Karta szkoleniowa CDI

|  |  |
| --- | --- |
| **Tytuł** | Jak zidentyfikować niekompletne informacje i fałszywe wiadomości online w kontekście związanym z kulturą |
| **Obszar szkoleniowy** | *Wybierz jedną lub więcej z następujących opcji:*   |  |  | | --- | --- | | Bezpieczeństwo online | X | | Umiejętność korzystania z kultury i mediów |  | | Transakcje gospodarcze |  | | Ochrona danych osobowych |  | | Tożsamość cyfrowa i reputacja online |  | |
| **Słowa kluczowe** | bezpieczeństwo online, kontekst kulturowy, fałszywe wiadomości,niekompletne informacje |
| **Dostarczone przez:** | Instytut Rozwoju Społeczności, CDI |
| **Język** | Polski |
| **Cele / cele / efekty uczenia się** | |
| Pod koniec tego modułu zdobędziesz wiedzę w zakresie rozpoznawania fałszywych i niekompletnych informacji, a także bezpieczeństwa online w kontekście kulturowym.  Moduł składa się z czterech części dostarczających informacji związanych z tematem,podzielonych na sekcje. Wszystkie treści poparte przykładami dla lepszego zrozumienia materiału, zdjęciami wyjaśniającymi i przydatnymi linkami, aby poszerzyć swoją wiedzę na ten temat.  Użytkownicy będą mieli możliwość zapoznania się z bezpieczeństwem online w kontekście kulturowym i spolecznym.Zagrożenia bezpieczeństwa online zostaną przedstawione poprzez wyjaśnienia różnych rodzajów zagrożeń, takich jak złośliwe oprogramowanie,atak phishingowy, proby kradziezy hasel itp.  Użytkownicy będą mogli:  ● Zrozumiec znaczenie bezpieczeństwa i ochrony w internecie  ● zrozumiec roznice między fałszywymi wiadomościami, dezinformacją i niekompletnymi informacjami  ● Korzystac z różnych wskazówek dotyczących bezpieczeństwa online w kontekście kulturowym | |
| **Opis:** | |
| Technologie cyfrowe zrewolucjonizowały każdy aspekt naszego życia. Wpłynęły one na łańcuchy wartości wszystkich sektorów kultury i sektora kreatywnego nie tylko w odniesieniu do procesu twórczego i jego realizacji, ale także w odniesieniu do tworzenia dzieła lub produktu sztuki oraz jego promocji, dystrybucji, marketingu i sprzedaży.  Ta czesc edukacyjna nauczy przyszlych uzytkownikow wykrywania potencjalnych oszustw, które mogą ich spotkać w internecie podczas korzystania lub wyszukiwania zasobów kulturowych. Dostarczy konkretnych przykładów typowych oszustw związanych z zasobami kulturowymi, takich jak fałszywa sprzedaż biletów, próby phishingu po zamówieniu online itp. Przedstawi również kluczowe punkty w identyfikacji bezpiecznych zasobów kulturowych w internecie.  W dzisiejszej erze technologii fałszywe wiadomości i niekompletne informacje są częścią codziennego obiegu i informacji online. Użytkownicy zostaną zapoznani z tym, jakie jest znaczenie fałszywych wiadomości, niekompletnych informacji, manipulacji przekazem, jak je rozpoznac rozpoznać i jak sie przed nimi chronic.  Wspieranie zdolności rozpoznawania i ochrony przed niekompletnymi informacjami i fałszywymi wiadomościami odbywa sie poprzez dostarczajączanie informacji i treści w odniesieniu do zdolności użytkowników. Porady i wskazówki są dostarczane wraz z przydatnymi przykładami i zdjęciami. | |

|  |  |
| --- | --- |
| **Zawartość ułożona w 3 poziomach** | |
| 1. **WPROWADZENIE** 2. **ZAWARTOŚĆ**   **Część 1: Co to jest bezpieczeństwo online?**  1.1 Rozumienie pojecia bezpieczenstwa w sieci.  1.2 Bezpieczeństwo online w treściach kulturowych  **Część 2: Największe zagrożenia dla bezpieczeństwa w internecie**   * 1. Rodzaje zagrożeń bezpieczeństwa   ● złośliwe oprogramowanie   * atak kryptologiczny (man-in-the-middle) * defraudacja * kradzież hasla   **Część 3: Identyfikacja niekompletnych informacji, dezinformacji, fałszywych wiadomości w kontekście kulturowym**  3.1 Skąd pochodzą fałszywe wiadomości?  