

stworzono i opracowano przez:



HACKI

Urządzenie do edukacji cyberbezpieczeństwa
instrukcja obsługi i scenariusze lekcji

NOTKA OD TWÓRCÓW



Cyber Safers

No cześć!

Jako autorzy zestawu który właśnie masz przed sobą chcielibyśmy serdecznie podziękować za przyczynianie się do rozwoju edukacji cyberbezpieczeństwa w Polsce. Włożyliśmy na prawdę dużo pracy i serca w stworzenie tego projektu, bo wierzymy, że najlepsza nauka to ta, którą można zobaczyć i przećwiczyć w praktyce.

Zatem życzymy miłej zabawy podczas eksplorowania cudownego świata cyberbezpieczeństwa i mamy nadzieję, że jeszcze się kiedyś zobaczymy :D

Zespół Cyber Safers

Ten zestaw nie powstałby bez



 PFR Fundacja



Centralny Dom
Technologii



Partner rzeczowy

Sponsor

organizator

Sponsor

HACKI

OSOBISTY PRZEWODNIK

W tej instrukcji znajdziesz wszystko dzięki czemu przeprowadzisz angażujące zajęcia z cyberbezpieczeństwa

SPIS TREŚCI

Podstawowe zasady bezpieczeństwa -----	strona 01
Na szybki start -----	strona 02
Jak korzystać? 01 -----	strona 03
Jak korzystać? 02 -----	strona 04
Jak nie przynudzać czyli wskazówki merytoryczne -	strona 05
Scenariusz lekcji 01 -----	strona 06
Scenariusz lekcji 02 -----	strona 07
Scenariusz lekcji 03 -----	strona 08



DLACZEGO ZESTAW JEST DARMOWY?

Bo za darmo to ucziwa cena! A tak na serio - wierzymy, że każdy ma prawo czuć się bezpiecznie w sieci, więc dzielimy się tym zestawem, żeby jak najwięcej osób mogło z tej wiedzy skorzystać.

Podstawowe zasady bezpieczeństwa



Bezpieczeństwo priorytetem

Najważniejsze jest dla nas Twoje bezpieczeństwo i nauka obrony przed atakami – dlatego przestrzegaj poniższych zasad.

Bezpieczne wskazówki



- ✓ Z urządzenia korzystaj **jedynie podczas zajęć** i używaj zgodnie z jego przeznaczeniem
- ✓ Dane wpisywane podczas ćwiczeń **podawaj jedynie fikcyjne** lub przykładowe
- ✓ Nigdy **nie testuj** poznanych mechanizmów poza zajęciami
- ✓ Zawsze **kończ działanie** modułu wyjściem z niego, zanim przejdziesz do kolejnego ćwiczenia

Na szybki start

Co zawiera zestaw?



Hacki - autorskie urządzenie edukacyjne



Rysik do ekranu



Kabel do ładowania



Nagrody dla aktywnych uczniów



Karta micro SD (na stałe w urządzeniu)



Jak zacząć korzystać?

1

Upewnij się, że urządzenie jest naładowane - jeżeli nie - podłącz je do zasilania

2

Włącz urządzenie za pomocą bocznego przycisku i poczekaj na pokazanie się loga

3

Z menu głównego wybierz pożądaną do wykonania przez siebie czynność

4

Po zakończeniu wykonywanej czynności wróć do menu głównego



Jeśli coś nie działa, zrób szybki reset - wyłącz urządzenie, odczekaj 5 sekund i włącz ponownie.

Jak korzystać? 01

BLE - Bluetooth spam



- **Na czym polega?** – tworzy mnóstwo fałszywych urządzeń Bluetooth w okolicy, przez co lista parowania robi się chaotyczna i myląca
- **Jak używać?** – działa od razu po naciśnięciu

Evil portal - fałszywe wifi



- **Na czym polega?** – tworzy sieć Wi-Fi z podstawioną stroną, która wygląda wiarygodnie i próbuje skłonić do kliknięcia lub wpisania danych
- **Jak używać?** – w ustawieniach wybierz plik HTML a następnie uruchom portal z menu głównego. Nazwa sieci to "cybersafers"

Deautoryzacja



- **Na czym polega?** – rozłącza urządzenia z wybranej sieci Wi-Fi, przez co internet nagle przestaje działać
- **Jak używać?** – uruchom skan wifi, w ustawieniach "SSID check" wybierz nazwę sieci, wróć do menu i uruchom atak

Jak korzystać? 02



Wifi spam

- **Na czym polega?** – tworzy tysiące losowych sieci na sekundę utrudniając tym samym ruch sieciowy oraz wybór sieci wifi
- **Jak używać?** – działa od razu po naciśnięciu



Skan wifi

- **Na czym polega?** – jest to narzędzie diagnostyczne do znalezienia i zapisania SSID pobliskich sieci wifi
- **Jak używać?** – działa od razu po naciśnięciu, łączy się z deautoryzacją i evil portalem



Ustawienia

SSID check



- **Jak używać?** – należy uprzednio skorzystać ze skanu wifi a następnie wybrać nazwę sieci do deautoryzacji i wrócić do menu głównego

HTML check



- **Jak używać?** – należy wybrać plik o nazwie "cybersafersep.html" następnie wrócić do menu głównego i uruchomić evil portal

Jak nie przynudzać czyli wskazówki merytoryczne



Storytelling jest ważny

Storytelling jest ważny, bo uczniowie nie zapamiętują narzędzi ani nazw ataków, tylko zapamiętują sytuacje i emocje typu pośpiech czy chaos oraz ten jeden moment, w którym prawie coś kliknęli. Jak zrobisz z lekcji historię, to załapią sens od razu, bo widzą człowieka w problemie, a nie abstrakcyjne działanie na ekranie. **Przykłady implementacji:**

- Zaczynaj od **scenki z życia** np. "jedziesz pociągami i nie masz zasięgu", żeby każdy rozumiał w jakiej sytuacji się znajdujemy
- Po pokazie zawsze domykaj historię **jednym wnioskiem** w formie reakcji, którą da się zastosować w prawdziwym życiu



Na początku lekcji upewnij się, że uczniowie **mają swoje telefony** pod ręką, aby mogli doświadczyć omawianych treści



Pytania które warto zadać

- Czy kiedykolwiek **łączyliście się** z darmowym wifi?
- Kto z was **zostawia Bluetooth włączony** nawet wtedy, gdy nie używa słuchawek?
- Kto z was ma **włączone auto-łącznie** z Wi-Fi?



Wskazówki

- Podczas pokazywania ataków najpierw pokaż efekt na **swoim telefonie** a następnie nakieruj uczniów jak to dostrzec na swoich
- Jeśli coś ma być kliknięte, powiedz to na głos i **poczekaj aż wszyscy nadgonią**

Scenariusz lekcji 01

Temat: Jak spam robi bałagan?

Cel lekcji

poziom trudności



Celem lekcji jest pokazanie, że czasem atak nie polega na przejęciu hasła, tylko na zrobieniu takiego bałaganu wokół ciebie, żebyś sam podjął złą decyzję, bo chcesz mieć spokój i szybko „coś wybrać”. Po tej lekcji uczniowie mają umieć rozpoznać sytuację, w której lista sieci lub urządzeń jest podejrzaną „zalaną”, i wiedzieć jak się zachować, żeby nie dać się wkręcić.

Treść lekcji

Wifi spam



Bluetooth spam



Na start dwie krótkie scenki:

- Chcesz podłączyć się do szkolnego Wi-Fi, bo masz coś do zrobienia na lekcji, ale gdy otwierasz listę sieci nagle pojawia się masa nazw i nie możesz znaleźć tej właściwej
- Jedziesz metrem i musisz pilnie do kogoś zadzwonić, ale telefon zaczyna świrować, bo dostaje mnóstwo losowych propozycji połączeń Bluetooth i wszystko staje się ciężkie do ogarnięcia, jakby urządzenie było „zasypane” powiadomieniami i listami.

To realne przykłady z życia kiedy nieśmieszne zabawy hakerów utrudniają innym życie

Ćwiczenia – czyli czas na pokaz!

Na start szybka teoria:

- Bluetooth spam – wystarczy kliknąć ikonkę z menu głównego
- Wifi spam – wystarczy kliknąć ikonkę z menu głównego

Teraz możesz zacząć razem z uczniami pokaz na żywo. Zacznij od uruchamiania na urządzeniu edukacyjnym spamu Wi-Fi i pokazania efektów na swoim telefonie, jak lista sieci nagle zamienia się w śmietnik i jak łatwo zgubić tę właściwą, a dopiero potem prosisz uczniów, żeby zobaczyli to samo u siebie.

Następnie przechodzisz do spamu Bluetooth i pokazujesz, jak wygląda zalew nazw i urządzeń lub wyskakujących propozycji w pobliżu, po czym znowu kierujesz uczniów, żeby zauważyli to na swoich telefonach i opisali, co w tym jest podejrzanego.

Podsumowanie czyli jak się bronić?

Zapytaj uczniów, co w tych dwóch sytuacjach było najbardziej wkurzające i co ich zdaniem popchnęłoby człowieka do kliknięcia byle czego. Na tablicy krótkie hasła z ich odpowiedzi, typu pośpiech, chaos, frustracja czy klikanie na oślep. Niech każdy uczeń zaproponuje dobre nawyki które już dzisiaj mógłby wprowadzić już dzisiaj do swojej higieny cyfrowej aby w przyszłości nie stawać się łatwym celem dla hakerowych śmieszek. Dobrym przykładem jest między innymi regularne wyłączenie bluetootha kiedy nie ma się potrzeby z jego korzystania tak samo jak automatycznego łączenia się z dostępnymi sieciami wifi.

Scenariusz lekcji 02

Temat: Lotniskowe Wi-Fi: eter potrafi kłamać

Cele lekcji

poziom trudności



Celem lekcji jest ukazanie, że w publicznym Wi-Fi najgroźniejszy jest moment, w którym użytkownik działa z pośpiechu i na autopilocie. Po tej lekcji uczniowie mają umieć rozpoznać, kiedy sieć lub strona "prosi o coś dziwnego" i wiedzieć, co zrobić zamiast bezmyślnego klikania

Treść lekcji

Evil portal



Na start krótka scenka:

„Jesteś na lotnisku i czekasz na swój lot powrotny z wakacji, znudzony chcesz obejrzeć film na swoim telefonie jednak jesteś za granicą i nie masz własnego internetu. Na szczęście okazuje się, że w dostępnych sieciach wifi znajduje się jedna o nazwie `airport_free_wifi`”

Zapytaj się uczniów czy w takiej sytuacji skorzystaliby z darmowego wifi lotniska. W codziennym życiu większa część z nas postanowiłaby skorzystać z darmowej sieci jednak czy aby na pewno jest to bezpieczne? Poniższa lista ćwiczeń uświadomi każdego odbiorcę jak niebezpieczne może być łączenie się do publicznych sieci wifi.

Ćwiczenia - czyli czas na pokaz!

Na sam początek:

- Wejść w ustawienia a następnie w ikonkę "HTML Check", wybierz plik z karty microSD o nazwie "cybersafersep.html" i wróć do menu głównego.
- Następnie uruchom Evil Portal i pozostaw go włączonego.

Pokaż uczniom na swoim telefonie, jak wygląda moment „podłączenia” i stronę, która wyskakuje po wejściu do sieci, jeżeli strona nie otworzy się samoczynnie należy wejść w sieci wifi i kliknąć w wymaganą przez sieć autoryzację. Dopiero wtedy poproś uczniów, żeby znaleźli to samo u siebie i zobaczyli efekt na własne oczy. Na stronie będzie widoczne okno logowania, to ten moment w którym oszuści są w stanie zdobyć nasze dane bowiem wszystko tam wpisane w prawdziwym życiu zostaje przechwytywane i wykorzystywane przez hakerów. Na potrzeby lekcji uczniowie mogą wpisać przykładowe dane jednak ze względów bezpieczeństwa nie zostaną one nigdzie przechytane ani zapisane.

Podsumowanie czyli jak się bronić?

Przechodźmy do wniosków - zapytaj uczniów, czy potrafiliby w tej sytuacji rozróżnić prawdziwą sieć od fałszywej. Następnie omówcie proste metody obrony, czyli żeby nie logować się przez przypadkowe strony po połączeniu z Wi-Fi, nie łączyć się tylko dlatego, że nazwa brzmi oficjalnie, wyłączyć auto-łączenie, nigdy nie wpisywać swoich realnych danych i w razie wątpliwości przejść na dane komórkowe jeżeli ma się taką możliwość. Zapamiętaj, że w prawdziwym życiu ta strona wyglądałaby wiarygodnie właśnie po to, żebyś kliknął szybko i bez zastanowienia. Na koniec niech każdy uczeń wybierze jedną rzecz, którą zmieni od dziś w telefonie, żeby nie wpaść w tę samą pułapkę.

