że strona internetowa jest bezpieczna.
  - *Ocena bezpieczeństwa stron internetowych:* przegląd stron internetowych i identyfikacja podejrzanych elementów, takich jak brakujące certyfikaty SSL lub wątpliwe formularze logowania.

Załącznik 5 | Rozpoznawanie zagrożeń w Internecie

Naucz seniorów rozpoznawania zagrożeń internetowych i ćwicz z nimi obsługę wiadomości e-mail, linków i haseł.

1. Przegląd metod wspierających seniorów w rozpoznawaniu podejrzanych sytuacji w Internecie

- **Opis**

  Nauczyciele powinni stosować różne metody, które pozwolą seniorom rozpoznawać podejrzane sytuacje w Internecie. Głównym celem jest uświadomienie, że nie wszystko, co wydaje się godne zaufania, faktycznie nim jest. Jasne i proste wytyczne mogą pomóc seniorom w samodzielnej ocenie, czy dana sytuacja jest bezpieczna.

- **Metody**

- Podstawowe zasady rozpoznawania podejrzanych sytuacji: Naucz seniorów, jak rozpoznawać podejrzane wiadomości e-mail, SMS-y lub fałszywe strony internetowe. Przykłady: brak certyfikatu SSL, błędy ortograficzne w wiadomościach, niespójne adresy URL.
- Zasada „nie ufaj nieznajomym”: wspólna dyskusja na temat sytuacji, w których seniorzy mogą otrzymać podejrzane oferty (np. fałszywe możliwości inwestycyjne, wygrane w konkursach lub nieznane prośby o podanie danych osobowych).
- Edukacja poprzez analogie: Porównanie sytuacji online do scenariuszy z życia codziennego, takich jak rozpoznawanie podejrzanego sprzedawcy na targu.

2. Przykłady ćwiczeń, które pomagają seniorom zapamiętać zasady bezpieczeństwa cybernetycznego

- **Opis**

  Praktyczne ćwiczenia angażujące seniorów pomagają utrwalić zasady cyberbezpieczeństwa i ostrożne zachowanie w Internecie. Seniorzy łatwiej zapamiętują te zasady, gdy mają możliwość zastosowania ich w bezpiecznym i kontrolowanym środowisku.

- **Ćwiczenia**

- Rozpoznawanie fałszywych wiadomości e-mail: Uczestnicy otrzymują różne przykłady wiadomości e-mail (autentycznych i fałszywych). Ich zadaniem jest zidentyfikowanie, które wiadomości mogą być oszustwem, a które są bezpieczne.
- Wykrywanie niebezpiecznych linków: Seniorzy ćwiczą rozpoznawanie podejrzanych linków w wiadomościach e-mail lub SMS-ach, ucząc się, jak sprawdzić, czy adres URL jest godny zaufania.
- Ćwiczenie dotyczące bezpieczeństwa haseł: Uczestnicy tworzą przykłady silnych i słabych haseł. Uczą się zasad tworzenia bezpiecznych haseł i sposobów ich bezpiecznego przechowywania.

3. Symulacje sytuacji online, w których seniorzy mogą popełniać błędy — i jak pomóc im nauczyć się ich unikać

- **Opis**

  Symulacje online to praktyczne ćwiczenia, które pozwalają seniorom nauczyć się poprzez doświadczenie, jak rozpoznawać i unikać błędów. Symulacje pomagają uczestnikom czuć się pewniej i być bardziej świadomym podczas korzystania z internetu.

❖ **Metody**

- **Symulacja phishingu:** edukator przedstawia scenariusz, w którym senior otrzymuje wiadomość e-mail, która wygląda jak autentyczna wiadomość z banku, z prośbą o podanie danych logowania. Seniorzy uczą się, jak nie dać się oszukać i które elementy wiadomości e-mail powinny wzbudzić podejrzenia.
- **Symulacja zakupów online:** Seniorzy odwiedzają strony internetowe imitujące sklepy internetowe. Ich zadaniem jest zidentyfikowanie podejrzanych elementów, takich jak zbyt niskie ceny, brak certyfikatu SSL lub dziwne metody płatności.
- **Symulacja fałszywej informacji o wygranej:** Nauczyciele przedstawiają sytuację, w której senior otrzymuje wiadomość o wygranej w konkursie, która w rzeczywistości jest oszustwem. Seniorzy uczą się rozpoznawać takie oszustwa i reagować na nie.

