Jak tworzyć silne i bezpieczne hasła

W świecie, w którym codziennie korzystamy z dziesiątek kont internetowych i systemów cyfrowych, hasła są podstawową linią obrony przed nieautoryzowanym dostępem. Ten rozdział pokaże Ci, jak tworzyć skuteczne i bezpieczne hasła oraz jak unikać najczęstszych błędów.

Dlaczego login i hasło są tak istotne?

Wiele systemów, zarówno firmowych jak i internetowych, zabezpiecza dostęp do poufnych danych poprzez konieczność podania loginu i hasła.

Dla porównania – login można porównać do karty płatniczej, a hasło do numeru PIN.

Co się stanie, jeśli ktoś przechwyci oba te elementy? Może dojść do kradzieży tożsamości, wycieku danych, strat finansowych, a nawet utraty pracy.

Dbaj o bezpieczeństwo informacji, które Ci powierzono – nie ułatwiaj działań cyberprzestępcom.

Hasło to Twoja osobista ochrona.

Jakie powinno być silne hasło?

Zestawmy dwa diametralnie różne przykłady:

HASŁO **Wlazł!Kotek@Na#Płotek$**

Drugie hasło, choć pozornie skomplikowane, bazuje na znanym wierszyku i kilku znakach specjalnych (!@#$), a jego litery początkowe są zapisane wielkimi literami.

Efekt? Pierwsze hasło można złamać w ułamku sekundy, drugie – wymagałoby milionów lat. Choć nie istnieje hasło nie do złamania, możesz sprawić, że jego odgadnięcie będzie zbyt kosztowne lub czasochłonne dla atakującego.

Zasady tworzenia bezpiecznego hasła:

- Minimum 12 znaków
- Wielka litera, cyfra i znak specjalny

Różne hasła = większe bezpieczeństwo

Czy naprawdę warto mieć inne hasło do każdego konta?

Zdecydowanie tak. Badania wskazują, że aż 91% użytkowników korzysta z jednego z tysiąca najpopularniejszych haseł. Znasz któreś z nich?

Przykłady popularnych haseł:

123456, hasło, qwerty, abc123, 000000, sunshine, księżniczka... i wiele innych

Pamiętaj:

Unikaj oczywistych kombinacji. Nie stosuj tego samego hasła w wielu miejscach – jeśli jedno konto zostanie przejęte, zagrożone są wszystkie pozostałe. Obawiasz się, że nie zapamiętasz wielu skomplikowanych haseł? Skorzystaj z menedżera haseł (np. KeePass), który pozwala bezpiecznie przechowywać dane logowania. Pamiętaj jednak o odpowiednim zabezpieczeniu hasła głównego!

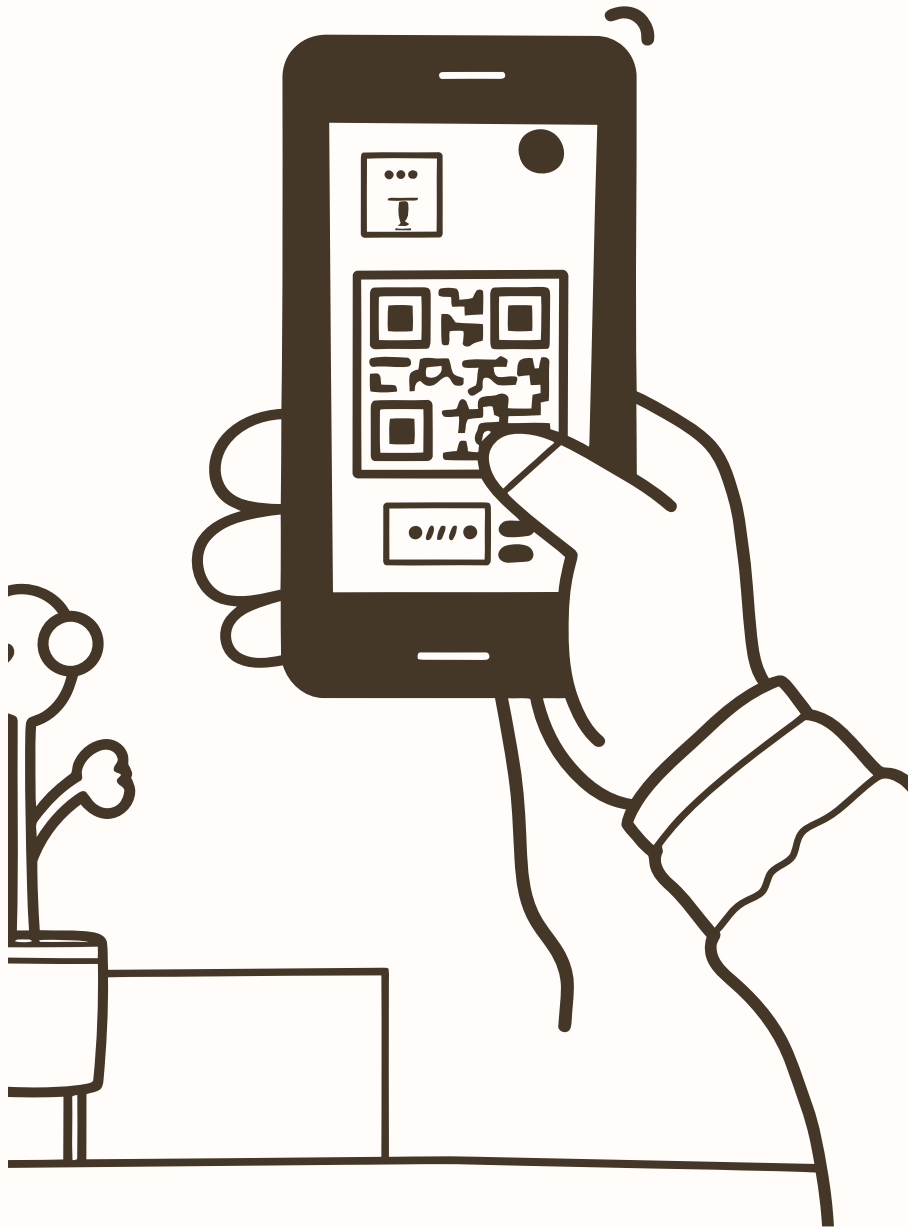
Przygotuj się na dodatkowe zabezpieczenia

Wyciek danych

Z uwagi na coraz częstsze przypadki wycieku danych z dużych serwisów (jak Dropbox, LinkedIn, Twitter), rośnie znaczenie tzw. **uwierzytelniania dwuskładnikowego (2FA)**.

Standardy bezpieczeństwa

Ten sposób logowania staje się standardem, ponieważ stanowi dodatkową warstwę ochrony.

Kod SMS

Poza hasłem wymagany jest jednorazowy kod – najczęściej przesyłany SMS-em na wcześniej wskazany numer telefonu. Kod ten jest krótki, łatwy do wpisania, a znacząco zwiększa bezpieczeństwo.