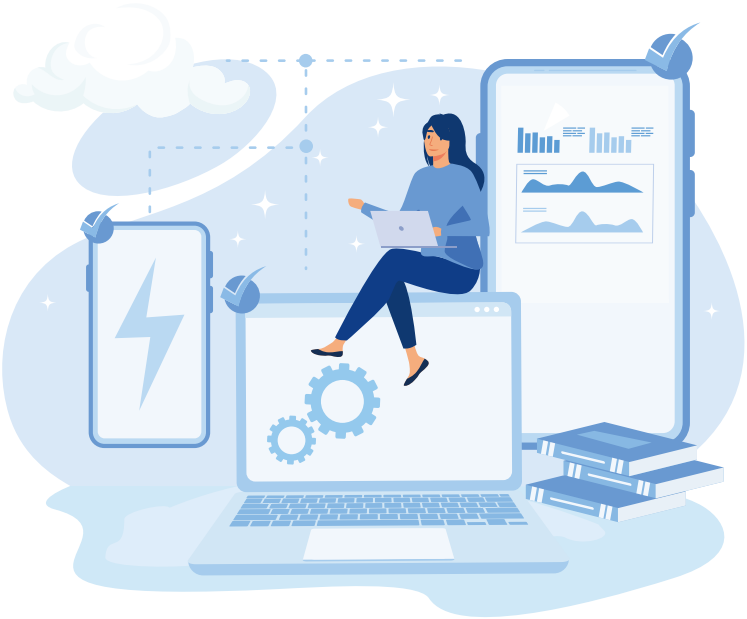
Scenariusz warsztatów
Cyberbezpieczeństwo

szkoła podstawowa

Cyberbezpieczeństwo – szkoła podstawowa

Warsztat porusza podstawowe zagadnienia związane z bezpieczeństwem w sieci i metodami ochrony swoich danych. Podczas zajęć, uczestnicy poznają niebezpieczeństwa obecne w sieci oraz mechanizmy kradzieży danych w Internecie. Celem warsztatu będzie rozwijanie umiejętności rozpoznawania tych zagrożeń w sieci oraz poznanie metod reagowania na nie. Efektem warsztatów ma być kształtowanie wiedzy i umiejętności realnego zwiększenie bezpieczeństwa swojego konta.



Czas trwania

- 90 min.

Grupa wiekowa

- 12 do 14 lat

Cele

1. Cele ogólne:
a. Zwiększenie bezpieczeństwa uczestników w sieci;
b. Wdrożenie przynajmniej jednego rozwiązania służące poprawie naszego bezpieczeństwa w sieci;
2. Cele szczegółowe:
a. Zapoznanie z najczęstszymi mechanizmami ataków w sieci;
b. Poznanie narzędzi służących zwiększeniu swojego bezpieczeństwa online;
c. Rozwijanie krytycznego myślenia;
d. Kreowanie bezpiecznych nawyków.

Potrzebne materiały:

- Komputery z systemem Windows, smartfony lub tablety z systemem android, połączenie internetowe, przeglądarka Google Chrome.

Przygotowanie dla trenera:

- Zapoznaj się ze źródłami i materiałami dodatkowymi przedstawionymi w scenariuszu.

Etapy realizacji

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Wprowadzenie:** Przywitaj uczestników, przedstaw się i powiedz, czym jest projekt Cyberbezpieczni i o czym jest dzisiejszy warsztat (bezpieczeństwo w sieci – zagrożenia i metody ochrony). Wcielimy się w rolę zespołów do spraw cyberbezpieczeństwa. Naszym zadaniem będzie zabezpieczenie naszej firmy przed kolejnym atakiem. W ramach tego zajmiemy się budowaniem zabezpieczeń, ale również łamaniem zabezpieczeń! Dlatego też powinniście pamiętać, że wszystko czego się dziś uczymy robimy w celach edukacyjnych, a nie by wykorzystywać to potem w nieetycznych działaniach. Następnie dobierz uczestników w pary lub zespoły czteroosobowe. Podkreśl, że wszyscy uczestnicy mogą pracować na telefonach i komputerach, ale że do prezentacji, powinien podłączyć się już tylko jeden reprezentant pary/zespołu. 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), zasada dobrej współpracy (pracujemy wspólnie i pomagamy sobie w zespole).	**Uwaga:** W zależności od doświadczenia i zaangażowania grupy, dobierz późniejsze ćwiczenia oraz sposób pracy. **Uwaga 2**: Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych. Uczestnicy wypełniają pretest i posttest na swoich urządzeniach (każdy osobno). Przez dalszą część warsztatu pracują już w grupie. Z każdej grupy do prezentacji powinno połączyć się jedno urządzenie.
15 min	**Podprowadzenie i diagnoza** Dziś doszło do strasznej sytuacji. Wasz nauczyciel informatyki, podczas podłączania się na spotkanie online został ugryziony przez komputerową mysz, a przez to zainfekowany wirusem omputerowym. Wirus ten zamienia ludzi w cyberprzestępców i internetowe trolle, które potem piszą w internecie komentarze typu „pierwszy!" Wirus ten umożliwia zarażonym łamanie wielu zabezpieczeń i infekowanie kolejnych urządzeń. Zarówno Wy, jak i Wasze urządzenia i konta znaleźliście się zatem w niebezpieczeństwie.	**https://www.mentimeter.com/app/presentation/alkg2zr64ok-gymg3fkc8cz3ifp89th3j**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	Wasz nauczyciel zamknął Was w sali warsztatowej i grozi takimi rzeczami jak publiczne udostępnienie historii Waszych przeglądarek, czy nagranie z Wami duetu na TikToku. Macie godzinę by wydostać się z Sali i podać nauczycielowi antidotum. Żeby dostać się do antidotum musicie przy tym pokonać jednak szereg zabezpieczeń i wyzwań, które dla Was przygotowaliśmy. Jeśli Wam się nie uda, wirus się rozprzestrzeni i w sytuacji zagrożenia znajdą się nie tylko wszyscy w Waszej szkole, ale również wszyscy w sieci. Los Internetu zależy zatem od Was! Podkreśl, że pierwszym krokiem jest dokonanie diagnozy – Wirus, o którym mówimy najczęściej atakuje bowiem komputery i osoby, które mają już „osłabioną odporność", czyli np. takie osoby, których maile lub hasła wyciekły już do sieci i są w niej obecne. Podkreśl zatem, że do stworzenia antidotum musimy nauczyć się diagnozować potencjalne ryzyka infekcji i im przeciwdziałać. **Pokaż i wytłumacz uczestnikom zasady działania stron:** **https://haveibeenpwned.com/ *** Strony takie jak haveibeenpwned.com zbierają informację o największych wyciekach danych z poszczególnych firm i serwisów. Gdy taki wyciek ma miejsce, w czeluściach Internetu zaczynają krążyć listy z danymi użytkowników danego serwisu. Haveibeenpwned zbiera tego typu listy byśmy mieli świadomość zagrożenia. Na tego typu stronie możecie sprawdzić czy Wasz adres nie pojawia się na jednej z tych list, czyli czy nie wyciekł. Poproś o wejście na nie i sprawdzenie adresów mailowych wszystkich osób w naszej grupie. Każda grupa ma wskazać ile osób wśród nich padło ofiarą wycieku danych, ile łącznie danych wyciekło oraz, które z nich są najgroźniejsze. Podkreśl, że w tym ćwiczeniu wygrywają dwie grupy – tej, w której wycieków było najmniej, oraz najwięcej. Daj grupom 10 minut na autodiagnozę i zbierz odpowiedzi: **Ile osób w grupie padło ofiarą wycieku danych:** **Ile danych łącznie wyciekło:** **(dodatkowo możesz zapytać) Które są najbardziej niebezpieczne:** Zauważcie, że wyciec mogą bardzo różne dane, od adresu IP po dane informujące o naszym zdrowiu i wynikach badań genetycznych. Najczęściej w wyciekach zobaczycie jednak „świętą trójcę", czyli e-mail, login i hasło. Podnieście teraz proszę ręce wszyscy Ci, którzy używają innego hasła do każdej witryny i aplikacji, do której się logują. Okej, dzięki. Czyli u reszty nasze hasło się czasem powtarza, czyli, że mamy jedne hasło do wielu witryn i aplikacji. To teraz wyobraźmy sobie, co dzieje się, gdy takie hasło wycieka. Jeśli ktoś ma jakieś nasze hasło, to trochę tak jakbyśmy zgubili klucz (jakiś klucz). Sam klucz wiele nam nie powie, ale jeśli ktoś zgubił go w kopercie wraz z naszym adresem (a tym po części jest nasz adres mailowy), to ktoś może już jechać z tym kluczem do naszego domu by spróbować otworzyć nim nasze drzwi.	Barometr Cyberbezpieczeństwa Uwaga: Uczestnicy, którzy nie mają wycieków ze swoich kont mogą sprawdzić konta mailowe najbliższej rodziny – np. Mamy i Taty. ***Uwaga: istnieją inne strony, podobne do strony haveibeenpwned.com np. strona dehashed.com, która umożliwia nie tylko wyszukanie adresu e-mail, ale również sprawdzenie jakie hasła były do niego przyporządkowane. Może zatem zostać wykorzystana również w sposób niebezpieczny. Co równie ważne, handluje ona danymi z wycieków, w sposób który w Polsce jest niedopuszczalny. Nie pokazuj jej i nie rekomenduj. Miej jednak świadomość jej istnienia w razie pytań od młodzieży/nauczycieli.** **- Komentarz dzięki uprzejmości Niebezpiecznik.pl**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	Jeśli ten klucz, który trzyma w ręku, to mało istotny klucz np. do zapięcia rowerowego, to może nam coś zabrać, ale nie dostanie się do naszego mieszkania. Jeśli jednak wpadliśmy na pomysł używania jednego magicznego klucza do zapięcia, do mieszkania, do garażu i do sejfu z kosztownościami, to może i jest to wygodne, ale staje się już bardzo niebezpieczne. Wytłumacz, że wycieki danych zdarzają się i zdarzać będą nawet na najlepiej zabezpieczonych serwisach. I nasze konta, podobnie jak nasze mieszkania, zawsze będą narażone na jakieś niebezpieczeństwo. Podkreśl, że w sytuacji wycieku, powinniśmy się „uodpornić", czyli: • **Zmienić hasło na nowe i silne** (o tym jakie hasła są silne powiemy sobie za chwilę). • **Odwiedzić zakładkę Ustawienia i bezpieczeństwo na naszym koncie mailowym i kontach społecznościowych** by zobaczyć kto ma dostęp do konta (coraz więcej stron oferuje możliwość sprawdzenia historii logowania, podejrzanych logowań oraz sprzętów podłączonych do konta). • **Skonfigurować uwierzytelnianie dwuetapowe, najlepiej wraz z menedżerem haseł*.** • **Przygotować się na kolejny krok w potencjalnym ataku.** Doceń grupy, które miały najmniej wycieków i doceń grupy, które miały najwięcej. Wytłumacz, że osoby z mniejszą ilością wycieków mogą czuć się nieco bezpieczniejsze (choć nie w pełni bezpieczne, bo np. nie wszystkie wycieki danych są zgłaszane). Z drugiej strony jednak, osoby i grupy z dużą liczbą wycieków powinny szczególnie zainteresować się dzisiejszą tematyką, bo im większa nasza aktywność w sieci, tym większa potrzeba lepszego zabezpieczenia naszych kont. Zaznacz, że jest możliwe, aby mieć dużą aktywność w sieci przy jednoczesnym bardzo dużym bezpieczeństwie naszych kont. Podkreśl, że teraz przejdziemy do tego kolejnego (i następnych kroków) w potencjalnym ataku i kolejnych metod zwiększenia naszego bezpieczeństwa.	***Uwaga: Już teraz możesz wspomnieć o znaczeniu takich rzeczy jak uwierzytelnianie dwuetapowe i menedżer haseł (jako ważnych elementach ochrony). O obu narzędziach jest jednak mowa w dalszej części scenariusza, więc dopasuj ilość treści w obu miejscach, aby nie powtarzać dwa razy tych samych informacji.** **- komentarz dzięki uprzejmości Niebezpiecznik.pl**
10 min	**Phishing** Podkreśl, że „uodpornieniu" po wycieku danych powinniśmy poddać przede wszystkim nasze skrzynki mailowe. Wirus może je bowiem atakować poprzez phishing – fałszywe wiadomości wysłane przez kogoś podszywającego się pod wybraną instytucję lub inną osobę, w celu kradzieży danych lub instalacji złośliwego oprogramowania. Podkreśl, że są to tak zwane socjotechniczne metody włamań, które wymagają treningu w ich rozpoznaniu i zwracania uwagi na szczegóły. Taki phishing będzie trafiać najczęściej na nasze maile (choć do innych kanałów również). Powinniśmy mieć zatem w tyle głowy, że skrzynka której adres wyciekł, może stać się celem ataków phishingowych. Podkreśl, że teraz przećwiczymy ochronę przed phishingiem.	https://www.mentimeter.com/app/presentation/al-cwj5x1kzbuxhpcum69qfkj-mkiuzn2w

