

Jak tworzyć i zapamiętywać silne hasła

Dla uproszczenia możesz po prostu przejść do naszego narzędzia do generowania haseł, które pozwala również przetestować siłę hasła. Jeśli jednak chcesz dowiedzieć się więcej o procesach związanych z generowaniem i zapamiętywaniem haseł oraz chcesz poznać przydatne narzędzia, czytaj dalej.

Za każdym razem, gdy wychodzisz z domu, z pewnością upewniasz się, że zabezpieczasz budynek – w końcu nie chciałbyś wrócić do domu i znaleźć intruza ani odkryć, że twoje cenne rzeczy zniknęły, prawda?

Podobnie, jestem pewien, że nie chciałbyś, aby ktokolwiek uzyskał dostęp do twojego komputera lub jakichkolwiek informacji, które przechowujesz w Internecie.

Dlatego potrzebujesz haseł.

Pod wieloma względami Twoje hasła, w połączeniu z nazwą użytkownika, są kluczem do Twojego cyfrowego życia i tak jak nie używałbyś klucza bez nacięć, nie chciałbyś polegać na słabych danych logowania, aby Cię zatrzymać bezpieczne.

Biorąc pod uwagę fakt, że nazwy użytkownika są używane w wielu różnych witrynach (w końcu jest to zazwyczaj adres e-mail), lepiej, aby twoje hasła były dobre, jeśli mają powstrzymać atakującego przed uzyskaniem dostępu do wszystkich twoich kont.

Zauważysz w tym momencie, że powiedziałem hasła - na pewno będziesz potrzebować więcej niż jednego, ponieważ jeśli tego nie zrobisz, włożysz wszystkie swoje jajka do jednego koszyka - jeśli to jedno hasło zostanie zhakowane lub ujawnione ze względu na stale rosnącą liczbę naruszeń danych, o których wciąż słyszymy, wszystkie Twoje konta internetowe są natychmiast zagrożone w tym samym czasie.

Pomyśl o tym przez chwilę - jak byś się czuł, gdyby ktoś mógł uzyskać dostęp do Twojej poczty e-mail, Facebooka, banku, zarejestrować Cię w nieodpowiednich witrynach i opublikować na Twoim koncie na Twitterze?

Chociaż cierpienie na jedno z powyższych byłoby złe, posiadanie narażenia na każde konto w tym samym czasie byłoby naprawdę tragiczne.

Menedżer haseł

Dlatego polecam menedżera haseł.

Korzystając z wysoko ocenianego programu, takiego jak [N-able Passportal](#), [LastPass](#), [KeePass](#) lub [1Password](#), możesz polegać na tym, że oprogramowanie zapamięta dla Ciebie wszystkie złożone hasła, pamiętając tylko hasło główne do samego programu. Aby uzyskać więcej opcji, sprawdź naszą listę najlepszych menedżerów haseł. Jeśli nadal nie jesteś pewien, przeczytaj nasz przewodnik po zaletach i wadach korzystania z menedżera haseł.

Biorąc pod uwagę, że główną wymówką wielu osób za nieużywanie silnych, unikalnych haseł jest niemożność ich zapamiętania, menedżer haseł jest naprawdę przydatnym narzędziem.

Tworzenie silnego hasła

Po skonfigurowaniu menedżera haseł będziesz dobrze przygotowany do rozpoczęcia tworzenia unikalnych i silnych danych logowania dla każdego konta online pod Twoją kontrolą.

Aby to zrobić, oto 5 wskazówek:

1. wykorzystaj całą klawiaturę - zbyt wiele haseł jest nadmiernie pisanych małymi literami, co czyni je słabymi i łatwymi do złamania. Zamiast tego mieszaj liczby, symbole (!"#\$%^&*) i wielkie litery
2. zmieniaj swoje hasło regularnie - z zainstalowanym menedżerem haseł nie będzie to zbyt uciążliwe zadanie i, jeśli nie będziesz nadążać za wiadomościami o naruszeniu danych, zapewni pewien stopień dodatkowego bezpieczeństwa, jeśli Twoje dane logowania zostaną naruszone przez incydent z osobą trzecią
3. jak już wspomnieliśmy, zawsze, zawsze używaj innego hasła do każdego konta - robienie inaczej to tylko proszenie o kłopoty
4. postaraj się, aby Twoje hasło było jak najdłuższe - im jest krótsze, tym łatwiej zostanie złamane przez automatyczne narzędzia do odgadywania haseł. Celuj w absolutne minimum 8 znaków, a jeśli to możliwe, dużo więcej, zwłaszcza gdy używasz menedżera haseł, który neguje potrzebę zapamiętywania nawet najbardziej skomplikowanych haseł
5. jeśli nie czujesz się do końca komfortowo przy korzystaniu z menedżera haseł, spróbuj połączyć kilka zapadających w pamięć słów - ale tam, gdzie to możliwe, zamień litery na cyfry, np. „e” staje się „3”, „a” staje się „4” i dodaj trochę znaków interpunkcyjnych i innych symbole dla stopnia dodatkowej złożoności

Istnieje kilka pułapek, których należy unikać przy wyborze hasła:

1. NIE używaj danych osobowych jako hasła - możesz pomyśleć, że nikt inny nie zna nazwiska panińskiego twojej matki ani daty urodzenia pierwszoročního, ale mylisz się - internet i rola wyborcza nigdy niczego nie zapominają
2. NIE twórz hasła składającego się wyłącznie z prostych słów, takich jak „kot” lub „Londyn” - atakujący mogą użyć czegoś, co nazywa się atakiem słownikowym, aby złamać takie hasło w milisekundach
3. nigdy nie używaj żadnego hasła, które pojawia się na liście najczęściej używanych, takich jak ponadczasowe klasyki „123456” lub „password1”, ponieważ zaskoczenie, zaskoczenie, często są one pierwszymi, których atakujący będzie próbował użyć, próbując włamać się Twoje konto
4. nigdy, przenigdy nie udostępniaj nikomu swojego hasła - jeśli zadałeś sobie trud stworzenia silnego hasła, dlaczego miałbyś chcieć cofnąć całą tę dobrą pracę, a potem ją oddać? Pamiętaj też, że robienie tego w pracy może być poważnym wykroczeniem i całkiem słusznie
5. nigdy nie wysyłaj hasła w wiadomości e-mail - żadna ważna firma nigdy by Cię o to nie poprosiła. Nigdy też nie podawaj swojego hasła przez telefon - niektóre firmy mogą poprosić Cię o potwierdzenie jednego lub dwóch znaków w celu weryfikacji, ale nigdy całego
6. nie rób tego, aby Twoje hasło było identyczne z nazwą użytkownika - zdarza się to zbyt często i hakerzy doskonale zdają sobie z tego sprawę
7. nigdy nie zapisuj swoich haseł i zdecydowanie nie umieszczaj ich na karteczce przyklejonej do monitora - to tylko prośba o kłopoty
8. również uważaj na tajne pytania - niektóre witryny oferują możliwość odzyskania utraconego lub zapomnianego hasła poprzez wpisanie odpowiedzi na wcześniej wybrane pytanie. Jeśli nie będziesz tutaj ostrożny, możesz niechcący uczynić odpowiednią odpowiedź łatwiejszą do odgadnięcia niż samo hasło.

Jeszcze jedna rada - jeśli witryna oferuje uwierzytelnianie dwuskładnikowe (środek potwierdzania tożsamości za pomocą dodatkowej metody kontroli, takiej jak telefon komórkowy), poważnie rozważ skorzystanie z niego, ponieważ prawie na pewno zaoferuje silne, dodatkowa warstwa bezpieczeństwa.