RODO

Jak utworzyć bezpieczne hasło

Jak utworzyć bezpieczne hasło

W ramach szkolenia pracowniczego

szkolenie dedykowane : Pogotowie Ratunkowe we Wrocławiu

Jak utworzyć bezpieczne hasło

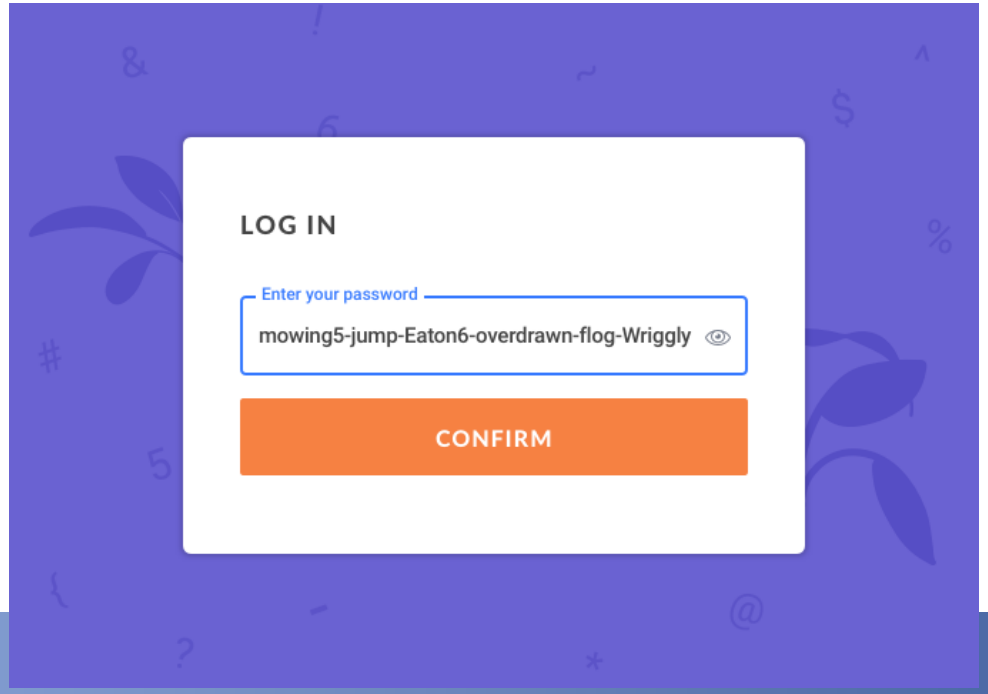
Hasło do poczty elektronicznej, konta w social mediach, do telefonu, komputera, bankowości elektronicznej... Jakie powinno być? Bezpieczne, silne i… do każdego konta inne! Oto wskazówki jak tego dokonać.

Jak utworzyć bezpieczne hasło

Na początek szybki quiz. Ręka w górę, kogo hasła to imię i rok urodzenia? Teraz niech rękę podniosą ci, którzy nie pamiętają, kiedy ostatnio zmieniali hasło np. do poczty elektronicznej. I na koniec – kto z Was ma to samo hasło do wielu kont? Jeśli należysz choćby do jednej z tych grup, wiedz że nie jest dobrze.

Łatwy cel

Dlaczego nie jest dobrze? Dlatego, że istnieje duża szansa, że wcześniej czy później zostaniesz ofiarą cyberataku. Cyberprzestępcy nie biorą sobie na cel tylko dużych i bogatych firm, znanych osób czy instytucji publicznych. Każdego dnia włamują się na konta wielu „szarych” ludzi. Po co? By wykraść dane, ukraść pieniądze z konta, szantażować. To nie film, takie są realia. Warto, by zdawać sobie z tego sprawę i zrobić wszystko, by takich sytuacji uniknąć.



Łatwy cel

Istnieje wiele sposobów, w jaki cyberprzestępcy mogą próbować zaatakować konta użytkowników. Część z nich opiera się właśnie na atakach celowanych w hasła.

Najczęściej popełniane przez użytkowników błędy, które ułatwiają pracę cyberprzestępcom, to zbyt łatwe hasło i wykorzystywanie jednego hasła do wielu witryn.

Łatwy cel

Hasła są jak klucze do sejfu lub domu. Jeśli ktoś je zdobędzie może przejąć nasze konto w mediach społecznościowych, ukraść naszą tożsamość, ogołocić konto bankowe i uzyskać dostęp do naszych prywatnych danych.

Jeśli wyjeżdżając na urlop nie zostawiacie w domu otwartych drzwi i okien – z hasłami też powinniście sobie poradzić.

Kilka wskazówek, które pomogą zabezpieczyć Nas w sieci. Jeśli zrealizujemy choć część z nich – zadbamy o swoje bezpieczeństwo.

Zaczynamy!

Im trudniej, tym lepiej

Na początek to, czego NIE robić:

- Nie stosuj najpopularniejszych haseł, jak: „hasło", „123456", „piłka nożna" itp.
- Hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy.
- Hasło nie powinno być imieniem nikogo z naszego najbliższego otocznia (członka rodziny, znajomego, ani zwierzaka).

Im trudniej, tym lepiej

Na początek to, czego NIE robić:

- Nie powinno zawierać danych osobowych Twoich lub Twojej rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.
- Nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: „abcde”, „12345", „QWERTY”.

Im trudniej, tym lepiej

Na początek to, czego NIE robić:

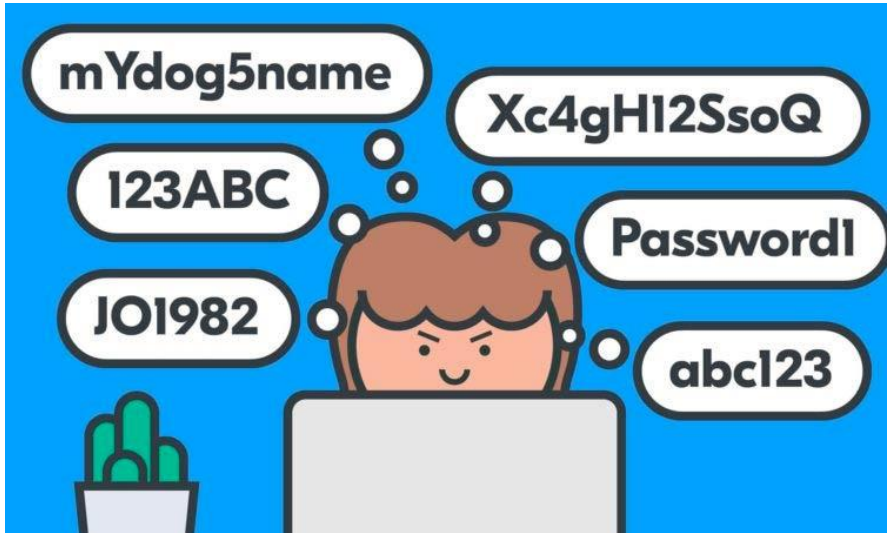
- Nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak, ani tego wyrazu poprzedzonego lub/i zakończonego znakiem specjalnym lub cyfrą.
- Nie używaj więcej niż trzech kolejnych znaków na klawiaturze, takich jak „abc” lub „123".
- Nie używaj więcej niż dwóch kolejno powtarzających się ciągów znaków np. ”bbbb2bbb”.
- Nie używaj oczywistych wyrażeń, takich jak np. „wpuscmnie".

Im trudniej, tym lepiej

- Gdy zmieniasz hasło do istniejącego konta, nie powinno ono być takie samo jak poprzednie hasło. Nie zmieniaj też go nieznacznie. Na przykład: z hasło1, na hasło2 itp.
- Tworzenie bardzo silnego hasła i zapisywanie go na papierze jest równie złą decyzją, co tworzenie łatwego do zapamiętania hasła bez zapisywania go. Nigdy nie zapisuj hasła na papierze.
- Używaj unikatowych haseł dla każdego z kont.

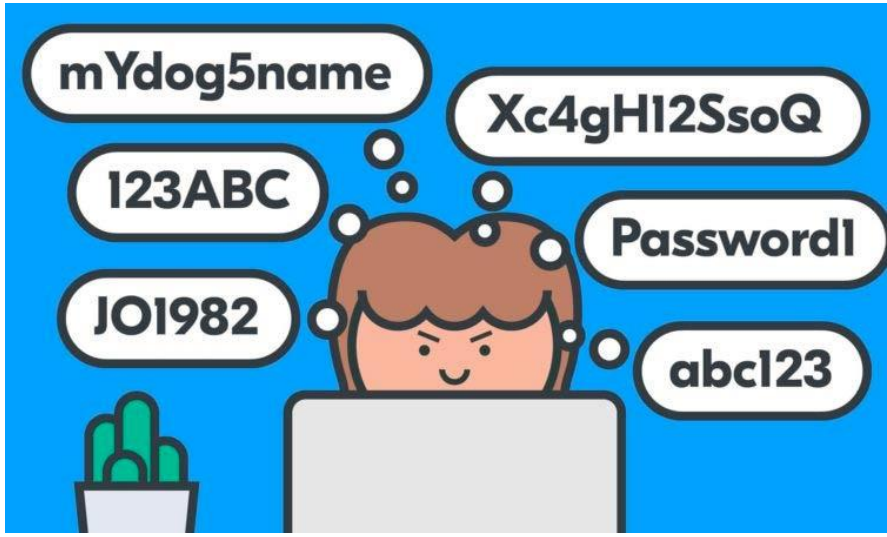
Już wiecie, czego nie robić. Czas na wskazówki jak działać:

