**Cyberbezpieczeństwo**

**Zgodnie z art. 22 ust. 1 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy niezbędne informacje w przedmiocie zagadnienia jakim jest cyberbezpieczeństwo.**

Cyberbezpieczeństwo jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

**By przeciwdziałać wystąpieniu zagrożenia w obszarze cyberbezpiczeństwa należy przestrzegać podstawowych zasad, w tym m.in.:**

* Pamiętaj, aby zawsze mieć aktualny system operacyjny oraz pozostałe oprogramowanie.
* Stosuj szyfrowanie w urządzeniach mobilnych, koniecznie ustaw PIN lub w inny sposób zabezpiecz dostęp do tych urządzeń.
* Stosuj szyfrowanie korzystając z przenośnych nośnikach danych.
* Chroń swoje urządzenia używając programów antywirusowych.
* Nie otwieraj podejrzanych wiadomości e-mail, załączników do tych wiadomości i linków w nich zawartych.
* Nie ufaj wiadomościom SMS i telefon z informacjami o komiczności dokonania zaległych płatności, nieodebranych niezamówionych przesyłkach, itp.
* Nie instaluj aplikacji z nieznanych i niezaufanych źródeł.
* Stosuj hasła o wysokim poziomie skomplikowania, regularnie zmieniaj hasła, nie stosuj tych samych haseł w różnych serwisach.
* Stosuj uwierzytelnianie dwuskładnikowe.
* Nie korzystaj z ogólnodostępnych sieci Wi-Fi.
* Przed wpisaniem danych do formularza zastanów się, jak się na nim znalazłeś i jaki jest zakres danych, które masz podać. Być może jesteś na stronie przygotowanej przez przestępców. Jeśli adres strony lub jakikolwiek jej element budzą Twoje wątpliwości – przerwij czynność i natychmiast zakończ działania.
* Przed zakupem sprawdź, od kogo kupujesz towar, jak długo istnieje dana firma, gdzie ma siedzibę, czy możesz dodzwonić się na infolinię sklepu, czy odpisują na wiadomości oraz jakie opinie wystawili inni kupujący.
* Nie ujawniaj żadnych danych, dopóki nie upewnisz się z kim rozmawiasz. Nie ufaj nieznanym rozmówcom.
* Uważnie czytaj wszystkie wyświetlane na stronach komunikaty, nie wyrażaj zgody jeżeli nie przeczytałeś całej treści komunikatu, lub masz jakiekolwiek wątpliwości.

**Zachęcamy do zgłaszania incydentów cyberbezpieczeństwa, być może uchroni to inne osoby przed zagrożeniem:**



**Zachęcamy również do śledzenia bieżących komunikatów dot. cyberbezpieczeństwia:**

* [Podatność w oprogramowaniu Apereo CAS](https://cert.pl/posts/2023/11/CVE-2023-4612/)

3 listopada 2023

W oprogramowaniu Apereo Central Authentication Service wykryto podatność pozwalającą na ominięcie wieloskładnikowego uwierzytelnienia (CVE-2023-4612).

* [Aktywnie wykorzystywana krytyczna podatność w oprogramowaniu CISCO IOS XE (CVE-2023-20198)](https://cert.pl/posts/2023/10/cisco-cve-2023-20198/)

20 października 2023

Firma Cisco opublikowała informację o krytycznej podatności CVE-2023-20198 w funkcjonalności Web User Interface oprogramowania Cisco IOS XE. Luka umożliwia nieautoryzowanemu złośliwemu użytkownikowi utworzenie konta administratora z poziomu interfejsu użytkownika i przejęcie kontroli nad urządzeniem docelowym.

* [Podatność w oprogramowaniu SmodBIP](https://cert.pl/posts/2023/10/CVE-2023-4837/)

10 października 2023

W oprogramowaniu SmodBIP wykryto podatność CSRF (CVE-2023-4837).

* [Podatność w oprogramowaniu Uptime DC](https://cert.pl/posts/2023/10/CVE-2023-4997/)

5 października 2023

W oprogramowaniu UptimeDC firmy ProIntegra S.A wykryto podatność pozwalającą na eskalację uprawnień (CVE-2023-4997).

* [CERT Polska poprawia bezpieczeństwo poczty elektronicznej](https://cert.pl/posts/2023/09/bezpiecznapoczta/)

15 września 2023

W CERT Polska stale pracujemy nad narzędziami które poprawiają bezpieczeństwo użytkowników internetu w Polsce. Właśnie dlatego stworzyliśmy serwis bezpiecznapoczta.cert.pl, którego celem jest ochrona użytkowników poczty elektronicznej i ułatwienie instytucjom sprawdzenia poprawności konfiguracji mechanizmów podnoszących jej bezpieczeństwo.

* [Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej](https://cert.pl/posts/2023/09/uznke/)

12 września 2023

25 sierpnia została ogłoszona ustawa z dnia 28 lipca 2023r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703)

* [Podatność w bibliotece lua-http](https://cert.pl/posts/2023/09/CVE-2023-4540/)

5 września 2023

CERT Polska otrzymał zgłoszenie o podatności w bibliotece lua-http i nadał jej numer CVE-2023-4540.

* [Wakacyjne oszustwo – nowa metoda cyberprzestępców](https://cert.pl/posts/2023/08/wakacyjne-oszustwo/)

4 sierpnia 2023

Wakacje to czas wyjazdów przede wszystkim dzieci i młodzieży. Poza domem nietrudno o pechowe przygody z telefonem, takie jak zagubienie czy zniszczenie smartfona. Jeśli dziecko znajdzie się w takiej sytuacji, dość prawdopodobne jest, że będzie się kontaktować z rodzicami z innego numeru i na tym właśnie opiera się schemat opisywanego przez nas oszustwa. Bądźcie ostrożni […]

* [Podatność w module WebInterface oprogramowania Telwin SCADA](https://cert.pl/posts/2023/08/CVE-2023-0956/)

3 sierpnia 2023

W module WebInteraface oprogramowania Telwin SCADA CERT Polska wykrył podatność typu Path Traversal (CVE-2023-0956).

* [Lista Ostrzeżeń przed niebezpiecznymi stronami – szkic nowej wersji specyfikacji](https://cert.pl/posts/2023/08/hole-v2-rfc/)

3 sierpnia 2023

Nasza Lista Ostrzeżeń obchodziła w tym roku swoje trzecie urodziny. W tym czasie udało nam się ograniczyć skutki wielu różnych kampanii phishingowych celujących w polskich użytkowników Internetu. W odpowiedzi na zmieniający się krajobraz zagrożeń postanowiliśmy wprowadzić parę zmian w działaniu naszej listy, które pozwolą nam lepiej chronić użytkowników. Zapraszamy do zapoznania się z proponowanymi zmianami […]

*Źródło komunikatów:*[*Cert.pl*](https://cert.pl/)

**Polecamy również specjalistyczne serwisy internetowe poświęcone cyberbezpiczeństwu, w tym m.in.:**

* <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
* [https://niebezpiecznik.pl](https://niebezpiecznik.pl/)
* [https://zaufanatrzeciastrona.pl](https://zaufanatrzeciastrona.pl/)