

# Cyberbezpieczeństwo

## Podstawy bezpiecznego poruszania się po sieci oraz rozpoznawania i unikania niebezpieczeństw

---

### Cele szkolenia

Celem szkolenia jest przekazanie uczestnikom wiedzy na temat podstaw bezpiecznego korzystania z internetu zarówno w pracy jak i prywatnie. Uczestnik w trakcie szkolenia nauczy się w jaki sposób rozpoznawać podstawowe ataki, próby wyłudzenia, jak poprawić swoje bezpieczeństwo oraz jakie narzędzia wspomagające ten cel można stosować. Ponadto

Podczas szkolenia, uczestnik dowie się:

- Dlaczego bezpieczeństwo informacji i systemów jest istotne?
- Jakie mogą być konsekwencje ataków?
- Jakie są typy ataków i jak na nie reagować?
- Jakie są metody rozpoznawania i obrony przed atakami?
- Jak chronić swoje hasła i dane poufne?
- Gdzie szukać informacji o lukach bezpieczeństwa?
- Jak dobezpieczać swoje komputery i urządzenia mobilne?

Dzięki omówieniu powyższych zagadnień w oparciu o realne przypadki ataków i wyłudzeń z ostatnich miesięcy uczestnik poszerzy swoją wiedzę z zakresu cyberbezpieczeństwa o metody rozpoznawania, analizy i reagowania na zagrożenia, jakie mogą spotkać każdego w realiach poruszania się po współczesnym wirtualnym świecie. Zbuduje także solidne podstawy pod dalszy rozwój w obszarze cybersecurity.

### Umiejętności

Dzięki umiejętnościom zdobytym na kursie uczestnik będzie:

- Identyfikował zagrożenia cyberbezpieczeństwa
- Rozpoznawał ataki, których będzie celem, np. phishing
- Prawidłowo reagował w przypadku ataków, wycieków danych
- Zwiększał poziom bezpieczeństwa swoich urządzeń bądź systemów, z których korzysta na co dzień w pracy i prywatnie
- Wiedział, gdzie i jak szukać informacji na temat bezpieczeństwa

- W bezpieczny sposób przechowywał swoje poufne dane oraz hasła
- Znał zalety i metody korzystania z uwierzytelniania wieloskładnikowego (MFA) i kluczy fizycznych.

## Profil uczestników

Szkolenie skierowane jest do każdego użytkownika urządzeń mobilnych i komputerów podłączonych do internetu we współczesnym świecie. W szczególności dla osób pracujących na stanowiskach, które wymagają operacji na danych poufnych.

Kurs jest skierowany m.in. do:

- początkujących pracowników IT
- przedsiębiorców chcących poznać ryzyka braku inwestycji w cyberbezpieczeństwo
- właścicieli i administratorów stron internetowych, sklepów internetowych
- analityków biznesowych, kierowników projektów
- osób prywatnych chcących poszerzyć swoją wiedzę z zakresu cyberbezpieczeństwa

Szkolenie jest skierowane do osób zarówno początkujących jak i posiadających podstawową wiedzę z zakresu cyberbezpieczeństwa, którą dzięki szkoleniu będą mogli poszerzyć i uporządkować.

## Przygotowanie uczestników

Szkolenie nie wymaga od uczestników specjalistycznego przygotowania ani posiadania technicznej wiedzy.

## Szczegółowy program szkolenia

1. Wprowadzenie do cyberbezpieczeństwa
  - 1.1 Czym jest i jakie znaczenie ma cyberbezpieczeństwo
  - 1.2 Higiena pracy z komputerem
  - 1.3 Konsekwencje braku zachowania podstawowych zabezpieczeń
2. Bezpieczeństwo haseł i kont użytkownika
  - 2.1 Słabe mechanizmy uwierzytelniania w oparciu o hasła
  - 2.2 Jak i gdzie przechowywać hasła
  - 2.3 Jak sprawdzić czy nasze hasło jest bezpieczne
  - 2.4 MFA i 2FA - czym jest i czy go potrzebujesz?
  - 2.5 Przyszłość - passwordless
3. Bezpieczeństwo danych
  - 3.1 Szyfrowanie dysków
  - 3.2 Jak bezpiecznie przesyłać/udostępniać dane poufne
  - 3.3 Jak chronić się przed wyciekami
4. Phishing
  - 4.1 Jak rozpoznać - przykłady z życia
  - 4.2 Jak się chronić i reagować
5. Malware i ransomware

- 5.1 Jak rozpoznać - przykłady z życia
- 5.2 Jak reagować - czy płacić okup?
- 5.3 Jak zapobiegać - dlaczego backup jest taki ważny?
- 5.4 Przykłady z życia
6. Inne zagrożenia
  - 6.1 Socjotechnika – ataki personalizowane
  - 6.2 Insider
  - 6.3 MITM
  - 6.4 Koparki kryptowalut
7. Bezpieczeństwo urządzeń mobilnych
8. Ochrona przed zagrożeniami
  - 8.1 Antywirus
  - 8.2 Aktualizacje
  - 8.3 VPN
  - 8.4 Backup (Two is one, one is none)
9. Podsumowanie

## Metoda realizacji szkolenia

Forma szkolenia ma na celu przedstawienie w sposób atrakcyjny i interesujący wiedzy i technik związanych ze zwiększeniem poziomu cyberbezpieczeństwa w życiu prywatnym i zawodowym.

Szkolenie będzie realizowane w formie:

- części teoretycznej w postaci prezentacji omawianych zagadnień
- części praktycznej realizowanej naprzemiennie z częścią teoretyczną w postaci:
  - praktycznych i intuicyjnych ćwiczeń polegających m.in. na rozpoznaniu phishingu i tworzeniu „mocnych haseł”
  - burzy mózgów – np. znalezieniu najlepszego sposobu zabezpieczenia swoich danych
  - dyskusji z uczestnikami
  - analizy przypadków (case studies) z życia prywatnego i zawodowego uczestników
  - quizów i ankiet.

## Liczba dni, liczba godzin szkoleniowych

1 dzień, 8 godzin szkoleniowych

## Ścieżka rozwoju po szkoleniu

Po zakończeniu szkolenia rekomendujemy szkolenie [Mechanizmy obrony przed atakami hakerskimi](#).

Data aktualizacji programu: 07.2024