

Media społecznościowe i prywatność

Warsztat poświęcony jest podstawowym zagadnieniom związanym z ochroną prywatności i wizerunku w internecie. Uczestnicy poznają mechanizmy profilowania zachowań użytkowników w sieci oraz wynikające z nich zagrożenia. Celem zajęć jest zwiększenie świadomości dotyczącej znaczenia prywatności online oraz rozwijanie umiejętności odpowiedzialnego i bezpiecznego korzystania z mediów społecznościowych. Efektem warsztatu ma być realne podniesienie poziomu bezpieczeństwa kont internetowych uczestników.

Czas trwania: 45 min.

Grupa wiekowa: 14 do 19.

Cele:

1) Cele ogólne:

- a) Rozwijanie umiejętności dbania o swój wizerunek w sieci,

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 o swoją prywatność i wizerunek w Internecie;
- d) Refleksja nad ochroną swojej prywatności a możliwościami kariery youtubera.

Potrzebne materiały:

Telefony lub komputery z systemem Windows, połączenie internetowe, przeglądarka Google Chrome; wydrukowana Lista zachowań – plik dla uczestnika (wycięte listy zgodnie z ilością par/grup) lub wydrukowane pliki Tabelka Podział Danych (jedna tabelka na parę/grupę).

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 krótko wyjaśnij, czym jest ścieżka Cyberbezpieczeństwo <i>Cyberbezpieczeństwo to nie tylko warsztaty w temacie cyberbezpieczeństwa, ale spójna ścieżka edukacyjna nastawiona na jeden główny cel: świadome i bezpieczne poruszanie się w cyfrowym świecie.</i> <i>Cyberbezpieczeństwo to nie tylko zabezpieczenie swojego maila silnym hasłem i dwuetapowym uwierzytelnianiem. Aby zabezpieczyć swoje konto mailowe, musisz umieć rozpoznać Phishing. Żeby rozpoznać phishing, musisz rozumieć mechanizmy manipulacji. Żeby nie dać się fake newsom i manipulacjom medialnym, musisz wiedzieć, jak działa Twoja uwaga. A żeby być uważnym na różnego rodzaju niebezpieczeństwa, musisz wiedzieć jakie mechanizmy w sieci odciągają i osłabiają Twoją uwagę i cyfrowy dobrostan. Podczas tej ścieżki uczysz się, jak działają cyberataki, algorytmy profilujące, czy mechanizmy kreujące uzależnienie od smartfona. Bez straszenia, bez teorii dla teorii. Czekają Cię praktyczne warsztaty, kurs online, pokazy z wykorzystaniem płytki hakerskiej oraz konkurs i test wiedzy.</i>	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 Diagnoza Mentimeter: https://www.mentimeter.com/app/presentation/alwdw53mfts3j21jyk2tqxuhbo8xjp/edit?source=share-modal

	<i>To program dla tych, którzy chcą być bezpieczniejsi w sieci, a także dla tych którzy cyberbezpieczeństwem już się interesują i pasjonują.</i> oraz jaki jest temat dzisiejszego warsztatu – media społecznościowe i prywatność w sieci, czyli jak świadomie chronić swoją prywatność online. Podziel uczestników na pary lub grupki 3-4 osobowe. Ustal z uczestnikami zasady towarzyszące nam podczas dzisiejszego warsztatu: • <i>zasada pauzy – będziemy pracować etapami, dlatego gdy usłyszycie słowo „pauza”, na chwilę się zatrzymujemy i odkładamy to, czym aktualnie się zajmujemy. To sygnał, że chcę przekazać Wam coś ważnego.</i> • <i>zasada 3+10 – od czasu do czasu będę potrzebował/a Waszej pełnej uwagi. Jest tak dlatego, że będę tłumaczył/a na czym polega kolejne zadanie lub pokazywał/a sposób obsługi danej aplikacji. Jeśli przez te 3 minuty się rozproszycie, będziecie gadać lub będziecie zajmować czymś innym, to wtedy przez kolejne 10 minut dla Was nie będziecie w stanie pracować samodzielnie.</i> • <i>zasada dobrej współpracy – pracujemy wspólnie, dzielimy się tabletem/komputerem i pomagamy sobie w parach i zespołach.</i> Diagnoza Wytłumacz, że zanim przejdziemy do kwestii prywatności w sieci, musimy poznać doświadczenie uczestników z social mediami. Diagnozę możesz przeprowadzić za pomocą Mentimetera, prosząc uczestników o dołączenie z telefonu lub komputera. Jeśli czas na to nie pozwala, wyświetl pytania w prezentacji lub zadaj je bezpośrednio grupie: • Ile masz osób obserwujących lub znajomych (największa liczba na dowolnej	
--	---	--

	platformie)? • Ile polubień lub reakcji miał twój najpopularniejszy post? • Jak często publikujesz coś w sieci? Zbierz wszystkie odpowiedzi i podkreśl, że nasza obecność w sieci będzie się najprawdopodobniej stawiała 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’ę. <i>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. Porozmawiamy dziś zatem o mediach społecznościowych. Waszym zadaniem będzie wcielenie się w rolę youtuberów i obrona swojego konta i bezpieczeństwa.</i> Podkreśl, że istnieją dwa kluczowe obszary dbania o dane. Po pierwsze są to dane, które sami udostępniamy w sieci – publikując posty, zdjęcia, komentarze czy informacje o sobie. Dane te mogą służyć nie tylko profilowaniu, ale również zostać wykorzystane przez osoby trzecie. Po drugie są to dane zbierane o nas przez media społecznościowe, m.in. poprzez profilowanie i śledzenie naszej aktywności online.	
	Możliwość wyboru przez edukatora zrobienia z uczestnikami ćwiczenia „Co udostępniamy” (15 min) lub „Jak powstaje cyfrowy profil?” (15 min).	

15 min	Co udostępniamy Wytłumacz, że w tym momencie zajmiecie się danymi, które sami udostępniamy w sieci – często nie zdając sobie sprawy, jak łatwo mogą zostać połączone w spójny obraz naszej osoby. Pokaż fragment filmu: https://www.youtube.com/watch?v=CLRBYhd7e4Q Następnie zapytaj grupę: Skąd pochodziły dane wykorzystane w tym materiale? Podkreśl, że były to ogólnodostępne informacje z mediów społecznościowych. Zaznacz jednocześnie, że wraz z rozwojem naszej aktywności online warto zwrócić uwagę na dwa typy danych, które możemy ujawniać. Dane osobowe to wszelkie informacje, które pozwalają zidentyfikować konkretną osobę – bezpośrednio lub pośrednio. Może to być pojedyncza informacja albo kilka połączonych ze sobą danych. Dane wrażliwe to szczególnie chronione dane osobowe, dotyczące bardzo prywatnych obszarów życia, których ujawnienie może prowadzić do dyskryminacji lub poważnej szkody. Są to m.in. dane, o które nie może zapytać Cię potencjalny pracodawca podczas rozmowy kwalifikacyjnej. Rozdaj parom/grupkom kartki Tabelka Podział Danych i poproś, aby wypisali dane wykorzystane w filmie i przypisali je do odpowiednich kategorii. Daj uczestnikom około 5 minut, a następnie wspólnie sprawdźcie poprawność tabeli.	Wydrukowany plik Tabelka Podział Danych – 1 na parę/grupkę. *Możesz też wskazać, że tworząc anonimowe adresy e-mail możesz wykorzystać fałszywe dane. Podkreśl, że zazwyczaj nie powinno się pisać/mówić nieprawdy, ale w sytuacjach związanych z cyberbezpieczeństwem i anonimowością w sieci, może czasem warto rozpatrzyć możliwość zanonimizowania swoich danych. Jest to jednak działanie, które warto dokładnie przemyśleć, gdyż może się obrócić przeciwko nam, jeśli stracimy dostęp do konta lub gdy naruszenie regulaminu zostanie wykryte. Komentarz dzięki uprzejmości Niebezpiecznik.pl
----------------------	---	--

	Przykładowe odpowiedzi: • Dane osobowe: imię i nazwisko, numer telefonu, adres e-mail, zdjęcie twarzy, adres zamieszkania, numer IP, lokalizacja, login w mediach społecznościowych. • Dane wrażliwe: stan zdrowia, niepełnosprawność, pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, orientacja seksualna, dane biometryczne (np. odcisk palca, skan twarzy). Część wiedzowa Zgodnie z RODO daną osobową jest każda informacja, która pozwala zidentyfikować konkretną osobę – bezpośrednio lub pośrednio. Kluczowe jest to, że nie każda informacja sama w sobie musi być od razu daną osobową, ale może się nią stać po połączeniu z innymi danymi. Przykładowo adres e-mail taki jak nick123@gmail.com nie zawsze pozwala jednoznacznie wskazać konkretną osobę. Jednak, jeśli ten sam adres jest używany na Facebooku, Instagramie lub forum, a na profilu widnieje zdjęcie twarzy, imię, szkoła lub miasto, to zestaw tych informacji umożliwia już identyfikację danej osoby. W takim przypadku, zgodnie z RODO, mamy do czynienia z danymi osobowymi. Podobnie jest z numerem IP – sam w sobie nie zawsze jest daną osobową dla zwykłego użytkownika, ale dla dostawcy internetu, administratora strony czy platformy może jednoznacznie wskazywać na konkretną osobę lub urządzenie. Dlatego RODO podkreśla, że to, czy dana informacja jest daną osobową, zależy od kontekstu i od tego, kto nią dysponuje.	
--	--	--

