Hasło jest dla hakera jak brakujący element układanki

Przeciętny użytkownik internetu codziennie musi zmierzyć się z zarządzaniem hasłami do kilkunastu lub więcej kont. Rocznie traci na zmienianie i ustanawianie nowych haseł aż 21 godzin. Nie da się jednak od tego uciec. Silne hasło to podstawowa forma ochrony przed cyberprzestępcami, a coraz powszechniej zaczynają ją wspierać dodatkowe sposoby uwierzytelniania. Tymczasem z badania „Cyberbezpieczeństwo Polaków", zrealizowanego dla BIK, wynika, że tylko mniej niż połowa z nas zabezpiecza hasłem wszystkie swoje urządzania elektroniczne. Warto sobie przypomnieć zasady ich tworzenia i korzystania, aby móc spać spokojnie.

Nie do końca doceniamy moc hasła jako zabezpieczenia przed wyłudzeniem danych. Z marcowego badania „Cyberbezpieczeństwo Polaków", wykonanego na zlecenie BIK, wynika, że do zabezpieczania hasłem swoich urządzeń elektronicznych przyznaje się mniej niż połowa (46%) respondentów. A szkoda, bo hasła są konieczne, ważne też, by miały siłę. O tym, czy są odporne na złamanie, decydują dwa czynniki: długość i złożoność. O ciągu liczb 12345 zdecydowanie należy zapomnieć.
- *Hasła stoją na straży ważnych informacji o nas. To jedno z podstawowych zabezpieczeń, jednak by hasło było skuteczne musi być długie i silne. Długie hasło to takie, które składa się z co najmniej 12 znaków. Inny komponent dobrego hasła to jego złożoność. Może ono być skonstruowane z fraz, zawierać kombinacje liter i cyfr. Tu jednak należy pamiętać, by nie były to zwroty oczywiste, łatwe do odgadnięcia daty, imiona czy numery. Pomocą w wygenerowaniu bezpiecznego hasła, może służyć menedżer haseł. Ma on jeszcze dodatkową zaletę, pomaga bezpieczne przechowywać hasła dla różnych kont* - mówi **Joanna Charlińska** z Biura Informacji Kredytowej.

Dobra jakość hasła i nie musisz go zmieniać
Zaangażowanie w cyfrowe transakcje bankowe i zakupy w sieci to permanentne wystawianie się na cyberataki. Oszuści czyhają na przejęcie danych uwierzytelniających, aby zyskać dostęp do cennych informacji, które mogą doprowadzić ich do cudzych pieniędzy. Środkiem do celu jest przejęcie danych uwierzytelniających. To jest jak brakujący element układanki. Łamiąc hasło, otwierają furtkę do innych danych dotyczących tożsamości. Pozyskane informacje, numery kart płatniczych oraz elektroniczne dokumenty mogą zostać wykorzystane m.in. do wyłudzenia kredytu lub pożyczki, zakupów na raty, podpisania umów (np. na abonament telefoniczny) lub do wyprowadzenia pieniędzy z konta bankowego.
Skala przestępstw z wykorzystaniem skradzionej tożsamości rośnie. Raport InfoDok dowodzi, że w samym I kwartale tego roku codziennie udaremniano 25 prób wyłudzeń. W kwartale było ich 2 888, cztery razy więcej niż rok temu. A wielu wyłudzeń nie udaje się wykryć.

