# Program szkolenia

**1**

**BLOK TEMATYCZNY**
**9:00-9:45**

Wstęp do cyberbezpieczeństwa:

- Jak odróżnić cyberbezpieczeństwo od cyberprzestrzeni?
- Podstawy bezpieczeństwa instytucji – czym jest Polityka Bezpieczeństwa Informacji i SZBI?
- Norma ISO 27001 jako powszechne rozwiązanie i standard bezpieczeństwa.
- Nowe wymagania i obowiązki wdrożeniowe w instytucji w związku z ustawą UKSC 2.0.
- Audyt systemów komputerowych, testy phishingowe i testy penetracyjne.

**POKAZ**
**9:45-10:45**

POKAZ: Ataki na „komputery” – omówienie wraz z demonstracją:

- Przegląd najczęstszych ataków komputerowych wykorzystywanych przez cyberprzestępców.
- Ataki przez fałszywe maile (kradzież tożsamości, kradzież haseł, tzw. oszustwa nigeryjskie).
- Ataki dokonywane przez telefony komórkowe (fałszywe wiadomości SMS, tzw. SMS Premium, przekierowania rozmów) – przykłady.
- Ataki dokonywane przez sieci bezprzewodowe (WiFi, Bluetooth).
- Malware – złośliwe oprogramowanie instalowane na komputerach, tabletach i smartfonach – przykłady.
- Phishing – podszywanie się pod osoby lub instytucje – przykłady.
- Oszustwa inwestycyjne – wykorzystanie zdalnego pulpitu w procederach przestępczych.

Szkolenia PPBW

# Program szkolenia

**POKAZ**
**9:45-10:45**

- Urządzenia mobilne i komunikatory internetowe – podstawy bezpiecznego użytkowania.
- Spoofing telefoniczny – zagrożenia wynikające z możliwości podszywania się pod cudzy numer telefonu.

**10:45-11:00**

Przerwa

**2**

**BLOK TEMATYCZNY**
**11:00-12:00**

**Socjotechnika, czyli ataki na „człowieka” – omówienie wraz z demonstracją:**

- Jak rozpoznać, że jest się celem ataku socjotechnicznego?
- Przykłady ataków socjotechnicznych: Ataki dokonywane z użyciem social media (Facebook, Instagram), w tym przez komunikatory (Messenger, Skype).
- Miejsca, gdzie zostawiamy swoje dane – działania świadome i nieświadome.
- Sztuczna Inteligencja (AI) – najnowsze zagrożenia: Zagrożenia wynikające z możliwości generowania obrazów i wizerunków.
- Generowanie głosu przez AI: Możliwości złośliwego wykorzystania technologii deepfake.
- Tworzenie złośliwego oprogramowania i skryptów obchodzących zabezpieczenia systemów przy użyciu AI.
- Wykorzystanie sztucznej inteligencji przez oszustów w praktyce.
- Działania ochronne i sposoby wykrywania ataków wspieranych przez AI.

Szkolenia PPBW

# Program szkolenia

**3**

**BLOK TEMATYCZNY**
**12:00-13:00**

Reagowanie w przypadku rozpoznania cyberprzestępstwa:

- Gdy instytucja pada ofiarą cyberataku lub cyberprzestępstwa – kogo i jak poinformować (zgodnie z wymogami UKSC 2.0).
- Sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania.
- Współdziałanie z organami ścigania w zakresie rozpoznawania i zwalczania cyberprzestępczości.
- Jak skutecznie zabezpieczyć dowody cyberprzestępstwa?

Podsumowanie i dyskusja.

## KONTAKT

**Aneta Jabłońska**
Specjalista ds. Organizacji Szkoleń
tel. **+48 61 861 24 46** | kom. **+48 695 386 963**
e-mail: **aneta.jablonska@ppbw.pl**

Szkolenia PPBW