

CYBERBEZPIECZEŃSTWO

W związku z realizacją zadań publicznych oraz obowiązkami wynikającymi z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, **Żłobek Gminny Bobo w Piławie Górnej** udostępnia informacje pozwalające użytkownikom usług publicznych na zrozumienie cyberzagrożeń oraz stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług. W praktyce dotyczy to ochrony danych, urządzeń, kont użytkowników, poczty elektronicznej, stron internetowych, systemów informatycznych oraz bezpiecznego korzystania z usług cyfrowych.

Najczęstsze cyberzagrożenia

Do najczęściej występujących zagrożeń w cyberprzestrzeni należą:

1. **Phishing** – fałszywe wiadomości e-mail, SMS lub komunikaty, których celem jest wyłudzenie danych, haseł, numerów kart płatniczych albo nakłonienie użytkownika do kliknięcia w niebezpieczny link.
2. **Smishing i vishing** – oszustwa prowadzone przez SMS lub rozmowy telefoniczne, w których przestępcy podszywają się np. pod bank, urząd, firmę kurierską, operatora płatności lub inną zaufaną instytucję.
3. **Złośliwe oprogramowanie** – wirusy, trojany, ransomware i inne programy, które mogą szyfrować pliki, kraść dane albo przejmować kontrolę nad urządzeniem.
4. **Fałszywe strony internetowe** – strony podszywające się pod banki, urzędy, sklepy internetowe, portale płatności lub znane serwisy.
5. **Kradzież danych logowania** – przejęcie loginu i hasła do poczty elektronicznej, bankowości elektronicznej, profilu zaufanego, mediów społecznościowych albo systemów służbowych.
6. **Nieuprawniony dostęp do danych** – sytuacje, w których osoba nieupoważniona uzyskuje dostęp do informacji, dokumentów, korespondencji lub systemów informatycznych.
7. **Deinformacja i fałszywe komunikaty** – rozpowszechnianie nieprawdziwych informacji, które mogą wprowadzać użytkowników w błąd lub nakłaniać do niebezpiecznych działań.

Jak chronić się przed cyberzagrożeniami

Aby zwiększyć swoje bezpieczeństwo w cyberprzestrzeni:

1. Nie klikaj w podejrzone linki otrzymane w wiadomościach e-mail, SMS, komunikatorach lub mediach społecznościowych.
2. Sprawdzaj adres strony internetowej, na której podajesz dane. Szczególną ostrożność zachowaj przy logowaniu do bankowości elektronicznej, profilu zaufanego, ePUAP, e-Doręczeń oraz innych usług publicznych.
3. Nie podawaj loginów, haseł, numerów PESEL, danych kart płatniczych ani kodów autoryzacyjnych osobom kontaktującym się telefonicznie, e-mailowo lub przez SMS.
4. Stosuj silne i unikalne hasła. Nie używaj tego samego hasła w wielu serwisach.

5. Włącz uwierzytelnianie wieloskładnikowe, jeżeli dana usługa daje taką możliwość.
6. Regularnie aktualizuj system operacyjny, przeglądarkę internetową, program antywirusowy oraz aplikacje.
7. Instaluj aplikacje wyłącznie z oficjalnych i zaufanych źródeł.
8. Nie otwieraj załączników od nieznanych nadawców, zwłaszcza jeżeli wiadomość wywołuje presję czasu, straszy konsekwencjami lub obiecuje szybki zysk.
9. Regularnie wykonuj kopie zapasowe ważnych danych.
10. Korzystaj z zabezpieczonej sieci Wi-Fi i unikaj logowania do ważnych usług przez publiczne, niezabezpieczone sieci.
11. W przypadku podejrzenia oszustwa zachowaj wiadomość, zrzut ekranu, adres strony internetowej lub inne informacje, które mogą pomóc w wyjaśnieniu sprawy.

Bezpieczny kontakt z podmiotem publicznym

Podmiot Publiczny nigdy nie żądać przekazania hasła, pełnych danych logowania, kodów autoryzacyjnych ani danych karty płatniczej za pośrednictwem poczty elektronicznej, SMS lub rozmowy telefonicznej.

W przypadku otrzymania podejrzanej wiadomości, która wygląda jak korespondencja od naszej placówki, należy zachować szczególną ostrożność i skontaktować się z nami oficjalnym kanałem komunikacji dostępnymi w zakładce kontakt.

Zgłaszanie incydentów i podejrzanых wiadomości

Jeżeli zauważysz podejrzaną wiadomość, fałszywą stronę internetową, próbę wyłudzenia danych, naruszenie bezpieczeństwa lub inne zdarzenie mogące mieć wpływ na cyberbezpieczeństwo, możesz zgłosić sprawę do właściwych instytucji.

Podejrzane wiadomości SMS zawierające linki można przekazywać do CERT Polska pod numer **8080**. Podejrzane incydenty można zgłaszać również przez formularz internetowy CERT Polska.

W przypadku zdarzeń dotyczących usług, systemów lub korespondencji naszego podmiotu, prosimy również o kontakt z nami.

Zgłoszenie powinno zawierać, jeżeli to możliwe:

- opis zdarzenia,
- datę i godzinę wystąpienia,
- adres podejrzanej strony internetowej,
- treść podejrzanej wiadomości lub zrzut ekranu,
- informację, czy kliknięto link, pobrano załącznik albo podano dane.

Przydatne źródła wiedzy o cyberbezpieczeństwie

Zachęcamy do korzystania z materiałów edukacyjnych, komunikatów i ostrzeżeń publikowanych przez właściwe instytucje zajmujące się cyberbezpieczeństwem:

- **CERT Polska / CSIRT NASK** – aktualne ostrzeżenia, poradniki oraz zgłaszanie incydentów: <https://cert.pl> oraz <https://incydent.cert.pl>. Zespołowi CERT Polska powierzono obowiązki CSIRT NASK wynikające z ustawy o krajowym systemie cyberbezpieczeństwa.
- **Ministerstwo Cyfryzacji** – informacje, komunikaty i baza wiedzy dotycząca cyberbezpieczeństwa: <https://www.gov.pl/web/cyfryzacja>. Na stronie Ministerstwa Cyfryzacji znajdują się również informacje o zespołach CSIRT poziomu krajowego.
- **Baza wiedzy Ministerstwa Cyfryzacji** – materiały edukacyjne dotyczące bezpiecznego korzystania z internetu: <https://www.gov.pl/web/baza-wiedzy>.
- **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego: <https://csirt.gov.pl>.
- **Zgłoszenie incydentu do CSIRT GOV**: <https://csirt.gov.pl/cer/zgloszenie-incydentu>. CSIRT GOV wskazuje możliwość zgłaszania incydentów m.in. przez System S46 albo formularz na stronie CSIRT GOV.

Zgłaszanie podejrzanych wiadomości SMS

Podejrzane wiadomości SMS zawierające linki lub treści mogące wskazywać na próbę oszustwa można przekazać do **CERT Polska / CSIRT NASK** na numer **8080**. Przekazanie podejrzanego SMS-a na numer 8080 jest bezpłatne na terenie Polski.

Podejrzane wiadomości e-mail, fałszywe strony internetowe oraz inne incydenty można zgłaszać przez formularz: <https://incydent.cert.pl>.

Podstawa prawna

Informacja została opublikowana w celu realizacji obowiązku wynikającego z **art. 9 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**, zgodnie z którym podmiot kluczowy lub podmiot ważny zapewnia użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez udostępnianie informacji na swojej stronie internetowej.