# CYBERBEZPIECZEŃSTWO

**Informacja dotycząca zagrożeń CYBERBEZPIECZEŃSTWA**

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2026r. poz. 20), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne zabezpieczyć się przed tymi zagrożeniami.

**Najpopularniejsze zagrożenia w cyberprzestrzeni:**

**1. ataki z użyciem szkodliwego oprogramowania** (malware, wirusy, robaki, itp.): hakerzy mogą wysyłać złośliwe oprogramowanie za pośrednictwem wiadomości e-mail lub załącznika dołączonego do e-maila.;

**Aby zapobiegać takim atakom, nie otwieraj podejrzanych wiadomości oraz załączników. W przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do konta w Twoim Banku.**

**2. oszustwo telefoniczne** (vishing): przestępcy, w tym przypadku mogą do Ciebie zadzwonić i podawać się za pracownika Urzędu lub innej instytucji. Poproszą Cię o przekazanie Twojego loginu, hasła, numeru PESEL, numeru dowodu osobistego. Podanie tych danych może skutkować kradzieżą Twojej tożsamości. Umożliwisz tym samym przestępcy logowanie się do systemu informatycznego Urzędu itp.

**Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz. Swoje hasła do systemów informatycznych zachowuj tylko dla siebie. Nie zdradzaj ich nigdy i nikomu.**

**3. Phishing –** jest to tworzenie fałszywych stron internetowych, żeby wyłudzić dane (loginy i hasła) użytkowników Internetu; w tym celu najczęściej wysyłają wiadomości e-mail zawierające odnośniki do tych stron.

**Aby się ochronić – weryfikuj adresy stron WWW zanim się na nich zalogujesz. Nie wpisuj swojego loginu i hasła na podejrzanych stronach internetowych.**

**Pamiętaj! Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz. Swoje hasła do systemów informatycznych zachowuj tylko dla siebie. Nie zdradzaj ich nigdy i nikomu.**

**Będziesz bezpieczny w sieci Internet jeżeli zastosujesz zasadę ograniczonego zaufania i podwyższonej ostrożności.** Podstawowe kroki aby to osiągnąć przedstawiamy poniżej:

1. używaj oprogramowania antywirusowego i zapory sieciowej (firewall);
2. unikaj korzystania z sieci publicznych, w przypadku logowania się do systemów informatycznych zawierających cenne dane lub dane podlegające ochronie;
3. korzystaj wyłącznie z legalnego i aktualnego oprogramowania;
4. regularnie aktualizuj oprogramowania oraz bazy danych wirusów;
5. nie korzystaj ze stron WWW, które nie mają ważnego certyfikatu (np. brak protokołu https);
6. nie otwieraj podejrzanych e-maili oraz ich załączników;
7. nie pozostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach internetowych;
8. nie wysyłaj e-mailem poufnych danych bez ich szyfrowania;
9. czytaj dokładnie Regulaminy i Polityki serwisów WWW oraz weryfikuj zakres wyrażanych zgód.

**Zapamiętaj! Urzędy, banki, czy inne instytucje nie wysyłają korespondencji e-mail do swoich klientów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji!**

**Będziesz bezpieczny w sieci Internet jeżeli zastosujesz zasadę ograniczonego zaufania i podwyższonej ostrożności.**

**Aby dodatkowo zabezpieczyć się w przypadku korzystania z systemów informatycznych oraz urządzeń mobilnych stosuj też inne zasady przedstawione poniżej:**

1. Nie udostępniaj nikomu swoich haseł i loginów do systemów informatycznych;
2. Stosuj blokady ekranów swoich urządzeń (np. hasło, PIN).;
3. Wpisuj swoje hasło, pin czy login będąc pewnym, że nikt Cię nie nagrywa lub nie widzi tego, co wpisujesz;
4. Unikaj stosowania haseł, które są łatwe do odgadnięcia (np. poprzez powiązanie z Twoją osobą);
5. Regularnie zmieniaj hasła. Stosuj długie hasła. Hasła powinny mieć co najmniej 12 znaków oraz zawierać litery małe i duże, cyfry oraz znaki specjalne;
6. Nie zapisuj haseł na kartkach, w notatniku;
7. Nie powtarzaj hasłeł w różnych systemach informatycznych;
8. Unikaj logowania do systemów z cudzych, niepewnych urządzeń;
9. Nie zapisuj haseł w pamięci przeglądarki;
10. Jeżeli zamierzasz sprzedać lub przekazać komuś swoje urządzenie, upewnij się, że wszystkie twoje dane zostały z niego usunięte;
11. Jeżeli masz taką możliwość, w miejscach publicznych, korzystaj z nakładek prywatyzujących na monitor (również w urządzeniu mobilnym);
12. Instaluj i aktualizuj systemy antywirusowe oraz ochronę sieciową także na swoich urządzeniach mobilnych;
13. Pamiętaj o aktualizacjach aplikacji i systemu operacyjnego w swoim urządzeniu mobilnym.
14. Niezbędne aplikacje instaluj i pobieraj wyłącznie z oficjalnych sklepów z aplikacjami;
15. Nie „klikaj” w linki przesłane w wiadomości SMS lub e-mail, jeśli nie masz pewności, że pochodzą z bezpiecznego i zaufanego źródła;
16. Uważaj na prośby dopłacenia do przesyłek, zapłacenia za zakup dokonany przez internet czy też prośby o pożyczkę, jeśli otrzymałeś SMSa z prośbą o dokończenie procesu zamówienia przesyłki np.: w postaci brakującej kwoty (wymagana dopłata kilku groszy);
17. Jeżeli w danym momencie nie korzystasz z Wi-Fi lub Bluetooth, wyłącz je;
18. tam gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowe (2FA) uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego;
19. wykonuj kopie bezpieczeństwa;
20. podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard szyfrowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarką a serwerem;

1. nie używaj prywatnych kont poczty elektronicznej i komunikatorów do korespondencji służbowej;
2. nie używaj prywatnych komputerów i telefonów do spraw służbowych;
3. nie używaj służbowych komputerów i telefonów do spraw prywatnych (w szczególności do czytania prywatnej poczty

elektronicznej), nie udostępniaj ich członkom rodziny;

4. logując się na konto zawsze sprawdź czy domena danego portalu jest prawidłowa. Domena to nazwa zawierająca się między https://, a pierwszym kolejnym znakiem /;

5. ignoruj wszystkie inne prośby o podanie swojego hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta;

6. używaj opcji automatycznego kasowania wiadomości po upływie określonego czasu – nie da się ukraść czegoś, czego już nie ma.

Po więcej bezpłatnych informacji można zasięgnąć i stale śledzić pod podanym linkiem https://www.gov.pl/web/baza-wiedzy/aktualnosci

Pozostałe (odnośniki do stron) dotyczące cyberbezpieczeństwa: Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl

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

Zgłoszenie incydentu, szkodliwych treści: W sieci udostępniono formularz poprzez który można łatwo i anonimowo zgłosić nielegalne i szkodliwe treści, na które natknąłeś się w sieci: https://incydent.cert.pl/