Bitdefender

Ochrona ważnych informacji: czy używanie różnych wariantów tego samego hasła jest bezpieczne?

07.11.2023

Z podstawowych zasad dotyczących higieny cyberbezpieczeństwa wynika, że nie powinniśmy ponownie używać tego samego hasła na różnych kontach. Takie postępowanie tworzy wytrychy dla cyberprzestępców, którzy mogą zagrozić Twojemu cyfrowemu życiu. Jednak spójrzmy prawdzie w oczy. Niewiele osób chce (lub jest w stanie) zapamiętać kilkanaście różnych haseł do TikTok, Instagram, Snapchat, Facebook, do rezerwacji lotów i pokoi hotelowych, płacenia rachunków itp. Dlatego zespół Bitdefender postanowił przygotować krótki poradnik, w jaki sposób tworzyć bezpieczne hasła.

Różne warianty tego samego hasła – czy to bezpieczne?

Zgodnie z wynikami najnowszych badań Bitdefender połowa internautów używa tego samego hasła do wszystkich swoich kont online. Jedna trzecia przyznaje, że tworzy kilka haseł, a następnie używa ich ponownie, a około jedna czwarta powszechnie używa prostych (słabych) haseł. Niektórzy jednak przyjmują inne podejście – remiksowanie tego samego hasła na różnych kontach, używając różnych dodatków, na przykład:

TikTok –> Hasło T1kT0k

Facebook –> Fac3b00khasło

Twitter (teraz X) –> Tw1tt3rhasło

Jest to z pewnością mądrzejsze niż używanie wszędzie tego samego hasła, ale wiąże się z dużą dawką ryzyka. Dlaczego?

Zmotywowany atakujący może znaleźć wzór

Używanie logicznych zamian znaków do remiksowania haseł wymaga wzorca – najprostszym przykładem jest powyższy przykład, obejmujący część statyczną i część dynamiczną.

„Jeśli ktoś odkryje Twój wzór, może łatwo złamać Twoje pozostałe hasła. W pewnym sensie jest to prawie tak samo ryzykowne, jak używanie wszędzie tego samego hasła, co oznacza, że tworzysz pojedynczy punkt awarii, który hakerzy mogą wykorzystać do złamania Twoich pozostałych kont” – mówi Dariusz Woźniak z firmy Marken

Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Na przykład, jeśli przypadkowo padniesz ofiarą oszustwa typu phishing, cyberprzestępca może wykryć Twój punkt odniesienia i spróbować znaleźć Twój wzór, aby odkryć hasła do innych kont.

Blokady kont

Ideą stosowania remiksów tego samego hasła jest ułatwienie zapamiętania unikalnych haseł. Jednak dla tych, którzy zarządzają dziesiątkami różnych kont w Internecie, metoda remiksu może być myląca i możesz zapomnieć, jakiej odmiany użyłeś dla konkretnego konta. Może to prowadzić do scenariuszy resetowania haseł i blokowania kont.

Niektóre aplikacje i usługi mają zasady, które zablokują Twoje konto po określonej liczbie nieudanych prób logowania. Jeśli próbujesz zapamiętać odmiany hasła, to co prawda masz coraz mniej problemów związanych z cyberbezpieczeństwem, jednak może to także doprowadzić do tego, że Twoje konta zostaną zablokowane. Ostatnią rzeczą, której chcesz, jest utrata konta, którego potrzebujesz do wykonywania pracy lub płatności bankowych.

Upychanie poświadczeń i brutalne wymuszanie

Hakerzy często korzystają z list znanych nazw użytkowników i haseł wyciekających w wyniku naruszeń bezpieczeństwa danych, aby

przeprowadzać ataki polegające na fałszowaniu danych uwierzytelniających na popularnych stronach internetowych, z których wszyscy korzystają, takich jak platformy mediów społecznościowych. Jeśli znajdą jedną odmianę Twojego hasła, mogą spróbować użyć podobnych odmian, aby uzyskać dostęp do innych Twoich kont.

Podobnie, jeśli atakujący celuje w Ciebie, może spróbować brutalnie wymusić Twoje hasło, systematycznie wypróbowując jego odmiany.

Remiksy czytelne gołym okiem

Jeśli używasz odmian haseł, najprawdopodobniej oznacza to, że Twoje hasła są czytelne – a nie silne, jak hasła generowane maszynowo (1!4@5#HG$L&^%... itp.). Oznacza to, że jeśli ktoś zobaczy Twój ekran podczas logowania, nie tylko zobaczy Twoje hasło podczas jego wpisywania, ale może również zauważyć wzór. Jeśli hasło było łatwe do zapamiętania, mogą spróbować złamać logikę stojącą za nim i zhakować Twoje inne konta.

Krótko mówiąc, staraj się unikać remiksowania haseł

Używanie remiksowanych haseł jest wygodne i na pewno lepsze niż używanie wszędzie tego samego hasła. Jednakże, jak opisano w powyższych scenariuszach, praktyka ta wprowadza różne zagrożenia bezpieczeństwa, które mogą prowadzić do naruszenia bezpieczeństwa wielu kont, a nawet ich blokady. Hasła są ważnym atutem i muszą być strzeżone w sposób święty. Pamiętaj, aby do każdego konta używać unikalnych, silnych haseł, najlepiej zarządzanych przez menedżera haseł,

włączaj uwierzytelnianie wieloskładnikowe w każdej usłudze, która to oferuje i zawsze korzystaj ze skutecznego systemu antywirusowego.

Źródło: https://bitdefender.pl/czy-uzywanie-roznych-wariantow-tego-samego-hasla-jest-bezpieczne/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 07.11.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.