

Bezpieczeństwo Urządzeń i Podstawowe Zasady

Warsztaty

Prowadzący: prof. dr hab. Maciej Rybczyński

Jak aktualizacje chronią nas przed zagrożeniami?

1. Aktualizacje eliminują znane luki bezpieczeństwa.
2. Regularne poprawki zapobiegają atakom ransomware i innym zagrożeniom.
3. Brak aktualizacji zwiększa ryzyko przejęcia urządzenia przez hakerów.

Jak działają wirusy i jak się przed nimi chronić?

1. Wirusy mogą uszkadzać systemy, kraść dane lub wymuszać okup (ransomware).
2. Oprogramowanie antywirusowe wykrywa i blokuje zagrożenia.
3. Nie pobieraj plików z podejrzanych stron i załączników e-mailowych.

Oprogramowanie antywirusowe – czy jest konieczne?

1. System Windows posiada wbudowaną ochronę (Windows Defender).
2. Dodatkowe antywirusy mogą oferować bardziej zaawansowane funkcje.
3. Antywirusy pomagają blokować nieznane zagrożenia i podejrzane pliki.

Szyfrowanie danych i kopie zapasowe – dlaczego warto?

1. Szyfrowanie danych zapobiega dostępowi osób niepowołanych.
2. Narzędzia jak BitLocker, VeraCrypt pozwalają zabezpieczyć pliki.
3. Kopie zapasowe chronią przed utratą danych w wyniku awarii lub ataku.

Interaktywne zadanie: Konfiguracja 2FA na kontach online

1. Sprawdź, czy Twoje konto (np. Google, Facebook) obsługuje uwierzytelnianie dwuskładnikowe (2FA).
2. Włącz 2FA i wybierz metodę (SMS, aplikacja, klucz sprzętowy).
3. Przetestuj logowanie i zobacz, jak 2FA zwiększa bezpieczeństwo.

Podsumowanie i kluczowe zasady bezpieczeństwa

1. Regularnie aktualizuj systemy i aplikacje.
2. Korzystaj z antywirusa i zapory sieciowej.
3. Szyfruj dane i twórz kopie zapasowe.
4. Włącz 2FA dla dodatkowej ochrony kont.

Q&A – Pytania i dyskusja

Masz pytania?

Czas na dyskusję i podsumowanie zajęć!