

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

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 lub skopiuj prezentacje mentimeter na swoje konto, abyś mógł/mogła się nimi posłużyć.

ETAPY REALIZACJI

Czas	Opis ćwiczenia	Potrzebne materiały / uwagi
10 min	Wprowadzenie: Przywitaj uczestników, przedstaw się i powiedz, czym jest ścieżka Cyberbezpieczeństwa: <i>Cyberbezpieczeństwo to nie tylko warsztaty w temacie cyberbezpieczeństwa, ale spójna ścieżka edukacyjna nastawiona na jeden główny cel: świadome i bezpieczne poruszanie się w cyfrowym świecie.</i> <i>Cyberbezpieczeństwo to nie tylko zabezpieczenie swojego maila silnym hasłem i dwuetapowym uwierzytelnianiem. Aby zabezpieczyć swoje konto mailowe, musisz umieć rozpoznać Phishing. Żeby rozpoznać phishing, musisz rozumieć mechanizmy manipulacji. Żeby nie dać się fake newsom i manipulacjom medialnym, musisz wiedzieć, jak działa Twoja uwaga. A żeby być uważnym na różnego rodzaju niebezpieczeństwa, musisz wiedzieć jakie mechanizmy w sieci odciągają i osłabiają Twoją uwagę i cyfrowy dobrostan. Podczas tej ścieżki uczysz się, jak działają cyberataki, algorytmy profilujące, czy mechanizmy kreujące uzależnienie od smartfona. Bez straszenia, bez teorii dla teorii. Czekają Cię praktyczne warsztaty, kurs online, pokazy z wykorzystaniem płytki hakerskiej oraz konkurs i test wiedzy.</i> <i>To program dla tych, którzy chcą być bezpieczniejsi w sieci, a także dla tych którzy cyberbezpieczeństwem już się interesują i pasjonują.</i>	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.

	Opowiedz o czym jest dzisiejszy warsztat (bezpieczeństwo w sieci – zagrożenia i metody ochrony). <i>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.</i> 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.	
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): Cisco - Anatomy of an Attack - Inside the mind of a hacker Kraft Technology Group (https://www.youtube.com/watch?v=j0EZpH_elsY)	https://www.mentimeter.com/app/presentation/alcjghdnc4qij1ww695jghn6t3hfgkw/edit?source=share-modal Barometr Cyberbezpieczeństwa: https://kpmg.com/pl/pl/wie

	Wytłumacz, że film ten w dobry sposób ukazuje realne ataki hakerskie, które mają miejsce. Według raportu Barometr Cyberbezpieczeństwa, w 2024 roku 83% firm w Polsce odnotowało przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa. Na liście Cyberzagrożeń stanowiących największe ryzyko dla organizacji najwyższe miejsce zajmuje obecnie (według ocen samych organizacji) wyciek danych za pośrednictwem złośliwego oprogramowania. Drugie miejsce zajmuje phishing nakierowany na wyłudzenie danych uwierzytelniających. Cyber Kill Chain, czyli stworzony przez firmę Lockheed Martin model rozpoznawania i zapobiegania atakom też zaczyna się od widocznej na filmie fazy rekonesansu i wystania 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 zajęci 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 strony: https://haveibeenpwned.com/ Strony takie jak haveibeenpwned.com zbierają informację o największych wyciekach	dza/technologia/barometr-cyberbezpieczenstwa-2025.html 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
--	--	--

	<i>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.</i> Poproś o wejście na nią i sprawdzenie adresów mailowych wszystkich osób w naszej grupie. Każda grupa ma wskazać ile osób wśród nich padło ofiarą wycieku danych, oraz ile łącznie danych wyciekło. 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: <i>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 trójkę”, 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 jedno 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 zabrać rower, ale nie dostanie się do naszego mieszkania. Jeśli jednak wpadliśmy na pomysł używania jednego magicznego</i>	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. Uwaga dzięki uprzejmości Niebezpiecznik.pl
--	--	---

	<i>klucza do zapięcia, do mieszkania, do garażu i do sejfów z kosztownościami, to może i jest to wygodne, ale staje się już bardzo niebezpieczne.</i> Wytłumacz, że wycieki danych zdarzają się i zdarzać będą nawet na najlepiej zabezpieczonych serwisach. I nasze konta, 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. Docień grupy, które miały najmniej wycieków i docień 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 i da się 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.	
15 min	Profilowany Phishing* <i>Jedną z pierwszych technik, które zobaczyliście na filmie była socjotechnika, czyli</i>	*ćwiczenie nieobowiązkowe, zrób je w grupie zaawansowanej,