3.2 Jak rozpoznać fałszywe wiadomości, dezinformację, niekompletne informacje w kontekście kulturowym  **Część 4: Ochrona przed zagrożeniami bezpieczeństwa online**  4.1 Chroń się w trybie online   * 1. Wskazówki dotyczące bezpieczeństwa online w kontekście kulturowym   **4. KONKLUZJA**  **Moduł: Jak zidentyfikować brakujące informacje i fałszywe wiadomości online w kontekście związanym z kulturą**   1. **WPROWADZENIE**   Technologie cyfrowe zrewolucjonizowały każdy aspekt naszego życia. Wpłynęły one na łańcuchy wartości wszystkich sektorów kultury i sektora kreatywnego nie tylko w odniesieniu do procesu twórczego i jego realizacji, ale także w odniesieniu do tworzenia dzieła lub produktu sztuki oraz jego promocji, dystrybucji, marketingu i sprzedaży. W miarę jak trwa cyfrowa zmiana, coraz więcej artystów, filmowców, producentów, muzyków rozpowszechnia swoje produkty cyfrowo.  Pod koniec tego modułu zdobędziesz wiedzę jak rozpoznawac fałszywe i nieuczciwe informacje, a także zrozumiesz bezpieczeństwo online w kontekście kulturowym.  W świecie, w którym atak hakerski odbywa się mniej więcej co 39 sekund, bezpieczeństwo online nie może być już lekceważone. W przeciwnym razie wszystkie twoje dane osobowe mogą być zagrożone.  Ale czym dokładnie jest bezpieczeństwo online? Jakie zagrożenia występują w sieci i co możesz zrobić, aby się przed nimi chronić?  Zagrożenie bezpieczeństwa online odnosi się do każdego możliwego ataku, który ma na celu bezprawnie uzyskac dostęp do prywtnych danych lub/ i zakłócic operacje cyfrowe. Obecnie, bardziej niż kiedykolwiek, treści kulturowe są szeroko dostępne, są również otwarte na wszelkie zagrożenia online. Kazda nieprawdziwa informacja, falszywa wiadomosc moze prowadzic do zniszczenia osobistego dorobku lub renomy przedsiewziecia.  **Część 1: Co to jest bezpieczeństwo i ochrona online?**  **1.1 Pojecie bezpieczeństwa i ochrony w internecie**  Bezpieczeństwo i ochrona w internecie składa się z szeregu taktyk zabezpieczajacych w celu ochrony działań i transakcji przeprowadzanych online. Taktyki te mają na celu ochronę użytkowników przed zagrożeniami, takimi jak włamania do systemów komputerowych, adresów e-mail lub stron internetowych. Bezpieczeństwo i ochrona w internecie jest specyficznym aspektem szerszych pojęć, takich jak cyberbezpieczeństwo i bezpieczeństwo komputerowe, koncentrując się na konkretnych zagrożeniach i lukach w dostępie do internetu i korzystaniu z internetu..  **Odpowiednie zabezpieczenie online** chroni osoby korzystające internetu przed zagrozeniami poprzez odpowiednia świadomość, edukację, informacje i technologię. Ochrona online jest świadoma charakteru możliwych zagrożeń, które możesz napotkać podczas angażowania się w aktywność za pośrednictwem internetu, dlatego tez, zarządza i skutecznie zabezpiecza twoje dane osobowe przed szkodliwymi lub nielegalnymi treściami.  **1.2 Bezpieczeństwo treści kulturowych online**  Technologie cyfrowe zrewolucjonizowały każdy aspekt naszego życia, a kultura nie jest wyjątkiem. Wpłynęły one na łańcuchy wartości wszystkich sektorów kultury i sektora kreatywnego nie tylko w odniesieniu do procesu twórczego i jego realizacji, ale także w odniesieniu do tworzenia dzieła lub produktu sztuki oraz jego promocji, dystrybucji, marketingu i sprzedaży. Niektóre procesy produkcyjne mają charakter wyłącznie cyfrowy, a technologia ma ogromny potencjał, aby uczynić kulturę dostępną dla wszystkich, poprzez demokratyzację zarówno konsumpcji, jak i zaangażowania w tworzenie kultury.  Jednocześnie instytucje kulturalne, takie jak muzea, archiwa, biblioteki oraz producenci filmowi, telewizyjni i muzyczni, digitalizują swoje zbiory, starając się je zachować i szerzej udostępnić.  Czasami digitalizacja jest koniecznym krokiem, jak w przypadku filmow analogowch, których nie można już wyświetlać w oryginalnej formie, ponieważ kina są wyposażone wyłącznie w technologię cyfrową.  