**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. Skanuj podłączane urządzenia zewnętrzne.
19. Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
20. Kontroluj uprawnienia instalowanych aplikacji.
21. Unikaj z korzystania otwartych sieci Wi-Fi.
22. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarką a serwerem.
23. zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym,
24. aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie),
25. nie otwieraj plików nieznanego pochodzenia,
26. 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,
27. nie używaj niesprawdzonych programów zabezpieczających czy też publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony),
28. co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe - jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami 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
29. sprawdzaj pliki pobrane z internetu za pomocą skanera,
30. staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, lub łatwy zarobek przy rozsyłaniu spamu)- często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia,
31. nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich,
32. nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny,
33. wykonuj kopie zapasowe ważnych danych,
34. 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,

**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.

**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/>

[https://www.lex.pl/cyberbezpieczenstwo-w-jst-dobre-praktyki-dla-samorzadow,8350.html](https://www.lex.pl/cyberbezpieczenstwo-w-jst-dobre-praktyki-dla-samorzadow%2C8350.html)

**Katalog dobrych praktyk cyberbezpieczeństwa w samorządzie to:**

1. **Inwentaryzacja zasobów informacyjnych, ustalenie ich wartości i powiązanych** **procesów**
**Poznanie własnych zasobów i procesów** jest istotnym elementem pracy z nimi. Dzięki temu łatwiej można zauważyć ewentualne nieprawidłowości. Dodatkowo jest to udogodnienie w codziennej pracy i może zwiększyć jej efektywność.
2. **Zorientowanie ochrony na podatności zasobów i procesów (ang. Vulnerabilitydriven security)**
Skoncentrowanie się na własnych podatnościach (słabościach) **przynosi lepsze rezultaty** niż zagrożeniach, które mogą wcale na nas nie oddziaływać. Zorientowanie się wśród swoich słabych stron pomaga również przy realizacji punktu 6. katalogu.
3. **Czyste biurko i ekran**
Jak zauważa Ministerstwo Cyfryzacji w [poradniku stworzonym dla pracowników samorządowych(Nowe okno)(Link do innej strony)](https://sip.lex.pl/komentarze-i-publikacje/poradniki/poradnik-dla-samorzadow-bezpieczny-pracownik-w-sieci-151362202), należy pamiętać, że **własne działania** również **mogą przyczynić** się do obniżenia lub zwiększenia bezpieczeństwa informacyjnego w jednostce samorządu terytorialnego. Czyste biurko, poukładana dokumentacja i przejrzystość posiadanych zasobów zdecydowanie pomogą zachować wymagany poziom bezpieczeństwa oraz ułatwią codzienną pracę.
4. **Ograniczone zaufanie wobec podmiotów zewnętrznych i użytkowanych przez nie systemów**
Zarówno tak, jak na drodze stosujemy zasadę ograniczonego zaufania, tak i w zakresie cyberbezpieczeństwa jest to praktyka niezwykle ważna, mogąca uchronić przed wieloma zagrożeniami. **Nie ufajmy od razu**, sprawdzajmy możliwe i dostępne opcje, aby w jak największym stopniu ograniczyć ryzyko wystąpienia incydentu.
5. **Ochrona “w głąb” (ang. Defense in depth), czyli warstwowość zabezpieczeń i ich spójność pionowa i pozioma**
Ochroną "w głąb" można nazwać, tzw. ochronę pionową. Co oznacza to w praktyce? Ochrona w głąb zakłada, że istnieje **kilka warstw zabezpieczeń**. W przypadku, w którym jedna z nich zawiedzie, zawsze jest kolejna, która zapewnia wystarczający poziom bezpieczeństwa. Działa to jedynie w sytuacji, w której między danymi warstwami nie ma luki bądź niespójnych elementów.
6. **„Najsłabsze ogniwo” (ang. Weakest link in the chain)**
Każdy system jest **tak bezpieczny, jak jego najsłabiej chroniony element.** Poprzez najsłabsze ogniwo możliwe jest ominięcie wszelkich innych stosowanych zabezpieczeń (tzw. backdoor) i należy o tym pamiętać podczas konstruowania systemu bezpieczeństwa.
7. **Minimalne przywileje (ang. Least privilege)**
Ograniczanie przywilejów (uprawnień) tylko do tych, które są **konieczne dla danego pracownika**. Dzięki temu w znaczący sposób obniża się ryzyko wystąpienia incydentu.
8. **Rozdział obowiązków użytkowników (ang. Separation of duties)**
Warto pamiętać, że w przypadku zadań wiążących się z transferem dużych środków finansowych należy wprowadzić mechanizm **wzajemnej kontroli urzędników**. Chroni to nie tylko przed wystąpieniem incydentu, ale również przed błędami pracowników. W przypadku braku użytkownika czuwającego występuje większe **prawdopodobieństwo popełnienia uchybienia.**
9. **Zarządzanie zmianami (ang. Change management)**
Należy pamiętać o ustawieniu odpowiedniej konfiguracji programu (również aktualizacji) czy **wykonywaniu kopii zapasowych.** Takie działania mogą w dużym stopniu uprościć wykonywanie codziennych działań oraz ograniczają możliwość błędu.
10. **Korzystanie z doświadczeń (ang. Learn from experience)**
Uczmy się zarówno **na własnych jak i cudzych błędach**. Wszelkie doświadczenia i praktyki (złe oraz dobre) są ogromną bazą danych wiedzy, która pozwala uniknąć wielu zagrożeń i incydentów.

[https://www.lex.pl/cyberbezpieczenstwo-w-jst-dobre-praktyki-dla-samorzadow,8350.html](https://www.lex.pl/cyberbezpieczenstwo-w-jst-dobre-praktyki-dla-samorzadow%2C8350.html)