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Kolejnym Waszym zadaniem jest sprawdzenie niedawnych wiadomości, które zaczęły trafiać do uczniów waszej szkoły. Waszym celem jest wyłapanie wiadomości phishingowych i ostrzeżenie kolegów przed nimi. Za każdą poprawnie zidentyfikowaną wiadomość dostajecie jeden punkt! Wyświetl uczestnikom prezentację z przykładowymi wiadomościami e-mail. Daj im 10-15 sekund na przeczytanie treści i podjęcie decyzji czy jest to prawdziwa wiadomość czy phishing. Wyświetl slajdy z prezentacji i przeprowadź głosowanie w klasie. Podsumuj na co powinniśmy zwracać uwagę w wiadomościach e-mail (adres nadawcy, podpisy i stopki, błędy ortograficzne, przyciski i dziwne linki oraz, co najważniejsze, metody socjotechniczne próbujące pobudzić nasze emocje i "wyłączyć myślenie"). **Podkreśl, że jeśli nie jesteśmy pewni danego linku lub załącznika (a mimo wszystko powinniśmy go sprawdzić), to możemy wykorzystać narzędzie: https://www.virustotal.com/gui/home/upload pozwalające na sprawdzenie strony lub danego pliku*.** Doceń grupy o najlepszych wynikach. Podkreśl, że dzięki staraniom grup udało się ograniczyć ilość wiadomości phishingowych do minimum. Część infekcji się jednak przedarła...	**Uwaga: wypada też dodać, że pozytywna ocena VirusTotal nie oznacza, że jesteśmy w 100% bezpieczni. Należy też uważać z tym, co się tam podsyła ponieważ oznacza to dzielenie się tym plikiem z serwisem. Warto uczulić, że przesyłanie plików na cudzą stronę i korzystanie z usług webowych może umożliwiać komuś dostęp do naszych plików.** **- Komentarz dzięki uprzejmości Niebezpiecznik.pl**
	Łamanie haseł Wasz informatyk dotknięty infekcją, wykorzystał jednak porty USB w laptopach do rozniesienia wirusa dalej. Są to laptopy oraz komputery uczniów i nauczycieli (a nawet rodziców), które były najsłabiej chronione. Musicie zatem złamać ich zabezpieczenia (podobnie jak Wasz informatyk) by uruchomić na sprzętach skanowanie antywirusowe i zostawić na nich wskazówki dla ich lepszego zabezpieczenia. Wytłumacz, że w tym ćwiczeniu zajmiemy się pierwszą furtką, czyli hasłami. Pozyskanie informacji o użytkownikach i ich haseł (z wycieków danych lub przy pomocy phishingu), pozwala często na odgadniecie nawet nowych haseł (jeśli ktoś nie potrafi dobrze ich tworzyć). Waszym zadaniem jest wykorzystanie informacji o właścicielach laptopów, złamanie ich haseł, wejście na ich komputery i zostawienie im notatki o tym jakie powinno być silne hasło i jak je tworzyć. Im więcej komputerów zhakujecie, tym więcej o zasadach tworzenia haseł się nauczycie!	Zapoznaj się z: https://www.mentimeter.com/app/presentation/alc-1pqq6xsm67z6gyxm99fre9n5n-zoj9 https://www.mentimeter.com/app/presentation/albmuiy6c4ac-ng1dp9eso17vbd7i7nps https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. Podkreśl, że po wykryciu wycieku lub w sytuacji podejrzenia włamu na konto, w pierwszej kolejności powinniśmy zatem zmienić hasło do danego serwisu, a najlepiej wszystkie hasła. Nowe hasło powinno być silne, czyli: • **długie** (najlepiej w formie frazy- „PassPhrase" zamiast „Password") * • **abstrakcyjne** (pozbawione logiki, przewidywalności, systemu, który można złamać) • **różne do każdego serwisu** • **łatwe do zapamiętania** (dyskusyjne) • **z cyframi i znakami specjalnymi** (dyskusyjne) **Silne hasło** Daj uczestnikom pięć minut na stworzenie tego typu hasła. I poproś o przetestowanie go na stronie: https://www.security.org/how-secure-is-my-password/ Następnie zapytaj czy jesteśmy w stanie powtórzyć ten proces i zapamiętać wszystkie te hasła dla wszystkich innych witryn i aplikacji? **Podkreśl, że jest to raczej mało prawdopodobne i że dobrym sposobem może być wykorzystanie menadżera haseł – programu tworzącego i zapamiętującego za nas hasła. Podkreśl, że mogą być to programy dostępne w chmurze takie jak Last Pass czy Avira Password Menager lub programy dostępne offline, na dysku naszego komputera**. Podkreśl, że obecne przeglądarki takie jak Google Chrome czy Safari również oferują taki menedżer. Ma on dobre szyfrowanie i co ciekawe, menadżery haseł działające w przeglądarce mogą nas uchronić przed atakiem IDN Homograph, czyli takim atakiem, w którym cały adres strony lub jakaś jego część jest napisana innym alfabetem (np. cyrylicą). Taki adres dla naszego oka może się wydawać nie do odróżnienia, ale menadżer analizując adres strony „zobaczy", że nie ma tej witryny w swojej bazie logowania i haseł i że jest to zatem nowa, inna witryna.** Z menadżerów haseł możemy korzystać pod jednym warunkiem. Zapytaj grupę jaki jest skrót klawiszowy do blokady ekranu i komputera (Control + Command + Q na systemie MAC oraz Windows + L na systemie Windows)? Podkreśl, że możemy korzystać z menadżerów i zapamiętywania haseł tylko pod warunkiem, że mamy ustawione blokady ekranu i hasła zarówno na komputerze, jak i na komórce. Nawyk wygaszania ekranu i blokowania komputera to kolejne ważne przyzwyczajenie, który powinniśmy w sobie rozwijać.	https://niebezpiecznik.pl/post/uwaga-na-niewykrywalny--phishing-poprzez-domeny-ze--znakami-unicode-podobnymi--do-liter-z-alfabetu-lacinskiego/ ***Uwaga: Podkreśl, że długość stanowi najważniejszy parametr hasła. Cyfry i znaki nie są złą rekomendacją, ale nie mogą zastępować długości. Kwestia łatwości zapamiętania hasła będzie natomiast dyskusyjna, bo zależna od sposobu ich przechowywania (można korzystać z menedżera haseł). Zwróć przy tym uwagę na jak wiele z tych wyzwań odpowiada (dodatkowo w łatwy sposób) menedżer haseł, który powinniśmy stosować.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl ***Każdy menedżer będzie ok, ale dla bardziej ambitnych/zaawansowanych użytkowników rekomendowany jest KeePass. Użycie menedżerów w przeglądarce będzie natomiast ok, pod warunkiem że: hasła są mocne i unikalne, tylko my korzystamy z danej przeglądarki i konta oraz urządzenie jest dobrze chronione przed dostępem osoby niepowołanej.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**2FA** Podkreśl, że silne hasło uchroni nas przed jego złamaniem przez algorytmy deszyfrujące (a przynajmniej bardzo ten proces utrudni). **Zapytaj jednak co zrobić w sytuacji, gdy ktoś zna nasze silne hasło (bo np. wyciekło). Jak możemy obronić się w takiej sytuacji?** **Podkreśl, że najważniejszym sposobem ochrony okazuje się w tej (i wielu innych sytuacjach) weryfikacja dwuetapowa (lub wieloskładnikowa).** Wytłumacz, że jest to dodatkowy (oprócz hasła) sposób weryfikowania czy to aby na pewno my, logujemy się na nasze konto. Może on przybrać formę karty kodów jednorazowych (dawne rozwiązanie popularne w bankach i wciąż obecne np. na gmailu), kodów SMS, kodów lub potwierdzeń w dedykowanej aplikacji authenticator, potwierdzeń mailowych lub forę klucza U2F, czyli urządzenia przypominającego pendrive z dodatkowym modułem NFC do łączności bezprzewodowej. Taki klucz nawiązuje łączność z daną stroną internetową i potwierdza naszą tożsamość. Waszemu informatykowi udało się przejąć kontrolę nad kontami wielu rodziców i nauczycieli z powodu braku dwuetapowej weryfikacji. Aby poprawić bezpieczeństwo kont Waszych najbliższych, musicie dobrać optymalny sposób dwuetapowej weryfikacji do każdej osoby. Podkreśl, że teraz zadaniem uczestników jest znalezienie najlepszego sposobu dodatkowej weryfikacji w każdym z przedstawionych za chwilę w prezentacji case'ów. Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. Podkreśl, że w ostatnim pytaniu prawie wszystkie odpowiedzi są poprawne, gdyż najlepsza dodatkowa weryfikacja, to taka, która rzeczywiście jest stosowana. **Może być to klucz U2F (jako jedyny sposób dodatkowego uwierzytelniania chroniący w pełni przed phishingiem) lub aplikacja Authenticator (Google lub Microsoft)** ale najważniejsze jest, aby przede wszystkim włączyć tę dodatkową opcję na swoich kontach!	https://www.mentimeter.com/app/presentation/aljewew7moj-5d6ouecysruo9dtnsgrwz **Uwaga: włączenie weryfikacji dwuetapowej to jeden z najlepszych sposobów ochrony swojego konta. Jeśli chcesz włączyć ją z uczestnikami w trakcie zajęć, upewnij się, że znajdują się oni na bezpiecznej sieci (na prywatnych sieciach komórkowych lub sieci domowej), nie jest rekomendowane zmienianie ustawień swojego konta poprzez publiczną sieć Wi-Fi.** Zapoznaj się z: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/2-wykorzystanie-kluczy-sprzetowych-u2f/
10 min	**Pomocne programy** **Podkreśl, że obok cyberprzestępców, w sieci obecne są również wirusy – programy komputerowe wykorzystujące luki w zabezpieczeniach i wykonujące różnego rodzaju szkodliwe działania na naszym komputerze – mogą monitorować to co wpisujemy na klawiaturze(Keylogger),**	https://www.mentimeter.com/app/presentation/alb1dt8b2dn-4kdzgdbckyfyeufx2icoa

