Społeczna Grupa Medialna

Senior Bezpieczny w Sieci

Podręcznik dla prowadzącego

Publikacja opracowana przez Społeczną Grupę Medialną

Opracowanie
Petros Tovmasyan

Wydawca
Społeczna Grupa Medialna
ul. Marszałkowska 31,
Zawiecie

Kontakt
kontakt@mediagroup.org.pl
579 643 667

Projekt dofinansowany ze środków programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021–2025.Edycja 2024

Spis Treści

Wstęp

Niniejszy materiał został stworzony z myślą o prowadzących warsztaty z zakresu bezpieczeństwa w sieci dla seniorów. Celem projektu jest zwiększenie świadomości osób starszych na temat zagrożeń w Internecie oraz nauczenie ich, jak skutecznie chronić swoje dane osobowe, korzystać z bankowości online i mediów społecznościowych.

Dzięki temu podręcznikowi dowiesz się, jak krok po kroku realizować zajęcia z pięciu kluczowych tematów. Zawiera on szczegółowe scenariusze, przykłady codziennych sytuacji oraz praktyczne ćwiczenia, które pomogą uczestnikom zdobyć niezbędne umiejętności cyfrowe.

Każdy warsztat jest interaktywny i praktyczny, co sprzyja efektywnej nauce. Wierzymy, że wiedza, którą przekażesz uczestnikom, nie tylko uczyni ich bardziej bezpiecznymi w sieci, ale także zwiększy ich pewność siebie w korzystaniu z nowych technologii.

Metodyka pracy z seniorami

Realizując warsztaty dla seniorów należy pamiętać o kluczowych elementach, które gwarantują skuteczność oraz przyjemność z nauki dla uczestników. Każdy z tych elementów jest nieodłączną częścią procesu edukacyjnego i przyczynia się do tworzenia pozytywnego, wspierającego środowiska, które sprzyja aktywnemu uczestnictwu i zdobywaniu wiedzy.

Tworzenie atmosfery komfortu, na początku warsztatów prowadzący powinien przywitać uczestników, przedstawić plan zajęć i zbudować przyjazną atmosferę poprzez anegdoty lub pytania zachęcające do interakcji.

Dostosowanie do potrzeb uczestników, kluczowym aspektem jest indywidualne podejście do każdego uczestnika. Ważne jest, aby pamiętać o dostosowaniu tempa i poziomu trudności materiału do zdolności grupy. Jest to szczególnie istotne, gdyż seniorzy mogą mieć różnorodne doświadczenia i umiejętności związane z nowymi technologiami. Warto zatem zapewnić możliwość powtarzania i szczegółowego wyjaśniania trudniejszych zagadnień, aby każdy uczestnik miał szansę na zrozumienie i przyswojenie materiału.

Dostępność sprzętu, zapewnienie odpowiedniego sprzętu, takiego jak laptopy czy tablety, jest niezbędne. Ważne jest, aby każdy uczestnik miał do niego dostęp i został przeszkolony w jego obsłudze. Wyjaśnienie, jak korzystać ze sprzętu, jest fundamentalne, szczególnie dla osób, które wcześniej nie miały z nim styczności.

Miejsce warsztatów, lokalizacja, w której odbywają się warsztaty, musi być dostosowana do potrzeb seniorów. Sala warsztatowa powinna być przystosowana dla osób z ograniczoną mobilnością, zapewniając łatwy dostęp i komfortowe warunki.

Łączenie teorii z praktyką, warto wykorzystywać realne przykłady i anegdoty. Takie historie i przykłady z życia, które są znaczące dla seniorów, pomagają w lepszym zrozumieniu i przyswojeniu wiedzy.

Metodyka pracy z seniorami

Udostępnienie materiałów, każdy uczestnik powinien otrzymać przygotowany zestaw materiałów zawierający zarówno teoretyczne wprowadzenie do poszczególnych tematów, jak i praktyczne zadania do wykonania. Dzięki temu uczestnicy będą mogli kontynuować naukę i ćwiczenia zarówno w trakcie zajęć, jak i w domowym zaciszu. Materiały powinny być wydrukowane w dużym, czytelnym formacie, aby maksymalnie ułatwić korzystanie z niego osobom starszym.

Ćwiczenia krok po kroku, ćwiczenia powinny być one prowadzone krok po kroku, z upewnieniem się, że każdy uczestnik nadąża. Taki sposób nauczania pozwala na dokładne zrozumienie każdego etapu pracy i jest szczególnie przyjazny dla osób, które dopiero zaczynają swoją przygodę z nowymi technologiami.

Przypomnienie kluczowych punktów, regularne powtarzanie najważniejszych informacji jest niezbędne. Należy to robić po każdej części warsztatów oraz na ich zakończenie. Powtórka kluczowych punktów pomaga w utrwaleniu wiedzy i zapewnia, że żaden ważny aspekt nie zostanie pominięty.

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

Czas trwania - 5 godzin

1. WPROWADZENIE

Przywitanie się i przedstawienie, wyjaśnienie celu warsztatów.
Ważne jest, aby prowadzący zbudował atmosferę, w której uczestnicy czują się komfortowo i bezpiecznie dzieląc się swoimi doświadczeniami i pytaniami.
Podzielenie się anegdotą lub historią o realnym zagrożeniu w sieci.

2. RODZAJE ZAGROŻEŃ W SIECI

Czym jest zagrożenie w sieci?
Zagrożenia w sieci to różnorodne formy oszustw i ataków, których celem jest wykorzystanie naszej nieuwagi lub nieznajomości zasad bezpiecznego korzystania z internetu. Ich głównym celem są pieniądze, dane osobowe lub infekowanie naszych urządzeń.

Phishing
Phishing to metoda, w której oszust podszywa się pod znaną firmę lub instytucję, próbując wyłudzić poufne informacje (np. dane logowania, hasła, numery kart kredytowych)
Przykład: E-mail od „banku", proszący o weryfikację konta, z linkiem prowadzącym do fałszywej strony.

