Media społecznościowe i manipulacje

Warsztat porusza podstawowe zagadnienia związane z ochroną swojej prywatności i wizerunku w sieci oraz manipulacjami medialnymi. Podczas zajęć, uczestnicy poznają mechanizmy profilujące nasze zachowanie w sieci oraz związane z tym zagrożenia. Celem warsztatu jest uświadomienie uczestnikom potrzeby dbania o swoją prywatność i wizerunek w sieci oraz rozwijanie umiejętności świadomego korzystania z mediów społecznościowych. Efektem warsztatów ma być realne zwiększenie bezpieczeństwa swojego konta, w przeciwieństwie do słuchania o tym, co powinno zostać wdrożone.

Czas trwania: 90 min.

Grupa wiekowa: 12 do 18

Cele:

1) **Cele ogólne:**
    a) Rozwijanie umiejętności dbania o swój wizerunek w sieci,
    b) Rozwijanie umiejętności wykrywania manipulacji medialnych
2) **Cele szczegółowe:**
    a) Stworzenie bezpiecznego adresu e-mail;
    b) Uświadomienie zagrożeń związanych z udostępnianiem swojego wizerunku i danych w sieci;
    c) Poznanie metod i sposobów dbania i swoją prywatność i wizerunek w Internecie;
    d) Rozwijanie umiejętności krytycznego myślenia i weryfikowania informacji;
    e) Poznanie metod i narzędzi służących weryfikacji informacji.

Potrzebne materiały:

Komputery z systemem Windows, połączenie internetowe, przeglądarka Google Chrome

Projekt finansowany ze środków Kancelarii Prezesa Rady Ministrów w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli „Cyberbezpieczni”

Przygotowanie dla trenera:

Zapoznaj się z dodatkowymi materiałami i narzędziami obecnymi w scenariuszu. Przejdź przez ścieżki zmiany ustawień prywatności w mediach społecznościowych.

ETAPY REALIZACJI

Czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Wprowadzenie:** Przywitaj uczestników, przedstaw się i powiedz, czym jest CDT i o czym jest dzisiejszy warsztat (media społecznościowe i prywatność w sieci – jak ochronić swoją prywatność w sieci oraz rozpoznawać manipulacje medialne). Ustal z uczestnikami zasady towarzyszące nam podczas dzisiejszego warsztatu (nie przejmujemy się problemami technicznymi, zasada 5+5= 5 minuty pełnego skupienia dla edukatora i 5 minuty pracy i zabawy dla uczestników). Podkreśl, że w ramach dzisiejszego warsztatu będziesz musiał zaprezentować uczestnikom wiele różnego rodzaju linków. Najłatwiejszym sposobem na zrobienie tego będzie wyświetlenie kodu QR. Poproś zatem wszystkich o zainstalowanie na swoich telefonach aplikacji do skanowania kodów: np. obiektywu Google. Wytłumacz, że zanim przejdziemy do kwestii prywatności w sieci, musimy poznać doświadczenie uczestników z social mediami.	Uwaga: W zależności od doświadczenia grupy z programowaniem, dobierz późniejsze ćwiczenia oraz sposób pracy. Uwaga 2: Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych.