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	włączać kamerkę i służyć późniejszemu szantażowi (Ransomware), szyfrować nasze dyski, czy zamienić nasz komputer w koparkę BitCoinów (Botnet). Powiedz, że ostatnim zadaniem grup jest poprawienie bezpieczeństwa sprzętu poprzez włączenie skanowania antywirusowego na komputerach, na które udało nam się włamać. Poproś uczestników, aby wszyscy włączyli w tym momencie skanowanie antywirusowe/bezpieczeństwa na swoim sprzęcie (smartfonie lub komputerze) i żeby grupy napisały jakie skanowania włączyły. Zadanie wygrywa grupa, który włączy najwięcej i najbardziej istotnych skanowań. Podkreśl, że z powodu ogromnej liczby różnych sprzętów i urządzeń, nie ma jednej metody i jednego idealnego programu. Ważnymi skanowaniami, które zaliczymy grupom do wykonania zadania będą: **Na komputerach:** • Skanowanie Windows Defender • Skanowanie zewnętrznym programem antywirusowym • Skanowanie Windows update **Na smartfonach i tabletach*:** • Skanowanie Google Play Protect • „Skanowanie bezpieczeństwa" w panelu sterowania lub ustawieniach • Skanowanie aktualizacji • Skan zewnętrznym programem antywirusowym (w większości wypadków nic to nie zmienia, gdyż programy te nie mają dostępu do innych obszarów pamięci telefonu – działanie w wydzielonym obszarze pamięci/sanbox. Z drugiej strony, renomowane programy antywirusowe nie zaszkodzą też pod względem bezpieczeństwa telefonowi, okazjonalnie potrafią wykryć więcej, niż Google Play Protect). Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. Wyświetl slajd z przydatnymi programami i wytłumacz, że powinniśmy: • Dbać o aktualizację naszych urządzeń (w ten sposób usuwamy luki w zabezpieczeniach).	Zapoznaj się z: https://niebezpiecznik.pl/post/sprawdz-czy-twoj-smartfon-jest--zhackowany/ https://zaufanatrzeciastrona.pl/post/podstawy-bezpieczenstwa--czy-wspolczesne-smartfony--potrzebuja-antywirusa/ *Uwaga: Zapoznaj się również z: https://sklep.niebezpiecznik.pl/opis/11 **Podkreśl też, że większość nowoczesnych smartfonów wykonuje dużo z tych procesów samodzielnie (okresowo, w tle). W przypadku smartfonów i tabletów bardziej istotne są zatem nawet ustawienia konfiguracji:** • **dobra blokada ekranu,** • **PIN na karcie SIM,** • **włączone śledzenie urządzenia,** • **konieczność bardzo dobrego chronienia hasła do Google/Icloud (bo przecież mamy śledzenie),** • **aktualizacja Systemu i osobno aplikacji.**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	• Uważać na wyłączanie zabezpieczeń i instalowanie programów z niebezpiecznych źródeł (Jailbreak na IOS, włączanie debbugowania przez USB na telefonie, instalacja aplikacji spoza oficjalnych sklepów). „Skanowania bezpieczeństwa" w smartfonach często włączają właśnie na powrót domyślne ustawienia zabezpieczeń, które wyłączyliśmy. • **Ustawić blokady chroniące sprzęt przed dostępem osoby niepowołanej (blokady ekranu, Kod PIN na kartach SIM, mocne hasła na kotach Google/Icloud.** • Zdawać sobie sprawę, że mamy domyślne filtry i zabezpieczenia (Microsoft Defender i Zapora Windows, Skanowanie aplikacji w Google Play, system działający na zasadzie ograniczania uprawnień/ sandbox na androidzie i IOS). • Okazjonalnie zeskanować komputer przy użyciu dodatkowego programu wybranego z aktualnej listy: https://www.av-test.org/en/ ; https://www.av-comparatives.org/; https://www.mrg-effitas.com/; https://www.virusbulletin.com/; https://selabs.uk/ Podkreśl, że obok oprogramowania antywirusowego warto zainstalować sobie również dwa inne programy, czyli Menagera Haseł (tu również warto sprawdzić aktualne, polecane listy) oraz aplikację do uwierzytelniania dwuetapowego dla innych programów: Microsoft Authenticator czy Google Authenticator. Zapytaj również czy istnieją pliki, z którymi skanery antywirusowe mogą sobie nie poradzić? Podkreśl, że możemy również mieć na swoim dysku lub mailu pliki zaszyfrowane. Podkreśl, że to dobra i bezpieczna metoda na przesyłanie danych osobowych lub wrażliwych - np. Dokumentów. Zaznacz, że opcję zaszyfrowania i opatrzenia danego folderu/archiwum hasłem mają takie programy jak winrar czy 7zip. W przypadku plików szyfrowanych, powinniśmy przesyłać hasło drugim sposobem komunikacji (np. Jakimś rodzajem komunikatora lub sms-em). Otwierając taki plik, powinniśmy mieć z kolei pewność, że pochodzi z zaufanego źródła. Na koniec podkreśl, że wszystkie operacje związane z hasłami i zakupami powinniśmy robić zawsze na bezpiecznej sieci – sieci domowej(zabezpieczonej hasłem) lub poprzez swój transfer danych, ewentualnie poprzez VPN – wewnętrzny tunel maskujący naszą aktywność i nasze dane. Tu również trzeba jednak uważać na darmowe VPN-y, które mogą gromadzić nasze dane.	**Czyli, dobra i bezpieczna konfiguracja telefonu.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl **W kontekście wirusów i złośliwego oprogramowania, warto również powiedzieć o ostrożności/niewchodzeniu w interakcje z podejrzanymi plikami i systemami. Np. (nieotwieraniu lub ostrożnym otwieraniu) plik ZIP ukrytych za hasłem czy też włączaniu makr/ zawartości w dokumentach Worda. - Komentarz dzięki uprzejmości Niebezpiecznik.pl**

W

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Podsumowanie** Wyświetl prezentację Pigułka i poproś o wybranie najważniejszej rzeczy, której uczestnicy się nauczyli. Doceń i nagródź najlepszych uczestników w tym ćwiczeniu i w całej grze. Zachęć do „wzięcia tej pigułki", czyli wybrania najlepszego, najbardziej przydatnego sposobu ochrony i jego wdrożenie – np. zmiana hasła lub ustawienie weryfikacji dwuetapowej. Podkreśl, że celem naszych zajęć nie jest straszenie i twierdzenie, że Internet jest zły lub niebezpieczny. Naszym celem jest wyposażenie wszystkich w wiedzę, umiejętności i narzędzia, które pozwalają być bezpieczniejszym w sieci. Zaproś przy tym uczestników do metody małych kroków – instalacji jednego programu/wdrożenia jednej metody i przyzwyczajenia się do niej – zmienienia swoich nawyków. Podkreśl, że najlepsza metoda ochrony, to taka, którą rzeczywiście stosują. Dzięki Waszemu zaangażowaniu, wiedzy i umiejętnościom udało się pokonać wirusa. Pigułki wiedzy, które stworzyliście w pełni usunęły wirusa z organizmu Waszego nauczyciela informatyki oraz z całej sieci szkolnej. Uczyniliście bezpieczniejszymi zarówno siebie, jak i waszych bliskich! Pamiętajcie jednak, że wspomniany wirus i inne zagrożenia z sieci mogą jeszcze powrócić, np. w nowej, zmutowanej formie. Warto zatem budować swoją odporność i nie zapominać o „lekach" – pigułkach wiedzy, które wspólnie stworzyliście. Stosowanie silnych haseł, wprowadzenie uwierzytelniania dwuetapowego czy dbanie o aktualizacje systemu, to proste działania które powinniśmy wykonywać regularnie by zachować odporność na zagrożenia z sieci! Podziękuj za zajęcia, uwagę uczestników i uczestniczek oraz pomoc nauczycieli i nauczycielek. Poproś o ustawienie się do wspólnego „zdjęcia"/screena za zajęć. Wytłumacz, że posłuży on tylko dokumentacji odbycia się zajęć zdalnych. Kto chce może zatem zasłonić swoją twarz (ochrona prywatności, którą zajmiemy się na kolejnym warsztacie)	https://www.mentimeter.com/app/presentation/ale4etesooz-3cbjs9yizw1r27r51s1ne

PFR Fundacja

Centralny Dom Technologii

NIEBEZPIECZNIK.PL

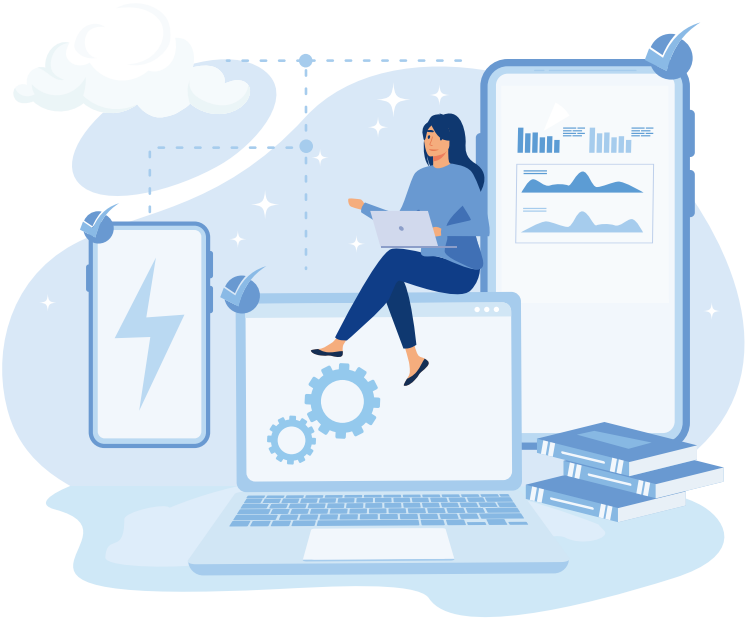
Projekt jest finansowany ze środków **Kancelarii Prezesa Rady Ministrów** w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli **„Cyberbezpieczni”.**

Scenariusz warsztatów
Cyberbezpieczeństwo

szkoła ponadpodstawowa

Cyberbezpieczeństwo – szkoła ponadpodstawowa

Warsztat porusza podstawowe zagadnienia związane z bezpieczeństwem w sieci i metodami ochrony swoich danych. Podczas zajęć, uczestnicy poznają niebezpieczeństwa obecne w sieci oraz mechanizmy kradzieży danych w Internecie. Celem warsztatu będzie rozwijanie umiejętności rozpoznawania tych zagrożeń w sieci oraz poznanie metod reagowania na nie. Efektem warsztatów ma być kształtowanie wiedzy i umiejętności realnego zwiększenie bezpieczeństwa swojego konta.



Czas trwania

- 90 min.

Grupa wiekowa

- 14 do 19 lat

Cele

1. Cele ogólne:
a. Zwiększenie bezpieczeństwa uczestników w sieci;
b. Wdrożenie przynajmniej jednego rozwiązania służącego poprawie naszego bezpieczeństwa w sieci;
2. Cele szczegółowe:
a. Zapoznanie z najczęstszymi mechanizmami ataków w sieci;
b. Poznanie narzędzi służących zwiększeniu swojego bezpieczeństwa online;
c. Rozwijanie krytycznego myślenia;
d. Kreowanie bezpiecznych nawyków.

Potrzebne materiały:

- Komputery z systemem Windows, smartfony lub tablety z systemem android, połączenie internetowe, przeglądarka Google Chrome.

Przygotowanie dla trenera:

- Zapoznaj się ze źródłami i materiałami dodatkowymi przedstawionymi w scenariuszu. Przygotuj prezentacje na podstawie linków.

Etapy realizacji

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Wprowadzenie:** Przywitaj uczestników, przedstaw się i powiedz, czym jest projekt Cyberbezpieczni i o czym jest dzisiejszy warsztat (bezpieczeństwo w sieci – zagrożenia i metody ochrony). Wcielimy się w rolę zespołów do spraw cyberbezpieczeństwa. Naszym zadaniem będzie zabezpieczenie naszej firmy przed kolejnym atakiem. W ramach tego zajmiemy się budowaniem zabezpieczeń, ale również łamaniem zabezpieczeń! Dlatego też powinniście pamiętać, że wszystko czego się dziś uczymy robimy w celach edukacyjnych, a nie by wykorzystywać to potem w nieetycznych działaniach. Następnie dobierz uczestników w pary lub zespoły czteroosobowe. Podkreśl, że wszyscy uczestnicy mogą pracować na telefonach i komputerach, ale że do prezentacji, powinien podłączyć się już tylko jeden reprezentant pary/zespołu 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), zasada dobrej współpracy (pracujemy wspólnie i pomagamy sobie w zespole). Następnie przejdź do podprowadzenia.	**Uwaga:** W zależności od doświadczenia i zaangażowania grupy, dobierz późniejsze ćwiczenia oraz sposób pracy. **Uwaga 2**: Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych. Uczestnicy wypełniają pretest i posttest na swoich urządzeniach (każdy osobno). Przez dalszą część warsztatu pracują już w grupie. Z każdej grupy do prezentacji powinno połączyć się jedno urządzenie.
15 min	**Podprowadzenie i diagnoza** Podkreśl, że dziś wcielamy się rolę pracowników pewnej firmy i to bardzo konkretnej firmy, poproś wszystkich o uwagę i wyświetl fragment filmu Anatomia Ataku (zapauzuj w momencie mowy o drugim ataku): https://www.youtube.com/watch?v=HwqVv94ODgU	**https://www.mentimeter.com/app/presentation/algi3zu18jq8i-8mapvvknrh6pjf3eftw**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	Wytłumacz, że film ten w dobry sposób ukazuje realne ataki hakerskie, które mają miejsce. Według raportu Barometr Cyberbezpieczeństwa, w 2022 roku 58% firm w Polsce odnotowało przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa. Na liście Cyberzagrożeń stanowiących największe ryzyko dla organizacji najwyższe miejsce zajmuje (według ocen samych organizacji) phishing nakierowany na wyłudzanie danych uwierzytelniających. Kolejne miejsce zajmują APT czyli Zaawansowane ataki ukierunkowane. Są to zaawansowane, trwałe ataki przeprowadzane przez specjalistów i obejmujące szereg narzędzi, a często zaczynające się od Spear phishingu, czyli właśnie phishingu ukierunkowanego na konkretną osobę. Cyber Kill Chain, czyli stworzony przez firmę Lockheed Martin model rozpoznawania i zapobiegania atakom też zaczyna się od widocznej na filmie fazy rekonesansu i wysłania przygotowanego załącznika mailem. I tutaj zaczyna się wasze zadanie: Wy wcielacie się dziś w rolę pracowników tej firmy, którzy w na szybko powołanych zespołach do spraw cyberbezpieczeństwa mają jak najszybciej uodpornić firmę na dalsze ataki. Jak widzicie na filmie (który możecie w domu sami dokończyć) atak wciąż trwa. Wszyscy informatycy są zajęcie mierzeniem się ze skutkami głównego, najpoważniejszego ataku, więc to do Was należy jak najszybsze wdrożenie w całej firmie podstawowej wiedzy, umiejętności i zachowań poprawiających bezpieczeństwo w sieci wszystkich pracowników! Podkreśl, że pierwszym krokiem jest dokonanie diagnozy – sprawdzenie czy nasze dane i dane innych pracowników już gdzieś nie wyciekły i czy nie są one dostępne w sieci i wręcz gotowe do wykorzystania w kolejnym ataku. **Pokaż i wytłumacz uczestnikom zasady działania stron:** **https://haveibeenpwned.com/** Strony takie jak haveibeenpwned.com zbierają informację o największych wyciekach danych z poszczególnych firm i serwisów. Gdy taki wyciek ma miejsce, w czeluściach Internetu zaczynają krążyć listy z danymi użytkowników danego serwisu. Haveibeenpwned zbiera tego typu listy byśmy mieli świadomość zagrożenia. Na tego typu stronie możecie sprawdzić czy Wasz adres nie pojawia się na jednej z tych list, czyli czy nie wyciekł.	Barometr Cyberbezpieczeństwa: Uwaga: Uczestnicy, którzy nie mają wycieków ze swoich kont mogą sprawdzić konta mailowe najbliższej rodziny – np. Mamy i Taty. ***Uwaga: Pomiędzy APT (atakiem ukierunkowanym na konkretną firmę/osobę), atakiem oportunistycznym (szeroki zasięg, np. masowy atak ransomware lub masowy atak phishingowy) możemy również wyróżnić ataki prowadzone pod kątem konkretnych luk w zabezpieczeniach. Jest to rosnący trend.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl **Uwaga: istnieją inne strony, podobne do strony haveibeenpwned.com np. strona dehashed.com, która umożliwia nie tylko wyszukanie adresu e-mail, ale również sprawdzenie jakie hasła były do niego przyporządkowane. Może zatem zostać wykorzystana również w sposób niebezpieczny.**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	Poproś o wejście na nie i sprawdzenie adresów mailowych wszystkich osób w naszej grupie. Każda grupa ma wskazać ile osób wśród nich padło ofiarą wycieku danych, ile łącznie danych wyciekło oraz które z nich są najgroźniejsze. Podkreśl, że w tym ćwiczeniu wygrywają dwie grupy – tej, w której wycieków było najmniej, oraz najwięcej. Daj grupom 10 minut na autodiagnozę i zbierz odpowiedzi: Wytłumacz, że wycieki danych zdarzają się i zdarzać będą nawet na najlepiej zabezpieczonych serwisach. I nasze konta, podobnie jak nasze mieszkania, zawsze będą narażone na jakieś niebezpieczeństwo. Podkreśl, że w sytuacji wycieku, powinniśmy się „uodpornić", czyli: **Ile osób w grupie padło ofiarą wycieku danych:** **Ile danych łącznie wyciekło:** **Które są najbardziej niebezpieczne:** Zauważcie, że wyciec mogą bardzo różne dane, od adresu IP po dane informujące o naszym zdrowiu i wynikach badań genetycznych. Najczęściej w wyciekach zobaczycie jednak „świętą trójcę", czyli e-mail, login i hasło. Podnieście teraz proszę ręce wszyscy Ci, którzy używają innego hasła do każdej witryny i aplikacji do której się logują. Okej, dzięki. Czyli u reszty nasze hasło się czasem powtarza, czyli, że mamy jedne hasło do wielu witryn i aplikacji. To teraz wyobraźmy sobie, co dzieje się, gdy takie hasło wycieka. Jeśli ktoś ma jakieś nasze hasło, to trochę tak jakbyśmy zgubili klucz (jakiś klucz). Sam klucz wiele nam nie powie, ale jeśli ktoś zgubił go w kopercie wraz z naszym adresem (a tym po części jest nasz adres mailowy), to ktoś może już jechać z tym kluczem do naszego domu by spróbować otworzyć nim nasze drzwi. Jeśli ten klucz, który trzyma w ręku, to mało istotny klucz np. do zapięcia rowerowego, to może nam coś zabrać, ale nie dostanie się do naszego mieszkania. Jeśli jednak wpadliśmy na pomysł używania jednego magicznego klucza do zapięcia, do mieszkania, do garażu i do sejfu z kosztownościami, to może i jest to wygodne, ale staje się już bardzo niebezpieczne. Wytłumacz, że wycieki danych zdarzają się i zdarzać będą nawet na najlepiej zabezpieczonych serwisach. I nasze konta, podobnie jak nasze mieszkania, zawsze będą narażone na jakieś niebezpieczeństwo. Podkreśl, że powinniśmy wtedy: • **Zmienić hasło na nowe i silne** (o tym jakie hasła są silne powiemy sobie za chwilę). • **Odwiedzić zakładkę Ustawienia i bezpieczeństwo na naszym koncie mailowym i kontach społecznościowych by zobaczyć kto ma dostęp do konta** (coraz więcej stron oferuje możliwość sprawdzenia historii logowania, podejrzanych logowań oraz sprzętów podłączonych do konta). • **Skonfigurować uwierzytelnianie dwuetapowe, najlepiej wraz z menedżerem haseł*.** • **Przygotować się na kolejny krok w potencjalnym ataku.**	**Co równie ważne, handluje ona danymi z wycieków, w sposób który w Polsce jest niedopuszczalny. Nie pokazuj jej i nie rekomenduj. Miej jednak świadomość jej istnienia w razie pytań od młodzieży/nauczycieli.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl ***Uwaga: Już teraz możesz wspomnieć o znaczeniu takich rzeczy jak uwierzytelnianie dwuetapowe i menedżer haseł (jako ważnych elementach ochrony). O obu narzędziach jest jednak mowa w dalszej części scenariusza, więc dopasuj ilość treści w obu miejscach, aby nie powtarzać dwa razy tych samych informacji.** **- komentarz dzięki uprzejmości Niebezpiecznik.pl**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Profilowany Phishing** Jedną z pierwszych technik, które zobaczyliście na filmie była socjotechnika, czyli wywieranie wpływu na odbiorcę poprzez odwołanie się do emocji. Może być to strach (powodowany przez email od szefa) lub emocje pozytywne związane np. z tym, że jesteś 1000000 klientem danej strony i wygrałeś dzięki temu Ipada (oczywiście nie wygrałeś). Przećwiczymy teraz różne scenariusze wiadomości wykorzystujących socjotechnikę poprzez stworzenie takiej przykładowej wiadomości, na podstawie której przetestujemy podatność kluczowych pracowników. Wyświetl dwa profile potencjalnych celów na prezentacji. Poproś grupy o wybranie jednego celu i ułożenie potencjalnej wiadomości phishingowej. Zachęć do wykorzystania wiedzy z poprzedniego ćwiczenia oraz przemyślenia, którym kanałem komunikacji mogłaby zostać wysłana taka wiadomość i do czego miałaby nakłaniać. **Oceń pracę grupy według schematu:** • Odwołanie do emocji +1 punkt • Dobranie sposobu komunikacji do celu +1 punkt • Przemyślenie jakie dane wyciągamy od użytkownika +1 punkt • Przemyślenie zachęcenia do działania (pobranie pliku lub kliknięcie linka) + 1punkt • Pomysł na wykorzystanie danych z poprzedniego ćwiczenia +1 punkt Pamiętajcie, że wiadomości te tworzyliśmy tylko w celach edukacyjnych – by poznać metody ich tworzenia. Przypominam, że nie powinniśmy wykorzystywać tej wiedzy do próby podszywania się pod innych, do prób włamów lub do zwykłego robienia „żartów" kolegom, bo mogą nas za to spotkać poważne konsekwencje. „Zakłócenie działania systemu komputerowego" według Art. 269a. Kodeksu Karnego podlega karze pozbawienia wolności od 3 miesięcy do lat 5. A „uporczywe nękanie i Kradzież tożsamości" według Art. 190a. KK podlega karze pozbawienia wolności nawet do 8 lat.	https://www.mentimeter.com/app/presentation/alwicz-c473j6xbpt3hovvq38g9mq24dg

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Phishing** Podkreśl, że „umocnieniu" po wycieku danych powinniśmy poddać przede wszystkim nasze skrzynki mailowe. Phishing profilowany, który tworzyliśmy wyżej może nas dosięgnąć każdym kanałem komunikacji. „Standardowy" phishing (wysyłany do wielu odbiorców) będzie trafiać najczęściej na nasze maile (choć do innych kanałów również). Powinniśmy mieć zatem w tyle głowy, że taka skr zynka (której adres wyciekł) może stać się celem ataków phishingowych.Podkreśl, że teraz przećwiczymy ochronę przed phishingiem. Kolejnym Waszym zadaniem jest sprawdzenie niedawnych wiadomości, które trafiły do waszych współpracowników w firmie. Waszym celem jest wyłapanie wiadomości phishingowych i ostrzeżenie kolegów przed nimi. Za każdą poprawnie zidentyfikowaną wiadomość dostajecie jeden punkt! Wyświetl uczestnikom prezentację z przykładowymi wiadomościami e-mail. Daj im 10-15 sekund na przeczytanie treści i podjęcie decyzji czy jest to prawdziwa wiadomość czy phishing – wiadomość wysłana przez kogoś podszywającego się pod instytucję lub inną osobę i wysłana w celu kradzieży danych lub instalacji złośliwego oprogramowania. Podkreśl, że są to tak zwane socjotechniczne metody włamań, które wymagają treningu w ich rozpoznaniu i zwracania uwagi na szczegóły. Wyświetl slajdy z prezentacji i przeprowadź głosowanie w klasie Podsumuj na co powinniśmy zwracać uwagę w wiadomościach e-mail (adres nadawcy, podpisy i stopki, błędy ortograficzne, przyciski i dziwne linki oraz, co najważniejsze, metody socjotechniczne próbujące pobudzić nasze emocje i "wyłączyć myślenie"). **Podkreśl, że jeśli nie jesteśmy pewni danego linku lub załącznika (a mimo wszystko powinniśmy go sprawdzić), to możemy wykorzystać narzędzie: https://www.virustotal.com/gui/home/upload pozwalające na sprawdzenie strony lub danego pliku*.** Podkreśl, że phishing wykorzystywać może dotychczasowe wycieki danych (ktoś pisze na adres, który znalazł w sieci, podając hasło do naszego konta i liczy, że go nie zmieniliśmy). Może również doprowadzić do przekazania przez nas danych logowania na podstawionej stronie. Samo hasło, nawet jeśli jest długie to zatem za mało.	https://www.mentimeter.com/app/presentation/alyzjdter6z-chiqr3th4upa24u76gkm4 Uwaga: wypada też dodać, że pozytywna ocena VirusTotal nie oznacza, że jesteśmy w 100% bezpieczni. Należy też uważać z tym, co się tam podsyła ponieważ oznacza to dzielenie się tym plikiem z serwisem. Warto uczulić, że przesyłanie plików na cudzą stronę i korzystanie z usług webowych może umożliwiać komuś dostęp do naszych plików. - Komentarz dzięki uprzejmości Niebezpiecznik.pl

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Łamanie haseł** Wytłumacz, że w tym ćwiczeniu zajmiemy się pierwszą furtką, czyli hasłami. Przetestujemy czy po włamie, nasi współpracownicy na pewno utworzyli silne hasła. Pozyskanie informacji o użytkownikach i ich haseł (z wycieków danych lub przy pomocy phishingu), pozwala też często na odgadniecie nawet nowych haseł (jeśli ktoś nie potrafi dobrze ich tworzyć). Waszym zadaniem jest wykorzystanie informacji o waszych współpracownikach, złamanie ich haseł, wejście na ich komputery i zostawienie im notatki o tym, jakie powinno być silne hasło i jak je tworzyć. Im więcej komputerów zhakujecie, tym więcej o zasadach tworzenia haseł się nauczycie! Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. Podkreśl, że po wykryciu wycieku, w pierwszej kolejności powinniśmy zatem zmienić hasło do danego serwisu, a najlepiej wszystkie hasła. Nowe hasło powinno być silne, czyli: • **długie** (najlepiej w formie frazy- „PassPhrase" zamiast „Password")* • **abstrakcyjne** (pozbawione logiki, przewidywalności, systemu, który można złamać) • **z cyframi i znakami specjalnymi** (dyskusyjne) • **różne do każdego serwisu** • **łatwe do zapamiętania** (dyskusyjne) ***Silne hasło** Daj uczestnikom pięć minut na stworzenie tego typu hasła. I poproś o przetestowanie go na stronie: https://www.security.org/how-secure-is-my-password/ Następnie zapytaj czy jesteśmy w stanie powtórzyć ten proces i zapamiętać wszystkie te hasła dla wszystkich innych witryn i aplikacji? Podkreśl, że jest to raczej mało prawdopodobne i że dobrym sposobem może być wykorzystanie menedżera haseł – programu tworzącego i zapamiętującego za nas hasła. **Podkreśl, że mogą być to programy dostępne w chmurze takie jak Last Pass czy Avira Password Menager lub programy dostępne offline, na dysku naszego komputera*. Podkreśl, że obecne przeglądarki takie jak Google Chrome czy Safari również oferują taki menedżer. Ma on dobre szyfrowanie i co ciekawe, menedżery haseł działające w przeglądarce mogą nas uchronić przed atakiem IDN Homograph, czyli takim atakiem, w którym cały adres strony lub jakaś jego część jest napisana innym alfabetem (np. cyrylicą).**	https://www.mentimeter.com/app/presentation/al9smohxb-franzzzo35d65wwt7ngfzj2 https://www.mentimeter.com/app/presentation/al2g6statijuwf-fwdooxjakgumz6hg79 **Zapoznaj się z:** https://cert.pl/posts/2022/01/kompleksowo-o-haslach/ https://niebezpiecznik.pl/post/uwaga-na-niewykrywalny--phishing-poprzez-domeny-ze--znakami-unicode-podobnymi--do-liter-z-alfabetu-lacinskiego/ **Uwaga: Podkreśl, że długość stanowi najważniejszy parametr hasła. Cyfry i znaki nie są złą rekomendacją, ale nie mogą zastępować długości. Kwestia łatwości zapamiętania hasła będzie natomiast dyskusyjna, bo zależna od sposobu ich przechowywania (można korzystać z menedżera haseł). Zwróć przy tym uwagę na jak wiele z tych wyzwań odpowiada (dodatkowo w łatwy sposób) menedżer haseł, który powinniśmy stosować.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Taki adres dla naszego oka może się wydawać nie do odróżnienia, ale menedżer analizując adres strony „zobaczy", że nie ma tej witryny w swojej bazie logowania i haseł i że jest to zatem nowa, inna witryna.** Z menedżerów haseł możemy korzystać pod jednym warunkiem. Zapytaj grupę jaki jest skrót klawiszowy do blokady ekranu i komputera (Control + Command + Q na systemie MAC oraz Windows + L na systemie Windows)? Podkreśl, że możemy korzystać z menedżerów i zapamiętywania haseł tylko pod warunkiem, że mamy ustawione blokady ekranu i hasła zarówno na komputerze, jak i na komórce. Nawyk wygaszania ekranu i blokowania komputera to kolejne ważne przyzwyczajenie, który powinniśmy w sobie rozwijać.	***Każdy menedżer będzie ok, ale dla bardziej ambitnych/ zaawansowanych użytkowników rekomendowany jest KeePass. Użycie menedżerów w przeglądarce będzie natomiast ok, pod warunkiem że: hasła są mocne i unikalne, tylko my korzystamy z danej przeglądarki i konta oraz urządzenie jest dobrze chronione przed dostępem osoby niepowołanej.** - Komentarz dzięki uprzejmości Niebezpiecznik.pl
10 min	**2FA** Podkreśl, że silne hasło uchroni nas przed jego złamaniem przez algorytmy deszyfrujące (a przynajmniej bardzo ten proces utrudni). **Zapytaj jednak co zrobić w sytuacji, gdy ktoś zna nasze silne hasło (bo np. wyciekło). Jak możemy obronić się w takiej sytuacji?** **Podkreśl, że najważniejszym sposobem ochrony okazuje się w tej (i wielu innych sytuacjach) weryfikacja dwuetapowa (lub wieloskładnikowa).** Wytłumacz, że jest to dodatkowy (oprócz hasła) sposób weryfikowania czy to aby na pewno my, logujemy się na nasze konto. Może on przybrać formę karty kodów jednorazowych (dawne rozwiązanie popularne w bankach i wciąż obecne np. na gmailu), kodów SMS, kodów lub potwierdzeń w dedykowanej aplikacji authenticator, potwierdzeń mailowych lub forę klucza U2F, czyli urządzenia przypominającego pendrive z dodatkowym modułem NFC do łączności bezprzewodowej. Taki klucz nawiązuje łączność z daną stroną internetową i potwierdza naszą tożsamość. W Waszej firmie weryfikacja dwuetapowa nigdy nie została wprowadzona, bo pracownicy nie mogli ustalić najlepszej jej formy. Każdemu zawsze coś nie pasowało z danym sposobem potwierdzania swojej tożsamości...	https://www.mentimeter.com/app/presentation/al726ko2z-4kwkxfhyov9o8r44o6zwhbp **Uwaga: włączenie weryfikacji dwuetapowej to jeden z najlepszych sposobów ochrony swojego konta. Jeśli chcesz włączyć ją z uczestnikami w trakcie zajęć, upewnij się, że znajdują się oni na bezpiecznej sieci (na prywatnych sieciach komórkowych lub sieci domowej), nie jest rekomendowane zmienianie ustawień swojego konta poprzez publiczną sieć Wi-fi.**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Podkreśl, że teraz zadaniem uczestników jest znalezienie najlepszego sposobu dodatkowej weryfikacji w każdym z przedstawionych za chwilę w prezentacji case'ów. Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. Podkreśl, że w ostatnim pytaniu prawie wszystkie odpowiedzi są poprawne, gdyż najlepsza dodatkowa weryfikacja, to taka, która rzeczywiście jest stosowana. **Może być to klucz U2F (jako jedyny sposób dodatkowego uwierzytelniania chroniący w pełni przed phishingiem) lub aplikacja Authenticator (Google lub Microsoft)** ale najważniejsze jest, aby przede wszystkim włączyć tę dodatkową opcję na swoich kontach!	**Zapoznaj się z**: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/2-wykorzystanie-kluczy-sprzetowych-u2f/
10 min	**Pomocne programy** **Podkreśl, że obok cyberprzestępców, w sieci obecne są również wirusy – programy komputerowe wykorzystujące luki w zabezpieczeniach i wykonujące różnego rodzaju szkodliwe działania na naszym komputerze – mogą monitorować to, co wpisujemy na klawiaturze (Keylogger),** włączać kamerkę i służyć późniejszemu szantażowi (Ransomware), szyfrować nasze dyski, czy zamienić nasz komputer w koparkę BitCoinów (Botnet). Powiedz, że ostatnim zadaniem grup jest poprawienie bezpieczeństwa sprzętu poprzez włączenie skanowania antywirusowego na komputerach, na które udało nam się włamać. Poproś uczestników, aby wszyscy włączyli w tym momencie skanowanie antywirusowe/bezpieczeństwa na swoim sprzęcie (smartfonie lub komputerze) i żeby grupy napisały jakie skanowania włączyły. Zadanie wygrywa grupa, który włączy najwięcej i najbardziej istotnych skanowań. Podkreśl, że z powodu ogromnej liczby różnych sprzętów i urządzeń, nie ma jednej metody i jednego idealnego programu. Ważnymi skanowaniami, które zaliczymy grupom do wykonania zadania będą: **Na komputerach:** • Skanowanie Windows Defender • Skanowanie zewnętrznym programem antywirusowym • Skanowanie Windows update	https://www.mentimeter.com/app/presentation/albqus4st-9186n8moysadrg2jmpbtmgq **Zapoznaj się z:** https://niebezpiecznik.pl/post/sprawdz-czy-twoj-smartfonjest--zhackowany https://zaufanatrzeciastrona.pl/post/podstawybezpieczenstwa--czywspolczesne- smartfonypotrzebuja-antywirusa/ ***Uwaga: Zapoznaj się również z:** https://sklep.niebezpiecznik.pl/opis/11

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Na smartfonach i tabletach*:** • Skanowanie Google Play Protect • „Skanowanie bezpieczeństwa" w panelu sterowania lub ustawieniach • Skanowanie aktualizacji • Skan zewnętrznym programem antywirusowym (w większości wypadków nic to nie zmienia, gdyż programy te nie mają dostępu do innych obszarów pamięci telefonu – działanie w wydzielonym obszarze pamięci/sanbox. Z drugiej strony, renomowane programy antywirusowe nie zaszkodzą też pod względem bezpieczeństwa telefonowi, okazjonalnie potrafią wykryć więcej niż Google Play Protect). Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i doceń grupę z najlepszym wynikiem. **Wyświetl slajd z przydatnymi programami i wytłumacz, że powinniśmy:** • Dbać o aktualizację naszych urządzeń (w ten sposób usuwamy luki w zabezpieczeniach). • Uważać na wyłączanie zabezpieczeń i instalowanie programów z niebezpiecznych źródeł (Jailbreak na IOS, włączanie debbugowania przez USB na telefonie, instalacja aplikacji spoza oficjalnych sklepów). „Skanowania bezpieczeństwa" w smartfonach często włączają właśnie na powrót domyślne ustawienia zabezpieczeń, które wyłączyliśmy. • **Ustawić blokady chroniące sprzęt przed dostępem osoby niepowołanej (blokady ekranu, Kod PIN na kartach SIM, mocne hasła na kontach Google/Icloud.** • Zdawać sobie sprawę, że mamy domyślne filtry i zabezpieczenia (Microsoft Defender i Zapora Windows, Skanowanie aplikacji w Google Play, system działający na zasadzie ograniczania uprawnień/ sandbox na androidzie i IOS). • Okazjonalnie zeskanować komputer przy użyciu dodatkowego programu wybranego z aktualnej listy: https://www.av-test.org/en/ ; https://www.av-comparatives.org/ ; https://www.mrg-effitas.com/ ; https://www.virusbulletin.com/ ; https://selabs.uk/. Podkreśl, że obok oprogramowania antywirusowego warto zainstalować sobie również dwa inne programy, czyli Menagera Haseł (tu również warto sprawdzić aktualne, polecane listy) oraz aplikację do uwierzytelniania dwuetapowego dla innych programów: Microsoft Authenticator czy Google Authenticator.	**Podkreśl też, że większość nowoczesnych smartfonów wykonuje dużo z tych procesów samodzielnie (okresowo, w tle). W przypadku smartfonów i tabletów bardziej istotne są zatem nawet ustawienia konfiguracji:** • dobra blokada ekranu, • PIN na karcie SIM, • włączone śledzenie urządzenia, • konieczność bardzo dobrego chronienia hasła do Google/ Icloud (bo przecież mamy śledzenie), • aktualizacja Systemu i osobno aplikacji. Czyli, dobra i bezpieczna konfiguracja telefonu.

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Zapytaj również czy istnieją pliki, z którymi skanery antywirusowe mogą sobie nie poradzić? Podkreśl, że możemy również mieć na swoim dysku lub mailu pliki zaszyfrowane. Podkreśl, że to dobra i bezpieczna metoda na przesyłanie danych osobowych lub wrażliwych – p.. Dokumentów. Zaznacz, że opcję zaszyfrowania i opatrzenia danego folderu/archiwum hasłem mają takie programy jak winrar czy 7zip. W przypadku plików szyfrowanych, powinniśmy przesyłać hasło drugim sposobem komunikacji (np. Jakimś rodzajem komunikatora lub sms-em). Otwierając taki plik, powinniśmy mieć z kolei pewność, że pochodzi z zaufanego źródła. Na koniec podkreśl, że wszystkie operacje związane z hasłami i zakupami powinniśmy robić zawsze na bezpiecznej sieci – sieci domowej (zabezpieczonej hasłem) lub poprzez swój transfer danych, ewentualnie poprzez VPN – wewnętrzny tunel maskujący naszą aktywność i nasze dane. Tu również trzeba jednak uważać na darmowe VPN-y, które mogą gromadzić nasze dane.	
10 min	**Podsumowanie** Doceń i nagródź najlepszych uczestników i drużyny w całej symulacji. Gratulacje! Udało Wam się zabezpieczyć wasze miejsce pracy, zmienić nawyki waszych współpracowników na bardziej bezpieczne i tym samym uratować Waszą firmę! Gratulujemy ukończenia i wygrania naszej symulacji! Poproś uczestników o zastanowienie się nad wszystkimi sposobami ochrony, o jakich dzisiaj słyszeli. Poproś ich o wybranie kolejnego kroku, czyli ich zdaniem najlepszego, najbardziej przydatnego sposobu i jego wdrożenie. *Daj uczestnikom 5 minut na wdrożenie jednego ze sposobów/metod ochrony swoich danych. Dla ułatwienia, możesz wyświetlić im listę propozycji z prezentacji. Podkreśl, że celem naszych zajęć nie jest straszenie i twierdzenie, że Internet jest zły lub niebezpieczny. Naszym celem jest wyposażenie wszystkich w wiedzę, umiejętności i narzędzia, które pozwalają być bezpieczniejszym w sieci. Zaproś przy tym uczestników do metody małych kroków – instalacji jednego programu/wdrożenia jednej metody i przyzwyczajenia się do niej – zmienienia swoich nawyków. Podkreśl, że najlepsza metoda ochrony, to taka, którą rzeczywiście stosują.	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Nie ma nic gorszego, niż wybranie sobie “najlepszej” metody ochrony, a potem jej porzucenie dlatego, że jest za trudna. Zróbcie jeden krok, wprowadźcie jedno rozwiązanie i starajcie się przy nim pozostać – zmienić trwale swoje nawyki na bardziej bezpieczne. Gdy to się Wam uda, wtedy pomyślcie nad drugim krokiem, kolejnym, bardziej bezpiecznym rozwiązaniem. W ten sposób będziecie coraz bezpieczniejsi w sieci. Podziękuj za zajęcia, uwagę uczestników i uczestniczek oraz pomoc nauczycieli i nauczycielek. Poproś o ustawienie się do wspólnego „zdjęcia”/screena z zajęć. Wytłumacz, że posłuży on tylko do dokumentacji odbycia się zajęć zdalnych. Kto chce może zatem zasłonić swoją twarz (ochrona prywatności, którą zajmiemy się na kolejnym warsztacie).	

PFR Fundacja

Centralny Dom Technologii

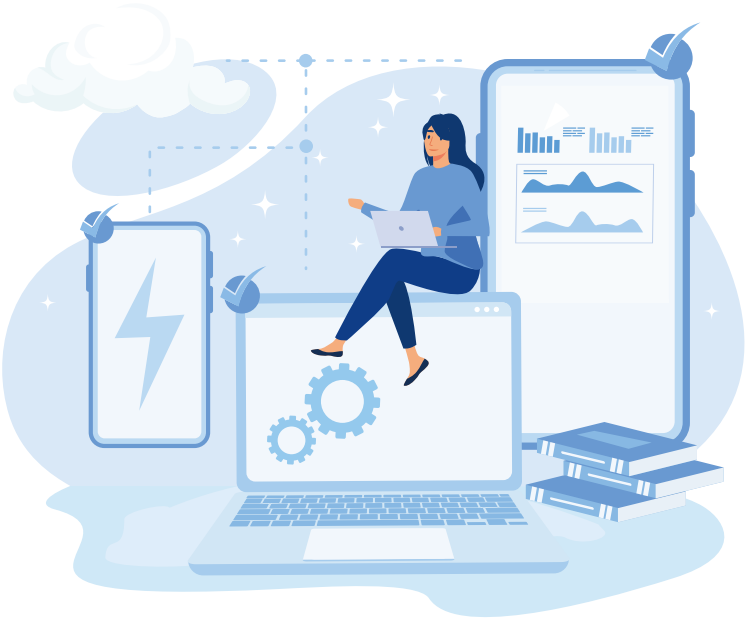
NIEBEZPIECZNIK.PL

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

Scenariusz warsztatów
Media społecznościowe i manipulacje

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 sieci.



Czas trwania

- 90 min.

Grupa wiekowa

- 12 do 14 lat

Cele

1. Cele ogólne:
a. Rozwijanie umiejętności dbania o swój wizerunek w sieci,
b. Rozwijanie umiejętności wykrywania manipulacji medialnych naszego bezpieczeństwa 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. 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.

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 projekt Cyberbezpieczni i o czym jest dzisiejszy warsztat (media społecznościowe i prywatność w sieci – jak ochronić swoją prywatność w sieci oraz rozpoznawać manipulacje medialne). Następnie dobierz uczestników w pary lub zespoły czteroosobowe. Podkreśl, że wszyscy uczestnicy mogą pracować na telefonach i komputerach, ale że do prezentacji, powinien podłączyć się już tylko jeden reprezentant pary/zespołu. 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), zasada dobrej współpracy (pracujemy wspólnie i pomagamy sobie w zespole). Wytłumacz, że zanim przejdziemy do kwestii prywatności w sieci, musimy poznać doświadczenie uczestników z social mediami. 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 fanpage. 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 – tych społecznościowych i tych tradycyjnych, oraz manipulacjach, które w nich występują. Sprawdzimy dziś ile media wiedzą o nas i czy są w stanie nami manipulować, a ile my wiemy o nich i czy jesteśmy w stanie się przed tego typu manipulacjami obronić. Wcielicie się dziś zatem w dwie różne role przy dwóch ćwiczeniach wcieleniowych. Waszym zadaniem będzie wcielenie się w rolę youtuberów i obrona swojego konta i bezpieczeństwa oraz obrona przed fake newsami i manipulacjami medialnymi jako dziennikarze. Zanim jednak przejdziemy do mediów tradycyjnych, sprawdźmy czy potraficie przeciwdziałać manipulacji ze strony mediów społecznościowych.	https://www.mentimeter.com/app/presentation/alfwhfj7y4ebv-2cj9pfhx5beap7i15ts ***Możesz zrezygnować z Diagnozy w przypadku ograniczonego czasu.** **Uwaga 2:** Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych. **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

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	*Powiedz, że zaczniemy od diagnozy tego, co media społecznościowe wiedzą o nas. Podkreśl, 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 samodzielnie i które mogą służyć nie tylko profilowaniu, ale również zostać wykorzystane przez osoby trzecie.	
10 min	**Co wiedzą o nas algorytmy** Podkreśl, że zaczniemy od pierwszego obszaru i dowiemy się co wie o nas Google, Facebook lub Tik Tok. 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 z ogromnej liczby 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 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 może być określane 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/	***Nie jest to ćwiczenie obowiązkowe w tej grupie wiekowej** https://www.mentimeter.com/app/presentation/al1bv5mo8cck-nq9spg2h76hpf75bme93

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	**Co udostępniamy** 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 grupę: • 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. Podkreśl, że wraz z coraz większą obecnością w sieci i coraz większą liczbą 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. • **Używaj anonimowego nicku,** • **Jeśli używasz nazwiska, masz swoją stronę internetową, ukryj swoje inne dane osobowe,** • **Zmień ustawienia prywatności w mediach, w których kontaktujesz się z rodziną i przyjaciółmi (np. listy znajomych),** • **Wyłącz lokalizację,** • **Wykorzystuj adresy e-mail stworzone dla twojej działalności (np. z twoim nickiem, a nie nazwiskiem)*.**	https://www.mentimeter.com/app/presentation/alhd8cg3cj-8pvt2zwk2u76fuxthu3ng8 ***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 rozpatrzeć 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

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Wciel się w rolę** Pokaż uczestnikom stronę z ustawieniami prywatności konta Facebook lub innego konta w mediach społecznościowych np. TikToka. Poproś żeby zapoznali się z tą ścieżką dojścia do tych ustawień. Następnie poproś uczestników o zapoznanie się z ćwiczeniem wcieleniowym i ułożenie minimum trzech dobrych praktyk dla ochrony swoich danych w sieci. Zapytaj wtedy o to, które ustawienie prywatności byłoby najlepsze do włączenia/wdrożenia? Zachęć do włączenia danego ustawienia lub wprowadzenia w życie danej zasady. Podkreśl, że nawet jeśli dane ustawienia czy zasady nie przydadzą nam się obecnie, warto wiedzieć jak postąpić w przypadku nagłej sytuacji, która może dotknąć Was, lub co ważniejsze, waszego kolegę lub koleżankę. Może być to wyciek danych, przechwycenie prywatnych zdjęć, stalking czy trolling, a może nawet zmasowany hejt, którego doświadcza np. wiele osób o rozpoznawalnych w sieci profilach. Według badań: Co piąty nastolatek przyznaje, że doświadczył przemocy w internecie. Najczęstszymi jej przejawami są: wyzywanie (29,7%), ośmieszanie (22,8%) czy poniżanie (22%). A jednocześnie, najczęstszym sposobem reakcji jest bierność: . 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 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. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html Podkreśl, że warto zatem znać podstawowe ustawienia prywatności i warto przemyśleć dodatkowe zasady bezpieczeństw. Nie chodzi tylko bowiem o zabezpieczenie swojej prywatności, ale również pomoc koledze czy koleżance, która może zgłosić się do mnie z tym problemem.	https://www.mentimeter.com/app/presentation/almkyq5e-h2t7z1ei84wng9br1ds7kxk3

Część II

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Artykuł** Wyświetl artykuł z dziennika bulwarowego i daj uczestnikom chwilę na jego przeczytanie: http://dziennikbulwarowy.pl/145/prawomocnie-uznany-za-trolla-internetowego.html?u=1:31:0:77: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 weryfikacji informacji znalezionych w sieci.	https://www.mentimeter.com/app/presentation/altwhmntp5fp-7di84xzv88d2tqjg3yfu
	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 np. **Testu CRAAP.**	https://www.mentimeter.com/app/presentation/alguujyd4g-gcqkwcjs6zdpwgdomz3ese

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	https://demagog.org.pl/analizy_i_raporty/jak-radzic-sobie-z-dezinformacja-12-zasad-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:** https://drive.google.com/drive/folders/1s9tHX6G4B3Pije-1sexghj07tE2BejRZ?usp=sharing 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?x	
	***Get Bad News** Poproś uczestników warsztatów o wejście na stronę getbadnews.pl oraz wcielenie się w rolę „Fakeowego dziennikarza", czyli twórcy fake newsów. Wytłumacz, że uczestnicy powinni przejść przez krótki tutorial (i najlepiej ominąć ankietę). Następnie, w ramach gry, wybierać będą Fake newsy do publikacji. Podkreśl, że na to ćwiczenie każda drużyna ma 15 minut, a następnie omówione zostaną wyniki drużyn – liczba obserwujących i wiarygodność. Podkreśl, że każda decyzja ma znaczenie i musimy starać się pilnować miernika wiarygodności przy jednoczesnym zwiększaniu zasięgów. Daj uczestnikom 15 minut na samodzielną grę i tworzenie fake newsów.	***Ćwiczenie dla grupy młodszej, które może być stosowane zamiast ćwiczenia Factcheckingowe narzędzia.**

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Po 15 minutach zakończ grę i poproś o wpisanie swoich wyników. Doceń najlepszą grupę. Wytłumacz przy tym, że celem gry nie jest zostanie realnym fake-newsowym dziennikarzem, lecz pokazanie mechanizmów manipulacji: • podszywanie się pod renomowane źródła lub znane osoby, • odwoływanie do emocji, • wybieranie tematów kontrowersyjnych • polaryzacja (potencjalnych) stron sporu, • dyskredytowanie instytucji i osób publicznych, • tworzenie spiskowych teorii, • trolling, czyli wzniecanie emocjonalnych dyskusji w internecie. https://www.getbadnews.pl/wp-content/uploads/2019/03/Bad-News-Game-info-sheet-for-educators-Polish.pdf Podkreśl, że teraz lepiej powinniśmy umieć rozpoznawać te mechanizmy w czytanych przez nas informacjach i artykułach.	
10 min	**Sprawdzenie i podsumowanie** Raz jeszcze wyświetl artykuł z dziennika bulwarowego. Zapytaj jakie wskazówki z materiałów pomocniczych mogłyby okazać się tu pomocne? 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? • Jakie źródła wskazane są w tekście (jaki sąd wydał wyrok? NSA? W Pcimiu Dolnym?)? • Jakie źródło informacji jest na końcu tekstu (Czym jest Orient? Czym jest PAPs? Czy chodzi o Onet i PAP?)? • **Czy artykuł jest sponsorowany (początek lub koniec tekstu)?** • Dowody/Potwierdzenia (czy da się znaleźć wyrok? Czy są materiały potwierdzające dane zdarzenie?)?	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 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. 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.	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Spis artykułów i rozwiązań:** **Avengers** – Clickbait – nic nie zostaje wyjaśnione w artykule. **Banksy** – Fałszywy artykuł z generatora Newsów **Chrzest** – Artykuł satyryczny z AszDziennika **Jakubiak** – Trudna do jednoznacznej klasyfikacji „wizualizacja" marzenia – wykreowanie własnego „wywiadu z Ellen" by zostać zaproszonym do The Ellen DeGeneres Show. **Pestki** – Pseudonauka (https://dietetyczny.blog.polityka.pl/2017/08/21/gorzka-prawda-o-amigdalinie/) **Rekin** – fake news – warto zwrócić uwagę na „metodę" obliczania wieku rekina: https://www.wprost.pl/swiat/10092700/najstarszy-w-historii-rekinem-polarnym-to-fake-news.html **Reptilianie** – teoria spiskowa **Yoga** – Artykuł sponsorowany **Mierzeja** – Manipulacja z kontekstem politycznym (odpowiedź w języku rosyjskim sugeruje bycie „agentem" obcego wywiadu). **Jeśli to prawda, będziemy mogli...** - słynny błąd, który obiegł świat: https://tvn24.pl/tvnmeteo/najnowsze/polecialy-glowy-za-neutrina-szybsze-od-swiatla-4879288 **Czy Hillary Clinton...** – Teoria spiskowa dotycząca handlu ludźmi, odbywającego się w piwnicy pewnej pizzerii, w który zamieszana była prezydent Stanów Zjednoczonych. Warto zwrócić uwagę na rażące przeinaczenia np. „sędzina" Antonina Scaliia, to mężczyzna. **Korwin** – manipulacja i teoria spiskowa. Warto zwrócić uwagę na rażące przeinaczenia np. mRNA nie oznacza „modyfikacji RNA". **Uchodźca na statku** – Manipulacja. Uchodźca stoi na tonącym kadłubie statku: https://factcheck.afp.com/drowning-refugees-hoax-resurfaces-north-america **Zełensky** – Fałszywa grafika edytowana w programie cyfrowym. Przy pomocy programu PhotoForencis można zobaczyć różnice w kompresji: https://fotoforensics.com/analysis.php?id=8af1f8680579588d7c355a8b4b53a21669adc0e1.147248 ; https://fotoforensics.com/tutorial-ela.php	

PFR Fundacja

Centralny Dom Technologii

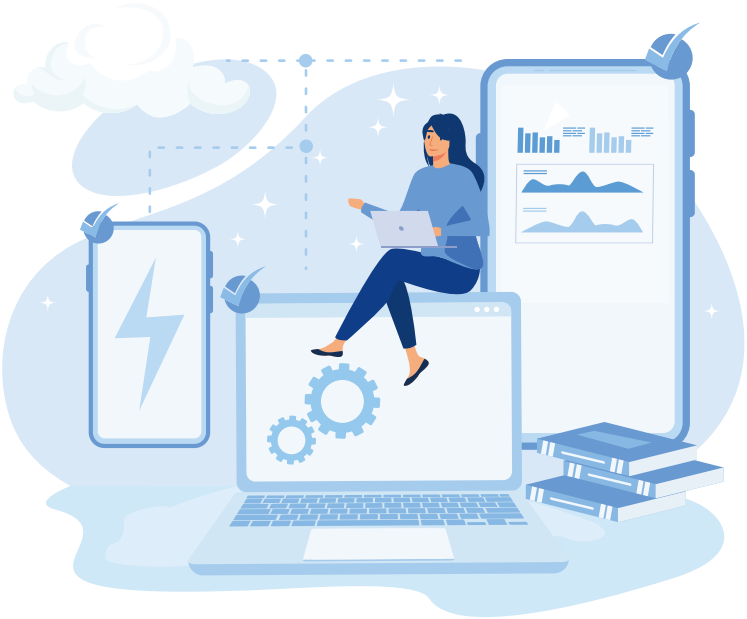
NIEBEZPIECZNIK.PL

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

Scenariusz warsztatów
Media społecznościowe i manipulacje

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 sieci.



Czas trwania

- 90 min.

Grupa wiekowa

- 14 do 19 lat

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 o 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.

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 projekt Cyberbezpieczni i o czym jest dzisiejszy warsztat (media społecznościowe i prywatność w sieci – jak ochronić swoją prywatność w sieci oraz rozpoznawać manipulacje medialne). Następnie dobierz uczestników w pary lub zespoły czteroosobowe. Podkreśl, że wszyscy uczestnicy mogą pracować na telefonach i komputerach, ale że do prezentacji, powinien podłączyć się już tylko jeden reprezentant pary/zespołu. 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), zasada dobrej współpracy (pracujemy wspólnie i pomagamy sobie w zespole). Wytłumacz, że zanim przejdziemy do kwestii prywatności w sieci, musimy poznać doświadczenie uczestników z social mediami. 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 fanpage. 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 – tych społecznościowych i tych tradycyjnych, oraz manipulacjach, które w nich występują. Sprawdzimy dziś ile media wiedzą o nas i czy są w stanie nami manipulować, a ile my wiemy o nich i czy jesteśmy w stanie się przed tego typu manipulacjami obronić. Wcielicie się dziś zatem w dwie różne role przy dwóch ćwiczeniach wcieleniowych. Waszym zadaniem będzie pomoc koledze lub koleżance w obronie swojego konta i bezpieczeństwa oraz obrona przed fake newsami i manipulacjami medialnymi. Zanim jednak przejdziemy do mediów tradycyjnych, sprawdźmy czy potraficie przeciwdziałać manipulacji ze strony mediów społecznościowych.	https://www.mentimeter.com/app/presentation/al4vyjks2f7f-nebct8iefmmzp8mgym3r ***Możesz zrezygnować z Diagnozy w przypadku ograniczonego czasu.** **Uwaga 2:** Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych. **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

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	*Powiedz, że zaczniemy od diagnozy tego, co media społecznościowe wiedzą o nas. Podkreśl, 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 samodzielnie i które mogą służyć nie tylko profilowaniu, ale również zostać wykorzystane przez osoby trzecie.	
10 min	**Co wiedzą o nas algorytmy** Podkreśl, że zaczniemy od pierwszego obszaru i dowiemy się co wie o nas Google, Facebook lub Tik Tok. 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 z ogromnej liczby 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 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 może być określane 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-od-zyskaj-kontrole-nad-tym-co-widzisz-w-internecie/	https://www.mentimeter.com/app/presentation/alaq86pq-ne1p4xcqehrnj96tikf5etc6

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
15 min	**Co udostępniamy** 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 grupę: • 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. Podkreśl, że wraz z coraz większą obecnością w sieci i coraz większą liczbą 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. • **Używaj anonimowego nicku,** • **Jeśli używasz nazwiska, masz swoją stronę internetową, ukryj swoje inne dane osobowe,** • **Zmień ustawienia prywatności w mediach, w których kontaktujesz się z rodziną i przyjaciółmi (np. listy znajomych),** • **Wyłącz lokalizację,** • **Wykorzystuj adresy e-mail stworzone dla twojej działalności (np. z twoim nickiem, a nie nazwiskiem)*.**	https://www.mentimeter.com/app/presentation/aly8g6bit2g-z8q3up1eziqfunsg177mv ***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 rozpatrzeć 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

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Wciel się w rolę** Pokaż uczestnikom stronę z ustawieniami prywatności konta Facebook lub innego konta w mediach społecznościowych np. TikToka. Następnie poproś uczestników o zapoznanie się z ćwiczeniem wcieleniowym i ułożenie minimum trzech dobrych praktyk dla ochrony swoich danych w sieci. Zapytaj wtedy o to, które ustawienie prywatności byłoby najlepsze do włączenia/wdrożenia? Zachęć do włączenia danego ustawienia lub wprowadzenia w życie danej zasady. Podkreśl, że nawet jeśli dane ustawienia czy zasady nie przydadzą nam się obecnie, warto wiedzieć jak postąpić w przypadku nagłej sytuacji, która może dotknąć Was, lub co ważniejsze, waszego kolegę lub koleżankę. Może być to wyciek danych, przechwycenie prywatnych zdjęć, stalking czy trolling, a może nawet zmasowany hejt, którego doświadcza np. wiele osób o rozpoznawalnych w sieci profilach. Według badań: Co piąty nastolatek przyznaje, że doświadczył przemocy w internecie. Najczęstszymi jej przejawami są: wyzywanie (29,7%), ośmieszanie (22,8%) czy poniżanie (22%). A jednocześnie, najczęstszym sposobem reakcji jest bierność: . 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 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. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html Podkreśl, że warto zatem znać podstawowe ustawienia prywatności i warto przemyśleć dodatkowe zasady bezpieczeństw. Nie chodzi tylko bowiem o zabezpieczenie swojej prywatności, ale również pomoc koledze czy koleżance, która może zgłosić się do mnie z tym problemem.	https://www.mentimeter.com/app/presentation/alfb5nt1j-3pgbqag4saicgd9edf4cdaj

Część II

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Artykuł** Wyświetl artykuł z dziennika bulwarowego i daj uczestnikom chwilę na jego przeczytanie: http://dziennikbulwarowy.pl/145/prawomocnie-uznany-za-trolla-internetowego.html?u=1:31:0:77: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 weryfikacji informacji znalezionych w sieci.	https://www.mentimeter.com/app/presentation/alda89in9m65j-kx8c3it5436wfru4wwo
	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 np. **Testu CRAAP.**	https://www.mentimeter.com/app/presentation/alcwhsmb4yyr-n2e7wdurijm59uns32j2

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	https://demagog.org.pl/analizy_i_raporty/jak-radzic-sobie-z-dezinformacja-12-zasad-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:** https://drive.google.com/drive/folders/1s9tHX6G4B3Pije-1sexghj07tE2BejRZ?usp=sharing 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?	
	Sprawdzenie i podsumowanie Raz jeszcze wyświetl artykuł z dziennika bulwarowego. Zapytaj jakie wskazówki z materiałów pomocniczych mogłyby okazać się tu pomocne? 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?	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	• Jakie źródła wskazane są w tekście (jaki sąd wydał wyrok? NSA? W Pcimiu Dolnym?)? • Jakie źródło informacji jest na końcu tekstu (Czym jest Orient? Czym jest PAPs? Czy chodzi o Onet i PAP?)? • **Czy artykuł jest sponsorowany (początek lub koniec tekstu)?** • Dowody/Potwierdzenia (czy da się znaleźć wyrok? Czy są materiały potwierdzające dane zdarzenie?)?	
	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.	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	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. 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.	
	Spis artykułów i rozwiązań: **Avengers** – Clickbait – nic nie zostaje wyjaśnione w artykule. **Banksy** – Fałszywy artykuł z generatora Newsów **Chrzest** – Artykuł satyryczny z AszDziennika **Jakubiak** – Trudna do jednoznacznej klasyfikacji „wizualizacja" marzenia – wykreowanie własnego „wywiadu z Ellen" by zostać zaproszonym do The Ellen DeGeneres Show. **Pestki** – Pseudonauka (https://dietetyczny.blog.polityka.pl/2017/08/21/gorzka-prawda-o-amigdalinie/) **Rekin** – fake news – warto zwrócić uwagę na „metodę" obliczania wieku rekina: https://www.wprost.pl/swiat/10092700/najstarszy-w-historii-rekinem-polarnym-to-fake-news.html **Reptilianie** – teoria spiskowa **Yoga** – Artykuł sponsorowany **Mierzeja** – Manipulacja z kontekstem politycznym (odpowiedź w języku rosyjskim sugeruje bycie „agentem" obcego wywiadu).	

czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	**Jeśli to prawda, będziemy mogli...** - słynny błąd, który obiegł świat: https://tvn24.pl/tvnmeteo/najnowsze/polecialy-glowy-za-neutrina-szybsze-od-swiatla-4879288 **Czy Hillary Clinton...** – Teoria spiskowa dotycząca handlu ludźmi, odbywającego się w piwnicy pewnej pizzerii, w który zamieszana była prezydent Stanów Zjednoczonych. Warto zwrócić uwagę na rażące przeinaczenia np. „sędzina" Antonina Scaliia, to mężczyzna. **Korwin** – manipulacja i teoria spiskowa. Warto zwrócić uwagę na rażące przeinaczenia np. mRNA nie oznacza „modyfikacji RNA". **Uchodźca na statku** – Manipulacja. Uchodźca stoi na tonącym kadłubie statku: https://factcheck.afp.com/drowning-refugees-hoax-resurfaces-north-america **Zełensky** – Fałszywa grafika edytowana w programie cyfrowym. Przy pomocy programu PhotoForencis można zobaczyć różnice w kompresji: https://fotoforensics.com/analysis.php?id=8af1f8680579588d-7c355a8b4b53a21669adc0e1.147248; https://fotoforensics.com/tutorial-ela.php	

PFR Fundacja

Centralny Dom Technologii

NIEBEZPIECZNIK.PL

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