NASK

CERT.PL >_

https://incydent.cert.pl / cert@cert.pl

Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych

- **Nie używaj prywatnych kont** poczty elektronicznej i komunikatorów do korespondencji służbowej
- **Nie używaj prywatnych komputerów** i telefonów do spraw służbowych
- **Nie używaj służbowych komputerów** i telefonów do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej), nie udostępniaj ich członkom rodziny

- Logując się na konto zawsze sprawdź **czy domena danego portalu jest prawidłowa**. Domena to nazwa zawierająca się między *https://*, a pierwszym kolejnym znakiem */*
- **Ignoruj wszystkie inne prośby o podanie swojego hasła**, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi deaktywacją konta
- Wszystkie podejrzane wiadomości na skrzynce służbowej zgłaszaj administratorom w swojej organizacji
- O wszystkie podejrzane wiadomości na prywatnej skrzynce możesz zapytać CERT Polska (https://incydent.cert.pl / cert@cert.pl)
- Szczególnie podejrzane są wiadomości:
  - Zawierające załączniki, a zwłaszcza archiwa i dokumenty Office z hasłem podanym w treści wiadomości
  - Wiadomości zmuszające do podjęcia natychmiastowej reakcji

- **Stosuj długie hasła** (powyżej 14 znaków)
- Dobrą metodą na długie hasło jest **wymyślenie całej frazy**, składającej się z kilku słów, np. 2CzerwoneRoweryJedzaNalesniki
- Unikaj haseł, **które łatwo powiązać z publicznymi informacjami na temat Twojej osoby** np. zawierających nazwisko, datę urodzenia itp.
- Hasło zmieniamy wtedy, gdy **mamy podejrzenie**, że mogła poznać je inna osoba. Nie ma potrzeby cyklicznej zmiany hasła.
- **Nie używaj tego samego hasła więcej niż raz** (w szczególności do konta email, banku i innych wrażliwych kont)
  - Dla ułatwienia **korzystaj z menedżerów haseł**. Te wbudowane w przeglądarkę czy telefon są bezpieczne i proste w użyciu

- **Włącz uwierzytelnianie dwuskładnikowe** (tzw. 2FA) tam gdzie jest to możliwe
  - Uwierzytelnianie dwuskładnikowe **w poczcie elektronicznej** i w **kontach społecznościowych** jest konieczne
  - Jeżeli obecny dostawca Twojej poczty nie udostępnia uwierzytelniania dwuskładnikowego, zmień go
  - Najlepszym drugim składnikiem uwierzytelniania i jedynym odpornym na ataki phishingowe jest **token sprzętowy U2F** (np. YubiKey),

- **Zweryfikuj wszystkie dane kontaktowe** w ustawieniach profilu poczty elektronicznej i mediów społecznościowych; dobra alternatywna metoda kontaktu ułatwi odzyskanie utraconego konta
- Jeżeli podejrzewasz, że ktoś mógł włamać się na twoje konto, **zmień hasło**, sprawdź dostępną w profilu **historię logowania** i **zakończ wszystkie aktywne sesje**

- Nie zaniedbuj **aktualizacji systemu operacyjnego i programów** na używanym komputerze
- Posiadaj **aktualny program antywirusowy**
- VPN **nie chroni** przed atakami phishingowymi i złośliwym oprogramowaniem!

- Do wrażliwej prywatnej komunikacji **używaj komunikatorów szyfrowanych end-to-end**, np. Signala
- Używaj opcji **automatycznego kasowania wiadomości** po upływie określonego czasu – nie da się ukraść czegoś, czego już nie ma