Jedno hasło do wszystkiego, czyli…do niczego

Nie dla wszystkich są jasne elementarne zasady korzystania z bezpiecznych haseł. Z najnowszego badania BIK wynika, że co dziesiąty Polak używa jednego wspólnego hasła do wszystkich swoich urządzeń, aplikacji i kont internetowych włącznie.
- Takie podejście znacznie zwiększa ryzyko naruszenia bezpieczeństwa informacji. W przypadku kradzieży jednego hasła, cyberprzestępcy mogą uzyskać dostęp do wielu kont jednocześnie - mówi Andrzej Karpiński, szef bezpieczeństwa Grupy BIK i podaje praktyczne wskazówki bezpiecznego hasła.

W dzisiejszym cyfrowym świecie bezpieczeństwo naszych urządzeń, kont, witryn, z których korzystamy jest kluczowe dla ochrony naszej prywatności, danych osobowych, a nawet pieniędzy. Skuteczną zaporą dla cyberprzestępców są hasła, ale pod warunkiem, że tworzymy je i używamy z głową.

Hasła towarzyszą na co dzień nie tylko osobom zaangażowanym zawodowo. Nawyk uwierzytelniania wszedł nam w krew w efekcie licznych kampanii edukacyjnych instytucji finansowych, w tym bankowości elektronicznej, która wręcz wymusza uwierzytelnianie podczas logowania się do kont osobistych z komputera, smartfona czy z aplikacji. Ale uwaga, jeśli posługujemy się jednym hasłem do wszystkich naszych kont, łamiemy zasadę cyberbezpieczeństwa.

Błąd: jedno hasło do wszystkich swoich systemów i kont

Naczelna zasada, której trzeba przestrzegać, by nie martwić się o swoje dane i pieniądze, to unikalność haseł dostępu do swoich urządzeń, do logowania się na różne strony internetowe, takie jak sklepy online, platformy streamingowe czy portale społecznościowe. Z konieczności różnicowania haseł zdaje sobie sprawę prawie połowa (46%) Polaków. To pozytywny znak, że rośnie świadomość ryzyka, jakie wiąże się z używaniem tego samego hasła w wielu miejscach. Jednak nie dla wszystkich ta zasada jest jasna.

Do posiadania jednego hasła do wszystkich systemów przyznaje się co 10-ty Polak, respondent badania opinii, pt. „Bezpieczeństwo urządzeń i logowania", zrealizowanego na zlecenie BIK w kwietniu tego roku.

Na czym polega ryzyko jednego hasła do wszystkiego, **wyjaśnia Andrzej Karpiński, szef bezpieczeństwa Grupy BIK:**- *Unikalne hasła do każdego możliwego systemu są pierwszą linią obrony przed nieautoryzowanym dostępem do naszych danych osobowych i finansowych. Jedno hasło do wszystkiego obarczone jest wielkim ryzykiem naruszenia bezpieczeństwa informacji. W przypadku kradzieży jednego hasła, cyberprzestępca niejako automatycznie otrzymuje klucz dostępu do wielu innych naszych kont i systemów jednocześnie. Uzyskuje dostęp do potencjalnie innych naszych zasobów, np. profili na Facebooku, na Linked In, do kont pocztowych. Taka wiedza na nasz temat to już bardzo duży zakres informacji, groźny w rękach cyberprzestępcy, ułatwiający mu podszywanie się pod naszą tożsamość w banku czy urzędzie.*

Prawda: możliwie najdłuższe hasła mają największą moc

Wzmocnieniem zasady unikalnych haseł do różnych systemów jest tworzenie tzw. haseł silnych. Co to oznacza i jakie czynniki nadają mocy naszym hasłom?

W opinii 56% respondentów badania BIK wpływ na siłę hasła ma ich skomplikowanie. Według nich hasła zawierające kombinację dużych i małych liter, cyfr oraz znaków specjalnych są trudniejsze do odgadnięcia przez potencjalnych hakerów.

Natomiast dwie grupy po 18% respondentów wskazały, że długość hasła i częstotliwość ich zmieniania mogą znacząco przyczynić się do zwiększenia ich zabezpieczeń.

Tylko 8% osób uważa, że w tworzeniu silnych i unikalnych kombinacji, trudnych do złamania przez cyberprzestępców pomaga generator haseł. Wynik ten może wskazywać na brak zaufania do automatycznie generowanych haseł lub niewystarczającej wiedzy na temat tego narzędzia.

Tym, co najbardziej wpływa na bezpieczeństwo haseł, dzieli się i tłumaczy Szef Bezpieczeństwa BIK:

- *Obecnie odchodzi się od praktyki bardzo częstej zmiany haseł na rzecz ich długości i skomplikowania. Długość hasła powoduje bowiem określoną moc obliczeniową, potrzebną na sprawdzenie wszystkich możliwych kombinacji haseł. Przy współczesnych komputerach i ich mocy obliczeniowej zakłada się, że 12-13 znakowe hasła to jest absolutne minimum, a krótsze - komputer jest w stanie złamać w ciągu ułamków sekund.*

Dane z badania pokazują, że użytkownicy internetu coraz bardziej doceniają znaczenie skomplikowanych haseł, jednak pojawia się problem, jak skutecznie zapamiętać, zwłaszcza kilka czy kilkanaście z nich.

- *Zestawienie różnorodnych znaków w wielu różnych długich hasłach może być karkołomne do zapamiętania. Uniwersalnym sposobem na to są możliwie najdłuższe hasła tworzone np. z wykorzystaniem rymowanek, zwrotki piosenki czy powiedzonka, z celowo wplecionym błędem czy znakiem znanym tylko nam. Wówczas stworzymy hasło nieoczywiste a przy tym dla nas proste do zapamiętania* - **dodaje Andrzej Karpiński**.

Narzędzie dla przezornych - ochrona 24/7 przez cały rok

Nigdy nie wiemy, kiedy nasze dane trafią w ręce przestępców. Dlatego oprócz świadomego stosowania i tworzenia haseł warto sięgnąć po ochronę antywyłudzeniową. Sprawdzą się w tym celu *Alerty BIK*, czyli smsy ostrzegające o próbie wykorzystania naszych danych. Działają one w czasie rzeczywistym – przychodzą w momencie, gdy ktoś próbuje zaciągnąć kredyt na nasze dane. Dzięki monitorowaniu zapytań o dane z Rejestru Dłużników BIG InfoMonitor, powiadomienie z Alertem BIK przyjdzie też w sytuacji, gdy ktoś w naszym imieniu podpisuje umowę, np. z firmą telekomunikacyjną na zakup drogiego telefonu z abonamentem. Taki jeden sms może uratować przed stratami finansowymi, uchroni przed nerwami i stresem, pomoże anulować kredyt czy pożyczkę, których sami nie zaciągnęliśmy.

Źródło: Badanie na zlecenie BIK, pt. Bezpieczeństwo urządzeń i logowania, zrealizowane przez Quality Watch, CAWI, N - 1090, 18+, kwiecień 2024 r.

***

Biuro Informacji Kredytowej jest partnerem programu edukacyjnego Nowoczesne Zarządzanie Biznesem, w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym”.

Więcej: www.nzb.pl *oraz* www.facebook.com/NowoczesneZarzadzanieBiznesem