CSIRT CEZ

Ochrona przed atakami phishingowymi

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

01. Identyfikacja podejrzanych wiadomości

- Nie otwieraj wiadomości od nieznanych nadawców.
- Jeśli nie spodziewasz się wiadomości, traktuj ją jako potencjalnie niebezpieczną.
- Zwracaj uwagę na błędy językowe i gramatyczne.
- Sprawdzaj poprawność adresu nadawcy (np. literówki sekretariat@zspital.pl czy support@micros0ft.com).
- Nie klikaj w linki i nie otwieraj załączników bez weryfikacji – zawsze sprawdzaj, dokąd prowadzi link, najeżdżając na niego kursorem (bez klikania w link).
- Ostrożnie podchodź do wiadomości z prośbą o pilne działanie. Phishing zwykle bazuje na presji czasu (np. „Twoje konto zostanie zablokowane w ciągu 24h!”).
- Zwracaj uwagę na nietypowe formaty plików. Oszuści często wysyłają zainfekowane pliki w formatach .exe, .scr, .js, .zip, a także makra w dokumentach Word oraz Excel.

02. Postępowanie w przypadku podejrzanych wiadomości

- Nie odpowiadaj na podejrzane wiadomości. Nawet, jeśli wydaje się, że pochodzą od znanej firmy, skontaktuj się z nią innym kanałem w celu weryfikacji.
- Nie podawaj loginów i haseł przez e-mail lub telefon. Żadna firma, bank ani dział IT nie powinni prosić o podanie hasła przez wiadomość lub telefon.
- W przypadku wątpliwości co do autentyczności wiadomości, zgłoś ją do działu IT.
- Nie usuwaj podejrzanych wiadomości. Mogą okazać się istotne podczas analizy w razie wystąpienia incydentu.
- Jeśli przypadkowo kliknąłeś w podejrzany link, natychmiast zgłoś to zdarzenie do działu IT.
- Jeśli e-mail zawiera link do logowania, nie używaj go. Zamiast tego wejdź na stronę ręcznie przez przeglądarkę.
- Po otrzymaniu podejrzanej wiadomości uprzedź współpracowników o możliwej próbie ataku.
- Nie ujawniaj żadnych informacji o wewnętrznych zabezpieczeniach, procedurach oraz innych wrażliwych danych.

CSIRT CEZ

03. Postępowanie z załącznikami

- Otwieraj wyłącznie pliki od nadawców, których tożsamość i adres e-mail możesz potwierdzić.
- Zwracaj uwagę na rozszerzenia, fałszywe pliki mogą mieć podwójne rozszerzenia (np. .pdf.exe).
- Unikaj bezpośredniego otwierania linków w e-mailach zapraszających do pobrania załącznika, jeśli nie masz pewności, że pochodzą z wiarygodnego źródła.
- Pamiętaj, że nawet obrazy (.jpg, .png, .gif) mogą zawierać złośliwy kod, zwłaszcza jeżeli pobrano je z niezaufanych stron.
- Zawsze skanuj pliki antywirusem, wykonuj to szczególnie przed otworzeniem grafik w e-mailach, które budzą Twoje wątpliwości.
- Nie klikaj w osadzone linki w grafikach, niektóre obrazy mogą przekierowywać do stron phishingowych lub pobierać złośliwe skrypty i wirusy.
- Włączaj makra wyłącznie, gdy jest to absolutnie niezbędne i tylko w przypadku plików, których źródła jesteś pewien.
- Zachowuj ostrożność przy plikach w formacie .xlsm, .docm, .pptm – to rozszerzenia dla dokumentów z domyślnie włączonymi makrami.
- Nigdy nie uruchamiaj makr, jeżeli dokument dotyczy tematu, który nie ma związku z Twoimi obowiązkami lub pochodzi od nieznanej osoby.
- Nie przesyłaj wrażliwych załączników na prywatne maile, dyski chmurowe czy komunikatory.
- Skanuj skompresowane archiwa oraz zawsze używaj antywirusa przed otwarciem plików: .zip, .rar, .7z itp.
- Weryfikuj zawartość załączników Jeśli w archiwum spodziewasz się jednego pliku .pdf, a znajdujesz wiele różnych plików (np. .exe czy .js), nie rozpakowuj pliku i skontaktuj się z działem IT.
- Jeśli wiadomość zawiera zaszyfrowany załącznik i jednocześnie w treści jest podane hasło, zachowaj szczególną ostrożność. Często w ten sposób omija się zabezpieczenia poczty.