

## Szkolenie: CIW CyberSecurity Essentials



W celu przeprowadzenia kalkulacji ceny tego szkolenia prosimy o kontakt z działem handlowym

### Cel szkolenia:

Internet zrewolucjonizował nasze życie, korzystają z niego osoby w różnym wieku, o różnych zainteresowaniach i do bardzo różnych celów. Wraz z jego upowszechnieniem wzrosła ilość przestępstw, które wykorzystują możliwości Internetu oraz nieświadomość samych użytkowników co do zagrożeń.

**Szkolenie CyberSecurity Essentials** ma na celu przybliżyć użytkownikom zagadnienia związane z **cyberbezpieczeństwem**. Przedstawione zostaną wyzwania na takich polach jak prawo autorskie, social media, cyberetyka, a także zagrożenia dla systemów komputerowych oraz sposoby ich ochrony. Zawiera również tematy szczególnie istotne przy korzystaniu z Internetu przez dzieci i młodzież: cyberprzemoc, gry internetowe, najlepsze praktyki i sposoby ograniczania ryzyka dla młodych i nowych użytkowników mediów internetowych.

**Szkolenie Cybersecurity Essentials** skierowane jest do wszystkich osób, które nie są zaznajomione z tematyką związaną z **cyberbezpieczeństwem** i **zagroženiami w sieci**, a chcą na co dzień **bezpiecznie korzystać z Internetu**.

Na kursie uczestnicy w szczególności dowiedzą się:

- Jak skutecznie chronić swoją tożsamość i prywatność w sieci, zwłaszcza korzystając z mediów społecznościowych i urządzeń mobilnych
- Jak stosować zabezpieczenia i dobre praktyki w celu ochrony danych osobowych
- Jak radzić sobie z zagrożeniami płynącymi ze strony społeczności i działań internetowych jak: cyberprzemoc, sexting i gry online
- Jak bezpiecznie i zgodnie z prawem korzystać z treści zamieszczonych w sieci, np. muzyki i filmów
- Jak są wytyczne dotyczące praw autorskich i dozwolonego użytku w Internecie
- Jak chronić swój system komputerowy przed takimi zagrożeniami jak wirusy czy złośliwe oprogramowanie
- Jakie są zagrożenia bezpieczeństwa dla urządzeń mobilnych
- W jaki sposób można chronić swój system komputerowy: wykonując regularne skanowanie antywirusowe, stosując silne hasła czy stosując się do zasad bezpiecznego korzystania z Internetu.

## Plan szkolenia:

- Ochrona tożsamości
  - Ochrona tożsamości i prywatności
  - Prywatność
  - Cyfrowy ślad
  - Strony społecznościowe, a prywatność
  - Techniki cyberbezpieczeństwa
  - Aktywność: Logowanie planu dnia
  - QUIZ
  - Analiza przypadku: Ujawnianie i bezpieczeństwo
- Zagrożenia bezpieczeństwa w aktywności online
  - Zagrożenia płynące z Internetu
  - Cyberprzemoc
  - Sexting
  - Gry online
  - Aktywność: Analiza scenariuszy i tworzenie PSA
  - QUIZ
- Prawne i etyczne problemy wynikające z treści w Internecie
  - Wykorzystanie treści z Internetu
  - Prezentacja wytycznych dozwolonego użytku
  - Analiza autorskich scenariuszy
  - QUIZ
- Ochrona komputera przed zagrożeniami bezpieczeństwa
  - Zabezpieczenie komputera
  - Wirusy i Malware
  - Ochrona urządzeń mobilnych
  - Silne hasła
  - Tworzenie karty praw
  - Tworzenie Cybershield
  - QUIZ
  - Analiza przypadku: Bezpieczeństwo podczas przeglądania Internetu
  - Analiza przypadku: Bezpieczeństwo i unikanie P2P

## Wymagania:

Do uczestnictwa w kursie **CyberSecurity Essentials** nie są wymagane żadne wcześniejsze przygotowania oprócz umiejętności podstawowej obsługi komputera.

## Poziom trudności



## Certyfikaty:

Każde ze szkoleń z programu **ICT** kończy się **egzaminem certyfikacyjnym**, który stanowi końcową ocenę zdobytej wiedzy i umiejętności przez uczestnika danego szkolenia. **Pozytywny wynik egzaminu** potwierdzany jest poprzez uzyskanie **imiennego certyfikatu w formie cyfrowej**, który można dodatkowo samodzielnie wydrukować.

Każdy **egzamin certyfikacyjny** zawiera **30 pytań wielokrotnego wyboru**, które są losowane z większej puli i generowane przez system testowy w losowej kolejności. Maksymalny czas trwania egzaminu to 45 min. Kandydaci, aby pozytywnie zakończyć egzamin i uzyskać certyfikat muszą zdobyć minimum 73% poprawnych odpowiedzi. Jeśli kandydat nie zda egzaminu certyfikującego za pierwszym razem ma maksymalnie dwa dodatkowe podejścia. Po uzyskaniu pozytywnego wyniku egzaminu nie ma możliwości jego powtórzenia np. w celu uzyskania lepszego rezultatu procentowego.

## Prowadzący:

Autoryzowany wykładowca CIW ( CIW Certified Instructor).

## Informacje dodatkowe:

Jednym z kluczowych elementów projektu „**ICT CyberSecurity Essentials**” są zarówno częściowe testy, które na bieżąco sprawdzają przyswajaną wiedzę jak i końcowy **egzamin certyfikacyjny**. Testy częściowe będące elementami poszczególnych modułów danego szkolenia pozwalają instruktorowi na ocenę bieżących postępów uczestnika, natomiast końcowy egzamin stanowi podsumowanie i potwierdzenie opanowania danej technologii.

## Testy sprawdzający

Testy sprawdzające są wykonywane pod nadzorem instruktora i stanowią one ocenę gotowości kandydata do egzaminu podsumowującego/certyfikacyjnego, który, co ważne, jest nadzorowany przez inną osobę niż ta, która prowadziła dane szkolenie. Instruktor na podstawie raportu podsumowującego wyniki testów sprawdzających może zidentyfikować osoby, które mogą potrzebować skorzystania z dodatkowych materiałów i ćwiczeń dotyczących określonego obszaru tematycznego. Uczestnicy szkoleń mogą powtarzać testy sprawdzające dowolną ilość razy w zależności od uznania instruktora.