Bogactwo cyfrowych treści kulturowych jest dostępnych online za darmo, za opłatą lub nielegalnie. Taka dostępność i obfitość treści kulturowych oraz różne sposoby wymieniania się nimi w internecie przynoszą nowe możliwości i zagrożenia wobec bezpieczeństwa danej osoby w internecie. Dlatego ważne jest, aby w erze cyfrowej być poinformowanym i znać zagrożenia online oraz wiedzic jak się chronić podczas pozyskiwania dostępu do treści kulturowych online.  **Część 2: Największe zagrożenia dla bezpieczeństwa w internecie**  **Rozdział 2.1 Rodzaje zagrożeń bezpieczeństwa online**  Zagrożenie bezpieczeństwa online odnosi się do każdego możliwego ataku, który ma na celu bezprawnie uzyskac dostęp do prywatnych danych lub zakłócic proces operacji cyfrowych.  W internecie istnieją dziesiątki zagrożeń bezpieczeństwa online, dlatego postanowiliśmy skupić się na tych najbardziej niebezpiecznych i powszechnych.  **Złośliwe oprogramowanie (Malware):**  Malware to złośliwe oprogramowanie szpiegujące, ransomware, wirusy i robaki. Złośliwe oprogramowanie jest aktywowane, gdy użytkownik kliknie na szkodliwy link lub załącznik, co prowadzi do zainstalowania niebezpiecznego oprogramowania, które po aktywacji może doprowadzic do:  ● Blokowania dostępu do kluczowych komponentów systemu (ransomware)  ● Zainstalowania innego szkodliwego oprogramowania  ● Nielegalnego uzyskiwania informacji poprzez przesyłanie danych z dysku twardego (oprogramowanie szpiegujące))  ● Zakłócania pracy poszczególnych części, co uszkadza system komputera    **Atak kryptologiczny(Man in the Middle, MITM):**  Atak kryptologiczny (MITM) zagrożenie występuje, gdy dwoje uzytkownikow(napastnikow) przystepuje do dwustronnej transakcji danych. Po przerwaniu transakcji mogą filtrować i kraść miedzy soba dane innych bez niczyjej wiedzy. Zagrożenie MITM jest często realizowane, gdy odwiedzający korzysta z niezabezpieczonej publicznej sieci Wi-Fi. Strony atakujace umieszczają się między odwiedzającym a siecią, a następnie wykorzystują wspomniane wcześniej złośliwe oprogramowanie do instalowania oprogramowania i bezprawnego wykorzystywania danych.  **Atak Phishingowy:**  Ataki phishingowe wykorzystują fałszywą komunikację, taką jak wiadomość e-mail, aby nakłonić odbiorcę do jej otwarcia i wykonania instrukcji w środku, np: podanie numeru karty kredytowej. Celem jest kradzież poufnych danych, takich jak dane karty kredytowej i dane logowania, lub zainstalowanie złośliwego oprogramowania na komputerze ofiary.  **Kradziez Hasła :**  Dzięki odpowiedniemu hasłu cyberprzestepca ma dostęp do bogactwa informacji. Inżynieria społeczna to rodzaj ataku hasłem, który jest definiowany jako "strategia, która w dużej mierze opiera się na interakcji międzyludzkiej i często polega na nakłanianiu ludzi do łamania standardowych praktyk bezpieczeństwa".  Inne rodzaje ataków na hasła obejmują dostęp do bazy haseł lub bezpośrednie zgadywanie.  **Część 3: Identyfikacja niekompletnych informacji,fałszywych wiadomości i manipulacji przekazem tresci w kontekście kulturowym**  Zagrożenie bezpieczeństwa online odnosi się do każdego możliwego ataku, który ma na celu bezprawnie uzyskac dostęp do prywtnych danych lub/ i zakłócic operacje cyfrowe. Obecnie, bardziej niż kiedykolwiek, treści kulturowe są szeroko dostępne, są również otwarte na wszelkie zagrożenia online. Kazda nieprawdziwa informacja, falszywa wiadomosc moze prowadzic do zniszczenia osobistego dorobku lub renomy przedsiewziecia.  **3.1 Co oznaczaja fałszywe wiadomości, dezinformacja i manipulacja przekazem tresci?**  **Fałszywe wiadomości** to celowo spreparowane, sensacyjne, naładowane emocjonalnie, wprowadzające w błąd lub całkowicie sfabrykowane informacje.  