Załącznik 6 | Ćwiczenie symulacyjne: Rozmowa z seniorem na temat cyberbezpieczeństwa

Przeprowadź odgrywanie ról dotyczące phishingu, oszustw, bezpieczeństwa kont i mediów społecznościowych, z przewodnictwem edukatora i praktyką seniora.

Scenariusz zadania

Nauczyciel i senior prowadzą rozmowę na temat zagrożeń internetowych, ucząc się, jak rozpoznawać i unikać ryzykownych sytuacji. Każdy scenariusz przedstawia różne typowe zagrożenia, z którymi seniorzy mogą spotkać się w Internecie.

Przykładowe tematy do omówienia podczas ćwiczenia

- Phishing (fałszywe e-maile, wiadomości)
  Jak rozpoznać phishing w wiadomościach e-mail, SMS-ach i na stronach internetowych?
  Jakie są typowe oznaki fałszywych wiadomości i linków?
- Fałszywe nagrody i oszustwa związane z konkursami
  Jakie są typowe oszustwa związane z nagrodami i wygranymi w konkursach?
  Jak należy reagować na oferty wymagające przedpłaty?
- Bezpieczeństwo kont internetowych
  Jakie są dobre praktyki w zakresie zabezpieczania kont w bankach, sklepach internetowych i mediach społecznościowych?
  Co sprawia, że hasło jest bezpieczne i dlaczego uwierzytelnianie dwuskładnikowe jest ważne?
- Bezpieczne korzystanie z mediów społecznościowych
  Jak rozpoznać fałszywe profile i oszustów w mediach społecznościowych?
  Jakie informacje należy chronić, a jakich nie należy udostępniać w Internecie?

Podział ról w ćwiczeniu (w parach)

- **Rola edukatora (trenera symulacji):**
  Zadaniem edukatora jest prowadzenie rozmowy, pomaganie seniorom w zrozumieniu zagrożeń internetowych i nauczanie ich, jak je rozpoznawać.
  Edukator powinien używać prostego i jasnego języka, cierpliwie wyjaśniać zagrożenia i zadawać pytania, aby zachęcić seniora do aktywnego udziału w rozmowie.
  Edukator jest również odpowiedzialny za przypomnienie seniorom o zasadach bezpieczeństwa w Internecie i upewnienie się, że zrozumieli oni przekazywane treści.

- **Rola seniora**
  Senior aktywnie uczestniczy w rozmowie, dzieląc się swoimi doświadczeniami związanymi z korzystaniem z Internetu. Może wyrażać wszelkie wątpliwości lub obawy dotyczące bezpieczeństwa w Internecie.
  Senior odpowiada na pytania edukatora, dzieli się swoją perspektywą i próbuje rozwiązać przedstawione problemy związane z zagrożeniami w Internecie.

❖ **Phishing (fałszywe e-maile, wiadomości)**

Jak rozpoznać phishing w wiadomościach e-mail, SMS-ach i na stronach internetowych?

Jakie są typowe oznaki fałszywych wiadomości i linków?

❖ **Fałszywe nagrody i oszustwa związane z konkursami**

Jakie są typowe oszustwa związane z nagrodami i wygranymi w konkursach?

Jak należy reagować na oferty wymagające przedpłaty?

❖ **Bezpieczeństwo kont internetowych**

Jakie są dobre praktyki w zakresie zabezpieczania kont w bankach, sklepach internetowych i mediach społecznościowych?

Co sprawia, że hasło jest bezpieczne i dlaczego uwierzytelnianie dwuskładnikowe jest ważne?

❖ **Bezpieczne korzystanie z mediów społecznościowych**

Jak rozpoznać fałszywe profile i oszustów w mediach społecznościowych?

Jakie informacje należy chronić, a jakich nie należy udostępniać w Internecie?

Załącznik 7 | Symulacje scenariuszy

Przeprowadź symulacje scenariuszy, w których seniorzy mają do czynienia z oszukańczymi połączeniami telefonicznymi, wiadomościami e-mail lub SMS-ami. Zapytaj, jak zareagowaliby, omów emocje i bezpieczne reakcje oraz przećwicz techniki uspokajające, takie jak oddychanie.

