SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ
CENTRALNY SZPITAL KLINICZNY
UNIWERSYTETU MEDYCZNEGO W ŁODZI

CYBERBEZPIECZEŃSTWO W SZPITALU

SZKOLENIE PODNOSZĄCE ŚWIADOMOŚĆ CYBERBEZPIECZEŃSTWA

DLACZEGO TO WAŻNE?

Bezpieczeństwo pacjentów zależy także od bezpieczeństwa IT.

Szpital to nie tylko miejsce leczenia.

To również:

- dane osobowe pacjentów,
- dokumentacja medyczna,
- wyniki badań,
- systemy diagnostyczne, laboratoryjne,
- aparatura medyczna podłączona do sieci,
- systemy finansowe.

DLACZEGO TO WAŻNE?

Cyberatak może spowodować:

- zagrożenie życia pacjentów,
- utratę danych,
- odwołanie zabiegów,
- opóźnienia leczenia,
- niedostępność dokumentacji.

DLACZEGO SZPITALE SĄ CELEM CYBERPRZESTĘPCÓW?

- duża liczba użytkowników,
- bardzo cenne dane (dane medyczne są znacznie cenniejsze od numerów kart płatniczych),
- częste korzystanie z poczty elektronicznej,
- wiele urządzeń medycznych,
- konieczność ciągłej pracy 24/7,
- presja czasu.

NAJCZĘSTSZE ZAGROŻENIA

- phishing,
- ransomware,
- złośliwe oprogramowanie,
- socjotechnika, fałszywe telefony,
- kradzież haseł,
- nieautoryzowany dostęp,
- wyciek danych,
- zainfekowane pendrive’y.

CZYM JEST PHISHING

Phishing to próba podszycia się pod zaufaną osobę lub instytucję i wyłudzenia:

- loginów, haseł,
- kodów MFA,
- danych pacjentów,
- pieniędzy.

Najczęściej odbywa się przez:

- e-mail, komunikatory
- telefon, SMS.

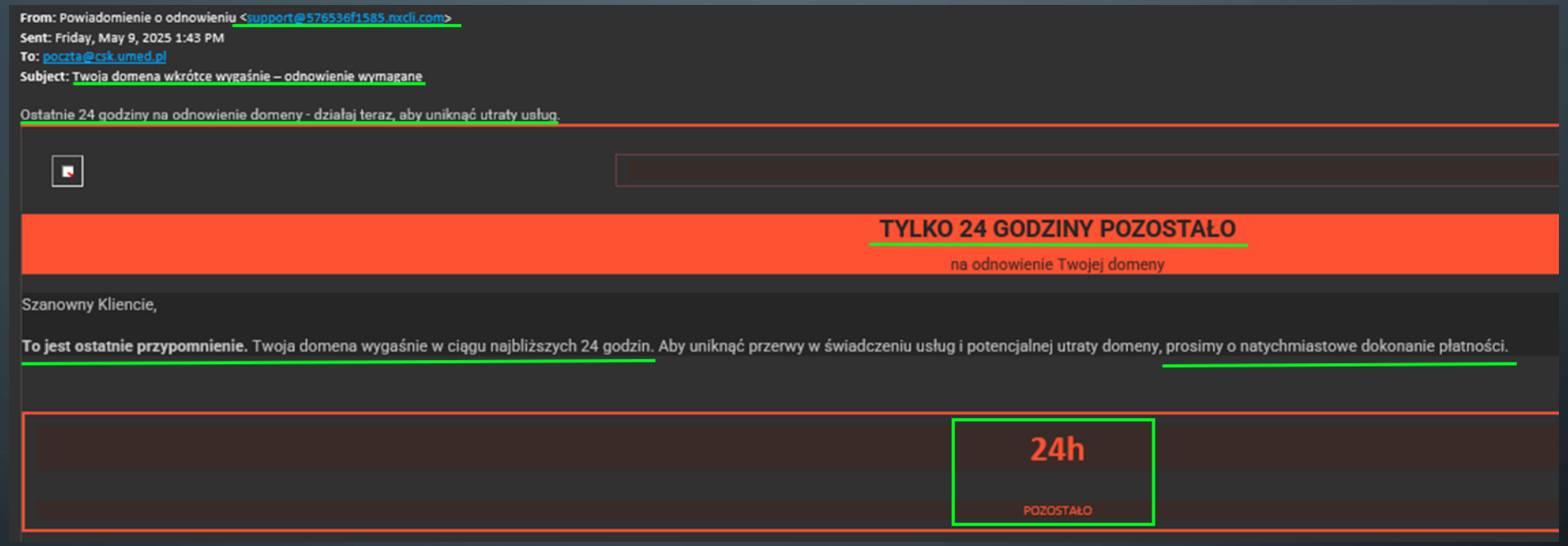
JAK ROZPOZNAĆ PHISHING?