Oszustwa SMS-owe
Oszustwa SMS-owe(smishing) to phishing za pośrednictwem wiadomości SMS. Oszuści wysyłają fałszywe SMS-y, zachęcając do kliknięcia w link lub oddzwonienia.
Przykład: SMS z informacją o wygranej w konkursie lub o zaległej płatności z linkiem do „opłacenia"

Spoofing - podszywanie sie pod inne osoby
Spoofing to technika, w której oszust udaje inną osobę lub instytucję, aby zdobyć nasze zaufanie i wyłudzić dane.
Przykład: Telefon od „pracownika banku" z prośbą o weryfikację danych

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

Niebezpieczne linki i załączniki
Niebezpieczne linki mogą prowadzić do stron zawierających wirusy lub złośliwe oprogramowanie, a załączniki mogą zainfekować nasze urządzenie po otwarciu.
Przykład: E-mail z ofertą „nie do odrzucenia" z linkiem do nieznanej strony lub załącznikiem.

Fake news i dezinformacja
Fake newsy to fałszywe informacje rozpowszechniane w sieci w celu manipulacji opinią publiczną, wywoływania paniki lub zysków finansowych.
Przykład: Artykuły rozpowszechniające nieprawdziwe informacje na temat zdrowia, polityki lub wydarzeń społecznych.

3. JAK ROZPOZNAĆ OSZUSTWA INTERNETOWE

Zwracanie uwagi na język i styl wypowiedzi.

- Phishingowe e-maile często zawierają literówki, błędy gramatyczne lub dziwnie sformułowane zdania.
- Wiadomości pisane w trybie „alarmującym" (np. „Twoje konto zostanie zamknięte, jeśli natychmiast nie podasz swoich danych!").

Sprawdzanie adresów e-mail i linków

- Zawsze sprawdzaj dokładnie adres e-mail nadawcy i upewnij się, że pochodzi z prawdziwej domeny (np. kontakt@mbank.pl, a nie kontakt@mbank-security.com)
- Przed kliknięciem w link, sprawdź jego adres. Fałszywe linki często zawierają drobne zmiany w nazwach domen.

Nie podawanie poufnych danych przez e-mail lub SMS.

- Wiarygodne firmy nigdy nie proszą o podanie danych osobowych, haseł lub numerów kart kredytowych przez e-mail lub SMS.

W przypadku wątpliwości zadzwoń bezpośrednio do instytucji korzystając z oficjalnych numerów kontaktowych dostępnych na stronach internetowych.

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

ZADANIE

Rozpoznanie podejrzanych e-maili i wiadomości SMS.
Przesłanie mailowo przykładowych prawdziwych jak i phisingowych wiadomości. Seniorzy muszą wskazać, które wydają się podejrzane.

4. BEZPIECZNE STRONY INTERNETOWE

Cechy bezpiecznych stron internetowych.

- Certyfikat SSL (Security Socket Layer) ikona kłódki, która oznacza, że strona używa szyfrowania SSL, co chroni dane przesyłane między użytkownikiem a stroną.
- Adres URL Bezpieczna strona zawsze zaczyna się od „https://” (z dodatkowym „s” oznaczającym zabezpieczenie). W przeglądarce obok adresu powinna pojawić się ikona kłódki.
- Nazwa domeny i różnice w adresach stron internetowych. Cyberprzestępcy często tworzą fałszywe strony, które wyglądają prawie identycznie jak oryginalne, zmieniając tylko drobne szczegóły w adresie URL (np. „gOOgle.com” zamiast „google.com”).

Jak sprawdzić linki przed kliknięciem

- Najechanie na link bez kliknięcia. pozwala zobaczyć, dokąd prowadzi. W lewym dolnym rogu przeglądarki pojawi się adres URL. Warto sprawdzić, czy rzeczywiście prowadzi do oczekiwanej strony.

ZADANIE

Rozpoznanie fałszywych stron internetowych.
Pokazanie przykładowych stron internetowych, seniorzy muszą wskazać na elementy które sugerują że strona może być oszustwem.

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

5. BEZPIECZNE KORZYSTANIE Z URZĄDZEŃ MOBILNYCH I KOMPUTERÓW

Unikanie niebezpieczeństw w sieci

- Korzystanie z zaufanych źródeł aplikacji Pobieraj aplikacje wyłącznie z oficjalnych źródeł, takich jak Google Play Store lub App Store. Unikaj pobierania programów z nieznanych stron internetowych.
- Wylogowanie się po zakończeniu sesji Po zakończeniu korzystania z ważnych usług online, takich jak bankowość internetowa lub konto pocztowe, zawsze wylogowuj się z konta, szczególnie jeśli korzystasz z publicznego lub wspólnego komputera.
- Dwustopniowe uwierzytelnianie to dodatkowy poziom zabezpieczenia, który wymaga nie tylko hasła, ale również potwierdzenia logowania poprzez SMS, e-mail lub aplikację uwierzytelniającą.
- Nieudostępnianie haseł. Hasło to osobista ochrona w sieci. Nigdy nie udostępniaj go nikomu, nawet jeśli ktoś prosi o nie pod pretekstem pomocy technicznej lub innej usługi.

Aktualizacja oprogramowania

Aktualizacje oprogramowania są kluczowe dla bezpieczeństwa urządzeń. Każda nowa aktualizacja zawiera poprawki, które chroni przed nowymi zagrożeniami w sieci. Warto ustawić automatyczne aktualizacje systemu operacyjnego i aplikacji, aby nie przegapić ważnych poprawek bezpieczeństwa.

Warto co jakiś czas sprawdzić, czy nasze urządzenie jest aktualne. Starsze wersje oprogramowania mogą być podatne na ataki, dlatego regularne aktualizowanie to podstawa bezpieczeństwa.

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

Bezpieczne korzystanie z publicznych sieci WI-FI
Publiczne sieci WI-Fi, np. w kawiarniach lub na lotniskach, nie są bezpieczne. Unikaj logowania się do kont bankowych lub przesyłania poufnych danych przez takie sieci.
Korzystanie z VPN (Virtual Private Network)
VPN to narzędzie, które szyfruje ruch internetowy i zapewnia większą prywatność oraz bezpieczeństwo, szczególnie w publicznych sieciach Wi-Fi.

ZADANIE

Sprawdzenie aktualizacji oprogramowania na swoim urządzeniu lub udostępnionym przez nas tablecie.

6. OCHRONA PRZED WIRUSAMI I ZAGROŻENIAMI

Rodzaje złośliwych oprogramowań:

- Wirusy komputerowe to programy, które kopiują się same i infekują inne pliki lub programy na komputerze. Wirusy mogą powodować uszkodzenia danych, spowalniać systemy, a czasem całkowicie unieruchomić urządzenie.
- Ransomware to oprogramowanie które blokuje dostęp do komputera lub danych, a następnie żąda okupu za ich odblokowanie. Ransomware często atakuje po kliknięciu w podejrzany link lub pobraniu zainfekowanego pliku.
- Spyware to oprogramowanie które potajemnie monitoruje działania użytkownika i zbiera informacje, takie jak dane logowania, przeglądane strony internetowe czy hasła.
- Trojany Złośliwe programy, które udają legalne oprogramowanie. Po zainstalowaniu mogą otworzyć dostęp do komputera dla hakerów lub instalować inne złośliwe oprogramowanie.

Warsztat I

RODZAJE ZAGROŻEŃ W SIECI — JAK NIE DAĆ SIĘ OSZUKAĆ

Programy antywirusowe

Programy antywirusowe są skuteczne w wykrywaniu i usuwaniu złośliwego oprogramowania. Regularne skanowanie pozwala na bieżąco monitorować stan bezpieczeństwa naszych urządzeń. Program antywirusowy powinien działać w tle i monitorować aktywność systemu w czasie rzeczywistym, blokując zagrożenia, zanim zainfekują urządzenie.

Przykłady programów antywirusowych

- Avast Free Antivirus: Darmowy program antywirusowy z ochroną w czasie rzeczywistym, prosty w obsłudze, oferujący solidną ochronę przed większością zagrożeń.
- Norton 360: Komercyjny program oferujący wszechstronną ochronę, w tym przed ransomware, spyware, phishingiem oraz ochronę sieci Wi-Fi.
- Kaspersky Internet Security: Znany z wysokiej skuteczności w testach, oferuje ochronę przed wirusami, ransomware, a także dodatkowe funkcje prywatności.

Co zrobić gdy podejrzewamy, że nasze urządzenie zostało zainfekowane?

- Odłączanie urządzenia od internetu.
- Uruchomienie programu antywirusowego i skanowania urządzenia Po odłączeniu urządzenia od internetu, uruchomcie pełne skanowanie za pomocą programu antywirusowego. To pomoże wykryć i usunąć wirusy oraz inne zagrożenia.
- Zresetowanie haseł jest szczególnie ważne, jeśli zauważysz podejrzane aktywności na swoich kontach, takie jak logowania z nieznanych lokalizacji.

ZADANIE

Pobranie programu antywirusowego na swoje urządzenie lub udostępniony tablet.

Warsztat II

TWORZENIE HASEŁ NIE DO WYKRYCIA ALE DO ZAPAMIĘTANIA

Czas trwania - 5 godzin

1. WPROWADZENIE

Przywitanie się i przedstawienie, wyjaśnienie celu warsztatów.
Hasła to pierwsza linia obrony przed wieloma zagrożeniami online, dlatego ważne jest, aby były one nie tylko trudne do złamania, ale również łatwe do zapamiętania. Dzisiejsze spotkanie pomoże Wam zrozumieć, jak to osiągnąć.

2. ZNACZENIE SILNYCH HASEŁ

Czym jest hasło?
Hasło to ciąg znaków używany do potwierdzenia tożsamości użytkownika podczas logowania do systemu, konta lub aplikacji.

Dlaczego hasło jest kluczowe?
Silne hasło utrudnia cyberprzestępcom przejęcie kontroli nad kontem poprzez ataki brute force (siłowe łamanie hasła) lub inżynierię społeczną.
Najczęściej używane hasła na świecie to '123456' i 'password'. Takie hasła są łatwe do zapamiętania, ale niestety, równie łatwe do odgadnięcia. Warto unikać prostych wzorców, takich jak imiona bliskich czy daty urodzenia, bo są to informacje, które można łatwo znaleźć.
Silne hasło to takie, które łączy wielkie i małe litery, cyfry oraz znaki specjalne, a jednocześnie jest odpowiednio długie.

Jak stworzyć silne hasło?

- Korzystanie z mnemotechnik czyli zdań lub fraz które sa dla nas znaczące przykład:„Mam dwa psy i jednego kota” – hasło: „M2p&1k!”.
- Hasła oparte na zdaniu czyli tworzenie hasła na podstawie zdań które sa dla nas łatwe do zapamiętania, przykład: „W moim ogrodzie kwitną róże" – hasło: „WmOkR”
- Stworzenie wzoru do hasła które łączy różne typy znaków (litery, cyfry, znaki specjalne) w złożony wzór, który jest trudny do odgadnięcia. Przykład: [Litera] [Cyfra] [Znak specjalny] A9!b7@C3$

Warsztat II

TWORZENIE HASEŁ NIE DO WYKRYCIA ALE DO ZAPAMIĘTANIA

3. ZASADY TWORZENIA HASEŁ

1. Długość hasła: minimum 8 znaków. Warto zapamiętać, że niektóre strony lub aplikacje posiadają wymagania co do minimalnej długości hasła.
2. Złożoność hasła, czyli powinno zwierać małe i duże litery, liczby, znaki specjalne.
3. Hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy.
4. Hasło nie powinno być imieniem nikogo z naszego najbliższego otoczenia (członka rodziny, znajomego ani zwierzaka).
5. Hasło nie powinno zawierać danych osobowych Twoich lub Twojej rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.

Nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: abcd, 1234, QWERTY

ZADANIE

Stworzenie przez każdego uczestnika 3 propozycji do silnego hasła.

4. METODY ZAPAMIĘTYWANIA HASEŁ

Menedżer haseł

Menedżery haseł to aplikacje, które pomagają przechowywać i zarządzać wieloma hasłami w bezpieczny sposób. Można w nich zapisać wszystkie swoje hasła, a dostęp do nich chroniony jest jednym głównym hasłem.

Warsztat II

TWORZENIE HASEŁ NIE DO WYKRYCIA ALE DO ZAPAMIĘTANIA

5. DWUSTOPNIOWA WERYFIKACJA

Dodatkowy poziom zabezpieczenia konta, który wymaga nie tylko podania hasła, ale także potwierdzenia tożsamości za pomocą drugiego kroku, np. kodu przesyłanego SMS-em, aplikacji uwierzytelniającej lub fizycznego klucza bezpieczeństwa.

Jak działa dwustopniowa weryfikacja?

- Krok 1: Użytkownik loguje się do konta, podając swoje hasło.
- Krok 2: System wymaga podania dodatkowego kodu weryfikacyjnego, który jest wysyłany SMS-em, generowany przez aplikację lub potwierdzany za pomocą klucza bezpieczeństwa.
- Przykład użycia: Logowanie do bankowości internetowej, które wymaga zarówno hasła, jak i kodu wysłanego SMS-em.

Metody dwustopniowej weryfikacji:

1. SMS jako drugi krok — najpopularniejszą metodą dwustopniowej weryfikacji jest kod SMS. Po wpisaniu hasła otrzymujecie na telefon kod, który musicie wprowadzić, aby zalogować się na swoje konto.
2. Aplikacje uwierzytelniające — takie jak Google generują jednorazowe kody, które zmieniają się co 30 sekund.

6. OCHRONA DANYCH OSOBOWYCH

Dane osobowe to wszelkie informacje, które mogą posłużyć do zidentyfikowania konkretnej osoby, takie jak imię i nazwisko, adres, numer telefonu, numer PESEL, adres e-mail, dane logowania, czy informacje o kartach płatniczych.

Warsztat II

TWORZENIE HASEŁ NIE DO WYKRYCIA ALE DO ZAPAMIĘTANIA

Zagrożenia związane z udostępnieniem danych osobowych:

- Kradzież tożsamości: Jak przestępcy mogą wykorzystać dane osobowe do podszywania się pod nas, aby uzyskać kredyty, dokonać zakupów online, czy wyłudzić pieniądze.
- Phishing: Wyjaśnienie, jak przestępcy wykorzystują fałszywe e-maile lub strony internetowe do wyłudzania danych osobowych.
- Udostępnianie danych na portalach społecznościowych: Jak nieświadome udostępnianie zbyt wielu informacji na profilach społecznościowych może prowadzić do naruszeń prywatności.

Jak chronić swoje dane osobowe w sieci?

- Bezpieczne korzystanie z mediów społecznościowych — na portalach społecznościowych warto ograniczyć widoczność swojego profilu tylko do zaufanych osób. Można tak kontrolować, jakie informacje są udostępniane publicznie. Regularne sprawdzanie i dostosowywanie ustawień prywatności jest kluczowe.
- Nieudostępnianie danych osobowych w nieznanych serwisach - Zawsze sprawdzajcie, czy strona, na której zamierzacie podać swoje dane, jest bezpieczna. Szukajcie kłódki obok adresu i upewnijcie się, że zaczyna się od 'https'. Jeśli strona wymaga podania danych osobowych, upewnijcie się, że jest to renomowany serwis.
- Silne hasła i dwustopniowe uwierzytelnianie - Silne hasła są kluczowe dla ochrony danych osobowych. Zawsze warto używać unikalnych haseł dla różnych kont oraz włączyć dwustopniowe uwierzytelnianie tam, gdzie jest to możliwe. Dzięki dwustopniowej weryfikacj, nawet jeśli ktoś pozna Wasze hasło, będzie musiał przejść dodatkową weryfikację.
- Nieudostępnianie danych osobowych przez telefon i e-mail - Instytucje takie jak banki nigdy nie będą prosić o podanie hasła przez telefon czy e-mail. Jeśli otrzymacie taki telefon lub wiadomość, bądźcie ostrożni – może to być próba wyłudzenia danych. Zawsze lepiej jest skontaktować się z daną instytucją bezpośrednio, aby zweryfikować, czy prośba jest prawdziwa.

Warsztat III

PHISHING I INNE METODY OSZUSTW W INTERNECIE — NIE DAJ SIĘ ZŁAPAĆ.

Czas trwania - 5 godzin

1. WPROWADZENIE

Przywitanie się i przedstawienie, wyjaśnienie celu warsztatów.
Phishing to metoda oszustwa, która polega na podszywaniu się przez oszustów pod zaufane instytucje lub osoby.

2. WPROWADZENIE DO PHISHINGU I OSZUSTW INTERNETOWYCH

Czym jest phishing?
Jest to rodzaj oszustwa internetowego, w którym oszuści podszywają się pod zaufane instytucje lub osoby, aby wyłudzić poufne informacje, takie jak hasła, numery kart kredytowych, czy inne dane osobowe.

Jak działa phishing?
Phishing działa na zasadzie wykorzystania naszego zaufania do znanych instytucji oraz presji czasu. Możecie otrzymać e-mail, który twierdzi, że Wasze konto zostanie zablokowane, jeśli natychmiast nie wprowadzicie pewnych danych. W rzeczywistości jest to tylko próba wyłudzenia informacji.

Formy phishingu
1. E-mail phishing
Jest to najpopularniejsza forma phishingu, polegająca na wysyłaniu fałszywych wiadomości e-mail, które wydają się pochodzić od zaufanych instytucji, takich jak banki czy serwisy internetowe. Oszuści często informują ofiary o rzekomych problemach z kontem i zachęcają do kliknięcia w link prowadzący do fałszywej strony logowania.
2. Spear phishing
To bardziej zaawansowana forma phishingu, w której atakujący kierują swoje wiadomości do konkretnych osób, wykorzystując wcześniej zdobyte informacje na ich temat. Dzięki temu wiadomości są bardziej przekonujące i mogą zawierać szczegóły dotyczące ofiary, co zwiększa szanse na sukces ataku.

Warsztat III

PHISHING I INNE METODY OSZUSTW W INTERNECIE — NIE DAJ SIĘ ZŁAPAĆ.

3. Smishing
Phishing za pośrednictwem SMS-ów. Oszuści wysyłają wiadomości tekstowe z prośbą o kliknięcie w link lub podanie danych osobowych. Często podszywają się pod instytucje finansowe lub inne organizacje, aby zdobyć zaufanie ofiary.

.4. Vishing
Polega na oszustwie telefonicznym, gdzie atakujący dzwoni do ofiary, podszywając się pod przedstawiciela banku lub innej instytucji. Celem jest wyłudzenie poufnych informacji przez manipulację emocjonalną.

5. Fałszywe strony internetowe
Są jednym z najczęstszych narzędzi wykorzystywanych przez cyberprzestępców do wyłudzania danych osobowych i pieniędzy. Oszuści tworzą witryny, które wyglądają niemal identycznie jak te prawdziwe, co sprawia, że użytkownicy mogą łatwo dać się nabrać.

3. RODZAJE OSZUSTW INTERNETOWYCH

Linki
- Instalacja złośliwego oprogramowania
- Fałszywe reklamy inwestycyjne
- Fałszywe strony internetowe
- Fałszywe strony banków i firm kurierskich

Czym jest link?
Linki to odnośniki, które umożliwiają użytkownikom internetu swobodne przemieszczanie się między materiałami i treściami na stronach internetowych lub między miejscami w danym dokumencie.

Warsztat III

PHISHING I INNE METODY OSZUSTW W INTERNECIE — NIE DAJ SIĘ ZŁAPAĆ.

Metoda „na wnuczka”
Oszustwo metodą „na wnuczka" to popularny schemat przestępczy, w którym oszuści wykorzystują zaufanie osób starszych, podszywając się pod członków rodziny lub funkcjonariuszy policji.

Schemat działania- Metoda na „wnuczka”
Krok 1: Przedstawienie się rozmówcy jako bliska osoba, informująca o sytuacji wymagającej natychmiastowej pomocy finansowej
Krok 2: W trakcie rozmowy oszust stara się zmanipulować emocjonalnie ofiarą , aby działała bez zastanowienia.
Krok 3: Po zdobyciu zaufania, oszust informuje, że nie może odebrać pieniędzy osobiście i prosi o przekazanie pieniędzy wydelegowanej osobie.

Metoda oszustwa- „nigeryjski przekręt”
Nigeryjski przekręt to rodzaj oszustwa internetowego, które polega na wciągnięciu ofiary w fikcyjny transfer dużej sumy pieniędzy. Przestępcy często kontaktują się z ofiarami za pośrednictwem e-maila, oferując udział w rzekomym transferze ogromnych kwot, co zazwyczaj kończy się wyłudzeniem pieniędzy.

Rodzaje „nigeryjskich przekrętów”
- Na uchodźcę politycznego: Oszust podaje się za uchodźcę lub dziedzica fortuny, oferując ofierze część pieniędzy w zamian za pomoc w ich przetransferowaniu. Ofiara jest zmuszana do pokrywania "kosztów operacyjnych".
- Na inwestora: Przestępca udaje młodego człowieka poszukującego pomocy w zainwestowaniu dużej sumy pieniędzy. Podobnie jak w poprzednim przypadku, ofiara pokrywa różne koszty.
- Na wygraną na loterii: Ofiara otrzymuje wiadomość o wygranej i musi uiścić opłaty związane z odbiorem nagrody, które trafiają do oszusta.

Warsztat III

PHISHING I INNE METODY OSZUSTW W INTERNECIE — NIE DAJ SIĘ ZŁAPAĆ.

- Na konta bez właściciela: Oszust podszywa się pod pracownika banku, informując ofiarę o istnieniu konta z dużą sumą pieniędzy, które nie ma właściciela. Aby przejąć te środki, ofiara musi pokryć koszty administracyjne.
- Na spadek: Oszust przekonuje ofiarę, że jest jedynym spadkobiercą dalekiego krewnego, który zmarł, a aby otrzymać spadek, musi uiścić różne opłaty.

4. ROZPOZNAWANIE PODEJRZANYCH WIADOMOŚCI I STRON INTERNETOWYCH

- **Błędy językowe,** wiele wiadomości phishingowych zawiera błędy gramatyczne, interpunkcyjne oraz ortograficzne. Zwracaj uwagę na brak polskich znaków diakrytycznych, co może świadczyć o oszustwie.
- **Nieznany nadawca,** sprawdź adres e-mail nadawcy. Często oszuści używają adresów, które przypominają prawdziwe, ale mają subtelne różnice (np. dodane znaki lub zmienione litery).
- **Bezosobowe powitanie,** wiadomości zaczynające się od „Drogi Kliencie” zamiast imienia i nazwiska powinny wzbudzić Twoją czujność.
- **Pilność i presja czasu,** wiadomości, które nakłaniają do szybkiego działania (np. „musisz podać dane w ciągu 24 godzin”) są często próbą wyłudzenia informacji.

5. METODY UNIKANIA OSZUSTW

Narzędzia do sprawdzania linków:

- Dostępne są serwisy internetowe takie jak: VirusTotal, PhishTank lub Google Transparency Report, które skanują linki pod kątem potencjalnych zagrożeń.

Narzędzia te analizują linki przy użyciu wielu silników antywirusowych i baz danych, dostarczając informacji o złośliwych oprogramowaniach.

Warsztat IV

BEZPIECZNA BANKOWOŚĆ I BEZPIECZNE ZAKUPY ONLINE

Czas trwania - 5 godzin

1. WPROWADZENIE

Przywitanie się i przedstawienie, wyjaśnienie celu warsztatów.
Phishing to metoda oszustwa, która polega na podszywaniu się przez oszustów pod zaufane instytucje lub osoby.

2. BEZPIECZNA BANKOWOŚĆ INTERNETOWA

Czym jest bankowość internetowa?
Bankowość internetowa to usługa, która umożliwia klientom dostęp do ich konta bankowego przez internet, umożliwiając wykonywanie różnorodnych operacji finansowych, takich jak sprawdzanie salda, przelewy, płatności rachunków, zakładanie lokat, itp. Z wszystkich tych usług można korzystać przy pomocy komputera lub telefonu.

Zagrożenia związane z korzystaniem z bankowości internetowej.

- Phising to próba wyłudzenia danych logowania przez fałszywe e-maile, SMS-y lub strony internetowe, które wyglądają jak komunikaty od banku.
- Malware to złośliwe oprogramowanie może zostać zainstalowane na komputerze lub urządzeniu mobilnym, aby przechwycić dane logowania do konta bankowego.
- Fałszywe aplikacje bankowe Cyberprzestępcy mogą tworzyć fałszywe aplikacje bankowe, które wyglądają jak oficjalne, ale służą do kradzieży danych logowania.

3. BLIK

BLIK, system płatności mobilnych, który pozwala na dokonywanie płatności bez użycia karty, za pomocą jednorazowych kodów generowanych przez aplikację bankową.

Ciekawostka dla seniorów Blik powstał w Polsce i funkcjonuje od 9 lutego 2025 roku.

Warsztat IV

BEZPIECZNA BANKOWOŚĆ I BEZPIECZNE ZAKUPY ONLINE

Jak działa blik?

- Generowanie kodu: Użytkownik loguje się do aplikacji mobilnej swojego banku i generuje jednorazowy kod BLIK.
- Wykorzystanie kodu: Kod jest następnie wprowadzany na terminalu płatniczym, stronie internetowej lub bankomacie w celu realizacji transakcji.
- Potwierdzenie transakcji: Każda transakcja musi być potwierdzona przez użytkownika w aplikacji mobilnej banku, co dodatkowo zabezpiecza operację.

Zalety korzystania z blik:

- Szybkość i wygoda BLIK jest niezwykle szybki i wygodny – wystarczy kilka kliknięć w aplikacji banku, aby wygenerować kod, którym zapłacicie za zakupy lub wypłacicie pieniądze z bankomatu, bez potrzeby używania karty płatniczej.
- Bezpieczeństwo transakcji BLIK jest bardzo bezpieczny, ponieważ każda transakcja musi być potwierdzona w aplikacji banku. Kod jest ważny tylko przez kilka minut, a po jego użyciu wygasa, co minimalizuje ryzyko oszustwa.
- Uniwersalność BLIK jest akceptowany w wielu miejscach – możecie go używać zarówno w sklepach stacjonarnych, jak i online. Dodatkowo umożliwia przelewy na telefon bez potrzeby znajomości numeru konta odbiorcy.

Ważne: BLIK działa tylko w Polsce.

Zagrożenie związane z blikiem.

Oszuści mogą próbować wyłudzić kody BLIK, podając się za znajomych lub członków rodziny, którzy „pilnie potrzebują pieniędzy”

O czym należy pamiętać przy bankowości internetowej:

- Ustawienie limitów transakcji na swoim koncie to dodatkowa ochrona przed nieautoryzowanymi przelewami. Dzięki temu nawet jeśli ktoś uzyska dostęp do Waszego konta, nie będzie mógł wydać więcej niż ustalony limit.

Warsztat IV

BEZPIECZNA BANKOWOŚĆ I BEZPIECZNE ZAKUPY ONLINE

- Sprawdzanie historii transakcji to najlepszy sposób na szybkie wykrycie podejrzanych operacji. Zwracajcie uwagę na wszystkie drobne, nieznane transakcje – mogą być one sygnałem, że ktoś próbuje oszukać Was na większą kwotę.

4. BEZPIECZNE ZAKUPY ONLINE

Czym są zakupy online?
Zakupy online to proces kupowania towarów lub usług przez internet za pośrednictwem stron internetowych, aplikacji mobilnych lub platform sprzedażowych.

Jak rozpoznawać bezpieczny sklep?
Opinie i recenzje, sprawdź opinie o sklepie w internecie, korzystając z platform takich jak Google czy portale społecznościowe. Upewnij się, że są one pozytywne i wiarygodne. Krótkie lub ogólne recenzje mogą budzić wątpliwości.
Historia firmy, zobacz, jak długo firma działa na rynku. Można to zweryfikować za pomocą narzędzi takich jak Baza Internetowa Regon.
Dane kontaktowe, upewnij się, że sklep podaje pełne dane kontaktowe, w tym adres fizyczny, numer telefonu i adres e-mail. Brak takich informacji powinien wzbudzić niepokój.
Bezpieczeństwo strony, sprawdź, czy strona korzysta z szyfrowania SSL (adres URL powinien zaczynać się od „https://”). Ikona kłódki w pasku adresu przeglądarki oznacza bezpieczne połączenie.
Ceny produktów, uważaj na podejrzanie niskie ceny, które mogą sugerować oszustwo. Ceny znacznie niższe niż w innych sklepach mogą być oznaką fałszywego sklepu.
Polityka zwrotów i regulamin, sprawdź, czy sklep ma jasno określoną politykę zwrotów oraz regulamin. Brak takich informacji jest sygnałem ostrzegawczym.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

Czas trwania - 5 godzin

1. WPROWADZENIE

Przywitanie się i przedstawienie, wyjaśnienie celu warsztatów.
Media społecznościowe, znane również jako social media, to aplikacje i strony internetowe, które pozwalają użytkownikom na tworzenie społeczności i dzielenie się informacjami w formie tekstów, zdjęć, filmów oraz linków do innych serwisów. Użytkownicy mogą tworzyć profile, które prezentują ich zainteresowania i aktywności, a także nawiązywać kontakty z innymi osobami.

2. FUNKCJE MEDIÓW SPOŁECZNOŚCIOWYCH

Komunikacja i interakcja, media społecznościowe ułatwiają nawiązywanie kontaktów oraz wymianę informacji między użytkownikami. Umożliwiają one zarówno prywatne wiadomości, jak i publiczne dyskusje, co sprzyja podtrzymywaniu relacji.
Budowanie relacji, media społecznościowe pozwalają na tworzenie i utrzymywanie więzi między członkami danej społeczności. Firmy mogą korzystać z tych platform do budowania relacji z klientami oraz partnerami biznesowymi.
Prezentacja treści, użytkownicy mogą publikować, udostępniać, oceniać oraz komentować różne formy treści, takie jak teksty, zdjęcia czy filmy. Ta funkcja wspiera interaktywną wymianę myśli i pomysłów.
Zarządzanie marką i marketing, media społecznościowe są wykorzystywane do promocji produktów i usług. Firmy mogą kierować kampanie marketingowe do konkretnych grup docelowych oraz informować o ofertach specjalnych, co może przyczynić się do wzrostu sprzedaży.
Informacje o klientach, dzięki narzędziom analitycznym dostępnych w serwisach społecznościowych, firmy mogą monitorować aktywność swoich klientów, co pozwala lepiej zrozumieć ich potrzeby i preferencje.
Monitorowanie trendów i opinii, użytkownicy mogą wyrażać swoje opinie na temat produktów i usług, co pozwala firmom na bieżąco reagować na feedback oraz zarządzać swoim wizerunkiem w sieci. Firmy mogą monitorować na bieżąco najnowsze trendy.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

3. SOCIAL MEDIA ZAGROŻENIA

Śledzenie i profilowanie, firmy mogą zbierać dane o zachowaniach użytkowników, co prowadzi do naruszenia prywatności.
Cyberprzemoc, media społecznościowe mogą być platformą dla cyberprzemocy, gdzie ofiary są nękane i hejtowane przez innych użytkowników.
Dyskryminacja i wykluczenie, osoby z różnych grup społecznych mogą być narażone na dyskryminację i wykluczenie.
Dezinformacja, rozprzestrzenianie nieprawdziwych wiadomości może prowadzić do paniki społecznej lub błędnych przekonań. Zorganizowane kampanie dezinformacyjne mogą wpływać manipulację opinią publiczną.
Uzależnienie, użytkownicy mogą stać się uzależnieni od mediów społecznościowych, co wpływa na ich zdrowie psychiczne i relacje interpersonalne. Ponadto częste porównywanie się z innymi użytkownikami może prowadzić do obniżenia poczucia własnej wartości.
Phishing, oszuści mogą wykorzystywać media społecznościowe do wyłudzania danych logowania lub informacji finansowych. – Kradzież tożsamość: Użytkownicy są narażeni na kradzieże kont i podszywanie się pod nich.

4. WPŁYW MEDIÓW SPOŁECZNOŚCIOWYCH NA ŻYCIE CODZIENNE

Komunikacja i relacje międzyludzkie
Pozytywne: Platformy społecznościowe umożliwiają szybki kontakt z rodziną, przyjaciółmi i współpracownikami, niezależnie od odległości.
Negatywne: Często relacje przenoszą się z rzeczywistego świata do świata cyfrowego, co może prowadzić do spłycenia kontaktów twarzą w twarz.
Neutralne: Media społecznościowe mogą zbliżać ludzi lub wprowadzać dystans, zależnie od sposobu korzystania i jakości komunikacji.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

Informacja i edukacja
Pozytywne: Użytkownicy mają dostęp do bieżących wydarzeń na całym świecie w czasie rzeczywistym. Platformy jak YouTube czy LinkedIn mogą być narzędziami do nauki, oferując materiały szkoleniowe, poradniki i kursy.
Negatywne: Niestety, media społecznościowe często są platformą do rozpowszechniania fake newsów i teorii spiskowych.

Wpływ na zdrowie psychiczne
Negatywne: Media społecznościowe sprzyjają porównywaniu się z innymi, co może prowadzić do obniżonej samooceny, stresu czy nawet depresji. Wiele osób doświadcza uzależnienia od mediów społecznościowych, co prowadzi do trudności w odłączeniu się od platform.
FOMO (Fear of Missing Out): Lęk przed tym, że coś nas omija, może generować stres i presję, by być stale online.

Kultura i styl życia
Pozytywne: Media społecznościowe są miejscem, gdzie rodzą się nowe trendy, zarówno w modzie, kulturze, jak i w zachowaniach społecznych. Platformy umożliwiają organizowanie kampanii społecznych i promowanie ważnych tematów, jak prawa człowieka, ekologia czy zdrowie psychiczne.
Negatywne: Użytkownicy często prezentują idealizowaną wersję swojego życia, co wpływa na postrzeganie siebie i innych.

Wpływ na produktywność
Pozytywne: media społecznościowe są wykorzystywane przez firmy i freelancerów jako narzędzie do promocji, networking'u i sprzedaży.
Negatywne: Częste powiadomienia i nawyk scrollowania mogą prowadzić do utraty koncentracji i obniżenia produktywności w pracy czy nauce.

Wpływ na rynek pracy
Pozytywne: Ludzie wykorzystują media społecznościowe do budowania swojej marki osobistej, co może wpływać na ich karierę. Portale takie jak LinkedIn umożliwiają nawiązywanie kontaktów biznesowych i poszukiwanie nowych możliwości zawodowych.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

5. NAJPOPULARNIEJSZE MEDIA SPOŁECZNOŚCIOWE

Youtube (Liczba użytkowników wynosi około 28 milionów. Platforma dociera do 78% wszystkich użytkowników internetu w Polsce) **Facebook** (Liczba użytkowników wynosi około 17 milionów. Platforma dociera do 42,1% wszystkich użytkowników internetu w Polsce).
Instagram (Liczba użytkowników wynosi około 11 milionów. Platforma dociera do 27,1% wszystkich użytkowników internetu w Polsce).
LinkedIn (Liczba użytkowników wynosi około 6,7 milionów).

