Cyberbezpieczeństwo

INFORMACJE OGÓLNE.

Szanowni Państwo,

uprzejmie informujemy, że Wojewódzki Szpital Zespolony im. dr. Romana Ostrzyckiego w Koninie decyzją Ministerstwa Zdrowia został uznany za **operatora usług kluczowych** w zakresie:

Dane Pełnomocnika ds. Cyberbezpieczeństwa: Pan Karol Michałkiewicz tel. 572-327-126

- Udzielania świadczenia opieki zdrowotnej przez podmiot leczniczy.
- Obrotu i dystrybucji produktów leczniczych.

DOBRE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO.

- **BEZPIECZNE KORZYSTANIE Z SIECI INTERNET.**
  - Podstawowym elementem bezpieczeństwa w sieci Internet jest zastosowanie zasady **ograniczonego zaufania i podwyższonej ostrożności.**
  - Pamiętamy o zainstalowaniu i aktualizowaniu programu ochrony przed złośliwym oprogramowaniem.
  - Aktualizujemy system operacyjny i aplikacje użytkowe.
  - Nie odwiedzamy stron powszechnie uznawanych za niebezpieczne.
  - Nie klikamy na linki do nieznanych stron internetowych.
  - Zwracamy uwagę na komunikaty programu antywirusowego i przeglądarek internetowych.
  - Ograniczamy do minimum podawanie swoich danych osobowych.
- **BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ.**
  - Zwracamy szczególną uwagę na poprawność adresata (adresatów) poczty elektronicznej.

- Zwracamy szczególna uwagę na nadawcę wiadomości.
- Nie klikamy na linki umieszczone w załączniku poczty.
- W przypadku przesyłania ważnych (wrażliwych) wiadomości stosujemy mechanizmy szyfrowania (np. zabezpieczony hasłem plik *.zip, niekomercyjne aplikacje szyfrujące).

BEZPIECZEŃSTWO URZĄDZEŃ MOBILNYCH.

- Zabezpieczamy hasłem dostęp do urządzenia :
  - Laptop hasło do BIOS/UEFI, hasło do systemu operacyjnego.
  - Smartphone – hasło do PIN, drugi poziom zabezpieczeń (hasło obrazkowe, biometryka).
- Aktualizujemy system operacyjny urządzenia oraz aplikacje użytkowe.
- Instalujemy oprogramowanie antywirusowe.
- Korzystamy z możliwości szyfrowania plików, katalogów lub całego dysku.
- W przypadku aplikacji na smartphone sprawdzamy do jakich usług aplikacja będzie miała dostęp oraz jaka jest wiarygodność producenta aplikacji.
- Regularnie tworzymy kopie zapasowe ważnych danych.
- Zachowujemy szczególną ostrożność przy korzystaniu z otwartych, publicznych sieci wifi.
- Szczególna uwagę zwracamy na podejrzane SMS lub MMS.

BEZPIECZNE HASŁA.

- Przy tworzeniu hasła wykorzystujemy cztery typy znaków (wielkie i małe litery, cyfry i znaki specjalne).
- Długość hasła powinna wynosić min. 8 znaków im dłuższe hasło tym częstotliwość zmiany może być mniejsza.
- Nie tworzymy haseł składających się z charakterystycznych cech jak np. imię, nazwisko, data urodzenia, imię psa, kota itp.
- Nie zapisujemy haseł na karteczkach dostępnych dla osób postronnych.
- Nie przesyłamy SMS lub za pomocą poczty elektronicznej haseł do systemów bankowości elektronicznej. Banki nigdy nie proszą o przesłanie hasła.
- Możemy wykorzystywać aplikacje typu menadżer haseł. Ograniczamy się do zapamiętania tylko hasła do menadżera.

- Drukuj

- PDF