Zwróć uwagę na:

- błędy językowe,
- presję czasu,
- groźby,
- nieznanego nadawcę, nietypowy adres e-mail,
- dziwne linki, nieoczekiwane załączniki.

Nigdy nie klikaj automatycznie!

PRZYKŁAD WIADOMOŚCI PHISHINGOWEJ



Co powinno wzbudzić podejrzenia:

- presja czasu (!),
- nieznany adres nadawcy,
- brak podpisu.

RANSOMWARE

Ransomware - wirus blokujący dostęp do danych i żądający okup - to złośliwe oprogramowanie:

- szyfruje pliki,
- blokuje komputery,
- uniemożliwia pracę.

Przestępcy żądają okupu.

Zapłacenie okupu nie gwarantuje odzyskania danych.

JAK DOCHODZI DO INFEKCJI?

- kliknięcie w link,
- zeskanowanie kodu QR,
- otwarcie załącznika,
- pobranie programu,
- niezaktualizowany komputer,
- pendrive.

OCHRONA DANYCH PACJENTÓW

Każdy pracownik odpowiada za bezpieczeństwo informacji.

Nie wolno:

- przekazywać danych osobom nieupoważnionym,
- fotografować dokumentacji,
- pozostawiać dokumentacji bez nadzoru,
- przesyłać danych prywatnym e-mailem.

RODO W PRAKTYCE – BEZPIECZNE PRZETWARZANIE I PRZESYŁANIE DANYCH

Pamiętaj:

- sprawdzaj odbiorcę wiadomości przed wysłaniem,
- udostępniaj dane wyłącznie osobom upoważnionym,
- zamykaj dokumentację po zakończeniu pracy,
- blokuj komputer podczas każdej nieobecności,
- niszcz wydruki zawierające dane zgodnie z obowiązującymi procedurami,
- nie przesyłaj danych medycznych za pośrednictwem prywatnych kont e-mail lub nieautoryzowanych komunikatorów.

SZYFROWANIE PLIKÓW

Jeżeli przesyłane dokumenty zawierają dane osobowe lub dokumentację medyczną:

- zabezpiecz plik hasłem lub zastosuj szyfrowanie zgodne z procedurami obowiązującymi w szpitalu,
- upewnij się, że plik został zaszyfrowany przed wysłaniem.

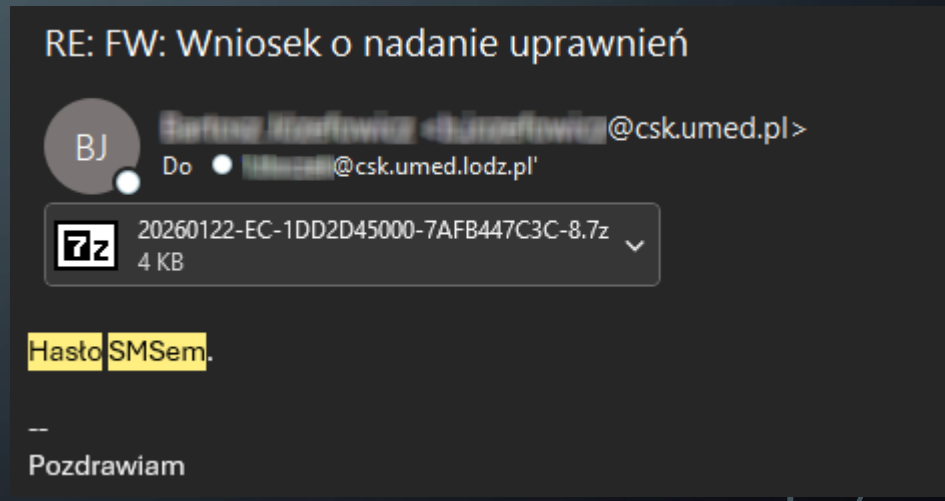
PRZEKAZYWANIE HASŁA

Nigdy nie wysyłaj hasła w tej samej wiadomości, do której dołączono zaszyfrowany plik.