Treść ćwiczenia

Przygotowanie do ćwiczenia
Rozpocznij sesję od krótkiej dyskusji na temat znaczenia zachowania spokoju w trudnych sytuacjach. Podkreśl, że oszuści często próbują wywołać panikę lub poczucie pilności, aby wywrzeć presję na seniorach i skłonić ich do podjęcia szybkich, nieprzemyślanych decyzji.

Symulacje scenariuszy zagrożeń

- **Scenariusz 1**
  Osoba starsza odbiera telefon od „pracownika banku", który twierdzi, że jej konto zostało zablokowane i prosi ją o zainstalowanie aplikacji. Co robi osoba starsza?
- **Scenariusz 2**
  Osoba starsza otrzymuje wiadomość e-mail o wygranej w konkursie i proszona jest o podanie danych osobowych oraz kliknięcie linku. Co robi osoba starsza?
- **Scenariusz 3**
  Osoba starsza otrzymuje SMS-a z podejrzaną wiadomością o konieczności uiszczenia dodatkowej opłaty za paczkę. Co robi osoba starsza?

Po każdym scenariuszu:

- Poproś seniorów, aby krótko opowiedzieli, jak zareagowaliby w takiej sytuacji.
- Zadaj pytania refleksyjne, takie jak
  Co czujesz, gdy otrzymujesz takie wiadomości?
  Jakie emocje się pojawiają?
  Jakie myśli wpływają na Twoje decyzje?

Następnie omówcie w grupie, jakie kroki należy podjąć, aby zachować spokój:
nie panikuj, nie działaj impulsywnie, zatrzymaj się i porozmawiaj z bliską osobą, zweryfikuj informacje.

Ćwiczenie świadomości emocjonalnej:
Poproś seniorów, aby zamknęli oczy i przypomnieli sobie sytuację, w której poczuli się zagrożeni w Internecie (np. otrzymali podejrzaną wiadomość e-mail).
Zapytaj: *Jakie emocje odczuwaliście w tym momencie? Jakie sygnały wysyłało Wasze ciało (np. przyspieszone bicie serca, uczucie niepokoju)?*
Zachęć ich do znalezienia sposobów kontrolowania tych emocji w sytuacji zagrożenia, np. poprzez zastosowanie omówionych wcześniej technik oddychania.

Podsumowanie ćwiczenia:
Podkreśl, jak ważne jest, aby przed podjęciem jakichkolwiek decyzji w obliczu potencjalnego zagrożenia zrobić sobie przerwę.

Wskaż, że nie zawsze konieczne jest natychmiastowe działanie. Przed podjęciem jakichkolwiek kroków warto poprosić o pomoc lub skonsultować się z bliskimi lub specjalistami.

Wskazówki dla nauczyciela:

- **Bądź cierpliwy:** seniorzy mogą potrzebować więcej czasu, aby zrozumieć zagrożenia i odpowiednio na nie zareagować. Cierpliwie wyjaśnij każde zagrożenie i przedstaw możliwe rozwiązania.
- **Dostosuj tempo:** upewnij się, że wszyscy uczestnicy rozumieją każde ćwiczenie i mają możliwość zadawania pytań.
- **Zwracaj uwagę na emocje:** zrozumienie wpływu emocji na podejmowanie decyzji ma zasadnicze znaczenie. Dlatego ważne są ćwiczenia relaksacyjne i rozpoznawanie emocji.

Ćwicz regularnie

Sesje te powinny być regularnie powtarzane, aby seniorzy czuli się pewniej i wiedzieli, jak reagować w obliczu zagrożeń.

Załącznik 8 | Ćwiczenie symulacyjne: Przykładowe raporty dotyczące zagrożeń cyber

Przeprowadź odgrywanie ról z przykładowymi cyberzagrożeniami; wyjaśnij, zidentyfikuj ryzyko i przećwicz bezpieczne reakcje.

Scenariusz zadania

Uczestnicy pracują w parach, wcielając się w role nauczyciela i seniora.
Każda para otrzymuje opis jednego z czterech przykładowych zgłoszeń dotyczących cyberzagrożeń.
Zadaniem edukatora jest przeprowadzenie spokojnej i jasnej rozmowy edukacyjnej z seniorem, podczas której:

- wyjaśniają charakter zagrożenia,
- pomaga seniorowi zrozumieć, jak rozpoznać oznaki zagrożenia,
- współpracuje z seniorem w celu znalezienia rozwiązań i bezpiecznych reakcji na daną sytuację.

Uczestnicy mogą zamienić się rolami i pracować nad nowym raportem.

Przykłady czterech zgłoszeń dotyczących cyberzagrożeń, które mogą dotyczyć seniorów

Zgłoszenie 1: SMS z prośbą o dodatkową opłatę za paczkę

Opis sytuacji: Senior otrzymał SMS-a z informacją, że paczka czeka na dostawę, ale wymagana jest dodatkowa opłata w wysokości 2 EUR. Wiadomość zawierała podejrzany link prowadzący do nieznanej strony internetowej.

Zgłoszenie 2: Fałszywy telefon z banku

Opis sytuacji: Senior otrzymał telefon od osoby podającej się za pracownika banku. Oszust twierdził, że konto zostało zablokowane i zasugerował zainstalowanie aplikacji w celu jego ochrony.

Zgłoszenie 3: E-mail dotyczący rzekomej nagrody

Opis sytuacji: Senior otrzymał wiadomość e-mail z informacją, że wygrał konkurs. W wiadomości poproszono go o podanie danych osobowych i kliknięcie linku prowadzącego do podejrzanej strony internetowej.

Zgłoszenie 4: Przejęcie konta na Facebooku

Opis sytuacji: Znajomi seniora otrzymali dziwne wiadomości z jego konta, zawierające linki lub prośby o pożyczkę. Senior nie wysłał tych wiadomości, co sugeruje, że jego konto zostało przejęte przez oszusta.

Sugestie dla nauczycieli dotyczące rozmowy o zagrożeniach:

- **Zrozumienie sytuacji:** Używaj prostego języka i analogii, aby wyjaśnić zagrożenia. Seniorzy często lepiej rozumieją sytuacje, gdy są one przedstawione w kontekście życia codziennego (np. porównując oszustwa cybernetyczne do tradycyjnych oszustw telefonicznych).
- **Przykłady i symulacje:** Regularnie przeprowadzaj ćwiczenia z wykorzystaniem symulowanych rozmów telefonicznych lub analizując przykłady podejrzanych wiadomości e-mail. Pomaga to seniorom skuteczniej reagować na rzeczywiste zagrożenia.
- **Pomoc w zgłaszaniu incydentów:** pomóż seniorom zgłaszać cyberzagrożenia odpowiednim instytucjom, takim jak CERT Polska, banki lub policja. Można to przećwiczyć podczas sesji szkoleniowej, aby zbudować ich pewność siebie.
- **Podkreślanie znaczenia uwierzytelniania dwuskładnikowego:** udzielaj wskazówek dotyczących włączania uwierzytelniania dwuskładnikowego, które może pomóc seniorom zabezpieczyć ich konta internetowe, zwłaszcza podczas korzystania z mediów społecznościowych.
- **Zachowanie spokoju:** Nauczyciele powinni uczyć seniorów, aby zachowywali spokój w sytuacjach zagrożenia i unikali impulsywnych działań, takich jak instalowanie nieznanych aplikacji lub udostępnianie danych osobowych.
- **Edukacja w zakresie narzędzi bezpieczeństwa:** Warto wprowadzić seniorów w korzystanie z oprogramowania antywirusowego, zabezpieczanie kont internetowych i weryfikowanie wiarygodności źródeł informacji (np. sprawdzanie oficjalnych numerów telefonów banków).

Załącznik 9 | Jak nauczyć seniorów bezpiecznego korzystania z aplikacji komunikacyjnych

Naucz bezpiecznego korzystania z aplikacji prostym językiem, ćwicz z użyciem ikon i identyfikuj wiadomości spamowe lub phishingowe.

Zakres treści i metody nauczania

1. Wyjaśnienie podstawowych funkcji aplikacji komunikacyjnych w języku potocznym

Zalecenia dla nauczyciela

- Unikaj żargonu technicznego – zamiast mówić „zaloguj się na swoje konto”, powiedz „wpisz swoje imię i hasło, aby otworzyć skrzynkę pocztową”.
- Zamiast „ustawień prywatności” powiedz „miejsce, w którym możesz wybrać, kto może Cię widzieć i kto może wysyłać Ci wiadomości”.
- Używaj analogii, np. „komunikator jest jak telefon z wiadomościami i zdjęciami”.

