

# Wprowadzenie do Cyberbezpieczeństwa

Warsztaty

Prowadzący: prof. dr hab. Maciej Rybczyński

# Co to jest cyberbezpieczeństwo?

**Ochrona systemów komputerowych, sieci i danych przed atakami**

1. Kluczowe aspekty:

- Poufność (Confidentiality)
- Integralność (Integrity)
- Dostępność (Availability)

2. Znaczenie cyberbezpieczeństwa w codziennym życiu.

# Najczęstsze zagrożenia w sieci

1. Malware (wirusy, trojany, ransomware)
2. Phishing – oszustwa e-mailowe i fałszywe strony
3. Ataki socjotechniczne – manipulacja użytkownikiem
4. Niebezpieczeństwa publicznych sieci Wi-Fi
5. Utrata danych i wycieki informacji

# Przykłady realnych ataków i ich skutki

1. Atak WannaCry (2017) – globalne zainfekowanie komputerów ransomwarem
2. Atak na Facebook (2019) – wyciek danych 530 mln użytkowników
3. Ataki phishingowe – oszustwa na bankowość internetową
4. Przechwycenie danych w publicznej sieci Wi-Fi

# Jak rozpoznać phishing?

1. Sprawdź adres nadawcy e-maila
2. Unikaj klikania podejrzanych linków
3. Fałszywe strony bankowe – sprawdzaj certyfikat SSL (https)
4. Nigdy nie podawaj danych logowania przez e-mail
5. Używaj uwierzytelniania dwuskładnikowego (2FA)

# Podstawowe zasady bezpiecznego korzystania z Internetu

1. Używaj silnych haseł i menedżerów haseł
2. Nie otwieraj podejrzanych załączników e-mail
3. Regularnie aktualizuj oprogramowanie
4. Korzystaj z antywirusa i zapory sieciowej
5. Unikaj publicznych sieci Wi-Fi bez VPN

# Interaktywne zadanie: Analiza przykładowych zagrożeń

1. Uczestnicy analizują próbki e-maili i stron
2. Jakie elementy wyglądają podejrzanie?
3. Jak można zweryfikować ich autentyczność?
4. Dyskusja i podsumowanie wniosków

# Podsumowanie i pytania

1. Kluczowe wnioski z pierwszej godziny warsztatów
2. Jakie kroki można wdrożyć od zaraz?
3. Sesja Q&A – pytania uczniów