



- [Strona główna](#)
- [Aktualności](#)
- [Grupy](#)
 - [BIEDRONKI](#)
 - [ŻABKI](#)
 - [MOTYLKI](#)
 - [PSZCZÓŁKI](#)
- [Zajęcia dodatkowe](#)
 - [Tańce](#)
 - [Rytmika](#)
 - [Angielski](#)
 - [Logopeda](#)
 - [Psycholog](#)
- [REKRUTACJA 2024](#)
- [Dla rodziców](#)
 - [Nauczanie zdalne](#)
 - [Dokumenty](#)
 - [Poradnik](#)
 - [Jadłospis](#)
 - [IPrzed szkole](#)
- [O nas](#)
 - [O nas](#)
 - [Baza placówki](#)
 - [Kadra](#)
 - [Zasady organizacji](#)
- [Kontakt](#)
- [Bezpieczeństwo](#)
 - [Inspektor Danych osobowych](#)
 - [Ochrona Danych Osobowych](#)
 - [Cyberbezpieczeństwo](#)
- [NPRCz 2.0](#)
- [Archiwum aktualności](#)
 - [ROK SZKOLNY 2022/2023](#)

Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami:

Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi mogą się Państwo spotkać, należą:

- ataki z użyciem szkodliwego oprogramowania (*malware*, wirusy, robaki, itp.),
- kradzieże tożsamości,
- kradzieże (wyludzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. *phishing*, czyli wyludzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania antywirusowego i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.

- Aktualizuj oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, posiadają połączenie szyfrowane, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

- **[STÓJ. POMYŚL. POŁĄCZ.](#)** jest polską wersją międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni. Zapoznaj się z **[dobrymi praktykami](#)** opublikowanymi na stronach kampanii oraz z dostępnymi na niej **[materiałami do pobrania](#)**.
- **[OUCH!](#)** To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagrożenia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację. Zobacz wszystkie polskie wydania **[OUCH!](#)** na stronie CERT Polska.
- Zespół **[CERT Polska](#)** działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska jest zespołem specjalistów zwalczających zagrożenia w sieciach komputerowych. Zapoznaj się z **[rocznymi raportami z działalności CERT Polska](#)** zawierającymi zebrane dane o zagrożeniach dla polskich użytkowników Internetu, w tym również opisy najciekawszych nowych zagrożeń i podatności.