E-MAIL TEŻ MOŻE BYĆ PUŁAPKĄ

Jak rozpoznać i unikać złośliwych wiadomości e-mail?

www.xemi.pl

- Kilka zasad, dzięki którym unikniesz kłopotów
- Po czym poznać, że e-mail jest podejrzany?
- Co zrobić jak już padniemy ofiarą zainfekowanego e-maila?

Głównym źródłem zarażenia komputerów wirusami szyfrującymi dane są obecnie **załączniki e-mail i niebezpieczne linki w treści wiadomości**.

Zainfekowany komputer zostaje całkowicie zablokowany, a za nim kolejne zasoby, które są z nim połączone. Częstą sytuacją oprócz zablokowania komputera jest kradzież danych, groźba upublicznienia ich oraz żądanie okupu. Warto wiedzieć, że **zapłacenie go nie daje żadnej gwarancji odzyskania danych**.

Skutkiem tych zdarzeń jest bezpowrotna utrata danych. Jedynym rozwiązaniem w tej sytuacji jest przywrócenie danych z posiadanych **kopii zapasowych**.

Kilka zasad, dzięki którym unikniesz kłopotów

NIE OTWIERAJ	wiadomości e-mail pochodzących z nieznanych źródeł.
NIE OTWIERAJ	załączników, które wyglądają jak załączone pliki faktur lub innych ważnych dokumentów, zwłaszcza z dołączonym hasłem w treści wiadomości.
NIE OTWIERAJ	podejrzanych powiadomień o przesyłkach z firm przewozowych takich jak GLS, FedEx, Poczta Polska itp. zwłaszcza w sytuacji, kiedy niczego nie zamawiałeś.
NIE PODAWAJ	loginów i haseł do stron bankowych.
NIE KLIKAJ	w linki (odnośniki) z podejrzanie wyglądających wiadomości e-mail, które mogą prowadzić do stron internetowych wyłudzających informacje.
NIE PODŁĄCZAJ	do komputera firmowego nieznanych pendrive'ów i innych dysków zewnętrznych.
NIE UŻYWAJ	prywatnych kont pocztowych do spraw służbowych.

Po czym poznać podejrzany e-mail?

Sprawdź nadawcę

Uważaj na wiadomości od nieznanych osób lub firm. Zwróć uwagę na adres e-mail nadawcy; oszuści często używają adresów, które są bardzo podobne do prawdziwych, np. zamiast firma@mila.com mogą użyć poczta@mi1a.com

Uważaj na podejrzane załączniki

Szczególnie niebezpieczne są pliki z rozszerzeniami .exe, .bat, .zip, .pdf, .cmd czy .scr, mogą one zawierać złośliwe oprogramowanie.

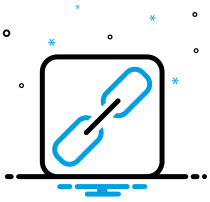
Zwróć uwagę na treść wiadomości

Błędy ortograficzne, gramatyczne czy stylistyczne mogą świadczyć o próbie oszustwa. Nie daj się zwieść personalizowanym wiadomościom zawierającym imię, nazwisko i szczegóły, które sprawiają, że wyglądają autentycznie. Często przypominają e-mail od szefa, współpracownika lub instytucji, z którą masz rzeczywiście kontakt.

Uważaj na nagrody i darowizny

Nie wierz w to, że bogacze rozdają milionowe darowizny przypadkowym użytkownikom poczty e-mail. Nie wierz w obietnice wygranej w konkursie, na który się nie zapisałeś, tym bardziej jeśli w grę wchodzi opłata manipulacyjna przed otrzymaniem nagrody.

Uważaj na linki w treści wiadomości



Zanim klikniesz w link lub podlinkowane zdanie/słowo, najedź na niego kursorem (bez klikania), aby sprawdzić, dokąd prowadzi.

Oszuści często maskują linki, aby wyglądały na zaufane, podczas gdy te prowadzą do złośliwych stron.

Zwróć uwagę na nietypowe prośby

Przestępcy, chcąc wyłudzić informacje podszywają się pod zaufane instytucje. Jeśli otrzymasz wiadomość z prośbą o podanie danych logowania, numerów kart kredytowych czy innych poufnych informacji, skontaktuj się bezpośrednio z daną instytucją, aby zweryfikować prawdziwość prośby.

Uważaj na pilne wezwania do działania

Zachowaj czujność jeśli wiadomość zawiera pilne wezwanie do działania np.: natychmiastowe podanie danych osobowych, pobranie bonu podarunkowego, uzupełnienie informacji lub wypełnienie ankiet poprzez kliknięcie w link. Linki te mogą prowadzić do fałszywych stron logowania lub pobierania złośliwego oprogramowania.

Co zrobić w przypadku podejrzenia zainfekowania komputera wirusem?

- **NIE UKRYWAJ TEGO!**
- Wykonaj zdjęcie komunikatu telefonem komórkowym.
- Odłącz komputer od sieci.
- Nie wyłączaj komputera, ponieważ może to usunąć ślady ataku, a te są kluczowe dla zespołu IT.
- **NATYCHMIAST** powiadom dział IT i/lub przełożonego o zaistniałej sytuacji i przekaż mu wszystkie szczegóły:
  - nadawcę e-maila;
  - temat wiadomości;
  - kliknąłeś/nie kliknąłeś w link;
  - otworzyłeś/nie otworzyłeś załącznika;
  - jakie działania zostały podjęte.

Pamiętaj!

Nie rób niczego pochopnie.
Zanim klikniesz w załącznik lub link,
upewnij się, że nie wzbudza Twoich podejrzeń.