**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 skuteczne 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.

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

**Sposoby zabezpieczenia się przed zagrożeniami:**

* Zainstaluj i używaj oprogramowania przeciw wirusom. Stosuj ochronę w czasie rzeczywistym;
* Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki;
* Aktualizuj oprogramowanie antywirusowe 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 SSL;
* Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
* Skanuj komputer i sprawdzaj procesy sieciowe – 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;
* 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;
* Sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego;
* Nie odwiedzaj 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 wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny;
* Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich;
* Pamiętaj o uruchomieniu firewalla na każdym urządzeniu;
* Wykonuj kopie zapasowe ważnych danych.

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

**Dodatkowe informacje:**

* zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: <https://www.cert.pl/ouch/>
* poradniki na witrynie internetowej Ministerstwa Cyfryzacji: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
* publikacje z zakresu cyberbezpieczeństwa: <https://www.cert.pl/>
* strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: <https://stojpomyslpolacz.pl/stp/>