15 min	**Diagnoza** Zapytaj o doświadczenie grupy z mediami społecznościowymi – W ilu SM mamy konta? Jakie są to aplikacje i strony? Ilu mamy łącznie followersów? Uczestnicy mogą wpisać orientacyjne liczby na czacie (część ilościowa). Zwróć uwagę na skalę liczb – czy są to duże liczby wskazujące na znaczną obecność w sieci, czy małe. Podkreśl, że nasza obecność w sieci będzie się najprawdopodobniej stawała coraz większa – będziemy mieć wiele kont, w różnych serwisach i korzystać z różnego rodzaju aplikacji. Nasze zasięgi też będą prawdopodobnie rosły – będziemy mieć więcej znajomych, followersów, a może nawet konta służbowe i funpage. Wszystko to nie jest niczym złym, jednak wraz ze wzrostem naszej obecności w mediach, warto zadbać również o nasze bezpieczeństwo (tym zajmowaliśmy się poprzednio) oraz naszą prywatność. Skupimy się zatem na oddzieleniu naszego życia prywatnego, prywatnych kont mailowych, ważnych danych, od tego, co udostępniamy w sieci. Tym właśnie zajmiemy się dzisiaj. Powiedz, że są dwa ważne obszary dbania o dane – dane, które zbierają o nas media społecznościowe (za pomocą profilowania i śledzenia naszej aktywności) oraz dane, które udostępniamy w sieci i które mogą służyć nie tylko profilowaniu, ale również zostać wykorzystane przez osoby trzecie. Podkreśl, że zaczniemy od pierwszego obszaru i dowiemy się co wie o nas google i facebook. Pokaż ścieżki dostępne w prezentacji: Następnie zapytaj: - Czy algorytmy dobrze nas sprofilowały? - Skąd algorytmy to wiedzą? Podkreśl, że algorytmy profilowania w poszczególnych sieciach społecznościowych korzystają	Zapoznaj się z materiałami: https://www.youtube.com/watch?v=uaaC57tcci0&t=3s https://www.youtube.com/watch?v=B8ofWFx525s https://www.youtube.com/watch?v=1J-90nGlzBE

	z ogromnej ilości danych. Będą się dla nich liczyły dane zadeklarowane przez nas wprost – co polubiliśmy, wpisaliśmy w zainteresowania, co dodaliśmy do „obserwowanych". Algorytmy będą jednak analizować rzeczy, z których my sami nie zdajemy sobie często sprawy – jak wiele czasu poświęciliśmy na obejrzenie danego filmiku? Gdzie zatrzymaliśmy się podczas skrolowania newsfeeda, co kliknęliśmy itp. Podkreśl, że jest to mechanizm, który staje się coraz bardziej zaawansowany ale niestety i niebezpieczny. Pozwala nam on algorytmom podsuwać nam treści, które rzeczywiście mogą nam się spodobać, ale pozwala on równocześnie na „sterowanie" naszymi zainteresowaniami i zamyka nas w tak zwanych bańkach filtrujących. Bańki mają potem wpływ na wiele rzeczy, które robimy – na nasze decyzje zakupowe, na nasze poglądy i opinie, a nawet na naszą aktywność polityczną. Algorytmy mogą służyć firmom, które chcą manipulować nami w celu kupienia określonego produktu, oszustom którzy chcą przekierować nas na fałszywą stronę internetową, politykom, trollom, a nawet piewcom teorii spiskowych. Ślepe podążanie śladem algorytmu często określane jest jako "wpadnięcie do króliczej nory", gdyż może zmanipulować nas nawet do przyjęcia poglądów skrajnie niebezpiecznych. Podkreśl, że dlatego właśnie warto wykonywać okazjonalnie tak zwany feeds reboot, czyli audyt, weryfikację i uporządkowanie stron, które obserwujemy. Więcej możecie o nim przeczytać tutaj: https://sektor3-0.pl/blog/feeds-reboot-zrestartuj-algorytmy-i-odzyskaj-kontrole-nad-tym-co-widzisz-w-internecie/	
15 min	**Moje dwie twarze** Wytłumacz, że w tym momencie zajmiemy się drugim aspektem udostępniania danych w sieci, czyli danymi, które udostępniamy my: Pokaż fragment: https://www.youtube.com/watch?v=CLRBYhd7e4Q	

