

Temat: Bezpieczeństwo w Sieci – Bezpieczne Hasło

Dlaczego silne hasło jest ważne?

W świecie cyfrowym Twoje hasło jest jak klucz do mieszkania. Jeśli jest słabe, złodziej (haker) może łatwo je "dorobić" i uzyskać dostęp do Twojej poczty, bankowości czy mediów społecznościowych.

Złote zasady tworzenia haseł

- **Długość ma znaczenie:** Minimum 12-14 znaków. Im dłuższe hasło, tym trudniejsze do złamania przez programy komputerowe.
- **Mieszaj znaki:** Używaj wielkich i małych liter, cyfr oraz znaków specjalnych (np. !, @, #, \$).
- **Unikaj oczywistości:** Nigdy nie używaj swojego imienia, daty urodzenia, imienia psa czy słowa "hasło123".
- **Metoda zdania:** Zamiast trudnego do zapamiętania ciągu znaków, wymyśl zdanie, np.: *Lubię pić kawę o 7 rano w poniedziałek!* → Twoje hasło to: **Lpk07rwP!**.

Zasada: Jedno konto, jedno hasło

To najczęstszy błąd. Jeśli używasz tego samego hasła do Facebooka i do banku, po wycieku danych z jednego serwisu, tracisz bezpieczeństwo na wszystkich pozostałych.

Jak zarządzać hasłami?

Nie musisz pamiętać wszystkiego w głowie. Polecamy dwa rozwiązania:

1. **Menedżer haseł:** Program, który bezpiecznie przechowuje Twoje hasła (np. Bitwarden lub KeePass). Pamiętasz tylko jedno hasło główne.
2. **Tradycyjny notes:** Jeśli wolisz papier, trzymaj go w bezpiecznym miejscu w domu, nigdy przy komputerze!

Weryfikacja dwuetapowa (2FA)

To "drugi rygiel" w drzwiach. Nawet jeśli ktoś pozna Twoje hasło, będzie potrzebował kodu z SMS-a lub aplikacji, aby się zalogować. Włączaj tę funkcję wszędzie, gdzie to możliwe!

Materiał jest udostępniany na licencji Creative Commons

