**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.

**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 i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
* Aktualizuj bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
* Regularnie aktualizuj oprogramowanie na komputerze, szczególnie oprogramowanie przeglądarek internetowych. Hakerzy szukają luk, a producenci cały czas „uszczelniają” wykryte luki w oprogramowaniu. Dzięki aktualizacjom mamy zawsze na komputerze najbardziej odporne na ataki hakerskie oprogramowanie.
* Nie instaluj na komputerze nielegalne oprogramowanie. Może ono zawierać przygotowane przez hakerów wirusy, które pomogą im w opanowaniu naszego komputera, wyłudzeniu danych, i w końcu pozwolą na okradzenie nas.
* Nie otwierajmy wiadomości i dołączonych do nich załączników z nieznanych źródeł. W załącznikach może być ukryte złośliwe oprogramowanie.
* Nie otwieraj plików nieznanego pochodzenia.
* Sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego.
* 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.
* Dokonuj płatności tylko z własnego komputera lub telefonu. Nie korzystaj do tych celów z publicznej sieci Wi-fi np. na lotnisku, w kawiarence internetowej.
* 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.
* 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.
* Zmieniaj regularnie hasła do swojego komputera oraz dostępu do konta internetowego. Powinny to być hasła trudne i różne do każdej usługi internetowej.
* Pamiętaj o uruchomieniu firewalla.
* 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/>