Biuletyn Bezpieczeństwa Komputerowego

Siła haseł

Czy jesteś zmęczony ciągłym tworzeniem skomplikowanych haseł? Frustruje konieczność zapamiętywania i wpisywania wszystkich tych znaków, symboli i cyfr? Jest na to rozwiązanie: silne hasła!

Hasła w formie zdań

Być może nie zdajesz sobie z tego sprawy, ale hasła są jednym z głównych wektorów ataku cyberprzestępców. Przestępcy atakują Twoje hasła i jeśli uda im się je odgadnąć lub złamać, mogą z łatwością uzyskać dostęp do Twojej poczty e-mail i kont bankowych. Im słabsze hasła, tym łatwiej je złamać. Dlatego silne hasła są jednym z najskuteczniejszych sposobów ochrony kont i cyfrowego życia. Tradycyjnie mówi się, że trzeba używać bardzo złożonych haseł. Zamysł tego był taki, że im większa złożoność, tym trudniej cyberprzestępcom i ich zautomatyzowanym programom odgadnąć hasło. Problem w tym, że złożone hasła są trudne zarówno do zapamiętania, jak i poprawnego wpisania. Jeszcze lepszym sposobem na utworzenie silnego i bezpiecznego hasła jest coś, co nazywa się passphrase(hasło w formie zdania lub wyrażenia). Zamiast złożoności, są one mocne ze względu na swoją długość. Oto kilka przykładów:

Czas na bardzo mocną kawę!
samotny-motyl-przy-plaży

Passphrase to nic innego jak ciąg wyrazów, który może zawierać ponad dwadzieścia znaków, jeśli witryna na to pozwala. To może wydawać się przytłaczające, ale oba powyższe przykłady zawierają więcej niż dwadzieścia znaków i w przeciwieństwie do haseł, hasła są znacznie łatwiejsze do zapamiętania i prostsze do wpisania. Im dłuższe wyrażenie, tym bezpieczniejsze. W niektórych sytuacjach możesz zostać poproszony o dodanie większej złożoności do hasła — np. dodanie symboli, wielkich liter lub cyfr. Najłatwiej to zrobić, modyfikując niektóre litery hasła za pomocą symboli lub cyfr. Na przykład, zastępując literę a cyfrą 4, powyższe przykłady staną się bardziej złożone, ale nadal będą wystarczająco łatwe do zapamiętania i wpisania:

Cz4s n4 bardzo mocn4 kawe!
s4motny-motyl-przy-pl4zy

Niech będą unikatowe

Aby hasło było naprawdę bezpieczne, musi być unikalne dla każdego konta. Jeśli ponownie użyjesz tego samego hasła lub wyrażenia zawierającego łatwy do zidentyfikowania wzór do wielu kont, narażasz się na niebezpieczeństwo.

Atakujący musi jedynie poznać witrynę, z której często korzystasz, ukraść hasło, którego używasz do tej konkretnej witryny, a jeśli wszystkie Twoje hasła/wyrażenia są takie same, uzyska dostęp do wszystkich pozostałych kont. Nie jesteś w stanie zapamiętać tych wszystkich długich, unikalnych haseł do każdego konta? Mamy dla Ciebie rozwiązanie: menedżery haseł.

Menedżery haseł to specjalne programy komputerowe, które bezpiecznie przechowują wszystkie hasła w zaszyfrowanej bazie chronionej głównym hasłem. Aby uzyskać dostęp do bazy, wystarczy zapamiętać główne hasło. Menedżer haseł może automatycznie używać hasła, kiedy tylko go potrzebujesz i automatycznie logować się do witryn internetowych. Menedżery haseł rozwijają się, aby zawierać inne funkcje, w tym przechowywanie odpowiedzi na tajne pytania, ostrzeganie w przypadku ponownego użycia hasła lub trafienia na fałszywą witrynę internetową, korzystanie z generatorów, które utworzą silne hasła lub wyrażenia i wiele innych. Większość menedżerów haseł zapewnia także bezpieczną synchronizację na prawie każdym komputerze lub urządzeniu, więc niezależnie od tego, jakiego systemu używasz, masz łatwy dostęp do wszystkich swoich haseł.

Ostatni krok – uwierzytelnianie wieloskładnikowe

Ostatnim krokiem, aby wyrażenia były naprawdę niezawodne, jest dodanie do nich drugiej warstwy ochrony — uwierzytelniania wieloskładnikowego (MFA). Uwierzytelnianie wieloskładnikowe wymaga dodatkowego potwierdzenia tożsamości podczas logowania się na swoje konta. Może to być Twoje hasło i dane biometryczne, takie jak odcisk palca; lub może to być Twoje hasło i automatycznie wygenerowany kod numeryczny, który zostanie wysłany na inne urządzenie lub konto e-mail. Kod jest za każdym razem unikalny i można go wygenerować z telefonu komórkowego lub innego zaufanego urządzenia. Ten proces gwarantuje, że nawet jeśli cyberprzestępca zdobędzie Twoje hasło, nadal nie będzie mógł dostać się na Twoje konto. Uwierzytelnianie wieloskładnikowe należy włączyć zawsze, gdy jest to możliwe, szczególnie w przypadku najważniejszych kont, takich jak konta bankowe lub osobiste konta e-mail. Jeśli korzystasz z menedżera haseł, zdecydowanie zaleca się zabezpieczenie go silnym hasłem ORAZ drugim składnikiem.

Hasła w formie wyrażeń to świetny sposób na prostsze zabezpieczenie kont. Aby cyfrowe życie było jeszcze prostsze i bezpieczniejsze, sugerujemy połączenie haseł w formie zdań, menedżerów haseł i uwierzytelniania wieloskładnikowego.

Redaktor gościnny

Quintana Pattersonjest kierownikiem ds. klinicznych i zgodności IT w kampusie medycznym Uniwersytetu Kolorado w Anschutz oraz przewodniczącą komisji na rzecz praw własności WiCyS (Kobiety w cyberbezpieczeństwie). Zależy jej na tym, aby kobiety w tej branży czuły się mile widziane, wspierane i cenione.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/
Biometria https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Zabezpieczenie kont online: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz