Karta szkoleniowa E-Seniors

|  |  |
| --- | --- |
| **Tytuł** | **Temat: Informacja i komunikacja za pośrednictwem mediów społecznościowych****Moduł 3. Zagrożenia i wyzwania w mediach społecznościowych: ZA i PRZECIW** |
| **Obszar** **szkoleniowy** | *Wybierz co najmniej jedno z poniższych:*

|  |  |
| --- | --- |
| Bezpieczeństwo w Internecie |  |
| Umiejętność korzystania z kultury i mediów | *X* |
| Transakcje gospodarcze |  |
| Ochrona danych osobowych |  |
| Tożsamość cyfrowa i reputacja online |  |

 |
| **Słowa** **kluczowe** **(metatag)** | **Media społecznościowe, komunikacja, bezpieczeństwo** |
| **Dostarczone przez** | **E-Seniors** |
| **Język** | **Polski** |
| **Cele i wyniki szkolenia** |
| Ten moduł ma na celu rozwijanie wiedzy i umiejętności użytkowników w zakresie wykorzystywania mediów społecznościowych do komunikacji oraz promocji kultury i kreatywności. Starsi użytkownicy zapoznają się z narzędziami mediów społecznościowych, zasobami kulturowymi w mediach społecznościowych, które umożliwiają im łatwą nawigację i odkrywanie możliwości kulturowych i komunikacyjnych. |
| **Opis** |
| Kurs jest podzielony na 3 poziomy: każdy moduł podzielony jest na rozdzialy i treści. Tytuły rozdzialow dają bardziej szczegółowe wyobrażenie o zawartości modułu. Ten konkretny moduł jest zbudowany w następujący sposób:**Temat: Informacja i komunikacja za pośrednictwem mediów społecznościowych****Moduł 3. Zagrożenia i wyzwania w mediach społecznościowych: ZA i PRZECIW****Rozdział 3.1:** Zagrożenia i wyzwania **Rozdział 3.2:** 10 dobrych praktyk do zastosowania w celu zapewnienia bezpieczeństwa w sieciach społecznościowych. |
| **Zawartość przedstawiona na 3 poziomach** |
| **Moduł 3. Zagrożenia i wyzwania w mediach społecznościowych: DOs and DONTs** Istnieje wiele zagrożeń i wyzwań związanych z przeglądaniem internetu, zarówno na komputerze, jak i smartfonie. Sieci społecznościowe nie są wyjątkiem. Korzystanie z sieci społecznościowych wiąże się z kilkoma zagrożeniami. Jeśli jednak zostaną podjęte środki ostrożności, surfowanie przy minimalnym ryzyku nie jest trudne.**Rozdział 3.1:** Zagrożenia i wyzwania* **Wyłudzanie informacji:** wyłudzanie informacji to rodzaj socjotechniki, w której atakujący wysyła oszukańczą wiadomość mającą na celu oszukanie osoby. Te wiadomości mają na celu nakłonienie Cię do ujawnienia danych osobowych, udając, że pochodzą z zaufanego źródła. Wiadomości mogą pochodzić od osób podających się za Twoich znajomych lub znaną firmę. Nigdy nie udostępniaj poufnych informacji i nigdy nie klikaj podejrzanie wyglądającego łącza internetowego.
* **Hakowanie psychologiczne:** Hakowanie psychologiczne to proces uzyskiwania poufnych informacji od osoby za pomocą oszustwa. Oszust może rozpocząć rozmowę o tym, co przeczytał w Twoim profilu, na przykład gdzie pracujesz itp. Następnie próbują nakłonić Cię do ujawnienia danych osobowych, podobnie jak w przypadku phishingu czyli wyłudzania informacji.
* **Malware:** Malware to złośliwe oprogramowanie zaprojektowane w celu infiltracji urządzeń. Krąży w sieciach społecznościowych jako linki z chwytliwymi tytułami. Gdy malware zostanie zinfiltrowane, może wysyłać wiadomości do kontaktów, uzyskiwać dostęp do danych osobowych lub uszkodzić urządzenie. Należy zachować ostrożność w przypadku pokusy kliknięcia linku z nieznanego źródła.
* **Mowa nienawiści:** mowa nienawiści jest powszechna w sieciach społecznościowych, ponieważ jej autorzy mogą pozostać anonimowi. Może się zdarzyć, że otrzymasz mowę nienawiści, czasami bez żadnej sieci, dlatego ważne jest, aby się od niej odciąć i nie wahać się zgłaszać ją jako niechcianą i złośliwą treść.
* **Cyberprzemoc:** to szkodzenie, które ma miejsce za pomocą urządzeń cyfrowych, takich jak telefony komórkowe, komputery i tablety. Cyberprzemoc może mieć miejsce za pośrednictwem SMS-ów, SMS-ów i aplikacji lub online w mediach społecznościowych, forach lub grach, w których ludzie mogą przeglądać, uczestniczyć lub udostępniać treści. Cyberprzemoc obejmuje wysyłanie, publikowanie lub udostępnianie negatywnych, szkodliwych, fałszywych lub złośliwych treści na temat innej osoby. Może to obejmować udostępnianie osobistych lub prywatnych informacji o kimś, co powoduje zakłopotanie lub upokorzenie. Niektóre przypadki cyberprzemocy przekraczają granicę, prowadząc do zachowań niezgodnych z prawem lub przestępczych.
* **Ageizm online:** Ageizm odnosi się do stereotypów (jak myślimy), uprzedzeń (jak się czujemy) i dyskryminacji (jak postępujemy) wobec innych lub samego siebie ze względu na wiek. Ageizm dotyczy wszystkich. Już 4-letnie dzieci uświadamiają sobie stereotypy wiekowe swojej kultury. Od tego wieku uwewnętrzniają i wykorzystują te stereotypy, aby kierować swoimi uczuciami i zachowaniem wobec ludzi w różnym wieku. Czerpią również ze stereotypów kulturowych dotyczących wieku, aby postrzegać i rozumieć siebie, co może skutkować samokierowanym ageizmem w każdym wieku. Ageizm przecina i pogłębia inne formy niekorzystnej sytuacji, w tym te związane z płcią, rasą i niepełnosprawnością.
* **Na co uważać, aby uniknąć oszustw na Facebooku:**
	+ Osoby, których nie znasz osobiście, proszą Cię o pieniądze lub dane bankowe.
	+ Niezweryfikowane strony, które twierdzą, że reprezentują dużą organizację lub osobę publiczną.
	+ Osoby, które proszą Cię o kontynuowanie rozmowy poza Facebookiem, w mniej publicznym lub mniej bezpiecznym ustawieniu, takim jak osobny adres e-mail.
	+ Osoby proszące o przesłanie im danych bankowych w celu otrzymania nagrody.
	+ Każdy, kto twierdzi, że jest twoim przyjacielem lub krewnym w niebezpieczeństwie.
	+ Ludzie, którzy kłamią o tym, gdzie mieszkają.
	+ Posty lub publikacje zawierające błędy ortograficzne i gramatyczne.
	+ Osoby lub konta, które przekierowują Cię na stronę, aby odebrać nagrodę

**Rozdział 3.2: 10 dobrych praktyk do zastosowania w celu zapewnienia bezpieczeństwa w sieciach społecznościowych:**1- **Chroń dostęp do swoich kont:** używaj silnych haseł, które różnią się w zależności od konta. Aplikacje do zarządzania hasłami ułatwiają zapisywanie haseł. **Na przykład https://keepassxc.org/**2- **Sprawdź swoje ustawienia prywatności:** Domyślnie ustawienia prywatności są często otwarte (w przypadku danych osobowych, takich jak imię i nazwisko, numer telefonu, adres e-mail). Dane te mogą być dostępne dla wszystkich abonentów sieci społecznościowej. Możliwe jest ograniczenie tej widoczności poprzez dostosowanie konfiguracji konta, aby zachować kontrolę nad tym, co widzą inni użytkownicy.3- **Kontroluj swoje posty:** Twoje posty mogą wymknąć się spod kontroli i zostać ponownie opublikowane lub zinterpretowane częściej, niż zamierzałeś. Nie publikuj danych osobowych ani poufnych.4- **Uważaj, z kim rozmawiasz.** Twoi znajomi mogą udostępniać złośliwe treści bez wiedzy lub sami zostali zhakowani. Nigdy nie wysyłaj pieniędzy bez weryfikacji tożsamości osoby, nie wysyłaj prywatnych filmów wideo, nie bądź podejrzliwy wobec konkursów, nieoczekiwanych wygranych lub „świetnych ofert”, które mogą ukrywać oszustwa.5-  **Kontroluj aplikacje innych firm:** Niektóre aplikacje oferują interakcję z jednym z kont sieci społecznościowych. Wymagają uprawnień, które należy dokładnie sprawdzić, ponieważ niektórzy z nich mogą mieć wtedy dostęp do Twoich danych. Uważaj, aby nie instalować aplikacji, które podejrzewasz, że są złośliwe.6- **Unikaj publicznych komputerów i sieci:** korzystanie z ogólnodostępnego komputera lub publicznej sieci Wi-Fi jest ryzykowne, ponieważ mogą one zostać naruszone lub znajdować się pod kontrolą cyberprzestępców. Unikaj wprowadzania poufnych informacji lub używania ich, jeśli to możliwe.7- **Regularnie sprawdzaj loginy konta:** Większość sieci społecznościowych pozwala zobaczyć aktywne połączenia lub sesje kont. Regularnie sprawdzaj te informacje, aby upewnić się, że inne urządzenie nie jest połączone z jednym z Twoich kont. Jeśli tak, odłącz je i zmień hasło.8- **Uważaj na fałszywe wiadomości:** niektóre publikowane informacje mogą być fałszywe, celowo lub nie. Przed rozważeniem lub przekazaniem jakichkolwiek informacji sprawdź ich autentyczność. 9- **Sprawdź swoje dane identyfikacyjne z kontami:** Niektóre witryny oferują możliwość zarejestrowania się na koncie sieci społecznościowej. Pozwala to na przykład na uniknięcie konieczności tworzenia hasła, ale może dostarczyć stronie danych osobowych lub umożliwić cyberprzestępcy, który włamał się na twoją sieć społecznościową, na dostęp do twojego konta w tej witrynie.10- **Usuń swoje konto, jeśli już jego nie używasz:** Aby uniknąć wszystkich zagrożeń opisanych powyżej, aby upewnić się, że Twoje konto nie jest używane bez Twojej wiedzy, usuń konto, gdy już jego nie potrzebujesz. |
| **Treść w punktach** |
| * Najczęstsze zagrożenia i wyzwania związane z korzystaniem z mediów społecznościowych to obrona przed phishingiem, złośliwym oprogramowaniem, mową nienawiści itp.;
* Możesz uniknąć zagrożeń i ryzyka w mediach społecznościowych, postępując zgodnie z zaleceniami i radami określonymi w tym module szkoleniowym
 |
| **5 haseł ze słownika** |
| **Bezpieczeństwo mediów społecznościowych:** Bezpieczeństwo mediów społecznościowych odnosi się do wszystkich środków, które użytkownik powinien podjąć, aby uniknąć ryzyka, oszustw i ataków na jego konto osobiste.**Mowa nienawiści:** mowa nienawiści to wypowiadane słowa, które są obraźliwe, obraźliwe i/lub grożące osobie lub grupie w oparciu o konkretny atrybut tej osoby lub osób będących celem.**Hakowanie psychologiczne:** Hakowanie psychologiczne to proces uzyskiwania poufnych informacji od osoby za pomocą oszustwa. **Cyberprzemoc:** to znęcanie się, które ma miejsce za pomocą urządzeń cyfrowych, takich jak telefony komórkowe, komputery i tablety**Ageizm online:** Ageizm odnosi się do stereotypów (jak myślimy), uprzedzeń (jak się czujemy) i dyskryminacji (jak postępujemy) wobec innych lub samego siebie ze względu na wiek. Ageizm dotyka wszystkich. |
| **Referencje i więcej informacji na ten temat** |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)[**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) |
|  **Pięć pytań do samooceny wielokrotnego wyboru** | **1) Korzystanie z komputerów publicznych jest bezpieczne**1. **Prawda**
2. **Fałsz**

**Prawidłowo: B****2) Co to jest złośliwe oprogramowanie?**1. **Złośliwe oprogramowanie przeznaczone do infiltracji urządzeń**
2. **Oszustwo związane z tożsamością**
3. **Mowa nienawiści**

**Prawidłowo: A****3) Co to jest mowa nienawiści?**1. **Mowa nienawiści to wypowiadane słowa, które są obraźliwe i/lub grożące osobie lub grupie w oparciu o konkretny atrybut tej osoby lub osób będących celem.**
2. **Mowa nienawiści to proces uzyskiwania poufnych informacji od osoby za pomocą oszustwa.**
3. **Mowa nienawiści to złośliwe informacje mające na celu infiltrację urządzeń i atakowanie ludzi.**

**Prawidłowo: A** **4) Bezpieczeństwo w mediach społecznościowych:** 1. **Odnosi się do wszystkich środków stosowanych przez firmy w celu obrony przed oszustwami internetowymi.**
2. **Odnosi się do wszystkich środków, które użytkownik powinien podjąć, aby uniknąć ryzyka, oszustw i ataków na jego konto osobiste.**
3. **Odnosi sie do narzędzi mediów społecznościowych przeznaczonych dla użytkowników.**

**Prawidłowo: B****5) Co zrobić, jeśli natkniesz się na mowę nienawiści w internecie?**1. **Staraj się unikać napastników**
2. **Spróbuj zgłosić napastników**
3. **Wszystkie powyższe są poprawne**

**Prawidłowo: C** |
| **Powiązany material** | **Jak rozpoznać i uniknąć częstych oszustw w mediach społecznościowych:** [**https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/**](https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/)**Jak uniknąć oszustw w mediach społecznościowych:** [**https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html**](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)**Cyberprzemoc i mowa nienawiści:** [**https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf**](https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf) |
| **Powiązane PPT** |  |
| **Powiązany link** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **Film w formacie YouTube (jeśli istnieje)** | **Co to są media społecznościowe? W prostym angielskim:**[**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)**Niesamowity czytelnik ujawnia swój „dar”:** [**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |