testuj.pl

# Bezpieczeństwo użytkownika końcowego - 2 dni

**Korzyści dla uczestników:**

- Znajomość podstawowych zagadnień bezpieczeństwa,
- Zbudowanie intuicji bezpiecznego wykorzystywania sprzętu i korzystania z Internetu,
- Poznanie potencjalnych skutków typowych ataków,
- Definiowanie "czerwonych świateł", które mogą świadczyć o byciu celem ataku hakerskiego

- Co atakujący widzi o mnie w sieci?
  - Media społecznościowe
  - Biały wywiad
- Polityka zarządzania hasłami
  - Co to znaczy bezpieczne hasło?
  - Aplikacje do bezpiecznego zarządzania hasłami
- Bezpieczeństwo urządzeń mobilnych
  - Jak chronić swoje urządzenie mobilne przed malwarem
  - Bezpieczeństwo sklepów z aplikacjami (np. Google Play)
  - Aplikacje z niezaufanych źródeł
- Bezpieczne korzystanie z publicznych sieci WiFi
  - Zagrozenia wynikajace z laczenia sie do publicznych WiFi
  - Metody zabezpieczania danych wysyłanych przed publiczne WiFi
- Bezpieczeństwo pracy zdalnej
  - Typowe zagrożenia
  - Higiena bezpieczeństwa
- Typowe ataki socjotechniczne
  - Phishing, vishing, ransomware