

# Cyberbezpieczeństwo

Poniżej dostępne są odnośniki do ostatnich artykułów publikowanych na stronie urzędu dotyczących cyberbezpieczeństwa i ostrzeżeń przed zagrożeniami w sieci.

Zapraszamy też do odwiedzenia strony Niebezpiecznik.pl na której znajdują się porady bezpieczeństwa i aktualne ostrzeżenia.

☐ 14.09.2022 – [Ostrzeżenie przed szkodliwymi wiadomościami sms dot. PGE](#)

☐ 09.09.2022 – [Ostrzeżenie przed szkodliwymi wiadomościami e-mail dot. Biznes.gov.pl](#)

**Informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak zabezpieczyć się przed tymi zagrożeniami**

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa publikujemy informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak zabezpieczyć się przed tymi zagrożeniami.

☐☐ 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, Dz. U. 2020 r., poz. 1369 z dnia 11 sierpnia 2020 r.).

**Najpopularniejsze zagrożenia w cyberprzestrzeni:**

☐ Malware – oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.

☐ Phishing – atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.

- Spear Phishing – bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- Atak typu “Man in the Middle” (MitM) – atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- Trojan – (koń trojański) – oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące – ransomware, szpiegujące – spyware etc.).
- Ransomware – atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
- Atak DoS lub DDoS – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS atakuje z wielu miejsc równocześnie.
- Atak IoT – atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego – przemysłu etc.).
- Data Breaches (naruszenie danych) – atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).
- Malware w aplikacjach telefonów. Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.

### **Sposoby zabezpieczenia się przed zagrożeniami:**

- Aktualizuj oprogramowanie. System operacyjny, aplikacje użytkowe, programy antywirusowe wymagają stałej aktualizacji i baz zagrożeń. Brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu/aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu. Logowanie do e-usług publicznych, bankowości

elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.

□ Stosuj zróżnicowane hasła. Korzystaj z różnych haseł do różnych usług elektronicznych. Nie da się obronić przed atakami używając prostych haseł, takich jak „1234”. Odpowiednie, złożone hasło może ochronić konsumentów przed zagrożeniami cybernetycznymi.

□ Stosuj uwierzytelnianie dwuetapowe. 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.

□ Regularnie zmieniaj hasła.

□ Nie udostępniaj nikomu swoich haseł.

□ Pracuj na najniższych możliwych uprawnieniach użytkownika.

□ Wykonuj kopie bezpieczeństwa. Korzystaj z oddzielnych nośników na kopie. Nie przechowuj kopii wyłącznie na tym samym dysku co kopiowane dane.

□ Skanuj podłączane urządzenia zewnętrzne. Przy podłączeniu urządzenia do laptopa/komputera typu pendrive, karta pamięci, dysk przenośny, smartfon – najpierw zeskanuj nośnik zaktualizowanym oprogramowaniem antywirusowym.

□ Kontroluj uprawnienia instalowanych aplikacji.

□ Unikaj publicznych WiFi. W miarę możliwości, nie korzystaj z publicznych, otwartych (niezabezpieczonych) sieci Wi-Fi, stosowanych w hotelach, pubach, restauracjach do których dostęp ma wiele osób. Jeśli to możliwe, udostępnij Internet LTE ze swojego telefonu poprzez kabel USB lub zabezpieczoną sieć Wi-Fi na swój laptop, zamiast korzystać z publicznego Wi-Fi np.: do logowania w banku. Po zakończeniu, wyłącz udostępniany Internet w telefonie.

□ Sprawdź certyfikat SSL strony. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.

□ Sprawdź domenę strony. Kontroluj nazwę domeny strony, na której podajesz poufne dane. Jeśli strona logowania wygląda

jak strona banku, lecz ma nietypowy adres www, sprawdź czy nie trafiłeś na oszustwo (phishing).

□ Chroń kartę kredytową/bankomatową. Nie udostępniaj nikomu danych karty kredytowej lub bankomatowej w tym PINów, numeru karty, kodu weryfikacyjnego CVV/CVC znajdującego się na odwrocie karty, daty ważności karty. Nie zapisuj PINu na karcie lub przyklejonej karteczce. Stosuj PIN składający się z różnych cyfr rozmieszczonych na całej klawiaturze. Chroń wpisywanie PINu przy operacjach w sklepie, gdzie przebywa dużo osób w kolejce za Tobą.

□ Porównaj treść SMSa z operacją bankową. Przy dokonywaniu przelewów i autoryzacji np.: SMSem, sprawdzaj czy treść z SMSa dotyczy dokładnie tej samej operacji, którą wykonujesz wraz z numerem konta. Jeśli zauważysz nietypowe SMSy typu zmiana numeru telefonu do konta, dodanie urządzenia do logowania, zmiana limitów na karcie – skontaktuj się z bankiem i przerwij dalsze czynności autoryzacji i przepisywania hasła z SMSa.

□ Zadbaj o bezpieczeństwo routera. Ustal silne hasło do swojej sieci Wi-Fi, zmień nazwę sieci Wi-Fi, zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-Fi np. WPA2 lub WPA3, zaktualizuj oprogramowanie routera, wyłącz funkcję szybkiego logowania do sieci przez przycisk WPS na routerze.

□ Szyfruj dyski. Zabezpiecz trudnym hasłem twarde dyski w laptopie, dyski przenośne, pendrivy i karty pamięci.

□ Stosuj sprawdzone oprogramowanie antywirusowe. Subskrybuj dobrej jakości oprogramowanie antywirusowe oraz zaplanuj aktualizacje automatyczne systemu operacyjnego na Twoim urządzeniu.

□ Nie otwieraj plików nieznanego pochodzenia. Zachowaj ostrożność podczas otwierania załączników plików. Na przykład, jeśli otrzymasz wiadomość e-mail z załącznikiem PDF z opisem „zaległa faktura”, nie otwieraj go jeśli zobaczysz, że pochodzi on z nietypowego e-maila, takiego jak ann23452642@gmail.com. Przeskanuj załącznik w serwisie: [www.virustotal.com](http://www.virustotal.com)

□ Uważaj na strony z darmowym oprogramowaniem. Stron, które

oferują darmowe atrakcje (filmiki, muzykę, aplikacje) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.

☐ Zabezpieczaj swoje dane osobowe. Nie zostawiaj poufnych danych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie będą one widoczne dla osób trzecich.

☐ Uważaj na prośby o podanie haseł. Pamiętaj, że żadna instytucja nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji. Nawet pod pretekstem zablokowania konta, naliczenia opłat.

☐ Uważaj na prośby dopłacenia do przesyłek. Jeśli otrzymałeś SMSa z prośbą o dokończenie procesu zamówienia przesyłki np.: w postaci brakującej kwoty (wymagana dopłata kilku groszy), zablokuj nr skąd pochodzi SMS oraz skasuj SMS.

Odnośniki do stron dotyczących cyberbezpieczeństwa:

☐ Poradniki w bazie wiedzy <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>

☐ Publikacje z zakresu cyberbezpieczeństwa: <https://www.cert.pl>

☐ Szczegółowe porady i ostrzeżenia przed zagrożeniami w sieci: <https://niebezpiecznik.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>

☐ Kampania STÓJ. POMYŚL. POŁĄCZ mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: <https://stojpomyslpolacz.pl/stp>

Zgłoszenie incydentu, szkodliwych treści:

☐ Jeżeli chcesz anonimowo i łatwo zgłosić nielegalne i szkodliwe treści, na które natknąłeś się w sieci możesz zrobić to za pomocą tego formularza: <https://incydent.cert.pl/>