



POLSKIE CENTRUM
BADAŃ I CERTYFIKACJI



SZKOLENIE

CyberHigiena



Inseqr

Tworzymy kulturę bezpieczeństwa

**1 DZIEŃ
ONLINE**

**6 GODZIN LEKCYJNYCH
SYMBOL: O236**

Szkolenie opracowane przy współpracy
z partnerem biznesowym Inseqr sp.z.o.o.

Termin zgodnie z harmonogramem szkoleń
otwartych PCBC S.A. dostępnym na stronie:
www.pcbc.gov.pl

DLACZEGO MY?



Szeroki wybór
tematów



Realizacja
celu



Najlepsi
trenerzy



65 lat
na rynku



Atrakcyjna
forma



CERTYFIKACJA.
BADANIA.
SZKOLENIA.

Polskie Centrum Badań i Certyfikacji S.A.

ul. Puławska 469
02-844 Warszawa

Tel.: +48 22 46 45 200
pcbc@pcbc.gov.pl

O SZKOLENIU

Szkolenie, skierowane do menedżerów i pracowników. Celem szkolenia jest przygotowanie odbiorcy do bezpiecznych działań w cyberprzestrzeni, przeciwdziałanie potencjalnym zagrożeniom oraz nabycie praktycznych umiejętności jak radzić sobie z cyberatakami.

Zdefiniujemy ekosystem cyberbezpieczeństwa, przedstawimy jego głównych aktorów i zasady jakie w nim obowiązują. Omówimy najczęstsze zagrożenia w cyberprzestrzeni, z którymi użytkownik może spotkać się na co dzień, a także sposoby skutecznego reagowanie na incydenty. Podczas szkolenia rozłożymy na czynniki pierwsze realne cyberataki i ich konsekwencje.

Przedstawimy podstawowe zasady cyberbezpieczeństwa w pracy i w życiu prywatnym – bo świadomy i przygotowany na zagrożenia pracownik to cyberbezpieczna firma i instytucja. Na koniec podejmiemy próbę odpowiedzi na najczęściej zadawane pytanie – jak być bezpiecznym w sieci?

PROGRAM SZKOLENIA

- 📌 Cyberbezpieczeństwo - podstawowe pojęcia dotyczące cyberbezpieczeństwa.
- 📌 Przegląd agencji i organizacji z zakresu cyberbezpieczeństwa.
- 📌 Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców.
- 📌 Jak rozpoznać atak i jak na niego reagować? – przykłady realnych ataków i incydentów.
- 📌 Zrządzanie ryzykiem oraz podejmowanie właściwych decyzji dotyczących cyberbezpieczeństwa w organizacji.
- 📌 Bezpieczny pracownik – dobre praktyki związane z bezpiecznym wykorzystywaniem zasobów służbowych, w tym:
 - polityka haseł – jakie hasła są bezpieczne, jak nimi zarządzać?
 - ryzyka związane z wykorzystywaniem wymiennych nośników USB,
 - bezpieczna praca z pakietem biurowym i pocztowym,
 - bezpieczna praca z przeglądarką internetową,
 - ryzyka związane z wykorzystywaniem prywatnych adresów e-mail w celach służbowych,
 - jak bezpiecznie przekazywać poufne informacje za pośrednictwem poczty e-mail,
 - najważniejsze zasady cyberbezpiecznego pracownika.
- 📌 Nasze dane w SoMe – szansa czy zagrożenie? Ułatwienia, „bańka informacyjna”, profilowanie tworzenie haseł do ataku.
- 📌 Dezinformacja i Fake newsy - współczesna, skuteczna broń na froncie wojny informacyjnej.
- 📌 Dobre praktyki z zakresu cyberbezpieczeństwa.

KORZYŚCI

- 📌 Przygotowanie uczestników do bezpiecznego funkcjonowania w cyberprzestrzeni.
- 📌 Nabycie wiedzy i umiejętności identyfikacji cyberataków.
- 📌 Zminimalizowanie liczby cyberataków - nabycie umiejętności zwalczania zagrożeń oraz ograniczenia ich skutków.
- 📌 Kształtowanie nawyków i właściwych reakcji na potencjalne zagrożenia.
- 📌 Poznanie dobrych praktyk.

990 ZŁ

NETTO / OSOBA

Cena obejmuje: organizację szkolenia w trybie on-line,
materiały szkoleniowe w formie elektronicznej,
certyfikat uczestnictwa w formie papierowej.