- Hasło powinno mieć co najmniej 8 znaków. Jeszcze lepsze jest dłuższe hasło, składające się z 12 lub 14 znaków. Pamiętaj, że niektóre witryny, systemy operacyjne lub aplikacje mają swoje wymagania co do minimalnej długości hasła.
- Hasło powinno zawierać co najmniej jeden znak z każdej z następujących grup: małe litery, duże litery, liczby, znaki specjalne.



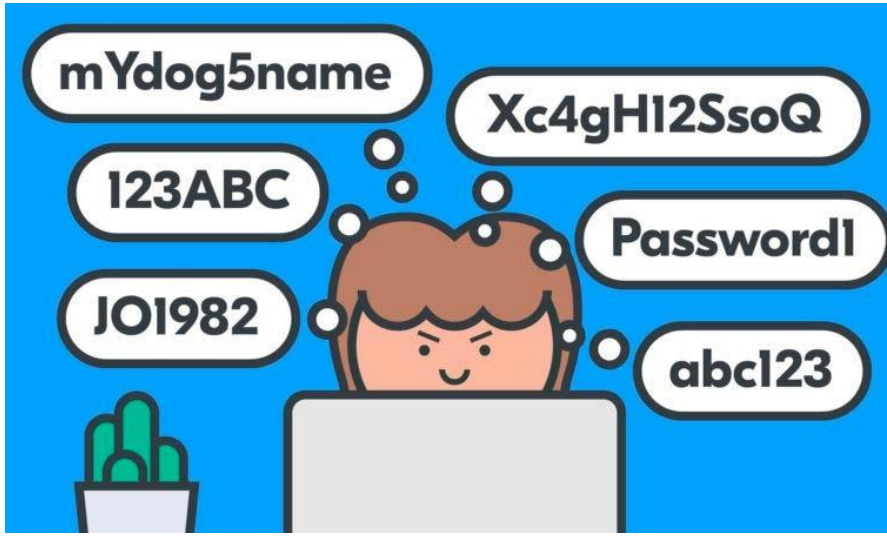
Już wiecie, czego nie robić. Czas na wskazówki jak działać:

- Tworząc hasło używaj frazy – wybierz np. łatwy do zapamiętania cytat z piosenki i użyj pierwszej litery z każdego słowa.
- Litery lub całe słowa zastępuj liczbami i symbolami. Przykład? Słowa „Mam dwadzieścia lat” można zapisać jako M@m2dzie$ciAl4T, a „Mam pieska” jako M@m%p$@sk@%.



Już wiecie, czego nie robić. Czas na wskazówki jak działać:

Specjaliści ds. cyberbezpieczeństwa zalecają też, aby hasła tworzyć przy użyciu trzech losowych słów. Wystarczy, że je połączysz, np. „kawatramwajryba” lub „ścianacienkikoszula”.



Warto wybrać słowa, które zapadają w pamięć, ale unikaj zwrotów łatwych do odgadnięcia (np. „jedendwatrzy”).

Pilnuj się!

- Nie wpisuj hasła, gdy ktoś patrzy Ci przez ramię.
- Nigdy nie wysyłaj hasła w wiadomości e-mail. Hakerzy często wysyłają maile, podszywając się pod np. pracowników pomocy technicznej i prosząc o dane logowania i hasło. Wiarygodne witryny i organizacje nigdy nie poproszą o nazwę użytkownika i hasło w wiadomości e-mail lub przez telefon.
- Zmieniaj hasło natychmiast, gdy zostanie naruszone - jeśli masz choć cień podejrzenia, że ktoś mógł ukraść Twoje hasło, zmień je natychmiast.
- Nie wpisuj hasła na komputerze, który nie należy do Ciebie.

Pilnuj się!

Używanie silnych haseł jest niezbędne, aby chronić swoją tożsamość, dane i informacje. Nie zawsze jest jednak wystarczające do ochrony kont.

Do tego konieczne jest również stosowanie dwuetapowej weryfikacji

Zapraszam do zadawania pytań

Dziękuję za uwagę
Waldemar Serafin