	A następnie zapytaj: - Skąd pochodziły te dane? - Jakiego typu były to dane? Podkreśl, że były to ogólnodostępne dane z mediów społecznościowych. Podkreśl jednocześnie, że rozwijając swoją aktywność online powinniśmy zwrócić uwagę na dwa typy danych: - Dane osobowe – są to dane, które umożliwiają naszą identyfikację. Np. nasz adres, numer Pesel, adres e-mail, imię i nazwisko. - Dane wrażliwe – są to dane dotyczące np. naszego stanu zdrowia, orientacji seksualnej, wyznawanej religii itp. Warto zwrócić uwagę na ten typ danych i informacji, gdyż są to informacje, o które nikt nie może spytać nas np. podczas rozmowy o pracę. Jednocześnie często dzielimy się nimi w mediach społecznościowych. Poproś uczestników o zapoznanie się z ćwiczeniem wcieleniowym i ułożenie minimum trzech dobrych praktyk dla ochrony swoich danych w sieci. Podkreśl, że wraz z coraz większą obecnością w sieci i coraz większą ilością obserwujących, warto zapoznać się ze sposobami ochrony swoich danych w mediach społecznościowych i że są to sposoby stosowane przez profesjonalnych youtuberów i influencerów: Pokaż fragment: https://www.youtube.com/watch?v=ut_0SVXPFTg oraz rekomendacje ułożone przez Nicka. *Jeśli masz czas, możesz pokazać uczestnikom stronę z ustawieniami prywatności konta facebook lub innego konta w mediach społecznościowych np. TikToka. Zapytaj wtedy o to, które ustawienie prywatności byłoby najlepsze do włączenia/wdrożenia?	
5 min	**Przerwa**	

10 min	**Fake news** Wyświetl artykuł z dziennika bulwarowego i daj uczestnikom chwilę na jego przeczytanie: http://dziennikbulwarowy.pl/145/prawomocnie-uznany-za-trolla-internetowego.html?u=1:30:0:77:QnVqYWs= Oraz zapytaj czy uczestnicy wiedzą jakie mogą być konsekwencje takiego orzecznictwa? Co się zmieni w przestrzeni internetowej? Zapytaj czy rzeczywiście uważają, że takie zmiany nastąpią? Następnie zapytaj czy ktoś kojarzy dziennik bulwarowy? Czy komuś ten artykuł nie wydał się podejrzany? Jeśli tak, zapytaj co budziło naszą wątpliwość? Wytłumacz, że jest to artykuł fałszywy, który każdy może wygenerować samodzielnie na stronie Dziennik Bulwarowy, podstawiając w nim swoje dane osobowe. Podkreśl, że weryfikacja tego typu artykułu może nam zająć około 5 sekund jeśli wiemy, gdzie szukać. Jeśli wcześniej nie udało nam się tego zrobić, to w tym momencie nauczymy się informacji znalezionych w sieci.	
20 min	**Factcheckingowe narzędzia** Podkreśl, że factchecking to często zadanie trudne i wymagające czasu. Zaznacz przy tym, że podstawowe zasady weryfikacji artykułu i źródeł powinien znać każdy świadomy odbiorca mediów. Wyświetl szereg factcheckingowych narzędzi na slajdzie i poproś o wybór "broni" - wybranie jednego narzędzia służącemu walce z dezinformacją i zapoznanie się z nim. https://demagog.org.pl/analizy_i_raporty/jak-radzic-sobie-z-dezinformacja-12-zasad-	Możesz przeprowadzić to ćwiczenie indywidualnie lub w grupach.

	stowarzyszenia-demagog/ https://www.szkolazklasa.org.pl/wp-content/uploads/2017/03/10-wskazowek_fake-news.pdf https://media.ceo.org.pl/aktualnosci/nie-tylko-fake-newsy https://mydigitallife.pl/uploads/CRAAP.pdf Następnie podkreśl, że wszyscy uczestnicy powinni wyobrazić sobie, że w tym momencie wcielają się w factcheckera - osobę zajmującą się weryfikacją informacji i źródeł. Ich zadaniem jest przejrzenie szeregu artykułów prasowych, które mają ukazać się w gazecie i decyzja czy są to treści prawdziwe czy zmanipulowane lub fałszywe. Jeśli fałszywe, to z jakim rodzajem oszustwa, manipulacji lub kłamstwa mamy do czynienia? Wyświetl link do folderu z artykułami: Daj uczestnikom 10 minut na weryfikację wybranego artykułu, następnie zapytaj czy jest on prawdziwy? Jeśli nie, jakim typem manipulacji/fake newsa jest? po czym możemy to poznać?	
10 min	**Sprawdzenie i podsumowanie** Raz jeszcze wyświetl artykuł z dziennika bulwarowego. Zapytaj jakie wskazówki z materiałów pomocniczych mogłyby okazać się tu pomocne? Dopytaj:	

