

Cyberbezpieczeństwo w praktyce: jak chronić siebie i organizację

Szkolenie „Cyberbezpieczeństwo w praktyce: jak chronić siebie i organizację” to interaktywny kurs online, dzięki któremu nauczysz się, jak chronić swoje dane, unikać zagrożeń i reagować na cyberataki – niezależnie od Twojego poziomu wiedzy technicznej.

Kurs możesz realizować we własnym tempie i o dowolnej porze w wygodnej formule self-learning. To praktyczne narzędzie, które pomoże Ci zbudować osobiste nawyki cyfrowego bezpieczeństwa!

Szkolenie składa się z 5 modułów tematycznych. Każdy moduł zawiera quizy sprawdzające wiedzę, a cały kurs wykorzystuje różnorodne techniki multimedialne, interaktywne ćwiczenia i praktyczne przykłady, aby zapewnić Ci efektywność nauki i maksymalne zaangażowanie.



Odbiorcy szkolenia

Grupa docelowa

Szkolenie jest stworzone z myślą o wszystkich pracownikach organizacji, niezależnie od działu czy doświadczenia technicznego. Skorzystają z niego osoby:

- korzystające na co dzień z komputerów i smartfonów,
- mające dostęp do danych firmowych lub klientów,
- zainteresowane wzmacnianiem cyfrowych kompetencji i ochroną prywatności online.

To szkolenie to nie tylko obowiązek – to realna wartość i inwestycja w bezpieczeństwo Twoje i Twojej firmy.



Korzyści

Korzyści dla uczestników

1. Rozpoznawanie zagrożeń online – nauczysz się identyfikować i unikać ataków phishingowych, złośliwego oprogramowania i manipulacji socjotechnicznych.
2. Zarządzanie hasłami – dowiesz się, jak tworzyć silne, unikalne hasła i bezpiecznie nimi zarządzać.
3. Zrozumienie działań cyberprzestępców – poznasz techniki hakerskie oraz nauczysz się skutecznie reagować na próby ataków.
4. Tworzenie kopii zapasowych – opanujesz zasady tworzenia backupów i zrozumiesz ich kluczową rolę w ochronie danych.
5. Świadomość zagrożeń AI – dowiesz się, jak rozpoznawać deep fake'i i inne formy cyfrowej dezinformacji związanej z rozwojem sztucznej inteligencji.

Korzyści dla organizacji

- Redukcja ryzyka incydentów cybernetycznych – zminimalizujesz szansę na skuteczne ataki hakerskie, oszustwa i wycieki danych.
- Budowanie kultury bezpieczeństwa – wzmocnisz świadomość zagrożeń wśród pracowników i zwiększysz ich zaangażowanie w ochronę firmowych zasobów.
- Ochrona reputacji i danych firmy – zabezpieczysz wrażliwe informacje przed nieautoryzowanym dostępem i zapobiegiesz kosztownym kryzysom wizerunkowym.
- Zmniejszenie błędów ludzkich – ograniczysz liczbę incydentów spowodowanych brakiem wiedzy lub nieuwagą pracowników.
- Odporność na nowe zagrożenia cyfrowe – zapewnisz organizacji gotowość na dynamicznie rozwijające się zagrożenia, w tym te związane ze sztuczną inteligencją i dezinformacją.



Program szkolenia

Program szkolenia

Szkolenie składa się z 5 modułów tematycznych, obejmujących kluczowe aspekty cyberbezpieczeństwa:

- Moduł 1: Podstawowe zagrożenia cybernetyczne
 - Phishing i spear phishing.
 - Ransomware.
 - Malware (wirusy, trojany, spyware).
- Moduł 2: Bezpieczeństwo haseł i tożsamości
 - Znaczenie silnych haseł i zarządzania tożsamością.
 - Zasady tworzenia bezpiecznych haseł.
 - Metody zarządzania hasłami (w tym menedżery haseł).
 - Sposoby wycieku haseł.

- Podstawowe zasady bezpieczeństwa haseł.
- Moduł 3: Jak jesteśmy atakowani – techniki hakerów
 - Przegląd wektorów ataków i metod socjotechnicznych.
 - Zagrożenia związane z Internetem Rzeczy (IoT).
 - Zasady obrony przed atakami.
- Moduł 4: Znaczenie kopii zapasowych (backup)
 - Rola i cel tworzenia backupu.
 - Rodzaje kopii zapasowych i metody ich tworzenia.
 - Znaczenie regularnego backupu dla ochrony danych.
- Moduł 5: (Nie)Bezpieczeństwo Sztucznej Inteligencji (AI)
 - Zagrożenia związane z AI (Deep Fake, fałszywe zdjęcia, teksty).
 - Metody rozpoznawania dezinformacji i fałszywych treści.



Oczekiwane przygotowanie uczestnika

Nie jest wymagane.



Czas trwania

1 dni / 2 godzin

Język

Język: polski.