Hasła są nieodzowną częścią korzystania z komputerów i urządzeń mobilnych podłączonych do Internetu. Używamy ich regularnie każdego dnia, niemal wszędzie: do naszych e-maili, kont bankowych, przechowywania danych w chmurze, dostępu do kont; w pracy i w domu.

Niektóre hasła są łatwiejsze do odgadnięcia niż inne.

Niektóre hasła są łatwiejsze do odgadnięcia niż inne. Co powinniśmy zrobić, aby nasze konta i dane były bezpieczne? Oto kilka pomysłów.

Hasła powinny być długie!

Jedną z metod hakerskich jest stosowanie tak zwanych *ataków brute force*. Polegają one na odgadnięciu każdego możliwego hasła. Hakerzy mogą próbować brute force albo bezpośrednio do systemu, albo – jeśli uzyskali dane – na hashach haseł. Dlaczego więc utrzymywanie długich haseł jest ważne?

Wyobraźmy sobie odgadnięcie każdego możliwego hasła, zaczynając od 3 liter. Będzie to wyglądać następująco: *aaa, aab, aac, aad* i tak dalej. W przypadku nowoczesnych komputerów z szybkim GPU wypróbowanie wszystkich kombinacji 3-literowych słów zajmie jedną *milisekundę*. W przypadku 5 znaków z cyframi zajmie to 1 sekundę. Jeśli zwiększymy tę liczbę do 7 – zajmie to 29 minut. Przy 8 znakach zajmie to około 1 dnia, a przy 9 znakach zajmie to około 3 miesięcy.

Oczywiście, hakerzy mogą używać botnetów, aby znacznie przyspieszyć ten proces, ale widać, jak niezbędny czas na złamanie hasła wydłuża się z każdym znakiem. Musimy więc używać długich haseł!

>

Hasła nie powinny być jednowyrazowe

Kolejną metodą stosowaną przez hakerów jest używanie słownika. Oznacza to, że zamiast próbować każdej kombinacji, jak w poprzednim przykładzie, haker będzie próbował tylko słów. Słowniki mogą być bardzo ogólne. Mogą próbować każdego słowa z *Encyclopedia Britannica* lub innego specjalnie spreparowanego (na przykład dla określonego języka) słownika. Oznacza to, że haker może próbować włamać się na twoją stronę internetową, tworząc słownik ze wszystkich słów faktycznie używanych na twojej stronie i ich synonimów.

>

Ale uwaga! Słownik dla hakera jest tylko bazą dla hasła! Oznacza to, że haker próbujący dostać się na stronę wynajmującego będzie próbował nie tylko haseł takich jak landlord, home, renting, ale także ich modyfikacji. Popularną metodą jest wzięcie roku początkowego – landlord1990 – lub z kombinacjami – jak LandlordCT90. Jak widać, ostatnie hasło – LandlordCT90 – jest dość długie, ale w rzeczywistości jest dość podatne na atak słownikowy.

Hasła są jak chusteczki – powinny być używane tylko raz!

Wyobraź sobie sytuację, w której masz bardzo silne hasło, ale używasz go wszędzie: do konta bankowego, do poczty e-mail, do smartfona, także do konta PC – ale także do mniej znaczących rzeczy, takich jak forum motoryzacyjne lub gra przeglądarkowa. Podczas gdy włamanie na konto bankowe jest oczywiście znacznie bardziej skomplikowane, hakerzy celują również w mniej zabezpieczone systemy. Powiedzmy teraz, że gra przeglądarkowa miała błąd, który pozwalał hakerowi zobaczyć całą bazę danych – z twoim adresem e-mail i hasłem w środku.

>

Co będzie dalej? Haker spróbuje sprawdzić, czy to hasło pasuje również do Twojego adresu e-mail – oczywiście, że tak! Następnie może przejrzeć twoje e-maile, aby znaleźć e-maile z twojego banku – jak miesięczne wyciągi – gdzie znajduje się twój numer konta bankowego. A następnie, mając zarówno konto bankowe, jak i hasło, może faktycznie zobaczyć wszystkie środki na koncie! Przerażające, nieprawdaż?

>

Aby temu zapobiec, radzę używać różnych haseł wszędzie. Oczywiście nikt nie jest w stanie zapamiętać setek haseł – w takim przypadku powinieneś użyć menedżera haseł, takiego jak Keepass, Bitwarden lub 1password. Jeśli to nie jest rozwiązanie dla ciebie – następnie spróbuj zrobić 3 różne hasła, które możesz zapamiętać – jeden dla ważnych, *wysokiego poziomu* rzeczy (takich jak konto bankowe), drugi dla mniej ważnych rzeczy (takich jak e-mail), a ostatni dla rzeczy, które mają najmniej znaczące informacje (takie jak gry przeglądarkowe). Powinieneś więc rozważyć różne opcje przechowywania haseł.

Oczywiście powinieneś używać uwierzytelniania dwuskładnikowego (za pomocą wiadomości tekstowej, klucza sprzętowego, aplikacji uwierzytelniającej), szczególnie w przypadku usług *wysokiego poziomu*.

Długi czy skomplikowany?

Podczas rozważania siły hasła, dwa czynniki są brane pod uwagę najbardziej: jeden to długość hasła, a drugi to ilość różnych użytych znaków (takich jak małe i wielkie litery, cyfry, znaki specjalne itp.) Istnieje coś takiego jak *entropia*, która jest miarą nieprzewidywalności hasła. Im wyższa entropia, tym lepiej. Bez wchodzenia w szczegóły obliczania entropii, porównajmy kilka haseł: pierwszym będzie *Kate1990* – to hasło ma 8 liter, wielkie litery i cyfry i jest łatwe do zapamiętania. Drugie to *De$.F9c1* – to jest bardzo trudne do zapamiętania, ale zawiera również znaki specjalne. I trzeci – *Let-sPlayAt8AM* – który jest dłuższy, zawiera wielkie litery, znak specjalny, liczbę i jest dość łatwy do zapamiętania.

>

Wiesz już, że pierwsze hasło byłoby łatwe do odgadnięcia, ponieważ zostałoby znalezione w ataku słownikowym. Jego entropia wynosi w rzeczywistości 27 bitów, co jest bardzo niskie i nigdy nie powinno być używane. Nie tylko jest podatne na atak brute force, ale także na atak słownikowy. Drugie hasło jest nieco lepsze – jego entropia wynosi 34 bity – chociaż jest bardzo trudne do zapamiętania i wpisania. Ale trzecie hasło & rsquo; entropia wynosi 70 bitów – to & rsquo; jest BARDZO silne i faktycznie bardzo łatwe do zapamiętania! Dla porównania, do ochrony konta bankowego zalecałbym użycie hasła, które ma co najmniej 60 bitów entropii – więc to by się kwalifikowało.

Szybkie podsumowanie

Myślę, że ten krótki przewodnik ułatwił ci zrozumienie, w jaki sposób powinieneś konstruować swoje hasła i o czym powinieneś pamiętać podczas konstruowania dobrych haseł, których nie zapomnisz. Jeśli obawiasz się, że Twoje hasło mogło zostać złamane, możesz spróbować sprawdzić je na stronie https://haveibeenpwned.com/. Oczywiście, ten poradnik nie obejmuje wszystkiego, to tylko wierzchołek góry lodowej, ale myślę, że od teraz będziesz w stanie uczynić swoje dane jeszcze bezpieczniejszymi.

SAILINGBYTE

>