	W praktyce w ten sposób działa tzw. biały wywiad (OSINT) – z pozornie niegroźnych, publicznych informacji zbieranych na różnych platformach można krok po kroku zbudować pełny profil osoby. Problemem nie jest jedna informacja, ale to, że internet bardzo dobrze łączy kropki. Jak chronią się twórcy internetowi? Podkreśl, że wraz z rosnącą obecnością w sieci i większą liczbą obserwujących warto stosować rozwiązania używane przez profesjonalnych youtuberów i influencerów w celu ochrony swoich danych. Pokaż fragment filmu: https://www.youtube.com/watch?v=ut_0SVXPFTg oraz rekomendacje Nicka: • używaj anonimowego nicku, • jeśli korzystasz z nazwiska lub masz własną stronę internetową – ukryj inne dane osobowe, • zmień ustawienia prywatności w mediach używanych do kontaktu z rodziną i przyjaciółmi (np. listy znajomych), • wyłącz udostępnianie lokalizacji, • korzystaj z adresów e-mail stworzonych specjalnie do działalności online (np. z nickiem zamiast nazwiska)*. Dodatkowe rady • usuwaj metadane ze zdjęć,	
--	--	--

	• starannie zamazuj wrażliwe informacje (najlepiej na screenach przerobionych obrazów), • stwórz „spamowy”, zanonimizowany adres e-mail do rejestracji w mniej istotnych serwisach (np. newslettery, sklepy internetowe), • włącz ochronę numeru PESEL w aplikacji mObywatel, • publikuj informacje i zdjęcia z opóźnieniem – gdy nie przebywasz już w danym miejscu, • do kontaktu z rodziną i bliskimi używaj: Messenger (z ograniczoną listą znajomych), WhatsApp, Signal, iMessage, SMS lub połączeń telefonicznych, Facebook – konto prywatne z zamkniętą listą znajomych, • do kontaktu z osobami obcymi lub obserwującymi używaj: Instagram (szczególnie konto publiczne), TikTok, YouTube (komentarze i wiadomości), X/Twitter, Twitch, Discord – serwery publiczne.	
15 min	Jak powstaje cyfrowy profil? Celem ćwiczenia jest zrozumienie, w jaki sposób na podstawie drobnych, codziennych zachowań w sieci tworzony jest profil użytkownika oraz jakie uproszczenia i ryzyka wiążą się z procesem profilowania. Rozdaj każdej parze lub grupce listę zachowa jednego użytkownika w sieci i poproś uczestników, aby zapoznali się z nimi. Następnie przedstaw zadanie: <i>Jesteście algorytmem. Na podstawie tych zachowań spróbujcie opisać, kim jest ta osoba oraz jakie treści lub reklamy mogłyby jej zostać wyświetlone.</i> Daj grupom kilka minut na pracę, a następnie poproś o krótkie zaprezentowanie wniosków.	Z wydrukowanego pliku „Lista zachowań – plik dla uczestników” wytnij poszczególne listy zachowań tak, aby każda grupa otrzymała zestaw opisujący zachowania jednego użytkownika.

	Następnie po zebraniu odpowiedzi zapytaj uczestników: • Które zachowania były dla was kluczowe przy „profilowaniu” tej osoby? • Czy algorytm mógł się w czymś pomylić? • Które z wymienionych reklam byłyby dla tej osoby pomocne, a które potencjalnie szkodliwe – i dlaczego? Podkreśl, że dokładnie w taki sposób działają algorytmy w mediach społecznościowych – analizując ogromne ilości danych, często na podstawie bardzo drobnych sygnałów. Część wiedzowa Algorytmy profilujące w mediach społecznościowych korzystają z dwóch głównych typów danych. Z jednej strony są to dane deklarowane wprost – to, co polubiliśmy, wpisaliśmy w zainteresowania, kogo obserwujemy lub jakie treści udostępniamy. Z drugiej strony algorytmy analizują także zachowania, których często sami nie zauważamy, takie jak: • ile czasu oglądamy dany film, • w którym miejscu zatrzymujemy się podczas scrollowania, • w co klikamy, a co pomijamy, • do jakich treści wracamy. Mechanizm coraz bardziej zaawansowany, ale jednocześnie potencjalnie niebezpieczny. Algorytmy potrafią podsuwać nam treści dopasowane do naszych zainteresowań, ale równocześnie mogą zawężyć naszą perspektywę i zamykać nas w tzw. bańkach filtrujących.	
--	---	--

	Bańki te mogą wpływać na: • nasze decyzje zakupowe, • poglądy i opinie, • sposób postrzegania świata, • a nawet aktywność polityczną. Algorytmy mogą być wykorzystywane przez firmy reklamowe, oszustów próbujących przekierować użytkowników na fałszywe strony, polityków, trolli czy osoby rozpowszechniające teorie spiskowe. Bezkrytyczne podążanie za podpowiedziami algorytmu bywa określane jako „wpadnięcie do króliczej nory”, ponieważ może prowadzić do stopniowej normalizacji treści skrajnych lub szkodliwych. Dlatego warto co jakiś czas świadomie przyjrzeć się temu, co widzimy w swoich mediach społecznościowych i wykonać tzw. <i>feeds reboot</i> – czyli audyt i uporządkowanie obserwowanych treści oraz kont. Możesz zakończyć tę część zdaniem: <i>Algorytm nie zna nas osobiście, ale potrafi dowiedzieć się o nas bardzo dużo. Dlatego warto od czasu do czasu sprawdzić, czy to my kontrolujemy feed, czy feed kontroluje nas.</i> Dodatkowe informacje na temat feeds reboot uczestnicy mogą znaleźć tutaj: https://sektor3-0.pl/blog/feeds-reboot-zrestartuj-algorytmy-i-odzyskaj-kontrolę-nad-tym-co-widzisz-w-internecie/	
15 min	Wciel się w rolę Pokaż uczestnikom stronę z ustawieniami prywatności konta Facebook lub innego konta w mediach społecznościowych np. TikToka. Wyświetl w prezentacji ścieżkę dojścia do tych	https://www.mentimeter.com/app/presentation/almkyq5eh2t7z1ei84wng9br1ds7kxk3

	ustawień i poproś uczestników, żeby się z nią zapoznali (sami spróbowali ją przejść w aplikacjach na swoich telefonach). Następnie poproś uczestników w grupach o wcielenie się w rolę Ani lub Janka (opisy w prezentacji) i ułożenie minimum trzech dobrych praktyk dla ochrony swoich danych w sieci. Zapytaj, które ustawienie prywatności byłoby najlepsze do włączenia/wdrożenia? Zachęć do włączenia danego ustawienia lub wprowadzenia w życie danej zasady. Podkreśl, że nawet jeśli teraz nie wszystkie ustawienia czy zasady wydają się nam potrzebne, warto wiedzieć, jak z nich skorzystać w razie nagłej sytuacji. Może ona dotyczyć zarówno nas samych, jak i kolegi lub koleżanki – np. w przypadku wycieku danych, przechwycenia prywatnych zdjęć, stalkingu, trollingu czy zmasowanego hejtu, którego doświadczają także osoby rozpoznawalne w sieci. Część wiedzowa Według badań: <i>Co piąty nastolatek przyznaje, że doświadczył przemocy w internecie. Najczęstszymi jej przejawami są: wyzywanie (29,7%), ośmieszanie (22,8%) czy poniżanie (22%).</i> A jednocześnie, najczęstszym sposobem reakcji jest bierność: <i>Należy zauważyć, że największy odsetek badanych (32,4%) przyjmuje bierną postawę i nie powiadamia nikogo o przemocy doświadczanej w internecie. Oznacza to, że co trzeci respondent nie zgłasza problemu i nie podejmuje żadnego działania – nawet rozmowy</i>	
--	---	--

	<i>z bliskimi i znajomymi. Również co trzeci nastolatek (31,9%) szuka wsparcia i pomocy u przyjaciół. Powiadomienie rodziców o takim incydencie zadeklarowało 24,1% badanych.</i> https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html	
5 min	Podsumowanie Podkreśl, że ustawienia prywatności i zasady bezpieczeństwa nie są jednorazową decyzją, ale czymś, do czego warto regularnie wracać wraz ze zmianą sposobu korzystania z mediów społecznościowych. Świadome zarządzanie swoją obecnością w sieci pozwala lepiej kontrolować to, jakie informacje o nas krążą w internecie i jakie sytuacje mogą nas zaskoczyć. Wiedza ta może być pomocna nie tylko w dbaniu o własne bezpieczeństwo, ale także w reagowaniu w sytuacjach, gdy ktoś z naszego otoczenia doświadcza problemów online.	