PRZEWODNIK PO ZAGROŻENIACH W INTERNECIE

Korzystanie z Internetu niesie wiele korzyści, ale wiąże się także z zagrożeniami, na które należy uważać. Właściwa ochrona i świadome zachowania online mogą pomóc uniknąć wielu problemów.

Podstawowe zasady bezpieczeństwa obejmują stosowanie aktualnego oprogramowania antywirusowego, unikanie podejrzanych stron i linków oraz regularne aktualizowanie systemu operacyjnego i aplikacji.

Brak ostrożności w Internecie może prowadzić do różnych zagrożeń, takich jak np.:

Najczęstsze zagrożenia

1. **Złośliwe oprogramowanie (malware)** – wirusy, trojany i ransomware mogą uszkodzić komputer lub wykraść Twoje dane.
    - *Jak się chronić?* Używaj aktualnego programu antywirusowego i nie pobieraj plików z podejrzanych stron.
2. **Phishing** – oszuści podszywają się pod firmy i instytucje, by wyłudzić dane logowania lub dane kart płatniczych.
    - *Jak się chronić?* Nigdy nie klikaj w podejrzane linki w e-mailach i SMS-ach. Sprawdzaj adresy stron przed podaniem danych.
3. **Ataki ransomware** – blokują dostęp do danych i żądają okupu za ich odzyskanie.
    - *Jak się chronić?* Regularnie twórz kopie zapasowe i nie otwieraj załączników od nieznanych nadawców.
4. **Ataki DoS/DDoS** – sprawiają, że serwery przeciążają się i przestają działać.
    - *Jak się chronić?* Korzystaj z usług zabezpieczających przed DDoS.
5. **Niebezpieczne sieci Wi-Fi** – publiczne sieci mogą być wykorzystywane do przechwytywania Twoich danych.
    - *Jak się chronić?* Korzystaj z VPN i unikaj logowania do bankowości przez otwarte Wi-Fi.
6. **Przejęcie konta (account takeover)** – atakujący uzyskuje dostęp do Twojego konta e-mail, bankowego lub mediów społecznościowych.
    - *Jak się chronić?* Używaj silnych haseł i włącz uwierzytelnianie dwuskładnikowe (2FA).
7. **Oprogramowanie szpiegujące (spyware)** – monitoruje Twoje działania i może kraść poufne informacje.
    - *Jak się chronić?* Instaluj tylko aplikacje z zaufanych źródeł i używaj programów antyszpiegowskich.

8. **Keyloggery** – zapisują to, co wpisujesz na klawiaturze, w tym hasła.
    - *Jak się chronić?* Korzystaj z menedżerów haseł i aktualizuj system.
9. **Fałszywe strony internetowe** – wyglądają jak oryginalne strony banków czy sklepów, ale służą do kradzieży danych.
    - *Jak się chronić?* Sprawdzaj dokładnie adresy stron i korzystaj tylko z bezpiecznych połączeń (https://).
10. **Ataki socjotechniczne (social engineering)** – manipulacja użytkownikami w celu uzyskania ich danych.

- *Jak się chronić?* Nigdy nie podawaj poufnych informacji przez telefon lub e-mail.

Jak zabezpieczyć swój komputer?

Windows:

- Regularnie aktualizuj system i programy.
- Używaj Microsoft Defender lub innego antywirusa.
- Włącz zaporę systemową (Windows Firewall).
- Nie instaluj programów z nieznanych źródeł.
- Korzystaj z konta użytkownika z ograniczonymi uprawnieniami.

macOS:

- Korzystaj z wbudowanej ochrony przed malware (XProtect).
- Instaluj aplikacje tylko z Mac App Store lub zaufanych stron.
- Włącz funkcję Gatekeeper, aby blokować nieznane programy.
- Regularnie aktualizuj system.
- Włącz FileVault, by szyfrować swoje dane.

Co zrobić, jeśli podejrzewasz zagrożenie?

1. **Odłącz urządzenie od internetu** – zapobiegniesz dalszemu rozprzestrzenianiu się zagrożenia.
2. **Uruchom skanowanie antywirusowe** – sprawdź i usuń wykryte zagrożenia.
3. **Zmień hasła** – szczególnie do bankowości i poczty e-mail.
4. **Przywróć system z kopii zapasowej**, jeśli infekcja jest poważna.
5. **Zgłoś problem** administratorowi IT lub dostawcy usług.