	<i>wywieranie wpływu na odbiorcę poprzez odwołanie się do emocji. Może być to strach (powodowany przez e-mail od szefa) lub emocje pozytywne związane np. z tym, że jesteś 1000000 klientem danej strony i wygrasz dzięki temu laptopa (oczywiście nie wygrasz). W firmach, zespół do spraw cyberbezpieczeństwa czasem “testuje” pracowników - wysyła im stworzone przez siebie maile phishingowe, by sprawdzić czy się na nie złapią. To właśnie teraz zrobimy w naszej firmie. Przetestujemy teraz różne scenariusze wiadomości wykorzystujących socjotechnikę poprzez stworzenie takiej przykładowej wiadomości, na podstawie której przetestujemy podatność kluczowych pracowników.</i> 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 miałyby 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 <i>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.</i> <i>„Zakłócenie działania systemu komputerowego” według Art. 269a. Kodeksu Karnego podlega karze pozbawienia wolności od 3 miesięcy do lat 5.</i>	zamiast kolejnego ćwiczenia ze „zwykłym” Phishingiem lub zrób oba jeśli masz dużo czasu i grupa sprawnie i szybko pracuje. https://www.mentimeter.com/app/presentation/alwuzjfmju8go65wz4bachhb3ntpu_bhk/edit?source=share-modal
--	---	--

	<i>A „uporczywe nękanie i Kradzież tożsamości” według Art. 190a. podlega karze pozbawienia wolności nawet do 8 lat.</i> Podkreśl, że po wycieku danych powinniśmy być szczególnie wrażliwi na tego typu wiadomości, a także poddać „umocnieniu” nasze skrzynki mailowe. Phishing profilowany (spear phishing), który tworzyliśmy wyżej może nas osiągnąć 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 skrzynka (której adres wyciekł) może stać się celem ataków phishingowych. Podkreśl, że teraz przećwiczymy ochronę przed “standardowym” phishingiem – tym rozsyłanym masowo i nie dopasowywanym do odbiorcy. *Jeśli nie masz czasu zrealizować kolejnego ćwiczenia, 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”)	
10 min	*Phishing <i>Kolejnym Waszym zadaniem jest sprawdzenie niedawnych wiadomości, które trafiły do waszych współpracowników w firmie z bardzo różnych adresów. Waszym celem jest wyłapanie wiadomości phishingowych i ostrzeżenie kolegów przed nimi. Za każdą poprawnie zidentyfikowaną wiadomość dostajecie jeden punkt!</i> 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	*Możesz pominąć to ćwiczenie w grupie zaawansowanej. https://www.mentimeter.com/app/presentation/al4z2kobia483ciexx6gsdtuj4y3yw9r/edit?source=share-modal Uwaga: wypada też dodać, że pozytywna ocena VirusTotal nie oznacza, że

	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.	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 umożliwić komuś dostęp do naszych plików. Komentarz dzięki uprzejmości: Niebezpiecznik.pl
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 odgadnięcie 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!	https://www.mentimeter.com/app/presentation/al66fubeedcq9rqyf1ck5u4pxnhs61mz/edit?source=share-modal https://www.mentimeter.com/app/presentation/almvoymzgbmo12q6pztp1tsk6hhyf7a6/edit?source=share-modal Uwaga: Zapoznaj się

	Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i docień 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) - mogą być z cyframi i znakami specjalnymi (przydatne, ale nie tak istotne jak długość) - różne do każdego serwisu - łatwe do zapamiętania (choć to jest dyskusyjne, zależy od metody przechowywania haseł) *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 Bitwarden czy Avira Password Menager lub programy dostępne offline, na dysku naszego komputera, np. KeePass*. 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.	z nowymi rekomendacjami CERT dotyczącymi haseł, gdyż część z nich jest odmienna od dawnych rekomendacji (np. brak okresowego wymogu zmiany haseł, brak wymogu cyfry i znaku specjalnego). https://cert.pl/posts/2022/01/kompleksowo-o-haslach/plakaty_informacyjne_hasla_a4.pdf 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
--	---	---

