Cyberbezpieczeństwo

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 realne zwiększenie bezpieczeństwa swojego konta, w przeciwieństwie do słuchania o tym, co powinno zostać wdrożone.

Czas trwania: 90 min.

Grupa wiekowa: 12 do 14

Cele:

1) **Cele ogólne:**
   a) Zwiększenie bezpieczeństwa uczestników w sieci;
   b) Wdrożenie przynajmniej jednego rozwiązania służącemu 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

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

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 CDT i o czym jest dzisiejszy warsztat (bezpieczeństwo w sieci – zagrożenia i metody ochrony). Zaproś do wypełnienia pretestu i przypomniej o liście. 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). Wytłumacz, że zanim przejdziemy do bezpieczeństwa w sieci, musimy poznać doświadczenie uczestników z Internetem.	Uwaga: W zależności od doświadczenia grupy z programowaniem, dobierz późniejsze ćwiczenia oraz sposób pracy. Uwaga 2: Na początku warsztatu, edukator/edukatorzy mogą spróbować rozwiązać część ewentualnych problemów technicznych.
15 min	**Diagnoza** Zapytaj o doświadczenie grupy z Internetem – Ile mamy aplikacji na telefonie oraz ilu mamy obserwujących w social mediach. Uczestnicy mogą wpisać orientacyjne liczby na czacie (część ilościowa). Zwróć uwagę na skalę liczb – czy są to duże liczby wskazujące na znaczną obecność w sieci, czy małe.	Uwaga: Uczestnicy, którzy nie mają wycieków ze swoich kont mogą sprawdzić konta mailowe najbliższej rodziny – np. Mamy i Taty.

	Możesz również dopytać o najczęściej używane przez młodych aplikacje (część jakościowa) – młodzi mogą wypisać ich ulubione i najczęściej używane aplikacje – zwróć uwagę na rodzaj aplikacji i używane przez nich dane. *Dzięki wielkie! Widzę sporo mediów społecznościowych ale również aplikacje do transportu np. Uber czy Lime. Widzę też wiele aplikacji sklepów.* Podkreśl, że nasza obecność w sieci będzie się najprawdopodobniej stawała coraz większa – będziemy mieć wiele kont, w różnych serwisach i korzystać z różnego rodzaju aplikacji. Nasze zasięgi też będą prawdopodobnie rosły – będziemy mieć więcej znajomych, followersów, a może nawet konta służbowe i funpage. Wszystko to nie jest niczym złym, jednak wraz ze wzrostem naszej obecności w mediach, warto zadbać również o naszą ochronę – nie chcielibyśmy bowiem pewnie dowiedzieć się, że ktoś przez noc skasował nasze konto ze 100 000 followersami, albo że ktoś napisał na naszym funpage'u obraźliwe wiadomości, za które teraz wszyscy winią nas. *Większa obecność w sieci i większa ilość aplikacji, to również większa ilość firm, które uzyskują dostęp do naszych danych. Pomyślcie o tym jakie dane znajdują się w apkach, z których korzystacie. Ja sam/a mam na telefonie około ... różnych aplikacji oraz kont w różnego rodzaju serwisach. W niektórych są moje dane kontaktowe, ale pod niektóre mam również podpięte karty kredytowe. Wraz z większą obecnością w sieci, musimy zatem wiedzieć więcej o sposobach pilnowania i ochrony naszych danych!* Wytłumacz, że porozmawiamy o tym, nie aby straszyć, lecz aby poznać metody ochrony przed tymi zagrożeniami. Podkreśl, że uczyni nas to bezpieczniejszymi w sieci – nigdy nie będziemy w 100% bezpieczni i nigdy nie ma jednego optymalnego rozwiązania, ale możemy zawsze być **bezpieczniejsi i to właśnie na tym małym kroku skupimy się na dzisiejszych warsztatach.** Wytłumacz, że pierwszym krokiem jest tu sprawdzenie czy nasze dane aby na pewno są bezpieczne i czy już w tym momencie nie są obecne gdzieś w sieci.	Uwaga: strona dehashed.com umożliwia nie tylko wyszukanie adresu e-mail, ale również sprawdzenie jakie hasła były do niego przyporządkowane. Może zatem zostać wykorzystana również w sposób niebezpieczny. Zastanów się czy powinieneś/nnaś ją pokazać w danej grupie.

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

	Pokaż uczestnikom stronę: https://haveibeenpwned.com/ oraz/lub https://www.dehashed.com/ Wytłumacz zasady działania tych stron oraz poproś o sprawdzenie swoich danych na stronie haveibeenpwned.com, daj na to uczestnikom 3 minuty. *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 informacje zwrotną czy dane uczestników wyświetlają się na czerwono, czy zielono. Zwróć uwagę na ewentualne wycieki danych i dopytaj o: - serwisy, z jakich dane wyciekły - typy danych, które wyciekły *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 teraz dowiemy się co zrobić, kiedy taki wyciek nam się przydarzy.	
15 min	**Pierwsza furtka** Wytłumacz, że w tym momencie zajmiemy się pierwszą furtką, czyli hasłem. Zwróć uwagę na dwie rzeczy: 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) - abstrakcyjne - z cyframi i znakami specjalnymi - różne do każdego serwisu - łatwe do zapamiętania 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 możemy z niego 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 kolejny ważny nawyk, który powinniśmy w sobie rozwijać.	
10 min	**Phishing** Podkreśl, że zmiana hasła będzie najważniejsza również na skrzynkach mailowych. Powinniśmy mieć również w tyle głowy, że taka skrzynka (której adres wyciekł) może stać się celem ataków phishingowych. Podkreśl, że teraz przećwiczymy ochronę przed phishingiem. 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.	
15 min	**Druga furtka** 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 nawet ważniejszym sposobem ochrony okazuje się w tej (i wielu innych sytuacjach) weryfikacja dwuetapowa. Wytłumacz, że jest to dodatkowy (oprócz hasła) sposób weryfikowania czy to aby na pewno my, logujemy się na nasze konto. Poproś uczestników o znalezienie opcji weryfikacji dwuetapowej na swoim koncie mailowym. Daj uczestnikom 5 minut na włączenie weryfikacji dwuetapowej, a przynajmniej sprawdzenie, gdzie się ona znajduje. Jeśli jest taka potrzeba omówicie wspólnie różne metody uwierzytelniania dwuetapowego: klucz U2F, potwierdzenie na telefonie itp.	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.

15 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). Poproś uczestników, aby wszyscy włączyli w tym momencie skanowanie antywirusowe/bezpieczeństwa na swoim sprzęcie (smartfonie lub komputerze). Zapytaj ilu osobom udało się to zrobić? Zapytaj co włączyli? Zapytaj ile osób nie wie, gdzie powinny włączyć skanowanie? Podkreśl, że z powodu ogromnej ilości różnych sprzętów i urządzeń, nie ma jednej metody i jednego idealnego programu. Wytłumacz, że powinniśmy: - dbać o aktualizację naszych urządzeń (w ten sposób usuwamy luki w zabezpieczeniach) - powinniśmy uważać na wyłączanie zabezpieczeń i instalowanie programów z niebezpiecznych źródeł (Jailbreak na IOS, włączanie debbugowania przez USB na telefonie, instalacja aplikacji spoza oficjalnych sklepów) - zdawać sobie sprawę, że mamy domyślne filtry i zabezpieczenia (Microsoft Defender i Zapora Windows, Skanowanie aplikacji w Google Play, system 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.	
10 min	**Podsumowanie** 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.	

	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. Zaproś do wykonania posttestu oraz przypomnij o przesłaniu listy obecności.	

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