**Cyberbezpieczeństwo**

|  |
| --- |
| **Realizując obowiązek wynikający z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369) przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne 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 (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 skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.   1. [**STÓJ. POMYŚL. POŁĄCZ.**](https://stojpomyslpolacz.pl/)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**](https://stojpomyslpolacz.pl/stp/dobre-praktyki) opublikowanymi na stronach kampanii oraz z dostępnymi na niej [**materiałami do pobrania**](https://stojpomyslpolacz.pl/stp/materialy-do-pobrania). 2. **OUCH** To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia 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. 3. Zespół [**CERT Polska**](https://www.cert.pl/) 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**](https://www.cert.pl/publikacje/) zawierającymi zebrane dane o zagrożeniach dla polskich użytkowników Internetu, w tym również opisy najciekawszych nowych zagrożeń i podatności. |