

JAK TWORZYĆ BEZPIECZNE HASŁA



DLACZEGO SILNE HASŁO JEST WAŻNE?

- Hasło to podstawowa bariera w ochronie naszych kont online
- Słabe hasła są łatwe do złamania, co może prowadzić do kradzieży danych

IM DŁUŻSZE HASŁO, TYM BEZPIECZNIEJSZE

- Zaleca się co najmniej 12 znaków
- Długie hasło zwiększa liczbę możliwości kombinacji, co utrudnia jego złamanie



UŻYCIE RÓŻNYCH TYPÓW ZNAKÓW

- wielkie litery (np. A, B, C)
- małe litery (np. a, b, c)
- cyfry (np. 1, 2, 3)
- znaki specjalne np. !, @, #, \$, %



UNIKAJ SEKWENCJI I POWTÓRZEŃ

Przykłady złych hasel:

- 123456
- Qwerty
- Aaaaaaa

PRZYKŁAD SILNEGO HASŁA: Sigma@Up!Niezłamią#28

RÓŻNE HASŁA DO RÓŻNYCH KONT

- Nie używaj tego samego hasła do wszystkich usług (np. bank, e-mail, media)
- Złamanie jednego hasła zagraża bezpieczeństwu wszystkich kont

ZMIANA HASŁ TO KLUCZOWA PRAKTYKA

- Zmień hasło, jeśli podejrzewasz wyciek danych
- Kiedy zmieniasz hasło nie powielaj starego zmieniając w nim np. kolejną cyfrę

PRZYKŁADY SILNYCH HASŁ

J7@ab&oP!Qw9^
nM92z%oVtp\$1Kq



UWAŻAJ, NIE DAJ SIĘ OSZUKAĆ!

1. **NIE UDOSTĘPNIAJ** innym swoich danych bankowych
- loginu, hasła, Pinu, kodu BLIK ...

2. **UWAŻAJ NA LINKI** zawarte w SMS-ach i e-mailach.

3. **NIE OTWIERAJ** e-maili i załączników pochodzących od nieznanych nadawców.

4. **UWAŻAJ NA REKLAMY INWESTYCJI** oferujące
"szybki, duży zysk".

5. **UWAŻNIE CZYTAJ** wiadomości autoryzacyjne.

6. **UWAŻAJ NA FAŁSZYWE TELEFONY** osób podających się za policjanta, prokuratora, pracownika banku, pracownika urzędu, ZUS-u itp.

7. **ZADBAJ O BEZPIECZNE HASŁO.**

8. **UWAŻAJ NA FAŁSZYWE WIADOMOŚCI** od kuriera, olx, vinted itp.

9. **UNIKAJ PUBLICZNYCH SIECI WI-FI**

10. **PAMIĘTAJ** - obietnice ponadprzeciętnych korzyści, gra na emocjach, wzbudzenie strachu, współczucia, presja czasu - to są elementy wskazujące, że możesz stać się ofiarą oszustwa!

