

## Cyberbezpieczeństwo

**Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tym zagrożeniom.**

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 (Dz.U. z 2020 r. poz. 1369 z późn. zm.).

### 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 informacji przez podszywanie się pod godną zaufania osobę lub instytucję)

### Sposoby zabezpieczenia się przed zagrożeniami:

- 1) stosuj zasadę ograniczonego zaufania do odbieranych wiadomości e-mail, sms, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu
- 2) nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych
- 3) instaluj aplikacje tylko ze znanych i zaufanych źródeł
- 4) nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz
- 5) każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) - w tym polu znajdziesz rzeczywisty adres serwera nadawcy
- 6) porównaj adres konta e-mail nadawcy adresem w polu „From” oraz „Reply to” – różne adresy w tych polach mogą wskazywać na próbę oszustwa
- 7) szyfruj dane poufne wysyłane pocztą elektroniczną
- 8) bezpieczeństwo wiadomości tekstowych (SMS):
  - sprawdź adres url, z którego domyślnie dany podmiot/instytucja wysyła do Ciebie smsy; cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę),
  - otrzymując smsa, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako nadawcę wiadomości sms
- 9) jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail – jak najszybciej zmień hasło
- 10) chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przed zagrożeniami typu: wirusy, robaki, trojany, niebezpieczne aplikacje (typu ransomware, adware, keylogger, spyware, dialer), phishing, narzędziami hakerskimi, backdoorami, rootkitami, bootkitami i exploitami
- 11) aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe; brak aktualizacji zwiększa podatność na cyberzagrożenia; hakerzy, którzy znają słabości systemu/aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu
- 12) logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko
- 13) korzystaj z różnych haseł do różnych usług elektronicznych
- 14) tam gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego
- 15) regularnie zmieniaj hasła
- 16) nie udostępniaj nikomu swoich haseł
- 17) pracuj na najniższych możliwych uprawnieniach użytkownika
- 18) wykonuj kopie bezpieczeństwa
- 19) skanuj podłączane urządzenia zewnętrzne
- 20) skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze
- 21) kontroluj uprawnienia instalowanych aplikacji.
- 22) unikaj z korzystania otwartych sieci Wi-Fi
- 23) podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL; protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarką a serwerem
- 24) zadбай o bezpieczeństwo routera (ustal silne hasło do sieci WI-FI, zmień nazwę sieci WI-Fi, zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-Fi np. WPA2 i wyższe, aktualizuj oprogramowanie routera, wyłącz funkcję WPS, aktywuj funkcję Gościenna Sieć Wi-Fi „Guest Network”
- 25) szyfruj dyski twarde komputera, przenośne.

Więcej informacji porad o cyberbezpieczeństwie uzyskasz na stronach:

<https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>

<https://www.cert.pl/publikacje/>

<https://akademia.nask.pl/publikacje/>

<https://stojpomyslpolacz.pl/>

<https://dyzurnet.pl/>

Zgłaszanie incydentów bezpieczeństwa: <https://incydent.cert.pl/>

## Metryka strony

Udostępniający: **Urząd Miejski w Kleszczelach**

Wytwarzający/odpowiadający: Walentyna Sidoruk - Referat Organizacyjny

Data wytworzenia: **2022-08-03**

Wprowadzający: **Walentyna Sidoruk**

Data modyfikacji: **2022-08-03**

Opublikował: **Walentyna Sidoruk**

Data publikacji: **2022-08-03**