

Cyberbezpieczeństwo w praktyce: jak chronić siebie i organizację – e-learning z Asystentem AI

Codzienna praca z pocztą, hasłami, urządzeniami i informacjami firmowymi wymaga świadomego reagowania na zagrożenia cyfrowe. Kurs rozwija praktyczną wiedzę z zakresu cyberbezpieczeństwa i pokazuje, jak rozpoznawać najczęstsze zagrożenia, chronić dane, bezpiecznie zarządzać hasłami, tworzyć kopie zapasowe oraz reagować na dezinformację i zagrożenia związane z AI. W tej wersji szkolenia każdy moduł został rozszerzony o pracę z Asystentem AI, który wspiera utrwalanie wiedzy, odpowiada na dodatkowe pytania i pomaga lepiej zrozumieć wybrane zagadnienia. Uczestnik może również odpowiadać własnymi słowami na pytania otwarte i otrzymywać informację zwrotną dotyczącą poziomu zrozumienia omawianych treści. Dzięki temu nauka obejmuje nie tylko zapoznanie się z materiałem, ale również aktywną pracę, powtórkę i sprawdzanie wiedzy po każdym module.

Dostęp do kursu przysługuje na 365 dni.



Odbiorcy szkolenia

Kurs jest przeznaczony dla wszystkich osób, które w codziennej pracy korzystają z komputerów, urządzeń mobilnych, poczty elektronicznej, usług online oraz mają kontakt z danymi firmowymi lub informacjami klientów. Sprawdza się niezależnie od poziomu wiedzy technicznej i pomoże uporządkować najważniejsze zasady bezpiecznego korzystania z technologii, rozpoznawania cyberzagrożeń oraz reagowania na podejrzane sytuacje.



Korzyści

1. Praktyczna wiedza o cyberbezpieczeństwie – uporządkujesz zasady ochrony danych, haseł, urządzeń i informacji oraz rozpoznawania najczęstszych zagrożeń cyfrowych.
2. Aktywna praca z Agentem AI po każdym module – po każdej części kursu możesz zadawać pytania, rozwijać wybrane zagadnienia i wyjaśniać kwestie, które wymagają dodatkowego doprecyzowania.
3. Utrwalanie wiedzy – wykorzystasz Agent AI do powtórzenia najważniejszych treści i lepszego zrozumienia omawianych zagadnień.
4. Sprawdzenie zrozumienia materiału – odpowiesz własnymi słowami na pytania otwarte, a Agent AI przeanalizuje odpowiedź i przekaże informację zwrotną.
5. Identyfikacja obszarów do powtórki – informacja zwrotna od Agent AI pomoże wskazać zagadnienia, do których warto wrócić przed przejściem dalej.
6. Nauka poprzez interakcję – zamiast ograniczać się do oglądania i czytania materiałów, aktywnie pracujesz z treścią, zadajesz pytania i sprawdzasz swoją wiedzę na kolejnych etapach kursu.



Program szkolenia

MODUŁ 1: Podstawowe zagrożenia cybernetyczne

- Phishing
- Ransomware
- Malware

MODUŁ 2: Bezpieczeństwo haseł i tożsamości

- Podstawowe pojęcia
- Tworzenie bezpiecznych haseł
- Czego NIE robić z hasłami
- Weryfikacja złożoności haseł
- Zarządzanie hasłami
- Jak wyciekają hasła?
- Reguła 3+1
- Bezpieczne przekazywanie danych wrażliwych

MODUŁ 3: Jak jesteśmy atakowani – techniki hakerów

- Przegląd wektorów ataków
- Specyfika zagrożeń IoT
- Ataki socjotechniczne
- 10 zasad obrony
- Koszty incydentów i rola człowieka

MODUŁ 4: Znaczenie kopii zapasowych (backup)

- Czym jest backup?

- Jak tworzyć kopie zapasowe?
- Jak często wykonywać backup?

MODUŁ 5: (Nie)Bezpieczeństwo Sztucznej Inteligencji (AI)

- Deep Fake
- Fake Photos (Fałszywe Zdjęcia)
- Fake News (Fałszywe Informacje)
- Problem dezinformacji w sieci
- Jak rozpoznawać i weryfikować autentyczność treści

MODUŁ 6: Test końcowy

- 10 pytań testowych



Oczekiwane przygotowanie uczestnika

Nie jest wymagane.



Czas trwania

1 dni / 2 godzin

Język

Polski