



# Security in practice

## **BEZPIECZEŃSTWO TELEINFORMATYCZNE -UKIERUNKOWANE NA ODBIORCĘ ZAAWANSOWANEGO**

### **Ataki komputerowe**

- Motywacje włamywaczy
- Kim może być atakujący
- Powody ataków
- Cel atakujących
- Ochrona przed atakami
- Wymagania prawne

### **Czynnik ludzki – zagrożenia socjotechniczne**

- Czym jest socjotechnika
- Przykłady zagrożeń socjotechnicznych – phishing
- Przykłady zagrożeń socjotechnicznych pisma
- Zagrożenia, do czego mogą prowadzić
- Zasady wykonywania przelewów – bankowość elektroniczna
- Zagrożenia, płatności kartami bankowymi
- Środki bezpieczeństwa
- Środki ostrożności

### **Zasady bezpieczeństwa – jak chronić się przed zagrożeniami**

- Czyste biurko i ekran
- Hasła, złożoność i stosowanie
- Bezpieczne surfowanie w sieci Internet
- Korzystanie z sieci komputerowych
- Przykłady narzędzi
- Reagowanie na incydenty i włamania