CSIRT CEZ

Bezpieczne korzystanie z internetu

w ramach zaleceń w zakresie podstaw bezpieczeństwa i ochrony danych dla użytkowników w sektorze ochrony zdrowia

01. Weryfikacja witryn internetowych

- Sprawdź, czy adres strony (URL) wygląda autentycznie. Unikaj stron z literówkami, podejrzanymi rozszerzeniami lub imitacją znanych nazw.
- Oceń wygląd i zawartość strony. Na oszustwo mogą wskazywać: brak aktualizacji grafiki, błędy językowe czy nieaktywne przyciski na stronie.
- Bądź czujny w przypadku wyskakujących okien proszących o ponowne dane logowania. To mogą być fałszywe strony.
- W razie wątpliwości dotyczących wiarygodności witryny skonsultuj się z działem bezpieczeństwa.

02. Ustawienia przeglądarek

- Regularnie aktualizuj przeglądarkę i wtyczki.
- Wyłącz zbędne rozszerzenia i wtyczki, ograniczaj liczbę dodatków tylko do tych, które są konieczne do pracy.
- Odrzucaj prośby o instalację nieznanych rozszerzeń.
- Wyłącz automatyczne zapisywanie haseł w przeglądarce.
- Włącz blokadę wyskakujących okien.
- Włącz ochronę przed śledzeniem.
- Ogranicz dostęp do informacji o lokalizacji.

CSIRT CEZ

03. Media społecznościowe

- Nie korzystaj z prywatnych mediów społecznościowych na urządzeniach służbowych.
- Nie publikuj i nie przesyłaj informacji dotyczących służbowych danych ani danych pacjentów poprzez komunikatory takie jak np. Messenger czy WhatsUp.
- Korzystaj z prywatnych ustawień profilu, ogranicz widoczność postów i danych osobowych do zaufanego grona.
- Weryfikuj zaproszenia i prośby o dodanie do znajomych. Nie akceptuj pochopnie próśb od nieznanych osób, które mogą podszywać się pod współpracowników.
- Nie udostępniaj zrzutów ekranu z systemów służbowych.
- Informuj dział IT o podejrzanych aktywnościach (np. próbach wyłudzenia danych w wiadomościach prywatnych).

04. Publiczne sieci Wi-Fi

- Korzystaj z VPN w miejscach publicznych (kawiarnie, lotniska, hotele), jeśli zamierzasz łączyć się z systemami służbowymi.
- W miarę możliwości używaj tetheringu (udostępnionego Internetu z telefonu), zamiast łączyć się z przypadkowymi punktami dostępowymi.
- Nigdy nie loguj się do poczty lub systemów służbowych w nieszyfrowanych sieciach otwartych.
- Weryfikuj nazwę hotspotów, aby przypadkowo nie połączyć się z fałszywą siecią o bardzo podobnej nazwie.
- Wyłącz automatyczne łączenie z nieznanymi sieciami Wi-Fi, by uniknąć przypadkowego połączenia do niebezpiecznego punktu dostępowego.

CSIRT CEZ