

Jak stworzyć silne hasło i zapamiętać je bez trudu

Krótki, praktyczny przewodnik. Bez żargonu, bez zbędnej teorii.

Dlaczego to ważne

Serwisy internetowe regularnie padają ofiarą włamań, a bazy danych z hasłami wyciekają do sieci. Jeśli używasz jednego hasła w kilku miejscach, wyciek z jednego, mało istotnego serwisu może dać obcej osobie dostęp także do Twojej poczty czy bankowości.

Słabe vs silne hasło

SŁABE	SILNE
Kasia1990	fioletowy-kubek-metro-92
qwerty123	7mostów!zaJeziołem
Hasło1!	rower-cytryna-lampa-92

Długość ma większe znaczenie niż komplikacja. Kilkanaście znaków, nawet zwykłych słów, jest trudniejsze do złamania niż osiem losowych znaków ze specjalnym znakiem.

Metoda hasła-frazy

Połącz 4-5 przypadkowych, niepowiązanych ze sobą słów, np. rower-cytryna-poniedziałek-lampa. To długie, praktycznie nie do złamania, a jednocześnie łatwe do zapamiętania. Używaj tej metody przynajmniej do hasła głównego menedżera haseł i do poczty.

Menedżer haseł

Menedżer haseł generuje i pamięta unikalne, silne hasło dla każdej strony, Ty pamiętasz tylko jedno hasło główne. Polecam: Bitwarden (darmowy), Menedżer haseł Google (wbudowany w Chrome), Hasła (wbudowany w urządzenia Apple), 1Password (płatny, dla rodzin i organizacji).

Weryfikacja dwuskładnikowa (2FA)

Dodatkowy, jednorazowy kod przy logowaniu. Nawet jeśli ktoś pozna Twoje hasło, bez tego kodu się nie zaloguje. Najlepiej sprawdzają się aplikacje authenticator (np. Google Authenticator), lepsze niż kody SMS.

Sprawdź, czy Twoje hasło wyciekło

Bezpłatne narzędzie haveibeenpwned.com pokazuje, czy Twój e-mail pojawił się w znanym wycieku danych. Nie wymaga rejestracji.

5 kroków na dziś

- Sprawdź swój e-mail na haveibeenpwned.com
- Zainstaluj menedżer haseł i ustaw jedno silne hasło-frazę jako główne
- Zmień hasło do poczty i bankowości w pierwszej kolejności
- Włącz weryfikację dwuskładnikową wszędzie, gdzie to możliwe
- Nigdy nie używaj ponownie hasła, które wyciekło