

## Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy informacje oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami. Podstawa prawna: ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, art. 22 ust. 1 pkt 4).

**Cyberbezpieczeństwo** to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”.

### Najpopularniejsze zagrożenia w cyberprzestrzeni:

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

### Jak można zabezpieczyć się przed zagrożeniami:

- zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym,
- aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy Twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie),
- aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki,
- zabezpieczaj swoje urządzenia mobilne. Laptopy, smartfony i tablety należy zabezpieczać przy pomocy PINu, odcisku palca lub innych metod oferowanych przez producentów urządzeń.
- wskazane jest korzystanie z urządzeń znanych producentów, zapewniających ciągle poprawki i aktualizacje do oficjalnego oprogramowania. Nie należy instalować aplikacji nieznanych producentów, bez autoryzacji sklepów z aplikacjami. Aplikacje nieznanych producentów mogą prowadzić do wycieku danych. Nie należy udostępnić swoich urządzeń mobilnych nieznanej osobie oraz pozostawiać ich bez osobistego nadzoru. Nie należy podłączać nieznanych nośników danych, które mogą zawierać zagrożenia w postaci szkodliwego oprogramowania.
- nie otwieraj plików nieznanego pochodzenia,
- nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna,
- nie używaj niesprawdzonych programów zabezpieczających czy też 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, lub 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 – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny,
- 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,
- nie loguj się do systemów z danymi wrażliwymi za pomocą publicznych sieci Wi-Fi,
- stosuj złożone hasła z wielką literą, cyfrą i znakiem specjalnym, regularnie je zmieniaj i nie stosuj zapamiętywania haseł w serwisach internetowych,
- nigdy nie wysyłaj za pomocą sieci publicznej niezaszyfrowanych danych wrażliwych, które mogą posłużyć do kradzieży tożsamości (PESEL, nr dowodu osobistego itp.),
- nie podłączaj nieznanego urządzenia do swojego komputera, np. znalezionej pendrive'a

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

**Poniżej znajdują Państwo informacje, które pozwolą Państwu na lepsze zrozumienie tematyki cyberbezpieczeństwa oraz skuteczne zabezpieczenie się przed zagrożeniami:**

- poradniki publikowane przez Ministerstwo Cyfryzacji
  - <https://www.gov.pl/web/cyfryzacja/edukacja>
  - <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
- zestaw porad bezpieczeństwa dla użytkowników komputerów
  - <https://www.cert.pl/ouch/>
- publikacje CERT Polska
  - <https://www.cert.pl/publikacje/>
- zgłoś incydent
  - <https://incydent.cert.pl/>