Istnieją dwa rodzaje fałszywych wiadomości:  1. Historie, które nie są prawdziwe. Są to całkowicie wymyślone historie mające na celu sprawienie, by ludzie uwierzyli w coś fałszywego, kupili określony produkt lub odwiedzili określoną stronę internetową.  2. Historie, które mają trochę prawdy, ale nie są w 100 procentach dokładne. Ponownie, może to być celowe, aby przekonać czytelników do określonego punktu widzenia.  Termin **dezinformacja** odnosi się do informacji, które są fałszywe lub niedokładne i często są szeroko rozpowszechniane wśród innych, niezależnie od zamiaru wprowadzenia w błąd lub nie.  Podczas gdy dezinformacja to fałszywe informacje, które są tworzone i rozpowszechniane niezależnie od intencji aby zaszkodzić lub oszukać, natomiast **manipulacja przekazem** jest stworzona, aby celowo wprowadzać w błąd. Oba formularze mogą być szeroko udostępniane, niezależnie od tego, czy współużytkujący wie czy nie, że informacje są błędne.  Platformy mediów społecznościowych pozwalają prawie każdemu publikować swoje przemyślenia lub dzielić się prywatnymi historiami ze światem. Problem polega na tym, że większość osob nie sprawdza źródła materiału, które publikuja i udostępniają online , co może prowadzić do szybkiego rozprzestrzeniania się fałszywych i niebezpiecznych wiadomości . Jednocześnie co raz trudniej jest zidentyfikować oryginalne źródło wiadomości, co doprowadza do manipulacji przekazem.  **3.2 Jak rozpoznać fałszywe wiadomości,dezinformacje i manipulacje przekazem tresci w kontekście kulturowym**  Jak rozpoznać fałszywe wiadomości, dezinformację i manipulacje przekazem tresci, zadaj sobie kolejne pytania i wykonaj następujące czynności: :  ● **Kto to napisał?** Sprawdź nazwisko autora. Czy nazwa jest dostępna, czy jej brakuje? Większość autorów, którzy poświęcają czas na dobrze zbadany artykuł, prawdopodobnie będzie miała dołączone do niego swoje nazwisko..  ● **Jakie są ich kwalifikacje?** Jeśli nazwisko autora znajduje się na liście, dowiedz się, kim jest ta osoba i jakie są jej poświadczenia.  ● **Sprawdź sekcję "O nas".** Na górze lub na dole strony powinna znajdować się sekcja o nazwie "O nas". W tej sekcji przedstawiono cel strony internetowej.  ● **Czy artykuł informuje o wszystkich stronach tematu?** Artykuły informacyjne powinny dostarczać faktów z różnych punktów widzenia.  ● **Czy treść pasuje do nagłówka artykułu?** Nagłówek powinien dać ci wyobrażenie o tym, o czym jest cały artykuł, ale może być również użyty do przekonania cię do uwierzenia w coś przed przeczytaniem artykułu.  ● **Kiedy ten artykuł został opublikowany?** Starsze artykuły mogą nie zawierać aktualnych faktów i mogą mieć uszkodzone linki.  ● **Czy artykuł został zmieniony lub zaktualizowany?** Zmieniona lub zaktualizowana treść ma zwykle zastrzeżenie na początku lub na końcu artykułu.  ● **Jak ważna jest data**? Data daje wskazówkę, kiedy artykuł został opublikowany.  ● **Czy ten adres internetowy (URL) wygląda poprawnie?** Wpisanie niewłaściwego adresu internetowego spowoduje przekierowanie do strony internetowej, której nie zamierzałeś odwiedzać. Może to doprowadzić do strony z wcześniej wymienionymi zagrożeniami bezpieczeństwa online.  ● **Czy znalazłem to w mediach społecznościowych?** Platformy mediów społecznościowych nie są organizacjami informacyjnymi. Są to platformy do tworzenia i/lub udostępniania treści.  ● **Czy znalazłem to na blogu / stronie internetowej?** Blogi zawierają treści napisane nieformalnie i prowadzone są przez osobę lub małą grupę.  **Część 4: Ochrona przed zagrożeniami bezpieczeństwa online**  **4.1 Chroń się podczas pracy online**  Oto kilka rzeczy, które możesz wykonać lepiej, aby chronić się w trybie online:   1. **Nie używaj niezabezpieczonych sieci WiFi**   Najlepiej unikać sieci Wi-Fi, która nie prosi o hasło, i po prostu użyć własnego planu taryfowego.  **2. Użyj silnego i sprawdzonego oprogramowania antywirusowego**  Oprogramowanie antywirusowe to najlepszy sposób na zabezpieczenie urządzenia przed wirusami lub złośliwym oprogramowaniem, o których mówiliśmy. Nie daj się zwieść nazwie - program antywirusowy walczy z wirusami, ale atakuje głównie złośliwe oprogramowanie (wirus jest rodzajem złośliwego oprogramowania). Upewnij się, że program jest aktualizowany i że uruchamiasz częste skanowanie - szczególnie po pobraniu nowych plików. Najlepiej nie otwierać ich bez uprzedniego zeskanowania.  **3. Zawsze używaj VPN Online**  VPN (Virtual Private Network) to usługa online, za pomocą której można ukryć swój prawdziwy adres IP i zaszyfrować komunikację online. Jest to jeden z najlepszych sposobów na zwiększenie bezpieczeństwa online i ukrycie cyfrowych śladów. Tak długo, jak stosowane są odpowiednie metody szyfrowania, nikt nie będzie w stanie monitorować ruchu online, aby zobaczyć, co robisz w Internecie.  **4. Unikaj prób wyłudzenia informacji**  Jeśli otrzymasz e-maile lub wiadomości rzekomo od kogoś bliskiego, twojego banku lub policji z prośbą o pobranie podejrzanych załączników, dostęp do skróconych linków lub udostępnienie poufnych informacji, zignoruj je. Zamiast tego skontaktuj się z domniemanym nadawcą, aby dowiedzieć się prawdy. Spróbuj wygooglować fragmenty wiadomości otrzymanej między cytatami. Jeśli jest to oszustwo phishingowe, prawdopodobnie uzyskasz wyniki, w których inne osoby mówią o otrzymaniu tej samej wiadomości.    **5. Nie trzymaj Bluetooth włączonego**  Podczas gdy Bluetooth ma swoje zastosowania, utrzymywanie go włączonego przez cały czas jest dość ryzykowne. W 2017 roku odkryto nową metodę hakowania Bluetooth, która dotknęła miliony urządzeń, umożliwiając hakerom korzystanie z mitM Man in the Middle w celu uzyskania informacji o urządzeniu. Podsumowując, lepiej być po bezpiecznej stronie i wyłączyć Bluetooth, gdy go nie używasz, aby zachować nienaruszone bezpieczeństwo online.  **6. Wyłączanie usług lokalizacji na urządzeniach mobilnych**  Usługi lokalizacyjne mogą być naprawdę przydatne, ale mogą być również bardzo ryzykowne. Istnieje fakt, że niektóre aplikacje mogą wyciekać z twojej lokalizacji. Jeśli tak się stanie, nie oznacza to, że będziesz w bezpośrednim niebezpieczeństwie ale twoje bezpieczeństwo online będzie zagrożone.  **7. Użyj blokerów skryptów w swoich przeglądarkach**  Blokowanie skryptów to rozszerzenia przeglądarki, których możesz użyć, aby upewnić się, że witryny, do których uzyskujesz dostęp, nie uruchamiają nieautoryzowanych skryptów i wtyczek w tle, które mogą zagrozić bezpieczeństwu w Internecie. Nie zapominaj - niektóre skrypty mogą być tak niebezpieczne, że mogą przejąć przeglądarkę, podczas gdy inne mogą uruchamiać przekierowania phishingowe lub reklamy, a nawet wydobywać kryptowaluty za pomocą procesora.  **8. Aktualizuj swój system operacyjny**  Nieinstalowanie najnowszych aktualizacji w systemie operacyjnym może poważnie zaszkodzić bezpieczeństwu online. Ponieważ złośliwi aktorzy mogą wykorzystywać potencjalne luki w zabezpieczeniach na swoją korzyść – luki, które mogły zostać naprawione za pomocą najnowszej aktualizacji.  **9. Rozważ użycie zaszyfrowanych aplikacji do przesyłania wiadomości i wiadomości e-mail**  Jeśli chcesz naprawdę upewnić się, że Twoja komunikacja online jest bezpieczna, możesz spróbować użyć różnych aplikacji do przesyłania wiadomości. Ta funkcja naprawdę potężnego szyfrowania.  Jeśli chodzi o e-maile, jest tak samo, szukaj w Internecie różnych aplikacji i jakie rodzaje bezpieczeństwa oferują.  **10. Używaj silnych haseł**  Posiadanie siuklnych haseł dla twoich kont jest niezwykle ważne, ale wymyślenie naprawdę dobrego jest łatwiejsze do powiedzenia niż do zrobienia.  Jeśli potrzebujesz pomocy, oto główne pomysły:  1. Użyj spacji, jeśli jest to dozwolone.  2. Używaj tylko długich haseł. Najlepiej nie trzymać się tylko jednego słowa.  3.Nie używaj słów słownikowych jako hasła.  4.Używaj zarówno wielkich, jak i małych liter i losowo je mieszaj.  5.Użyj symboli (takich jak $, % lub \*) w haśle.  6.Uwzględnij liczby w haśle.  7.Spróbuj ustawić hasło jako całe zdanie.  8.Odwróć niektóre słowa użyte w haśle (zamiast "stop" użyj "ostp").  9. Staraj się również nie używać tego samego hasła do wszystkich swoich kont. Lepiej jest używać różnych haseł lub przynajmniej kilku odmian głównego hasła.  **4.2 Wskazówki dotyczące bezpieczeństwa online w kontekście kulturowym**  Dzięki internetowi istnieje kilka sposobów na zdobycie biletów na nadchodzące wydarzenie. Minusem jest to, że istnieje również wiele pułapek, których konsumenci muszą unikać. Kliknięcie niewłaściwego linku lub zaufanie niewłaściwej stronie internetowej może doprowadzić do fałszywego biletu i utraty środków.  Oto kilka wskazówek, jak być bezpiecznym w Internecie, z konkretnym przykładem zakupu biletów online na wydarzenie kulturalne:  • **Kupuj bezpośrednio na miejscu, gdy tylko jest to możliwe**. Wielu oficjalnych agentów sprzedaży biletów oferuje teraz również dodatkowe opcje sprzedaży. Nie klikaj z e-maili lub reklam online; powszechną sztuczką oszustwa biletowego jest utworzenie adresu internetowego podobnego do znanej firmy.  **• Zastanów się nad źródłem**. Poznaj różnicę między profesjonalnym brokerem biletów (legalnym i akredytowanym sprzedawcą), skalperem biletów (nieuregulowanym i nielicencjonowanym sprzedawcą biletów) a oszustem sprzedającym falszywe bilety.  • **Poznaj zasady zwrotów**. Bilety należy kupować wyłącznie od sprzedawcy biletów, który podaje jasne szczegóły dotyczące warunków transakcji. Sprzedający powinni ujawnić kupującemu, przed zakupem, lokalizację miejsc reprezentowanych przez bilety, ustnie lub poprzez odniesienie do tabeli miejsc; a jeśli bilety nie są dostępne do natychmiastowego odbioru dla kupującego, powiadom, kiedy bilety zostaną wysłane lub będą dostępne do odbioru.  • **Zawsze używaj karty kredytowej**, w ten sposób masz możliwość rezygnacji, jeśli bilety nie są zgodne z przedstawionymi w ofercie. Karty debetowe, przelewy bankowe lub transakcje gotówkowe są ryzykowne; jeśli bilety są fałszywe, najprawdopodobniej nie będziesz w stanie odzyskaćswoich pieniędzy.    • **Uważaj na reklamy**. Kiedy przeszukujesz internet w poszukiwaniu biletów online, często pojawiają się reklamy tanich biletów. Kieruj się zdrowym rozsądkiem; niektóre z tych reklam będą oszustwami , zwłaszcza jeśli ceny są wyjatkowo niskie lub atrakcyjne .  • **Jeśli nie masz pewności, zweryfikuj swoje bilety**. Odwiedź miejsce, w którym ma odbyc się wydarzenie. Przedstaw swój bilet obsłudze klienta, a oni pomogą ci zweryfikować, czy Twój bilet jest legalny .   1. **KONKLUZJA**   Bezpieczeństwo online w szerszym kontekście kulturowym jest bardzo interesującym tematem, a szeroko dostępne treści kulturowe niestety są także przedmiotem zagrożeń online.  Technologie cyfrowe zrewolucjonizowały każdy aspekt naszego życia. Wpłynęły one na łańcuchy wartości wszystkich sektorów kultury i sektora kreatywnego nie tylko w odniesieniu do procesu twórczego i jego realizacji, ale także w odniesieniu do tworzenia dzieła lub produktu sztuki oraz jego promocji, dystrybucji, marketingu i sprzedaży. W miarę jak trwa cyfrowa zmiana, coraz więcej artystów, filmowców, producentów, muzyków rozpowszechnia swoje produkty cyfrowo.  