CYBERBEZPIECZEŃSTWO
WAŻNE INFORMACJE DLA PRACOWNIKÓW, PACJENTÓW i KLIENTÓW
SP ZOZ MSWiA w RZESZOWIE

Cyberbezpieczeństwo to odporność systemów informacyjnych (np. komputera, telefonu, Internetu) na działania, które mogą:

- ujawnić Twoje dane,
- zmienić lub zniszczyć informacje,
- zablokować dostęp do usług,
- podszyć się pod Ciebie lub inne osoby.
- Najczęstsze zagrożenia w sieci

Zagrożenia:

Phishing to Fałszywe e-maile/SMS-y podszywające się pod bank, szkołę, urząd.

Uważaj na adresy e-mail i błędy w wiadomościach. Nie klikaj podejrzanych linków.

Malware to złośliwe oprogramowanie (wirusy, robaki). Używaj aktualnego antywirusa. Nie instaluj programów z nieznanych źródeł.

Ransomware szyfruje Twoje dane i żąda okupu za ich odzyskanie. Rób kopie zapasowe i aktualizuj system.

Man-in-the-Middle Ktoś przechwytuje dane przesyłane między Tobą a serwisem. Korzystaj tylko ze stron z certyfikatem SSL (https://).

Cross-site scripting (XSS) Kod umieszczany na stronie, który może ukraść Twoje dane. Nie klikaj podejrzanych linków i reklam.

DDoS to atak na serwis internetowy, by go zablokować. Nie dotyczy zwykłych użytkowników, ale warto znać zjawisko.

Malvertising to Wirus ukryty w reklamie nawet na znanej stronie.

Używaj blokerów reklam i sprawdzonych przeglądarek

Jak się chronić w sieci? Zasady dla każdego użytkownika

- Zainstaluj i aktualizuj program antywirusowy
- Aktualizuj system operacyjny i aplikacje
- Nie otwieraj podejrzanych e-maili ani załączników
- Sprawdzaj adresy stron – powinny zaczynać się od „https://”
- Nie podawaj haseł i danych osobowych w wiadomościach e-mail
- Nie wchodź na nieznane strony oferujące „darmowe atrakcje”
- Chroń wizerunek dziecka i swój w Internecie
- Regularnie wykonuj kopie zapasowe danych
- Włącz zaporę sieciową (firewall)

Gdzie zgłosić incydent lub podejrzaną wiadomość?

- CERT Polska: *https://incydent.cert.pl*
- Aplikacja mObywatel – funkcja *„Bezpiecznie w sieci”*
- Nielegalne treści (rasizm, pornografia dziecięca): *https://dyzurnet.pl*
- SMS z podejrzanym linkiem? Wyślij go za darmo na 8080

Polecane źródła wiedzy o cyberbezpieczeństwie

- Ministerstwo Cyfryzacji: *gov.pl/cyberbezpieczenstwo*
- NASK – Naukowa i Akademicka Sieć Komputerowa: *nask.pl*
- UODO – Urząd Ochrony Danych Osobowych: *uodo.gov.pl*

Przydatne publikacje edukacyjne

- Poradnik dla rodziców – *Szkodliwe treści w Internecie*
- *https://akademia.nask.pl/publikacje/Szkodliwe%20tre%C5%9Bci%20w%20internecie_www.pdf*

Poradnik – Jak chronić dane?

- *https://uodo.gov.pl/pl/138/3414*
- *Wizerunek dziecka w Internecie – publikować czy nie?*
- *https://uodo.gov.pl/pl/138/3720*

PAMIĘTAJ!

Żaden bank, urząd nie prosi telefonicznie lub e-mailowo o podanie hasła, loginu ani numeru karty.

Bądź czujny – w sieci - myśl tak, jak w realnym świecie: jeśli coś wygląda podejrzanie, najprawdopodobniej takie jest.