Dobre hasło to dopiero początek
Przeciętny użytkownik internetu codziennie mierzy się z zarządzaniem hasłami do kilkunastu lub więcej kont. Chwila do chwili i w ciągu roku na tę właśnie czynność traci aż 21 godzin, podają specjaliści Yubico, firmy z branży technologii uwierzytelniających. Ale czy to konieczne?
Zdaniem specjalistów z NASK nie ma powodu, aby cały czas zmieniać hasła dostępu do poczty lub systemu firmowego. Wystarczy by hasło było silne i złożone. Im dłuższe, tym lepsze.
Jak tworzyć silne hasła oraz właściwie z nich korzystać, prezentuje poradnik i 8 uniwersalnych zasad bezpiecznego hasła.
Dla zmęczonych zarządzaniem niezliczoną liczbą haseł, nie ma dobrych wiadomości. Na zmierzch haseł nie ma co liczyć. Eksperci zauważają wręcz, że by zwiększać bezpieczeństwo danych potrzebne jest nie tylko hasło, lecz również dodatkowy element. Uwierzytelnianie się jedynie za pomocą hasła - a więc jednoskładnikowe - nie jest wystarczające do zapewnienia cyberbezpieczeństwa.

Co ciekawe, w 2021 roku CISA (Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury) dodała uwierzytelnianie jednoskładnikowe do swojej listy złych praktyk. Rekomenduje rozwiązania wieloskładnikowe i uwierzytelnianie użytkowników za pomocą dodatkowych elementów.

Jak logować się jeszcze bezpieczniej

Uwierzytelnianie za pomocą hasła bierze pod uwagę tylko jeden czynnik: **coś, co użytkownik wie**. Gdy wprowadzimy drugi czynnik, czyli **coś, co użytkownik posiada** (np. urządzenie mobilne), poziom bezpieczeństwa rośnie.

- O tym, co ustawimy jako tzw. drugi składnik uwierzytelniania na naszym urządzeniu, decydujemy sami. Najprościej jeśli podczas logowania wykorzystamy odcisk swojego palca. Wbudowany czytnik linii papilarnych posiadają nie tylko nasze smartfony, ale również wiele komputerów. To bardzo wygodna i szybka metoda uwierzytelniania. W ostatnim czasie upowszechniła się także metoda FaceID, polegająca na skanie naszej twarzy przy odblokowaniu smartfona. Kolejną metodą podwójnego logowania i równie popularną, są kody SMS. Jest ona do tego prosta i szybka zważywszy, że każdy z nas ma praktycznie zawsze pod ręką swój telefon. Wartym rozważenia rozwiązaniem są klucze bezpieczeństwa (U2F). Według specjalistów i praktyków są one na ten moment najbezpieczniejszą metodą uwierzytelniania z kategorii posiadania. Ten mały, podobny do pendrive'a, klucz pomaga nawet chronić przed najbardziej zaawansowanymi atakami. To profesjonalne urządzenie, ale z powodzeniem można je zakupić i stosować z domowym sprzętem - mówi **Monika Olesiejuk** z Digital Fingerprints.

Współczesna technologia oferuje jeszcze trzeci istotny czynnik: **to, kim jest użytkownik** (np. weryfikacja behawioralna). To jedna z najwygodniejszych dla użytkownika metod uwierzytelniania.

Można się o tym przekonać już dziś, jeśli np. bank, z którego korzystamy wdrożył system weryfikacji behawioralnej. Jak to działa? Technologia sprawdza czy osoba korzystająca z aplikacji na telefonie, w trakcie logowania na stronę w komputerze jest tą, za którą się podaje. Weryfikacja behawioralna jak wskazuje sama nazwa sprawdza zachowanie logującego czyli sposób korzystania z urządzenia np. tempa pisania na klawiaturze, ruchu myszą, sposobu posługiwania się urządzeniem mobilnym. To przełom w rozwiązaniach uwierzytelniania wieloskładnikowego.

Nowe technologie uwierzytelniające już wchodzą do powszechnego użytku. Warto zainteresować się i zaznajomić z nowymi metodami zabezpieczeń. O silnym haśle oczywiście nie można zapominać, bo to znaczące utrudnienie dostępu do cennych informacji o nas i naszych pieniędzy.

Źródło:
„Cyberbezpieczeństwo Polaków", marzec/kwiecień 2023 r., CAWI, Polacy w wieku 18+, N 1057.

*

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

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