Pod koniec tego modułu zdobędziesz wiedzę na temat rozpoznawania fałszywych informacji, a także bezpieczeństwa online w kontekście kulturowym. Korzystając ze wskazówek i podanych przykładów możesz zwiększyć swoje bezpieczeństwo w internecie. Ponieważ zagrożenia bezpieczeństwa, takie jak złośliwe oprogramowanie, oszustwa, phishing, hakowanie oraz rozprzestrzenianie dezinformacji, fałszywe wiadomości czy manipulacja przekazem tresci stają się coraz bardziej powszechne w dzisiejszych czasach, bezpieczeństwo online stało się ważniejsze niż kiedykolwiek.  Bezpieczeństwo online? / Kluczowe punkty  Zabezpieczenia online to reguły, których przestrzegasz; działania, które podejmujesz, i procesy, które mają na celu zapewnienie bezpieczeństwa internecie.  Zazwyczaj najlepszym sposobem, aby upewnić się, że jesteś bezpieczny w Internecie, jest użycie m.in silnego programu antywirusowego, niezawodnej sieci VPN, silnych haseł i blokerów skryptów.  Fałszywe wiadomości odnoszą się do celowego szerzenia nieprawdy lub historii, które zawierają pewną prawdę, ale które nie są całkowicie dokładne.  Niektórzy twierdzą również, że prawdziwe historie są "fałszywymi wiadomościami", tylko dlatego, że się z nimi nie zgadzają. Może to prowadzić do niebezpiecznego ignorowania istotnych porad.  Fałszywe wiadomości mogą mieć negatywny wpływ na społeczne i kulturowe aspekty społeczeństwa, dlatego ważne jest, aby wiedzieć, jak oddzielić prawdziwe wiadomości od fałszywych, a także rozpoznać, kiedy mamy do czynienia z niekompletnymi informacjami, dezinformacja lub manipulacja przekazu tresci. Możesz to zrobić, wykonując następujące sześć kroków:  1.Rozwijaj krytyczny sposób myślenia.  2.Sprawdź źródło.  3.Zobacz, kto jeszcze relacjonuje historię.  4.Zbadaj dowody.  5. Nie rób zdjęć  6.Sprawdź, czy tekst"brzmi poprawnie". | |
| **Zawartość w punktach** | |
| Treści kulturowe są szeroko dostępne w internecie i otwarte na zagrożenia online. Rozpowszechnianie niekompletnych informacji, fałszywych wiadomości i dezinformacji, moze wprowadzac w blad osobe zaintersowana wydarzeniem kulturalnym.   1. Bezpieczeństwo w internecie składa się z szeregu taktyk bezpieczeństwa w celu ochrony działań i transakcji przeprowadzanych online.  * Zagrożenie bezpieczeństwa online odnosi się do każdego możliwego ataku, który ma na celu bezprawnie dostac sie do prywatnych danych; zakłócic operacje cyfrowe lub zmanipulowac informacje..  1. Bezpieczeństwo w Internecie jest świadome charakteru możliwych zagrożeń, które możesz napotkać podczas angażowania się w aktywność za pośrednictwem Internetu, mogą to być zagrożenia bezpieczeństwa, ochrona i zarządzanie twoimi danymi osobowymi online oraz unikanie szkodliwych lub nielegalnych treści. Ochrona w internecie chroni osoby wykonujące działania online poprzez świadomość, edukację, informacje i technologię. 2. W Internecie istnieją dziesiątki zagrożeń bezpieczeństwa online, moduł ten koncentruje się na najbardziej niebezpiecznych i powszechnych, takich jak: Malware; atak kryptologiczny MITM; Phishing; kradziez hasła itp. 3. Internauci powinni wiedzieć, jak rozpoznawać fałszywe wiadomości i odpowiednio się chronić. Fałszywe wiadomości mogą mieć negatywny wpływ na społeczne i kulturowe aspekty społeczeństwa, dlatego ważne jest, aby wiedzieć, jak oddzielić prawdziwe wiadomości od fałszywych a także rozpoznać, kiedy mamy do czynienia z dezinformacja lub manipulacja przekazem tresci. | |
| **5 wpisow w glosariuszu** | |
