kod szkolenia: BEZ_ INT / PL AA 2d

Bądź bezpieczny w sieci - cyberbezpieczeństwo w praktyce

Celem szkolenia jest zwiększenie świadomości uczestników na temat zagrożeń cybernetycznych oraz wyposażenie ich w praktyczne umiejętności chroniące przed cyberatakami. Chcemy nauczyć uczestników rozpoznawania i unikania zagrożeń w sieci, zapewnić im wiedzę na temat bezpieczeństwa danych i zasad bezpiecznego korzystania z Internetu. Szkolenie ma na celu zwiększenie bezpieczeństwa cyfrowego uczestników i wzmocnienie ich odporności na ataki cybernetyczne.

Odbiorcy szkolenia

Szkolenie jest skierowane do wszystkich osób, które chcą zwiększyć swoje bezpieczeństwo w sieci, zarówno do użytkowników domowych, jak i pracowników firm, instytucji i organizacji. Szkolenie będzie szczególnie przydatne dla osób, które regularnie korzystają z Internetu, przechowują dane wrażliwe w sieci, lub pracują z informacjami poufnymi.

Korzyści

Ukończenie szkolenia pozwoli uczestnikom na:

• Zrozumienie zagrożeń cybernetycznych, rozpoznanie najczęstszych metod ataku i ich skutków.

• Zastosowanie zasad bezpiecznego korzystania z Internetu, w tym wybór silnych haseł, unikanie podejrzanych linków i bezpieczne korzystanie z sieci Wi-Fi.

• Ochronę swoich danych osobowych, w tym nauczenie się bezpiecznego przechowywania i udostępniania danych w sieci.

• Stosowanie programów antywirusowych i innych narzędzi zabezpieczających, aby chronić swoje

urządzenia przed atakami.
• Reagowanie na próby ataku, w tym rozpoznanie oznak ataku i właściwe postępowanie w takich sytuacjach.
Po ukończeniu szkolenia uczestnicy będą potrafili świadomie chronić się przed zagrożeniami cybernetycznymi, bezpiecznie korzystać z Internetu i chronić swoje dane osobowe.

Program szkolenia

Moduł I
Zrozumienie podstawowych zasad bezpieczeństwa- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
Zagrożenia w sieci i ich wpływ na codziennie życie prywatne i zawodowe
Moduł II
Podstawowe terminy i koncepcje (np. malware, phishing, ransomware) Znaczenie higieny cyfrowej w kontekście biznesowym
Hasła i zarządzanie nimi,
Przygotowanie planu reagowania na incydenty
Moduł III
Zaawansowana ochrona przed złośliwym oprogramowaniem, Bezpieczne korzystanie z Internetu i e-maila,
Ochrona przed phishingiem i innymi formami socjotechniki
Moduł IV
Podstawy bezpiecznej pracy zdalnej
Zaawansowana ochrona przed złośliwym oprogramowaniem Szyfrowanie danych i komunikacji
Bezpieczeństwo sieci firmowych i domowych
Moduł V
Wprowadzenie do bezpieczeństwa urządzeń mobilnych
Tworzenie i wdrażanie polityki bezpieczeństwa w firmie i warunkach domowych Symulacje ataków cybernetycznych i reakcje

Oczekiwane przygotowanie uczestnika

Brak specjalistycznych wymagań wstępnych.

Czas trwania

2 dni / 14 godzin

Język

język polski