Przykładowe ćwiczenie

- Rozdaj karty z ikonami popularnych aplikacji (np. poczta elektroniczna, WhatsApp, Messenger, Zoom).
- Poproś uczestników, aby opisali je własnymi słowami.
- Wspólnie stwórzcie prostą definicję każdej z nich.

Materiały pomocnicze

- Stwórzcie drukowany słownik prostych terminów (np. „wiadomość”, „połączenie wideo”, „załącznik”).

2. Ćwiczenia polegające na identyfikowaniu niebezpiecznych wiadomości (spam, phishing)

Zalecenia dla nauczyciela

- Zawsze używaj prawdziwych przykładów, aby pokazać zarówno bezpieczne, jak i fałszywe wiadomości.
- Omów, jak wygląda podejrzany adres e-mail, co oznacza „kliknij ten link” i jak rozpoznać oszustwo typu „wnuk za granicą”.

Przykładowe ćwiczenie

- Podziel uczestników na grupy i rozdaj im trzy wydrukowane wiadomości e-mail:
  - Prawdziwe zaproszenie do rozmowy
  - Fałszywy e-mail z linkiem do „faktury”
  - Wiadomość z błędami gramatycznymi i prośbą o podanie danych osobowych
- Zadanie: Określ, które wiadomości są podejrzane i dlaczego.

Materiały pomocnicze

- Stwórz arkusze robocze z przykładowymi wiadomościami e-mail do analizy
- Przedstaw 5 kluczowych pytań dotyczących każdej wiadomości:
  - Czy znam nadawcę?
  - Czy wiadomość ma sens?
  - Czy są w niej jakieś błędy?
  - Czy adres e-mail wygląda poprawnie?
  - Czy link wygląda podejrzanie?

3. Prezentacja ustawień prywatności i bezpieczeństwa

Zalecenia dla nauczyciela

- Pokaż każde zadanie krok po kroku na dużym ekranie lub projektorze.
- Pamiętaj: osoby starsze często uczą się poprzez powtarzanie – zaplanuj wspólne wykonanie każdego kroku.

Przykładowe ćwiczenie

Do wykonania wspólnie z uczestnikami:

- Przejdź do ustawień WhatsApp → „Prywatność” → „Zdjęcie profilowe” → wybierz „Moje kontakty”
- W Messengerze: pokaż, jak zablokować nieznajomego

Materiały pomocnicze

- Stwórz ilustrowane karty z instrukcjami krok po kroku, np.
  - „Jak zmienić hasło”
  - „Jak ustawić prywatność”
  - „Jak zablokować użytkownika”

4. Metody interaktywne – utrwalanie wiedzy i reagowanie na zagrożenia

Zalecenia dla nauczycieli:

- Symulacje są skuteczne – osoby starsze najlepiej uczą się poprzez realistyczne scenariusze.
- Wykorzystaj pary lub małe grupy, aby budować zaufanie i pracę zespołową.

Przykładowe ćwiczenia:

- Symulacja 1: „Otrzymałem dziwną wiadomość z banku” – co robić?
- Symulacja 2: „Nie mogę połączyć się z córką przez Zoom” – jak sprawdzić ustawienia?
- Odgrywanie ról: edukator wciela się w rolę oszusta, uczestnik w rolę seniora – następnie zamieniają się rolami.

Materiały pomocnicze:

- Stwórz scenariusze symulacji
- Karty ról: edukator/uczestnik/oszust
- Karty z przypomnieniem do zabrania do domu zawierające wskazówki dotyczące bezpieczeństwa (np. do przyklejenia na lodówce)

Załącznik 10 | Jak nauczyć seniorów korzystania z programów antywirusowych i aktualizacji systemu

Naucz seniorów, czym są wirusy i aktualizacje, pokaż, jak korzystać z programu antywirusowego, i przećwicz krok po kroku skanowanie i instalowanie aktualizacji systemu.

