kod szkolenia: BEZ_ INT / PL DL 1d

Bądź bezpieczny w sieci - cyberbezpieczeństwo w praktyce

Szkolenie wprowadza uczestników w świat cyberzagrożeń, przedstawiając realne metody działania cyberprzestępców oraz sposoby skutecznej ochrony danych i urządzeń. Uczestnicy uczą się rozpoznawać ryzykowne sytuacje, wzmacniać swoją odporność na ataki oraz stosować praktyczne zasady bezpiecznego korzystania z Internetu – zarówno w pracy, jak i w życiu prywatnym. Program łączy teorię z praktycznymi ćwiczeniami, symulacjami i wskazówkami możliwymi do wdrożenia od razu.

Odbiorcy szkolenia

Szkolenie jest skierowane do:

- osób chcących zwiększyć swoje bezpieczeństwo w sieci,
- użytkowników domowych, którzy na co dzień korzystają z Internetu i przechowują dane online,
- pracowników firm, instytucji i organizacji obsługujących dane poufne lub wrażliwe,
- osób regularnie korzystających z usług cyfrowych i komunikacji online,
- wszystkich, którzy chcą świadomie chronić siebie, swoje dane oraz urządzenia przed cyberzagrożeniami.

Korzyści

1. Cyberzagrożenia – poznasz najczęstsze metody ataku, ich skutki oraz sposoby rozpoznawania niebezpiecznych sytuacji w sieci.
2. Bezpieczny Internet – dowiesz się, jak tworzyć silne hasła, unikać podejrzanych linków i korzystać bezpiecznie z publicznych oraz domowych sieci Wi-Fi.
3. Ochrona danych – odkryjesz, jak bezpiecznie przechowywać i udostępniać dane osobowe oraz jak

zabezpieczać swoje urządzenia.
4. Skuteczne narzędzia – poznasz praktyczne zastosowania programów antywirusowych i innych rozwiązań ochronnych, które minimalizują ryzyko ataków.
5. Reakcja na incydenty – dowiesz się, jak rozpoznać oznaki cyberataku i jakie działania podjąć, aby szybko i skutecznie zareagować.

Program szkolenia

1. Moduł
   - Zrozumienie podstawowych zasad bezpieczeństwa- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
   - Zagrożenia w sieci i ich wpływ na codziennie życie prywatne i zawodowe
2. Moduł
   - Podstawowe terminy i koncepcje (np. malware, phishing, ransomware) Znaczenie higieny cyfrowej w kontekście biznesowym
   - Hasła i zarządzanie nimi,
   - Przygotowanie planu reagowania na incydenty
3. Moduł
   - Ochrona przed złośliwym oprogramowaniem, Bezpieczne korzystanie z Internetu i e-maila,
   - Ochrona przed phishingiem i innymi formami socjotechniki
4. Moduł
   - Podstawy bezpiecznej pracy zdalnej
   - Szyfrowanie danych i komunikacji
   - Bezpieczeństwo sieci firmowych i domowych
5. Moduł
   - Wprowadzenie do bezpieczeństwa urządzeń mobilnych
   - Przykładowe procedury możliwe do wdrożenia w firmie lub w domu
   - Analiza przykładowych sytuacji zagrożeń cybernetycznych i sposoby reagowania.

Oczekiwane przygotowanie uczestnika

Brak specjalistycznych wymagań wstępnych.

Czas trwania

> 1 dni / 7 godzin

Język

język polski