	- jaka jest data publikacji (czy licznik minut się zmienia? – czy ktoś zwrócił na to uwagę?) - Kto jest autorem/kontakt do autora - Kim jest redakcja/informacje o redakcji/kontakt do redakcji - Źródła wskazane w tekście (jaki sąd wydał wyrok? NSA? W Pcimiu Dolnym?) - Źródło informacji na końcu tekstu (Czym jest Orient? Czym jest PAPs? Czy chodzi o Onet i PAP?) - Dowody/Potwierdzenia (czy da się znaleźć wyrok? Czy są materiały potwierdzające dane zdarzenie)?	
5 min	**Zakończenie i podsumowanie** Zapytaj który serwis lub źródło informacji uczestnicy uważają za najbardziej rzetelny? Podkreśl, że fake newsy i manipulacje medialne tak silnie na nas wpływają, ponieważ najczęściej są powiązane z medialnymi bańkami i profilowaniem nas w sieciach społecznościowych – najczęściej potwierdzają one nasze wcześniejsze opinie i poglądy. Podkreśl, że metoda, którą pracujemy w Centralnym Domu Technologii opiera się zawsze na dwóch stronach: jedna strona to podejście krytyczne – analiza, weryfikacja, ostrożność i świadomość. To podejście przydatne zarówno w obszarze cyberbezpieczeństwa, prywatności w sieci, jak i w przeglądaniu informacji medialnych. Zbyt krytyczne podejście może nas jednak też zaprowadzić w złą stronę – możemy wdrożyć tak restrykcyjne zasady bezpieczeństwa, że potem sami nie będziemy ich przestrzegać lub wylądować na teoretycznie „bezstronnym" kanale z informacjami, który karmić nas będzie teoriami spiskowymi lub bardzo zmanipulowanym materiałem przebranym w hasło „niezależnego myślenia".	

	Drugą stroną w naszym podejściu jest zatem podejście konstruktywne. Takie podejście ma na celu wymierny pozytywny efekt – pozytywny konkret. Myśląc o bezpieczeństwie powinniśmy zatem skupiać się na jednym konkretnym kroku, który wykonam, a który zwiększy moje bezpieczeństwo w sieci. Np. uruchomieniu uwierzytelniania dwuetapowego na mailu. W kontekście prywatności w sieci, powinniśmy również myśleć o jednym ustawieniu które zmienimy, o jednym nawyku, który wprowadzimy by chronić nasze dane i prywatność – (np. ograniczymy odbiorców starych postów na naszej osi czasu lub założymy osobnego maila na spam i na zarządzanie naszą działalnością jako influencera). I tak samo w kontekście fake newsów, powinniśmy szukać i dodać do swoich kanałów przynajmniej jedno źródło, które uznajemy za rzetelne – dodać PAP do obserwowanych, polajkować stronę Demagoga. Zachęć uczestników do zrobienia jednej z tej wybranych rzeczy i podkreśl, że w miarę rozwoju naszej wiedzy i umiejętności możemy wtedy wykonać kolejny krok i kolejny. Zaproś uczestników do wypełnienia posttestów (kto skończy, może wprowadzić te ustawienia w swoim telefonie). Gdy wszyscy skończą wypełniać posttesty, podziękuj wszystkim uczestnikom za wspólną pracę i zaangażowanie. Podziękuj nauczycielom za wsparcie i zachęć do zapoznania się z dalszą ofertą CDT.	