Zakres treści i metody nauczania

1. Wprowadzenie – czym są wirusy, aktualizacje i funkcje bezpieczeństwa

Zalecenia dla nauczyciela:

- Pamiętaj, aby podczas wyjaśniania złożonych tematów używać analogii.
- Wyjaśnij, czym są „wirusy komputerowe” – użyj porównań do przeziębienia lub infekcji, które mogą zaatakować komputer.
- Wyjaśnij, że aktualizacje są jak „lekarstwo” dla komputera – pomagają zapobiegać awariom i atakom.

Przykładowe ćwiczenie

- Zadaj uczestnikom następujące pytania:
  - Czy kiedykolwiek słyszeliście o „wirusach komputerowych”?
  - Co przychodzi Ci na myśl, gdy słyszysz słowo „aktualizacja”?

2. Prezentacja oprogramowania antywirusowego

Zalecenia dla nauczyciela:

- Użyj bezpiecznego i intuicyjnego programu (np. Windows Defender, darmowa wersja Avast).
- Przejdź krok po kroku przez cały proces: otwarcie programu, sprawdzenie aktualizacji, wykonanie szybkiego skanowania. Procedurę można zademonstrować za pomocą projektora.

Przykładowe ćwiczenie:

- Poproś uczestników, aby otworzyli oprogramowanie antywirusowe na swoich urządzeniach (lub na wspólnym laptopie).
- Przeprowadźcie wspólnie skanowanie. Omówcie znaczenie wyników: „nie znaleziono zagrożeń” vs. „wykryto zagrożenia”.

3. Nauka aktualizowania systemu operacyjnego

Zalecenia dla nauczyciela:

- Pokaż, jak znaleźć ustawienia aktualizacji (np. w systemie Windows: Ustawienia → Aktualizacja i zabezpieczenia).
- Podkreśl, że aktualizacje zazwyczaj pojawiają się automatycznie – użytkownik musi tylko kliknąć „Zainstaluj teraz".

Przykładowe ćwiczenie:

- **Każdy uczestnik otrzymuje listę kontrolną:**
  - Otwórz „Ustawienia"
  - Znajdź „Windows Update"
  - Sprawdź dostępne aktualizacje
  - Zainstaluj aktualizację, jeśli jest dostępna

- **Uwaga: W przypadku korzystania z komputera współdzielonego ćwiczenie można przeprowadzić w formie demonstracji z komentarzem.**

4. Metody utrwalające – listy kontrolne, odgrywanie ról, dyskusje

Zalecenia dla nauczyciela:

- Podsumuj materiał w formie gry lub quizu.
- Zachęcaj uczestników do zadawania pytań i dzielenia się własnymi doświadczeniami.

-

Przykładowe ćwiczenia:

- Lista kontrolna bezpieczeństwa: uczestnik sprawdza krok po kroku, czy jego komputer/smartfon jest chroniony (hasła, aktualizacje, skanowanie).
- Symulacja rozmowy telefonicznej: Nauczyciel wciela się w rolę oszusta, mówiąc: „Twój komputer jest zagrożony – pobierz nasz program". Zadaniem seniora jest rozpoznanie zagrożenia i odpowiedź: „Najpierw sprawdzę ustawienia programu antywirusowego".

Materiały pomocnicze:

- Gotowe listy kontrolne: „Bezpieczny komputer – czy mam wszystko, czego potrzebuję?".

Załącznik 11 | Arkusz roboczy: Bezpieczne korzystanie z Internetu: praktyczne wskazówki i techniki dla seniorów

Wypełnij arkusz roboczy, odpowiadając na pytania dotyczące bezpiecznych zakupów, bezpieczeństwa urządzeń, prywatności w Internecie oraz pokonywania strachu przed technologią.

Bezpieczne zakupy online	
Jakie elementy oferty internetowej należy zwrócić uwagę seniorom jako potencjalnie niebezpieczne lub podejrzane?	
Jak przeprowadzić seniorów przez proces zakupów online – jak mówić, co pokazać i na co zwrócić uwagę, aby czuli się bezpiecznie?	
Bezpieczeństwo urządzeń	
Jakie techniki pomagają seniorom zrozumieć, jak bezpiecznie skonfigurować swoje urządzenia?	
Jakie aplikacje i ustawienia są niezbędne do ochrony urządzeń seniorów?	
Ochrona prywatności w Internecie	
Jakie metody zastosujesz, aby pomóc seniorom lepiej zrozumieć koncepcję ochrony prywatności w Internecie, zwłaszcza w kontekście korzystania z aplikacji komunikacyjnych, takich jak WhatsApp?	
Pokonywanie strachu przed technologią	
Jakie elementy szkolenia pomagają seniorom przezwyciężyć strach przed technologią i wzmocnić poczucie pewności siebie podczas korzystania z internetu?	
Jakie metody budowania pewności siebie warto stosować, aby seniorzy czuli się komfortowo w świecie nowych technologii?	

Załącznik 12 | Zalecenia dotyczące dalszej lektury i nauki dla uczestników

Strony internetowe poświęcone cyberbezpieczeństwu: europejskie i rządowe organizacje zajmujące się cyberbezpieczeństwem:

1) **ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa**
   Strona internetowa: https://www.enisa.europa.eu
   ENISA oferuje przewodniki, raporty i kampanie edukacyjne dotyczące cyberbezpieczeństwa. Zawiera materiały edukacyjne dla indywidualnych użytkowników, w tym seniorów, dotyczące bezpiecznego korzystania z poczty elektronicznej, haseł, smartfonów i bankowości internetowej.
2) **Komisja Europejska – Bezpieczny Internet**
   Strona internetowa: https://digital-strategy.ec.europa.eu/en/policies/safer-internet
   Program Komisji Europejskiej promujący bezpieczne korzystanie z Internetu dla wszystkich grup wiekowych, w tym seniorów. Strona internetowa zawiera kampanie informacyjne i linki do inicjatyw krajowych.
3) **Europejska Sieć Centrów Konsumenckich (ECC-Net)**
   Strona internetowa: https://www.eccnet.eu
   Sieć centrów konsumenckich w UE, oferująca porady dotyczące bezpiecznych zakupów online, ochrony danych osobowych i unikania oszustw internetowych, które mogą być szczególnie pomocne dla seniorów.
4) **Cyberprofilaktyka – program profilaktyki cyfrowej**
   Strona internetowa: https://cyberprofilaktyka.pl/
   Program profilaktyki cyfrowej, który zawiera sekcję z poradami dla seniorów dotyczącymi unikania zagrożeń internetowych. Zawiera również materiały edukacyjne, infografiki i przykłady rzeczywistych oszustw, które pomagają lepiej zrozumieć zagrożenia cyfrowe.

6.5 Moduł V – Test przed/po

1. Jaki jest główny cel modułu 5?

A) Nauczyć seniorów, jak korzystać z mediów społecznościowych dla przyjemności
B) Przeszkolenie nauczycieli w zakresie skutecznego wspierania seniorów w bezpiecznej cyfryzacji
C) Poszerzenie wiedzy seniorów na temat sztucznej inteligencji
D) Rozwijanie umiejętności programowania seniorów

2. Która z poniższych przeszkód jest najczęściej spotykana przez seniorów podczas nauki umiejętności cyfrowych?

A) Ciekawość nowych technologii
B) Strach przed porażką lub brak pewności siebie
C) Nadmierne korzystanie z mediów społecznościowych
D) Duża wiedza techniczna

3. Jaka jest jedna skuteczna metoda nauczania seniorów?

A) Używanie skomplikowanego żargonu, aby brzmieć profesjonalnie
B) Prowadzenie lekcji w szybkim tempie
C) Podzielenie instrukcji na małe, proste kroki
D) Skupianie się wyłącznie na wiedzy teoretycznej

4. Na co nauczyciele powinni kłaść nacisk podczas nauczania o bankowości internetowej i zakupach online?

A) Jak szybciej wydawać pieniądze
B) Jak rozpoznać bezpieczne strony internetowe i chronić dane osobowe
C) Jak zwiększyć widoczność w Internecie
D) Jak wyłączyć oprogramowanie antywirusowe

5. Które z poniższych jest dobrym przykładem próby phishingu?

A) Znajomy wysyła Ci znany link
B) E-mail od banku z prośbą o podanie loginu i hasła
C) Aktualizacja zaufanego programu komputerowego
D) Przypomnienie z aplikacji kalendarza