Hasło należy przekazać innym, niezależnym kanałem komunikacji, np.:

- telefonicznie, w wiadomości SMS,
- za pomocą zatwierdzonego komunikatora służbowego,
- osobiście.

Przykład dobrej praktyki:



Pamiętaj: samo ustawienie hasła nie zapewnia bezpieczeństwa,

jeśli hasło będzie przekazane tym samym kanałem co zaszyfrowany plik.

HASŁA

Dobre hasło powinno:

- składać się z minimum 14 znaków,
- zawierać litery, cyfry, znaki specjalne.

Nigdy nie używaj:

- swojego imienia/nazwiska,
- daty urodzenia,
- nazwy szpitala,
- prostych sekwencji.

www.gov.pl

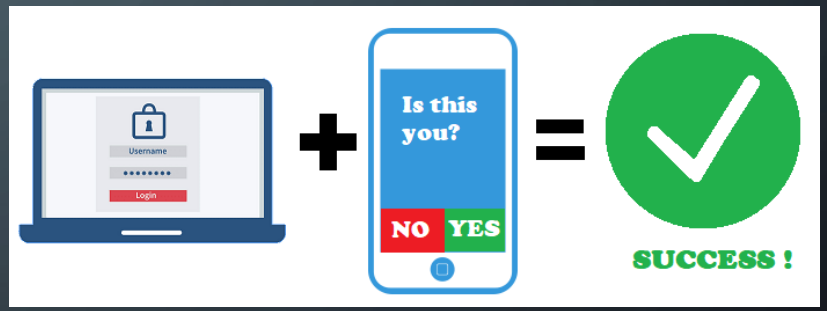
UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)

MFA (dodatkowe potwierdzenie logowania, np. kod SMS) oznacza logowanie przy użyciu:

- hasła,
- kodu wysyłanego SMSem,
- aplikacji,
- klucza bezpieczeństwa.

Korzyści:

- znacznie utrudnia przejęcie konta.



www.eduhk.hk

BEZPIECZNA POCZTA ELEKTRONICZNA

Przed otwarciem wiadomości zawsze sprawdź:

- nadawcę, jego adres e-mail,
- temat wiadomości,
- linki znajdujące się w treści,
- załączniki.

Nie otwieraj:

- nieoczekiwanych załączników,
- plików z nieznanych źródeł,
- podejrzanych linków.

ZGŁASZANIE PODEJRZANYCH WIADOMOŚCI

Jeżeli wiadomość e-mail wzbudza Twoje wątpliwości:

- nie otwieraj załączników,
- nie klikaj odnośników,
- nie odpowiadaj na wiadomość,
- nie przekazuj jej innym pracownikom.

Niezwłocznie zgłoś podejrzaną wiadomość do Działu IT zgodnie z obowiązującą w szpitalu procedurą (np. poprzez dedykowany adres e-mail lub system zgłoszeń).

ZGŁASZANIE PODEJRZANYCH WIADOMOŚCI

Jeżeli przypadkowo kliknąłeś link lub otworzyłeś załącznik:

- natychmiast poinformuj Dział IT,
- opisz, jakie działania zostały wykonane,
- nie próbuj samodzielnie usuwać skutków zdarzenia.

Pamiętaj: szybkie zgłoszenie podejrzanej wiadomości może zapobiec rozprzestrzenieniu się ataku i ochronić innych pracowników oraz dane pacjentów.

ZASADA CZYSTEGO BIURKA

Po zakończeniu pracy:

- schowaj dokumenty,
- zamknij szafki,
- usuń wydruki,
- wyloguj się lub zablokuj komputer.

www.x.com

ZASADA CZYSTEGO EKRANU

Nigdy nie zostawiaj odblokowanego komputera.