| **1) Bezpieczeństwo online**  Bezpieczeństwo w internecie składa się z szeregu taktyk bezpieczeństwa w celu ochrony działań i transakcji przeprowadzanych online przez Internet.  **2) Bezpieczeństwo w internecie**  Bezpieczeństwo w internecie jest świadome charakteru możliwych zagrożeń, które możesz napotkać podczas angażowania się w aktywność za pośrednictwem Internetu, mogą to być zagrożenia bezpieczeństwa, ochrona i zarządzanie twoimi danymi osobowymi online oraz unikanie szkodliwych lub nielegalnych treści. Bezpieczeństwo w internecie chroni osoby wykonujące działania online poprzez świadomość, edukację, informacje i technologię.  **3) Kontekst kulturowy**  Kontekst kulturowy jest związany ze społeczeństwem, w którym jednostki są wychowywane i w jaki sposób kultura wpływa na zachowanie. Zawiera wartości, które są wyuczone i postawy, które są wspólne dla grup ludzi. Obejmuje wierzenia, znaczenia, zwyczaje, idee, język, normy.  Odnosi się do znaczenia symbolicznego, wymiaru artystycznego i wartości kulturowych, które pochodzą lub wyrażają tożsamości kulturowe.  **4) Fałszywe wiadomości**  Fałszywe wiadomości, często o charakterze sensacyjnym, tworzone sa w celu szerokiego udostępniania lub rozpowszechniania w celu generowania przychodów lub promowania lub dyskredytowania osoby publicznej, ruchu politycznego, firmy itp.  **5) Brakujące informacje**  to niekompletne lub niedokładne informacje, które mają na celu odwrócenie uwagi od dokładnych informacji, spowodowanie zamieszania lub zmianę kontekstu zdania, działania, działania itp. | |
| **Bibliografia i dalsze odniesienia** | |
| * <https://www.mindtools.com/pages/article/fake-news.htm> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media> * <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf> * <https://www.nature.com/articles/s41586-021-03344-2> * <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf> * <https://academicguides.waldenu.edu/library/fakenews/examples> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690570> * <https://en.wikipedia.org/wiki/Fake_news> * <https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news> * <https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users> * <https://researchguides.austincc.edu/c.php?g=612891&p=4258046> | |
| **Pięć pytań samooceny wielokrotnego wyboru** | 1) Wiadomość e-mail w skrzynce odbiorczej prosi o zalogowanie się za pomocą hasła ze względów bezpieczeństwa. Co byś zrobił?   1. Nic, zignoruję wiadomość 2. Zrobię to, co o to poproszę, to ze względów bezpieczeństwa 3. Skontaktuję się z ekspertem IT, aby uzyskać więcej informacji   **Poprawna odpowiedź: A**  2) Jesteś na stronie internetowej, która sprzedaje bezpłatne bilety na wydarzenie kulturalne w pobliżu. Są one bezpłatne i proszą tylko o podanie niektórych danych osobowych. Co byś zrobił?   1. Kupię bilety i wprowadam moje dane osobowe 2. Sprawdzę stronę internetową, aby sprawdzić, czy jest prawdziwa, a jeśli nie, aby zgłoszam witrynę jako podejrzana   C . Udostępnię stronę, aby inni mogli również zdobyć bilety  **Poprawna odpowiedź: B**  3) Odbyłeś wirtualną wycieczkę po znanym miejscu kulturalnym. Zauważyłeś niekompletne informacje na jednej z witryn. Co byś zrobił?  A. Sam wypełnię brakujacy tekst  B. Poinformuję wirtualnego przewodnika o tym możliwym błędzie  C . Nic nie zrobię  **Poprawna odpowiedź: B**  4) Tworzysz konto na stronie internetowej i powinieneś utworzyć hasło. Które hasło jest najbezpieczniejsze?   1. Twoje imię i nazwisko 2. Losowa linia cyfr i liter, które możesz napisać na kartce papieru, aby zapamiętać 3. Twój numer ubezpieczenia społecznego PESEL   **Poprawna odpowiedź: B**  5) Czy przechowujesz swoje dane osobowe w bezpiecznym miejscu podczas korzystania z sieci społecznościowych   1. Tak 2. Nie 3. Nie jestem pewien   **Poprawna odpowiedź: Opcjonalnie, wszystkie odpowiedzi są poprawne** |
| **Powiązane materiały** | Jak zidentyfikować brakujące informacje i fałszywe wiadomości online w kulturze istotnej context\_PPT\_CDI |
| **Powiązane PPT** |  |
| **Link referencyjny** |  |
| **Film w formacie YouTube (jeśli istnieje)** | <https://youtu.be/vPAW5j_L4-c>  <https://www.youtube.com/watch?v=0yL-k5nB65o> |