Jaki są zasady, według których powinno się tworzyć hasło dla danego konta?

Ważne jest, żebyśmy stosowali hasła o właściwej długości, odpowiedniej strukturze i odpowiednim skomplikowaniu.

Wskazówki dotyczące dobrego hasła

Silne hasło może być łatwe do zapamiętania dla Ciebie, ale musi być prawie niemożliwe do odgadnięcia przez inną osobę. Dowiedz się, jakie warunki musi spełniać dobre hasło, a następnie zastosuj te wskazówki, tworząc hasło do swojego konta.

A. Wymyśl hasło, które będzie unikalne

Używaj innego hasła do każdego ważnego konta takiego jak konto e-mail czy bankowości internetowej.

Ponowne wykorzystanie hasła do ważnego konta jest ryzykowne. Jeśli ktoś pozna hasło do jednego z Twoich kont, może uzyskać dostęp do poczty e-mail, adresu, a nawet pieniędzy.

Wskazówka: jeśli nie potrafisz zapamiętać wielu haseł, dowiedz się, jak skorzystać z narzędzia do zarządzania zapisanymi hasłami.

B. Wymyśl hasło, które jest dłuższe i łatwiejsze do zapamiętania

Długie hasła są silniejsze, więc utwórz hasło, które będzie miało co najmniej 12 znaków. Poniższe wskazówki pomogą Ci tworzyć dłuższe hasła, które łatwiej zapamiętasz. Przykładowe rzeczy, których możesz użyć:

- tekst piosenki lub wiersza;
- ważny cytat z filmu lub przemowy;
- fragment książki;
- **ciąg słów, który ma dla Ciebie znaczenie;**
- skrót: utwórz hasło z pierwszych liter kolejnych słów w zdaniu.

Unikaj haseł możliwych do odgadnięcia przez:

- osoby, które znasz;
- osoby, które mają dostęp do Twoich podstawowych danych (np. Twojego profilu w mediach społecznościowych).

C. Unikanie danych osobowych i popularnych słów

1. Nie używaj danych osobowych

Unikaj tworzenia haseł na podstawie informacji, które inni mogą znać lub łatwo uzyskać. Przykłady:

- Twoje przezwisko lub inicjały;
- imię Twojego dziecka lub zwierzaka;
- ważne daty urodzin lub lata;
- nazwa Twojej ulicy;
- numery z Twojego adresu.

2. Nie używaj popularnych słów czy wzorców

Unikaj prostych słów, wyrażeń i wzorców, które łatwo odgadnąć. Przykłady:

- oczywiste słowa i wyrażenia, takie jak „hasło” czy „wpuscmnie”;
- ciągi znaków, takie jak „abcd” lub „1234”;
- wzorce z klawiatury, takie jak „qwerty” czy „qazwsx”.

Dbanie o bezpieczeństwo haseł

Po utworzeniu silnego hasła dbaj o jego poufność.

1. Ukrywanie zapisanych haseł

Jeśli musisz zapisać swoje hasło, nie zostawiaj go przy komputerze ani na biurku. Zadbaj o to, by wszystkie spisane hasła były przechowywane w nikomu nieznanym bądź zabezpieczonym miejscu.

2. Narzędzie do zarządzania hasłami

Jeśli nie potrafisz zapamiętać wielu haseł, dobrym rozwiązaniem może być zaufany menedżer haseł. Poświęć trochę czasu na zapoznanie się z opiniami i ocenami dotyczącymi takich rozwiązań.

Jakie hasło jest dobre a jakie złe?

Dobre hasło do logowania powinno spełniać następujące kryteria:

Być odpowiednio długie (min. **12** znaków według Microsoft (**było 8**))

Być odpowiednio skomplikowane

Nie może być używanym wyrazem słownikowym

Musi zawierać znaki specjalne

Musi być zmieniane raz na 1-3 miesiące

Łatwe do zapamiętania

Przykłady dobrych haseł

MoZoUr2WsDzKtKo**

DwPl1RoTrcoJePr#@!

Kldrobmodoma5gadozi

Ma2tyn@sppr

Przykłady złych haseł

Ania75

Bratek12

Qwerty

zaq1@WSX

Do tego dość skomplikowanego hasła stosuję jedno zdanie i cztery logiczne zasady.

Po pierwsze - z każdego wyrazu biorę dwie pierwsze litery

Po drugie - liczby zamieniam na pisane cyframi

Po trzecie - pierwsza litera każdego zdania (może być wyrazu) jest duża

Po czwarte - ucinam polskie ogonki

Jak brzmi moje sekretne zdanie?

Ma **Ma**m

2 - **dw**a

ty - **ty**godnie

n@ - **na**

sp - **sp**rawdzenie

pr -**pr**ac

Jak bezpieczne jest moje hasło?

Czuję się dość bezpiecznie, tym bardziej, że za miesiąc zmienię swoje hasło :).

Sprawdź jak silne jest Twoje hasło na

https://howsecureismypassword.net/

wymyśl swoje sekretne zdanie na ten miesiąc i ciesz się bezpieczeństwem swoich danych.

Kilka zasad.

Nigdy nie stosuj imion, czy zwykłych wyrazów jako hasła, nawet z dodatkowymi cyferkami. Hasło Adam1996 nie jest bezpieczne :)

Nigdy nie zapisuj swoich haseł na komputerze czy karteczce! Tak jak nie zapisujesz pinu na swojej karcie bankomatowej.

Masz dużo programów i różna hasła do zapamiętania? Korzystaj z bezpiecznych ułatwień typu: https://lastpass.com/

Zmieniaj hasła najrzadziej raz na 3 miesiące.

Nie możesz używać hasła, które:

- jest wyjątkowo słabe, np. „hasło123”;
- było używane wcześniej na Twoim koncie;
- zaczyna się lub kończy spacją.