Żeby zablokować komputer naciśnij klawisze:

- **Windows + L**

Pamiętaj: Zablokowanie komputera zajmuje zaledwie chwilę, a skutecznie chroni dane pacjentów przed dostępem osób nieuprawnionych. Nawet krótka nieobecność przy stanowisku pracy może zostać wykorzystana do odczytania, skopiowania lub zmodyfikowania informacji znajdujących się na ekranie.

BEZPIECZNA PRACA ZDALNA I KORZYSTANIE Z URZĄDZEŃ MOBILNYCH

Praca zdalna oraz dostęp do systemów szpitalnych spoza placówki wymagają zachowania szczególnej ostrożności.

Zasady bezpiecznej pracy zdalnej:

- korzystaj wyłącznie z urządzeń służbowych dopuszczonych przez Dział IT,
- nie używaj publicznych sieci Wi-Fi (np. w kawiarniach, hotelach czy na dworcach); w razie potrzeby korzystaj z bezpiecznego hotspotu z telefonu służbowego,
- nie zapisuj dokumentacji medycznej ani danych pacjentów na prywatnych komputerach, dyskach czy w nieautoryzowanych usługach chmurowych,
- nie udostępniaj komputera służbowego członkom rodziny ani osobom postronnym,
- zawsze blokuj ekran po odejściu od urządzenia i wyloguj się po zakończeniu pracy.

KORZYSTANIE Z URZĄDZEŃ MOBILNYCH

- zabezpiecz telefon lub tablet kodem PIN, hasłem lub biometrią,
- nie instaluj aplikacji z nieznanych źródeł,
- regularnie aktualizuj system operacyjny i aplikacje,
- w przypadku utraty lub kradzieży urządzenia służbowego niezwłocznie zgłoś zdarzenie do Działu IT oraz swojemu przełożonemu.

Pamiętaj: bezpieczeństwo danych pacjentów obowiązuje niezależnie od miejsca wykonywania pracy. Praca poza szpitalem wymaga zachowania takich samych standardów ochrony informacji, jak praca na terenie placówki.

INŻYNIERIA SPOŁECZNA

Cyberprzestępca może:

- zadzwonić,
- podać się za informatyka, lekarza lub za dyrekcję,
- poprosić o podanie danych lub hasła.

Nigdy nie podawaj hasła ani danych przez telefon! Zawsze weryfikuj tożsamość rozmówcy.

CO ZROBIĆ PO ZAUWAŻENIU INCYDENTU?

1. Nie panikuj.
2. Zgłoś do IT.
3. Odłącz komputer od sieci/Internetu.
4. Nie wyłączaj komputera.
5. Nie usuwaj śladów.

JAK ZGŁASZAĆ INCYDENTY?

Natychmiast poinformuj:

- dział IT,
- Administratora Systemów,
- Inspektora Ochrony Danych (jeżeli dotyczy danych osobowych),
- przełożonego.

Szybkie zgłoszenie umożliwia Działowi IT podjęcie działań ograniczających rozprzestrzenianie się zagrożenia i minimalizujących jego skutki.

10 ZASAD CYBERHIGIENY

1. Blokuj komputer.
2. Używaj silnych haseł.
3. Korzystaj z MFA (dwuetapowej autentykacji).
4. Aktualizuj oprogramowanie.
5. Nie klikaj podejrzanych linków.
6. Nie otwieraj podejrzanych załączników.
7. Chroń dane pacjentów.
8. Nie używaj prywatnych pendrive'ów.
9. Zgłaszaj incydenty.
10. Myśl, zanim klikniesz.

LINK DO QUIZU

https://forms.cloud.microsoft/r/dNpzgxQUrS?origin=lprLink

PODSUMOWANIE

Cyberbezpieczeństwo to odpowiedzialność każdego pracownika.

Pamiętaj:

- zatrzymaj się przed kliknięciem,
- sprawdzaj nadawcę,
- blokuj komputer,
- chroń dane pacjentów,
- zgłaszaj każdy incydent.

Każde zgłoszenie może zapobiec poważnemu cyberatakowi.