6. Co powinna zrobić osoba starsza, gdy otrzyma podejrzany telefon od „pracownika banku”?

A) Natychmiast zainstalować sugerowaną aplikację
B) Rozłączyć się i zadzwonić do banku pod oficjalny numer
C) Podać swój numer identyfikacyjny i dane konta
D) Całkowicie zignorować połączenie

7. Jaki jest najlepszy sposób, aby nauczyciele pomogli seniorom zrozumieć działanie programów antywirusowych?

A) Wyjaśnić za pomocą analogii, np. porównując wirusy do chorób
B) Całkowicie unikać wyjaśnień technicznych
C) Pominąć tematy związane z programami antywirusowymi, ponieważ są one zbyt zaawansowane
D) Pokazywanie wyłącznie wyjaśnień tekstowych

8. Co oznacza „świadomość cyfrowa” dla seniorów?

A) Umiejętność szybszego robienia zakupów online
B) Rozumienie i rozpoznawanie zagrożeń internetowych
C) Unikanie wszelkiego korzystania z technologii
D) Nauka projektowania stron internetowych

9. Co powinien zrobić nauczyciel, jeśli senior nie rozumie aplikacji podczas zajęć?

A) Przejść do następnego tematu
B) Powtórzyć i uprościć wyjaśnienie, wykazując cierpliwość
C) Poprosić innego seniora, aby go nauczył
D) Zignorować problem

10. Co powinni zrobić seniorzy, jeśli podejrzewają cyberatak na swoje konto?

A) Poczekać, czy problem sam się rozwiąże
B) Zgłosić to do banku lub odpowiednich organów i natychmiast zmienić hasła
C) Podzielić się tą informacją w mediach społecznościowych
D) Usunąć wszystkie swoje konta

Podsumowanie odpowiedzi: 1-B, 2-B, 3-C, 4-B, 5-B, 6-B, 7-A, 8-B, 9-B 10-B

7. Ankieta ewaluacyjna

Informacje podane w tej ankiecie posłużą jako wytyczne do poprawy poziomu szkoleń, w których uczestniczysz, a także skuteczności i atrakcyjności kolejnych programów szkoleniowych.

Prosimy o wypełnienie ankiety, odpowiadając samodzielnie lub zgodnie z poniższą skalą ocen, gdzie 1 oznacza najniższą ocenę, a 5 najwyższą.

I. **Ocena warsztatów:**

- Program szkolenia ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Metody prowadzenia zajęć ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Atmosfera podczas zajęć ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Przydatność szkolenia ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Przygotowanie trenera ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Dobór treści szkolenia ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Cele szkolenia zostały jasno określone ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

1. **Które zagadnienia były dla Ciebie przydatne i na pewno wykorzystasz je w przyszłości?**
   .....
   .....

2. **Które zagadnienia były dla Ciebie mniej przydatne?**
   .....
   .....

3. **Które z zagadnień nie zostały omówione podczas zajęć, ale Twoim zdaniem powinny zostać uwzględnione w programie i dlaczego?**
   .....
   .....

4. **Czy uważasz, że są jakieś tematy, które powinny zostać dodane lub usunięte z programu szkolenia? Wyjaśnij dlaczego.**
   .....
   .....

II. **Ocena materiałów szkoleniowych:**

- Treść ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Dostępność informacji ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Czytelność ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Przydatność materiałów ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

III. **Dodatkowe informacje:**

1. **Ogólna ocena szkolenia** ☐ **POZYTYWNA** ☐ **NEGATYWNA**

2. **Czy szkolenie spełniło Państwa oczekiwania i wymagania – czy osiągnięto zamierzone cele, efekty i wyniki?** ☐ **TAK** ☐ **NIE**

3. **Czy uważasz, że warto było zorganizować takie szkolenie (i dlaczego)?**
   .....
   .....

4. **Dodatkowe uwagi i spostrzeżenia:**
   .....
   .....

5. **Skąd dowiedziałeś się o szkoleniu?**
   .....
   .....

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

Institute of Entrepreneurship Development
iED

ILKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

"Finansowane przez UE. Wyrażone poglądy i opinie są poglądami i opiniami autora(-ów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Krajowej Agencji Programu Erasmus+.
Unia Europejska ani grantodawca nie ponoszą za nie odpowiedzialności.