

Pierwsza linia obrony

1. Hasło: Twój klucz do skarbca

Zacznijmy od rachunku sumienia. Czy używasz tego samego hasła do banku, poczty prywatnej i programu księgowego? A może Twoje hasło to **"Biuro2023"**?

Jeśli tak, zapraszasz złodzieja do środka. Ile czasu zajmuje hakerowi złamanie hasła? Nie musisz zapamiętywać skomplikowanych ciągów znaków. **Rozwiązaniem jest Manager Haseł** (np. Bitwarden, 1Password, KeePass). To cyfrowy sejf, który pamięta hasła za Ciebie.

Ty musisz znać tylko jedno - klucz do sejfu.

Hasło (Przykład)	Złożoność	Czas na złamanie
annaksieg	9 znaków, tylko małe litery	Natychmiast
Marek123	8 znaków, małe, duże litery, cyfry	Kilka godzin
Ksiegowosc!24	13 znaków, złożone	200 lat
Kawa!Rano#Biuro24	16+ znaków, złożone	Miliardy lat

ZADANIE NA 10 MINUT:

- ☐ Zainstaluj darmowy manager haseł w przeglądarce (wiele z nich ma dosyć zaawansowane "darmowe" wersje lub konta trial do przetestowania - np. Bitwarden, Proton Pass lub NordPass).
- ☐ Zmień hasło do swojej głównej skrzynki mailowej na długie zdanie (np. 4 losowe słowa + znak specjalny).
- ☐ Zapisz je teraz w nowo zainstalowanym managerze.



2. Wdrożenie 2FA - Podwójna tarcza



Hasło to za mało.

Wycieki z baz danych zdarzają się gigantom (Facebook, LinkedIn, Adobe). Jeśli Twoje hasło wycieknie, haker ma otwarte drzwi. Chyba że zamontujesz drugi zamek.

Uwierzytelnianie Dwuetapowe (2FA) sprawia, że nawet znając hasło, nikt nie zaloguje się na Twoje konto bez drugiego składnika, do którego dostęp masz tylko Ty.

Co wybrać?

- Token SMS: Popularne, ale najmniej bezpieczne (podatne na duplikaty kart SIM).
- Aplikacje (Google/Microsoft Authenticator): Generują kod ważny tylko 30 sekund.
- Klucz fizyczny (np. YubiKey): Wymaga włożenia urządzenia USB do komputera.



ZADANIE NA 10 MINUT:

- ☐ Pobierz aplikację (darmową) Google Authenticator na telefon.
- ☐ Włącz weryfikację dwuetapową na swojej skrzynce e-mail oraz w systemach księgowych (jeśli na to pozwalają).