

# Cyberbezpieczeństwo

**Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami.**

Cyberbezpieczeństwo, zgodnie z obowiązującymi przepisami, to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

## Zagrożenia w cyberprzestrzeni:

- Złośliwe oprogramowania (malware);
- SPAM – niechciana korespondencja;
- Ataki na aplikacje internetowe;
- Ataki socjotechniczne (również inżynieria społeczna) – stosowanie środków psychologicznych i metod manipulacji mających na celu przekazanie lub wyłudzenie określonych informacji bądź nakłonienie do realizacji określonych działań;
- Ataki z wykorzystaniem złośliwego kodu na stronach internetowych;
- Phishing, czyli bezpośrednie wyłudzenie poufnych informacji lub za pomocą złośliwego oprogramowania;
- Ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu;
- Botnet-y – sieci komputerów przejętych przez przestępców;
- Kradzież tożsamości;
- Naruszenie poufności, integralności lub dostępności danych;
- Zagrożenia wewnętrzne powodowane przez pracowników;
- Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych;
- Cyberszpiegostwo;
- Kradzież kryptowalut (cryptojacking).
- Ingerencja fizyczna, uszkodzenia oraz kradzież;

## Informacje i porady dotyczące cyberbezpieczeństwa:

- [Bezpieczne poruszanie po sieci](#)
- [Bezpieczeństwo konta bankowego](#)

- [Poradnik cyberbezpieczeństwa](#)
- [Jak reagować?](#)
- [Cyber profilaktyka NASK](#)
- [Zagrożenia w sieci – co robić?](#)
- [Netykieta, czyli savoir-vivre w Internecie](#)
- [Fałszywe strony internetowe](#)

### **Zgłaszanie incydentów:**

- [Zgłoszenia do CSIRT NAS](#)

### **Źródła:**

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.)
- Inżynieria społeczna (informatyka) - Wikipedia Wolna encyklopedia.
- Botnet (bezpieczeństwo komputerowe) - Wikipedia Wolna Encyklopedia
- Mocne hasło - Wikipedia Wolna Encyklopedia
- NASK dyżurnet.pl
- CERT.PL
- niebezpiecznik.pl
- Złośliwe oprogramowanie - Wikipedia Wolna encyklopedia.
- DDoS - Wikipedia Wolna Encyklopedia
- ENISA Threat Landscape