

---

# Cyberbezpieczeństwo

## **PORADNIK DOTYCZĄCY CYBERBEZPIECZEŃSTWA, PODSTAWOWE ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z INTERNETU**

W dzisiejszym świecie Internet jest nieodłączną częścią naszego życia. Umożliwia nam komunikację, zakupy, pracę i rozrywkę. Jednakże, korzystanie z Internetu wiąże się również z pewnymi zagrożeniami. W tym poradniku omówimy najczęstsze zagrożenia związane z korzystaniem z sieci oraz przedstawimy sposoby, jak się przed nimi zabezpieczyć.

### **PODSTAWOWE ZAGROŻENIA W SIECI**

#### **1. Phishing**

Phishing to technika oszustwa, polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia wrażliwych informacji, takich jak hasła, numery kart kredytowych czy dane logowania. Oszuści często wysyłają fałszywe e-maile lub tworzą strony internetowe, które do złudzenia przypominają te oryginalne.

Jak się chronić?

- Zawsze sprawdzaj adres nadawcy e-maila i unikaj klikania w linki w podejrzanych wiadomościach.
- Korzystaj z dwuskładnikowego uwierzytelniania (2FA), gdzie to możliwe.

#### **2. Złośliwe oprogramowanie (Malware)**

Malware to kategoria szkodliwego oprogramowania, które może uszkodzić twoje urządzenie, kraść dane lub przejmować kontrolę nad systemem. Do najczęstszych typów malware należą wirusy, trojany, robaki i spyware.

Jak się chronić?

- Instaluj oprogramowanie tylko z zaufanych źródeł.
- Regularnie aktualizuj system operacyjny i oprogramowanie antywirusowe.

#### **3. Ataki typu Ransomware**

Ransomware to rodzaj malware, który blokuje dostęp do plików lub systemu użytkownika i żąda okupu za ich odblokowanie. Ofiara jest zazwyczaj informowana o konieczności zapłaty okupu w kryptowalucie, aby odzyskać dostęp do swoich danych.

Jak się chronić?

- Regularnie twórz kopie zapasowe ważnych danych i przechowuj je na zewnętrznych nośnikach.
- Unikaj otwierania załączników z nieznanymi źródłami.

#### **4. Ataki typu DDoS**

Ataki typu Distributed Denial of Service (DDoS) polegają na przeciążeniu serwera, strony internetowej lub usługi online, co prowadzi do ich niedostępności dla użytkowników. Jest to jedna z najpopularniejszych form ataków cybernetycznych.

Jak się chronić?

- Używaj usług ochrony przed DDoS, oferowanych przez dostawców hostingowych lub firm zajmujących się cyberbezpieczeństwem.

#### **5. Kradzież tożsamości**

---

Kradzież tożsamości to sytuacja, w której ktoś przejmuje dane osobowe w celu dokonywania oszustw, np. zaciągania kredytów czy dokonywania zakupów na cudze nazwisko.

Jak się chronić?

- Chroń swoje dane osobowe i udostępniaj je tylko wtedy, gdy jest to absolutnie konieczne.
- Monitoruj swoje konta bankowe i raporty kredytowe.

## **6. Oszustwa internetowe**

Oszustwa internetowe przybierają różne formy, od fałszywych sklepów internetowych, przez piramidy finansowe, aż po oszustwa inwestycyjne. Ich celem jest wyłudzenie pieniędzy od niczego niepodważających użytkowników.

Jak się chronić?

- Sprawdzaj recenzje i wiarygodność stron internetowych przed dokonaniem zakupu.
- Bądź ostrożny w przypadku ofert, które wydają się zbyt dobre, by były prawdziwe.

## **JAK ZABEZPIECZYĆ SIĘ PRZED ZAGROŻENIAMI**

### **Używanie silnych haseł**

Silne hasła są podstawą bezpiecznego korzystania z internetu. Powinny być długie (co najmniej 12 znaków) i składać się z liter, cyfr oraz znaków specjalnych. Unikaj używania tego samego hasła do różnych kont.

### **Aktualizacje oprogramowania**

Regularne aktualizowanie systemu operacyjnego oraz aplikacji pomaga w zabezpieczeniu przed najnowszymi zagrożeniami. Aktualizacje często zawierają poprawki bezpieczeństwa, które mogą zapobiec atakom.

### **Korzystanie z programów antywirusowych**

Programy antywirusowe pomagają wykrywać i eliminować zagrożenia przed tym, jak mogą one zaszkodzić twojemu systemowi. Upewnij się, że program antywirusowy jest zawsze aktywny i regularnie aktualizowany.

### **Bezpieczne przeglądanie stron internetowych**

Zachowuj ostrożność podczas przeglądania stron internetowych, szczególnie tych, które wymagają podania danych osobowych lub finansowych. Zawsze upewnij się, że adres strony zaczyna się od "https://" oraz że na pasku adresu znajduje się ikona kłódki.

### **Zabezpieczenia w komunikacji online**

Podczas korzystania z komunikatorów internetowych i e-maili, dbaj o to, aby rozmowy były zabezpieczone (np. poprzez szyfrowanie). Unikaj wysyłania wrażliwych informacji przez niezabezpieczone kanały.

## **PODMIOTY ZAJMUJĄCE SIĘ CYBERBEZPIECZEŃSTWEM:**

Ministerstwo Cyfryzacji,

- CERT Polska, <https://cert.pl/>
- CSIRT GOV, <https://csirt.gov.pl/>
- CSIRT NASK, <https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html>

---

Cyberbezpieczeństwo to kluczowy aspekt korzystania z Internetu. Świadomość zagrożeń i stosowanie odpowiednich środków ostrożności może znacząco zmniejszyć ryzyko padnięcia ofiarą cyberataków. Pamiętaj, że bezpieczeństwo w sieci zaczyna się od Ciebie – bądź czujny i dbaj o swoje dane.