	cyrlicą). 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 haset i że jest to zatem nowa, inna witryna. Z menedżerów haset 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 haset tylko pod warunkiem, że mamy dobrze zabezpieczone nasze fizyczne urządzenia – np. ustawione blokady ekranu i hasła zarówno na komputerze, jak i na komórce. Nawyk wygaszania ekranu i blokowania komputera to kolejny ważny nawyk, który powinniśmy u siebie rozwijać.	zapamiętania hasła będzie natomiast dyskusyjna, bo zależna od sposobu ich przechowywania (można korzystać z menedżera haset). Zwróć przy tym uwagę na jak wiele z tych wyzwań odpowiada (dodatkowo w łatwy sposób) menedżer haset, 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
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). Wy tłumacz, 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), kodów SMS, kodów lub potwierdzeń w dedykowanej aplikacji authenticator, potwierdzeń mailowych lub formę klucza U2F, czyli urządzenia przypominającego pendrive z dodatkowym modulem NFC do łączności bezprzewodowej. Taki klucz nawiązuje łączność z daną stroną internetową i potwierdza naszą tożsamość. <i>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...</i> Podkreśl, że teraz zadaniem uczestników jest znalezienie najlepszego sposobu dodatkowej weryfikacji w każdym z przedstawionych za chwilę w prezentacji case'ów.	https://www.mentimeter.com/app/presentation/al73yr4n88um18qyqhwx9an7z551we8/edit?source=share-modal 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.

	Przejdź z grupą przez prezentację z zadaniami. Pogratuluj grupom starań i pomysłów i docień grupę z najlepszym wynikiem. Podkreśl, że w ostatnim pytaniu prawie wszystkie odpowiedzi są poprawne, gdyż najlepsza dodatkowa weryfikacja, to taka, którą rzeczywiście stosujecie. Może być to klucz U2F (najczęściej rekomendowany przez ekspertów jako jedyny sposób dodatkowego uwierzytelniania chroniący w pełni przed phishingiem) lub aplikacja Authenticator (Google lub Microsoft, też stosunkowo dobry, wygodny i bezpłatny sposób, lecz możliwy do przechwycenia np. przez phishing) 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/ <u>*Uwaga: możesz zwrócić uwagę na to, że jeśli korzystamy z narzędzi i przeglądarek dużych firm (np. google lub Microsoft), to może się okazać że nasz najważniejszy mail, menedżer haseł, a także aplikacja do uwierzytelniania znajdują się wszystkie na jednym koncie (pod jednym adresem mailowym). Skorzystanie z zewnętrznych programów lub wykorzystanie dwóch kont może nie być zatem złym pomysłem.</u>
10 min	Pomocne programy Podkreśl, że obok cyberprzestępców, w sieci obecne są również wirusy – programy komputerowe wykorzystujące luki w zabezpieczeniach i wykonujące różnego rodzaju	https://www.mentimeter.com/app/presentation/alme7yqpmuafzg8u4yimb3o6826jyq73/edit?source=share-

	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 ilości różnych sprzętów i urządzeń, nie ma jednej metody i jednego idealnego programu. Ważnymi skanowaniami, które zaliczymy grupom do wykonania zadania będą: Na komputerach (windows): - Skanowanie Windows Defender - Skanowanie zewnętrznym programem antywirusowym - Skanowanie Windows update (w poszukiwaniu aktualizacji) 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/sandbox. Z drugiej strony, renomowane	modal Zapoznaj się z: https://niebezpiecznik.pl/post/sprawdz-czy-twoj-smartfon-jest-zhackowany/ https://zaufanatrzeciastona.pl/post/podstawy-bezpieczenstwa-czy-wspolczesne-smartfony-potrzebuj-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
--	---	--

	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 staran i pomysłów i docień 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 debugowania 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, o których już mówiliśmy, 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.	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. 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
--	--	---

	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. Jakims rodzajem komunikatora lub sms-em). Otwierając taki plik, powinniśmy mieć z kolei pewność, że pochodzi z zaufanego źródła. Zasadę ograniczonego zaufania powinniśmy stosować do większości 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.	ostrożnym otwieraniu) plik ZIP ukrytych za hasłem czy też włączaniu makr/zawartości w dokumentach Worda. Komentarz dzięki uprzejmości Niebezpiecznik.pl
10 min	Podsumowanie Docień i nagródź najlepszych uczestników i drużyny w całej symulacji. <i>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!</i> Poproś uczestników o zastanowienie się nad wszystkimi sposobami ochrony, o jakich dzisiaj styszeli. 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 przyzwyczajania się do niej – zmienienia swoich nawyków. Podkreśl, że najlepsza metoda ochrony, to taka, którą rzeczywiście stosują. <i>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.</i> Podkreśl, że wszyscy uczestnicy warsztatów mogą również: 1. Przejść przez kurs na platformie Strefa wiedzy, gdzie omawiamy wiele bardziej zaawansowanych tematów. 2. Wziąć udział w ogólnopolskim teście wiedzy i konkursie. Zdobywcy najlepszych wyników zostaną nagrodzeni, więc na pewno warto uważać na kolejnych warsztatach, rozwijać swoją znajomość zagadnień cyberbezpieczeństwa oraz wziąć udział w ogólnopolskim teście wiedzy.	
--	--	--