



POLSKIE CENTRUM
BADAŃ I CERTYFIKACJI



SZKOLENIE

Bezpieczny pracownik w sieci

1 DZIEŃ
ONLINE

8 GODZIN LEKCYJNYCH
SYMBOL: O234

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



60 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, którego celem jest zwiększenie bezpieczeństwa informatycznego organizacji poprzez podnoszenie kompetencji pracowników w zakresie bezpieczeństwa IT, w szczególności w zakresie ochrony danych, informacji i wiedzy na temat zagrożeń sieciowych oraz inżynierii społecznej - socjotechniki stosowanej w naruszeniach bezpieczeństwa sieci. Szkolenie ma za zadanie nauczyć pracowników jak korzystać z urządzeń ICT - komputera, smartfonu i innych urządzeń teleinformatycznych, tak aby nie narażać danych prywatnych, firmowych na ataki cyberprzestępców.

PROGRAM SZKOLENIA

- 🔧 Zagrożenia w cyberprzestrzeni dla pracownika oraz dla zasobów organizacji – obecne trendy.
- 🔧 Socjotechniczne mechanizmy działania cyberprzestępców w domu i w firmie.
- 🔧 Dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami, w tym budowania skutecznych haseł, tworzenia kopii bezpieczeństwa.
- 🔧 Rozpoznawanie złośliwego oprogramowania i innych ataków na firmę oraz reagowanie na pojawiające się niebezpieczeństwa.
- 🔧 Krótkie omówienie obowiązku ochrony informacji i zabezpieczania środowiska pracy z podkreśleniem indywidualnej odpowiedzialności za utrzymanie bezpieczeństwa informacji i reputacji instytucji oraz zaufania klientów.
- 🔧 Przykładowe narzędzia pomocne w obronie przed atakami w sieci.
- 🔧 Przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym.
- 🔧 Profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN/WIFI.
- 🔧 Bezpieczeństwo urządzeń IOT (Internet of Things).
- 🔧 Pokaz przykładowych ataków:
 - atak MITM: podsłuch i modyfikacja wiadomości pomiędzy dwiema stronami,
 - kradzież haseł,
 - podmiana stron internetowych.
- 🔧 Pokaz wybranych ataków wykonywanych przez cyberprzestępców na smartfony.
- 🔧 Ochrona urządzeń mobilnych przed hakerami – oprogramowanie szpiegujące.

KORZYŚCI

- 🔧 Wzrost bezpieczeństwa IT, organizacja będzie bardziej odporna na ataki cybernetyczne, co przekłada się na zwiększone ogólne bezpieczeństwo.
- 🔧 Szkolenie pomoże w ochronie poufnych danych i informacji, zapobiegając wyciekom lub kradzieżom, co może potencjalnie zaszkodzić reputacji firmy czy prywatnej osoby.
- 🔧 Skuteczniejsza reakcja na incydenty: pracownicy będą lepiej przygotowani do rozpoznawania i reagowania na potencjalne zagrożenia, co może ograniczyć skutki ewentualnych incydentów.
- 🔧 Szkolenie pomaga zrozumieć znaczenie bezpieczeństwa IT i jakie są potencjalne konsekwencje naruszenia bezpieczeństwa, co przyczynia się do większej uwagi i zaangażowania w tym obszarze.

900 ZŁ

NETTO / OSOBA

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