Jeśli wiesz już jak tworzyć bezpieczne hasła i jesteś świadomy, że powinieneś używać różnych haseł, prawdopodobnie zastanawiasz się teraz, jak je zapamiętać, przechowywać lub nimi zarządzać. Zdecydowanie nie jest to oczywisty temat, więc opiszę różne metody przechowywania haseł, abyś mógł je porównać i zastanowić się, które z nich są dla Ciebie lepsze.

W Twojej głowie!

Ta metoda jest skuteczna, jeśli masz dobrą pamięć i niewielką liczbę haseł. Problem pojawia się jednak, gdy trzeba zapamiętać większą liczbę złożonych haseł, kodów PIN i innych istotnych informacji. Co się stanie, jeśli zapomnisz hasła? Pojawi się procedura przypomnienia (jeśli taka istnieje). W większości przypadków jest to szybkie, ale w innych może być problematyczne, na przykład w przypadku haseł do kont bankowych lub zaszyfrowanych kontenerów. Tak więc, metoda może być dobra, ale tylko w kilku przypadkach, takich jak hasła główne.

Na papierze

Zwykle nie polecam tej metody przechowywania haseł. Zwłaszcza, jeśli są one przechowywane w łatwo dostępnym miejscu, takim jak biurko, pod klawiaturą lub przyklejone do monitora. Każdy odwiedzający może wtedy zobaczyć je zapisane na kartce papieru. Zdarzały się nawet przypadki, że hasła przyklejone do monitora były widoczne dla telewidzów podczas wywiadów!

Istnieją jednak co najmniej dwa przypadki, w których zapisywanie haseł na papierze może być dobrym pomysłem. Po pierwsze, w testamencie ze wskazaniem dla rodziny, do czego służy to hasło i gdzie go używać (aby im to ułatwić). Po drugie, przechowywanie ważnych haseł, gdzieś głęboko i bezpiecznie, w kopercie z pieczęcią. Może to być na przykład przechowywane w skrytce depozytowej. Taka metoda może być dobra w przypadku rzadko używanych, ale wartościowych haseł, takich jak 12-wyrazowe klucze prywatne do portfeli blockchain.

Menedżer haseł „w przeglądarce”

Chociaż ta metoda jest łatwa i pozwala na korzystanie z haseł na dowolnym urządzeniu bez konieczności ich zapamiętywania, w ten sposób zezwalasz dostawcy menedżera haseł na dostęp do Twoich haseł. Może to być Google (jeśli używasz Chrome) lub Mozilla (jeśli używasz Firefox). Powstaje więc pytanie: jak bardzo ufasz

swojemu dostawcy przeglądarki w zakresie swoich najbardziej wrażliwych danych? Ponieważ jednak jest niezwykle prosty w użyciu i synchronizacji, może być dobrą opcją dla mniej wrażliwych danych, takich jak hasła do forów hobbystycznych.

Komercyjni dostawcy przechowywania haseł

Niektóre firmy oferują wtyczki do przeglądarek, takie jak 1Password, LastPass lub Bitwarden – które są całkiem dobre i zazwyczaj mają więcej opcji niż wbudowane menedżery haseł w przeglądarce. Problem z nimi jest jednak taki sam, jak w przypadku menedżera haseł w przeglądarce – musisz zaufać firmie w kwestii swoich haseł. Większość z nich ma zarówno darmowe, jak i płatne opcje, więc można je wypróbować przed zakupem właściwego planu.

Możesz również zadać sobie pytanie, czy te menedżery haseł są bezpieczne – w przeszłości zdarzały się wycieki i jeśli tak się stało z wybranym dostawcą, możesz chcieć pomyśleć jeszcze raz. Nawet jeśli ufasz firmie, że nie wykorzysta twoich haseł do złych celów, prawdopodobnie powinieneś zapytać wybranego dostawcę haseł: co się stanie, jeśli zostaniesz zhakowany? Pamiętaj, że nadal będziesz potrzebować hasła głównego, aby odblokować dostęp do innych haseł.

Zapisz w pliku

.

Ale absolutnie nie w postaci zwykłego tekstu, ponieważ istnieje wiele sposobów na łatwe złamanie haseł w postaci zwykłego tekstu. Powinieneś używać dedykowanego menedżera haseł. Oczywiście, ponownie pojawia się kwestia zaufania dla twórców kodu, jednak zawsze istnieją sposoby, aby to sprawdzić. Na przykład, KeePass i KeePassX to oprogramowanie Open Source, które pozwala każdemu na przeglądanie kodu źródłowego w celu sprawdzenia, czy jest on bezpieczny.

>

Jeśli chodzi o synchronizację między wieloma urządzeniami, możesz po prostu dodać plik z hasłem do dowolnego dostawcy synchronizacji. Plik jest szyfrowany (wybraną metodą: AES, Serpent, Blowfish itp.), więc jest bezpieczny, nawet jeśli dostawca chmury zachowuje się złośliwie lub zostanie zhakowany.

Ale pamiętaj o swoim haśle głównym – bez niego nie będziesz w stanie uzyskać

dostępu do zaszyfrowanych haseł – nigdy! Szyfrowanie plików haseł w menedżerach haseł jest niezwykle poważne i nawet brutalna siła będzie problematyczna ze względu na użycie wielu rund szyfrowania!

Używaj 2FA!

.

Technicznie nie jest to kolejna metoda przechowywania haseł, ale dodatkowa warstwa zabezpieczeń. Jest to po prostu kolejny sposób na udowodnienie, że jesteś faktycznym właścicielem hasła. Uwierzytelnianie dwuskładnikowe może przybierać różne formy: mobilnej wiadomości tekstowej, potwierdzenia e-mail lub aplikacji uwierzytelniającej (takiej jak Google Authenticator).

Wybierz najbardziej niezawodną ochronę

.

Nie jesteś pewien, czy Twoje hasła są bezpiecznie przechowywane lub szukasz rozwiązania biznesowego do zarządzania hasłami? Napisz do nas i porozmawiajmy. Wiemy najlepiej, jak bezpiecznie przechowywać hasła – w końcu mamy wiele do stracenia, jeśli nasze metody okażą się błędne. Dane naszych klientów i reputacja firmy to tylko dwie z wielu konsekwencji, z którymi musielibyśmy się zmierzyć, gdyby nasze hasła wyciekły. Zawsze chętnie pomożemy! Bezpieczeństwo naszych klientów jest najważniejsze.

>