UŻYTKOWNICY NIE ZMIENIAJĄ HASEŁ PO WYCIEKACH DANYCH

Użytkownicy nie zmieniają haseł po wyciekach danych i często korzystają z nich, mimo że zostały wykradzione - wynika z badania Google'a i Uniwersytetu Stanforda. Eksperci ocenili, że 1,5 proc. wszystkich kont usług internetowych zabezpieczają skradzione hasła.

Google zwraca uwagę, że w wyniku wielkich wycieków danych miliardy haseł dostępowych i loginów znalazły się bez żadnego zabezpieczenia w internecie. Znaczna część tych danych padła również łupem cyberprzestępców, którzy w swoich działaniach bardzo często wykorzystują metodę siłowego, zmasowanego logowania z użyciem zgromadzonych haseł do różnych kont w usługach internetowych. Według koncernu z Mountain View osoby, które używają do logowania tych samych danych (takich jak e-mail i hasło), mimo że ich bezpieczeństwo zostało naruszone w wyniku wycieku, same wystawiają się na ryzyko.

Google alarmuje, że powyciekowe hasła znaleziono w użyciu w usługach na ponad 746 tys. niepowtarzalnych domen internetowych. Jak twierdzą specjaliści, najbardziej narażone na przejęcie są konta użytkowników usług streamingowych oraz stron dla dorosłych (nawet 6,3 proc. wszystkich kont korzystało z haseł, które wyciekły już do sieci).

Jednocześnie jedynie 0,3 proc. wszystkich kont w usługach finansowych swoje zabezpieczenie opierało na potencjalnie zdobytych przez cyberprzestępców hasłach. W sektorze domen rządowych odsetek takich kont wyniósł zaledwie 0,2 proc. - wynika z badania przeprowadzonego przez specjalistów Google'a i Uniwersytetu Stanforda. Na blogu firmowym koncernu wskazano, że strony, na których znajdują się usługi finansowe i te działające w domenie .gov, mogą być bezpieczniejsze, gdyż zazwyczaj wymagają od użytkowników podania silniejszych i trudnych do zapamiętania haseł, co zmniejsza prawdopodobieństwo ich ponownego wykorzystania.

Z danych pozyskanych przez Google'a dzięki wtyczce do przeglądarki Chrome o nazwie Password Checkup pozwalającej na wykrycie naruszonych przez hakerów kompletów danych uwierzytelniających wynika, że użytkownicy podejmowali próbę zresetowania jednego na cztery (86 proc.) takich haseł. 94 proc. z nowo wybranych kodów dostępu było silniejszych bądź tak samo mocnych, jak hasło pierwotne, a 60 proc. było wystarczająco silnych, by zabezpieczać konto przed atakiem typu brute-force z użyciem zdefiniowanego przez hakerów słownika.

Wtyczka Password Checkup została wydana w lutym tego roku. Jej zadaniem jest ostrzeganie użytkowników przed możliwym naruszeniem bezpieczeństwa danych, z których korzystają do logowania się w usługach internetowych. W badaniu, które specjaliści zaprezentowali na sympozjum bezpieczeństwa w kalifornijskim Santa Clara, oparto się na danych pozyskanych z analizy 21 mln kompletów danych do logowania pochodzących od ponad 650 tys. użytkowników.

Według Google'a obecnie ponad 4 mld zestawów danych uwierzytelniających należy uznać za

publicznie dostępne dla potencjalnych cyberprzestępców, a zatem - za niezdatne do użytku.