Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak się przed nimi ustrzec.

Cyberbezpieczeństwo - zgodnie z Ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 roku, poz. 1369) to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Najczęstszymi zagrożeniami w cyberprzestrzeni są:

- 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 wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję.

Podstawowe sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania antywirusowe 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**,
- nie otwieraj plików nieznanego pochodzenia,
- nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu,
- nie używaj niesprawdzonych programów zabezpieczających,
- co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe - jeśli się na tym nie znasz, poproś o pomoc kogoś bardziej doświadczonego. 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, co do których 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,

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

Wszelkie porady dotyczące bezpieczeństwa dla użytkowników komputerów dostępne są między innymi na:

- witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym pod adresem: https://www.cert.pl/ouch ;
- na stronie internetowej: https://www.saferinternet.pl/
- witrynie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/baza-wiedzy/aktualnosci ;
- stronie internetowej kampanii STÓJ. POMYŚL. POŁĄCZ po adresem: https://stojpomyslpolacz.pl/stp/