6. BEZPIECZNE KORZYTSANIE Z FACEBOOKA I INNYCH MEDIÓW SPOŁECZNOŚCIOWYCH

Metody kradzieży tożsamości w social mediach?
– Phishing
– Tworzenie fałszywych profili
– Wyciek danych
– Ataki socjotechniczne
– Wykorzystanie złośliwego oprogramowania

Jak sprawdzić, czy grupa na Facebooku jest bezpieczna?
1. Sprawdź informacje o grupie — Przejrzyj opis grupy i regulamin, aby upewnić się, że są one jasne i zrozumiałe. Grupa powinna mieć jasno określony cel i zasady. – Sprawdź, kto jest administratorem grupy. Zaufane grupy mają administratorów, którzy aktywnie moderują treści. – Upewnij się, że grupa jest publiczna lub zamknięta, a nie tajna. Tajne grupy są trudniejsze do zweryfikowania.
2. Obserwuj aktywność w grupie: – Przejrzyj posty i komentarze w grupie. Unikaj grup, gdzie pojawiają się podejrzane linki, załączniki lub prośby o dane osobowe. – Bądź ostrożny z grupami, które mają mało aktywności lub gdzie administratorzy rzadko odpowiadają na pytania 3. Sprawdź opinie o grupie: – Poszukaj opinii o grupie poza Facebookiem, np. na forach internetowych lub w internecie. Unikaj grup z negatywnymi recenzjami. – Zapytaj znajomych, czy słyszeli o danej grupie i czy uważają ją za bezpieczną.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

7. CZEGO NIE WARTO UDOSTĘPNIAĆ W SOCIAL MEDIACH

Dane osobowe, imię i nazwisko, adres, numer telefonu, dane finansowe czy numery dokumentów tożsamości.
Informacje zdrowotne, użytkownicy powinni również unikać dzielenia się informacjami zdrowotnymi, takimi jak pytania dotyczące chorób czy leczenia.
Dokumenty i pliki osobiste, nie należy przesyłać dokumentów zawierających dane osobowe ani poufnych informacji związanych z pracą.
Lokalizacja, informacje o bieżącej lokalizacji, zwłaszcza w czasie rzeczywistym, mogą narazić Cię na niebezpieczeństwo. -Dane o rodzinie: Ujawnienie informacji o bliskich osobach bez ich zgody. Wrażliwe poglądy, ekstremalne opinie polityczne, religijne lub inne, które mogą prowadzić do konfliktów.
Intymne zdjęcia i filmy, jakiekolwiek materiały, które mogą być wykorzystane do szantażu lub które nie powinny być publicznie dostępne.

8. NETYKIETA I KONTROLA PRYWATNOŚCI

Netykieta to nieformalny zbiór zasad, które regulują sposób komunikacji w sieci. Obejmuje ona różnorodne aspekty interakcji online, od forów dyskusyjnych po media społecznościowe. Jej celem jest promowanie szacunku i uprzejmości w kontaktach między użytkownikami, co przyczynia się do stworzenia zdrowej i bezpiecznej przestrzeni w Internecie.

9. ZASADY NETYKIETY

1. Szanuj innych, traktuj innych użytkowników z szacunkiem, unikaj obraźliwych komentarzy oraz hejtu.
2. Unikaj pisania wielkimi literami, w Internecie oznacza to krzyk i może być odbierane jako agresywne.
3. Przestrzegaj zasad gramatyki i ortografii – Staraj się pisać poprawnie, aby Twoje wiadomości były zrozumiałe.

Warsztat V

BEZPIECZNE KORZYSTANIE Z MEDIÓW SPOŁECZNOŚCIOWYCH

4. Nie spamuj, unikaj wysyłania niechcianych wiadomości i linków.
5. Reaguj na hejt, jeśli zauważysz, że ktoś jest poniżany, zgłoś to administratorowi lub odpowiednim służbom.
6. Zachowuj się zgodnie z regulaminem platformy, każda grupa czy forum może mieć swoje specyficzne zasady, które należy przestrzegać.

Jak unikać spamu?
Nie klikaj na linki i posty o szokujących lub kontrowersyjnych tytułach.
Bądź ostrożny przy klikaniu na strony, które się otworzą po kliknięciu w link.
Zgłaszaj spamowe treści globalnej administracji Facebooka.

Społeczna Grupa Medialna

Jesteśmy młodym, ambitnym zespołem specjalistów składającym się z marketingowców, ekspertów ds. treści i analizy danych oraz programistów, którzy łączą swoje umiejętności, aby dostarczać innowacyjne rozwiązania dla naszych klientów. Pracujemy z pasją i zaangażowaniem, aby pomóc firmom osiągnąć sukces w dynamicznie zmieniającym się świecie marketingu cyfrowego.
Społeczna Grupa Medialna powstała 2020 roku. Na początku zajmowaliśmy się tworzeniem portali dla mediów lokalnych oraz marketingiem. Wraz z rozwojem sztucznej inteligencji rozwinęliśmy nasze działanie w kierunku AI, którym zajmujemy się aktualnie.

Nasze wartości
Innowacja: Dążymy do ciągłego wprowadzania innowacyjnych rozwiązań, które przyczyniają się do sukcesu naszych klientów i pomagają im osiągnąć przewagę konkurencyjną.
Skupienie na kliencie: Naszym priorytetem jest zrozumienie potrzeb i celów naszych klientów, aby dostarczyć im rozwiązania, które przynoszą realne korzyści.
Współpraca: Wierzymy, że współpraca i komunikacja są kluczem do osiągnięcia sukcesu. Nasz zespół ściśle współpracuje z klientami, aby osiągnąć wspólne cele.
Ciągłe doskonalenie: Jesteśmy zawsze otwarci na naukę i rozwój, aby być na bieżąco z najnowszymi trendami i technologiami, które pomogą nam dostarczyć najlepsze usługi dla naszych klientów.

+48 888 959 840

kontakt@mediagroup.org.pl

https://www.mediagroup.org.pl