Scenariusz lekcji 03

Temat: Gdy sieć wariuje – rozłączanie jako przynęta

Cele lekcji

poziom trudności



Celem lekcji jest pokazanie, że rozłączanie z siecią może być celowym działaniem, a nie tylko słabym zasięgiem, i że najgorszą reakcją jest klikanie w panice w pierwszą lepszą sieć lub potwierdzanie wszystkiego, żeby „zadziałało”. Po tej lekcji uczniowie mają umieć rozpoznać objawy takiej sytuacji, wiedzieć co zrobić od razu i jak nie dać się popchnąć do złej decyzji.

Treść lekcji

Deautoryzacja



Skan wifi



Na start krótka scenka:

„Jesteś w szkole lub w miejscu publicznym, internet nagle przestaje działać, strona się nie ładowa, a ty masz coś pilnego do zrobienia.”

Zapytaj uczniów co robią jako pierwsze w takiej sytuacji i co zwykle wybierają: czekanie, zmiana sieci, ponowne łączenie a może dane komórkowe? Zanotuj 2–3 najczęstsze odruchy i zaznacz jasno, że to właśnie klikanie w pośpiechu jest najczęstszą przyczyną problemów.

Ćwiczenia – czyli czas na pokaz!

Na początek parę formalności, musisz po kolei:

- włączyć skanowanie sieci i wrócić do menu głównego
- wejść do ustawień, przejść do SSID checku i wybrać nazwę waszej sieci
- wrócić do menu głównego i dopiero wtedy włączyć deautoryzację

Do tego ćwiczenia należy przygotować własną sieć Wi-Fi na dowolnym routerze szkolnym i ustawić ją na 2,4 GHz, żeby właśnie tę sieć wykorzystać w pokazie deautoryzacji. To opcja dla bardziej zaawansowanych i ciekawskich prowadzących, którzy chcą zrobić to konkretnie i mieć pełną kontrolę nad tym, co dzieje się na zajęciach.

Teraz zacznij pokaz na żywo: najpierw wszyscy łączą się z Wi-Fi, które podajesz na głos, a ty na swoim telefonie pokazujesz, że połączenie jest stabilne i działa. Następnie wykonujesz wcześniej wymienione kroki na sieci używanej na zajęciach i pokazujesz efekt na swoim telefonie, czyli nagłe rozłączenie, ponowne próby łączenia i to, że użytkownik zaczyna „ratować sytuację” na autopilocie. Dopiero po pokazaniu efektu kierujesz uczniów, żeby sprawdzili to samo u siebie i zauważyli, jak wygląda moment rozłączenia oraz co się dzieje w ustawieniach Wi-Fi.

Podsumowanie czyli jak się bronić?

Czas na wyciągnięcie wniosków – zapytaj uczniów co w tej sytuacji mogło być znakiem ostrzegawczym. Następnie omówcie pomysły na reakcje w takich sytuacjach, najlepszą z nich jest przede wszystkim nie klikanie po kolei w inne sieci oraz nie „naprawianie” problemu przypadkowymi połączeniami. Na koniec zwróćcie uwagę na to, że najniebezpieczniejszy jest moment decyzji i o to, że rozłączenie ma cię popchnąć do szybkiego, głupiego ruchu, który często oszusi łączą z innymi atakami takimi jak evil portale. Niech każdy uczeń wybierze jeden dobry nawyk, który będą od tej pory wykonywali.



Cyber Safers

projekt realizowany w ramach

zwolnieni ^z
teorii

Pełna, techniczna wersja instrukcji znajduje się na stronie cybersafers.pl oraz została wysłana na adres e-mail, którym szkoła zgłaszała się do konkursu.



Wpadnij na nasze media!



cybersafers.pl



[@cybersafers](https://www.tiktok.com/@cybersafers)



[@cybersafers](https://www.instagram.com/cybersafers)



[Cyber Safers](https://www.facebook.com/CyberSafers)



[@cybersafers](https://www.youtube.com/@cybersafers)

Ten zestaw nie powstałby bez



PFR Fundacja



Centralny Dom
Technologii



Partner rzeczowy

Sponsor

organizator

Sponsor