Tworzenie i używanie silnych haseł

Security, Windows 10, Windows 8.1, Windows 7, pulpit nawigacyjny konta Microsoft

Jednym z najważniejszych sposobów zabezpieczania interakcji online jest ochrona własnych haseł. Dobra wiadomość jest taka, że ochrona Twoich haseł leży w naszej gestii. Wszystko, co musisz zrobić, to utworzyć silne hasła, a następnie zachować je w tajemnicy. Postępuj zgodnie z tymi poradami, aby Twoje hasła nie dostały się w niepowołane ręce.

Tworzenie silnych haseł

Bezpieczeństwo haseł zaczyna się od ich siły. Silne hasło to:

- co najmniej o długości 12 znaków, ale składające się 14 lub więcej znaków jest lepsze;
- połączenie wielkich i małych liter, cyfr i symboli;
- Nie powinien to być wyraz, który można znaleźć w słowniku ani imię i nazwisko osoby, postaci, nazwa produktu czy organizacji
- hasło znacząco różniące się od poprzednio używanych haseł;

Porada: Nie chcesz wymyślać własnych silnych haseł? Przeglądarka Microsoft Edge może tworzyć i zapamiętywać unikatowe silne hasła. Zobacz Tworzenie bezpiecznych haseł przy użyciu generatora haseł.

Ochrona haseł

Po utworzeniu silnego hasła należy postępować zgodnie z poniższymi wskazówkami, aby było bezpieczne:

- Nie udostępniaj nikomu swojego hasła — ani znajomemu, ani nawet członkowi rodziny.
- Nigdy nie wysyłaj hasła pocztą e-mail, w wiadomości ani za pośrednictwem jakichkolwiek innych środków łączności, które nie są bezpieczne.
- Używaj unikatowych haseł do każdej witryny internetowej. Jeśli ktoś ukradnie hasło, którego używasz w wielu witrynach internetowych, zagrożone będą wszystkie informacje chronione w nich hasłem.
- Jeśli nie chcesz zapamiętywać wielu haseł, rozważ korzystanie z menedżera haseł. Najlepsze rozwiązania tego typu będą automatycznie aktualizować zapisane hasła, szyfrować je i wymagać uwierzytelniania wieloskładnikowego w celu uzyskania dostępu. Przeglądarka Microsoft Edge może zapamiętywać Twoje hasła i automatycznie je wprowadzać, gdy jest to potrzebne. Zobacz Zapisywanie i usuwanie haseł w Microsoft Edge.
- Nie przechowuj hasła w urządzeniu, które ma ono chronić.
- Zapisywanie haseł jest dobrą praktyką pod warunkiem, że są one przechowywane bezpiecznie. Nie zapisuj ich w notatkach programu Sticky Notes lub na kartach znajdujących się w pobliżu rzeczy, które one chronią, nawet jeśli uważasz, że są one dobrze ukryte.

Ewentualnie mała podpowiedź...

Zamiast zapisywać hasła, warto zastanowić się nad zapisaniem podpowiedzi, która przypomni Ci, jakie jest hasło. Jeśli hasło to „Paris4SpringVacation!”, możesz napisać je w postaci podpowiedzi „Moja ulubiona podróż”.

- Gdy to możliwe, zmień hasło natychmiast, jeśli podejrzewasz, że zabezpieczenia określonych kont mogły zostać naruszone, bądź nawet jeśli sądzisz, że samo hasło stało się przedmiotem włamania.
- Unikaj wprowadzania hasła na urządzeniu, jeśli nie masz pewności, że jest ono bezpieczne. Na urządzeniach wykorzystywanych przez wiele osób lub dostępnych do użytku publicznego może być zainstalowane oprogramowanie do rejestrowania naciśnięć klawiszy, które może przechwycić Twoje hasło podczas wpisywania go. Należy również unikać zezwalania na zapisywanie haseł na komputerach użytkowanych przez wiele osób lub komputerach publicznych.
- Włącz uwierzytelnianie wieloskładnikowe (MFA) zawsze, gdy jest dostępne. MFA to metoda kontroli dostępu, która wymaga do weryfikacji więcej niż jednego poświadczenia, np. zarówno hasła, jak i kodu PIN. Dodaje to kolejną warstwę zabezpieczeń, gdyby ktoś odgadł lub wykradł hasło. Aby uzyskać więcej informacji, zobacz Czym jest: Uwierzytelnianie wieloskładnikowe.

Porada: Jeśli zobaczysz monit o utworzenie odpowiedzi na pytania zabezpieczające, podaj niezwiązaną z nimi odpowiedź. Jeśli na przykład pytanie brzmi: „Jaki kolor lubisz najbardziej?”, możesz odpowiedzieć „Warszawa”. Odpowiedzi na takie pytania nie można znaleźć, przeglądając konta na Twitterze czy Facebooku. (Pamiętaj tylko, aby miały sens, żeby można je było zapamiętać).

Przestępcy mogą próbować złamać Twoje hasło, ale czasem łatwiej jest wykorzystać ludzką naturę i użyć podstępu.

Możesz otrzymać wiadomość e-mail od domniemanego sklepu online (takiego jak eBay czy Amazon) albo odebrać telefon od swojego „banku", a podczas rozmowy ktoś będzie próbował przekonać Cię o „rzeczywistej" potrzebie podania hasła lub innych informacji poufnych. Może to być próba wyłudzenia informacji. (Innym określeniem tego typu oszustw jest *socjotechnika*).

Oto kilka wskazówek, którymi należy się kierować, aby chronić hasła i inne informacje poufne:

- Ogólnie należy zachować ostrożność wobec wszystkich osób, które proszą o podanie informacji poufnych, nawet jeśli jest to ktoś, kogo znasz, lub firma, której ufasz. Oszust mógł na przykład przejąć konto znajomego i wysłać wiadomość e-mail do wszystkich z jego listy adresowej. Zachowaj ostrożność wobec wszystkich niespodziewanych próśb o podanie informacji poufnych.
- Nigdy nie udostępniaj hasła w odpowiedzi na prośbę telefoniczną lub przekazaną pocztą e-mail, np. w celu zweryfikowania Twojej tożsamości, nawet jeśli wydaje się ona pochodzić od zaufanej firmy lub osoby.
- Zawsze uzyskuj dostęp do witryn internetowych przy użyciu zaufanych linków. Oszuści mogą skopiować wygląd komunikatów firmowych, aby przekonać Cię do kliknięcia fałszywego linku lub załącznika, więc zachowaj ostrożność w odniesieniu do linków zamieszczonych w niezamawianych wiadomościach e-mail, SMS lub innych. W razie wątpliwości przejdź bezpośrednio do oficjalnej witryny sieci Web banku lub innej usługi, do której próbujesz uzyskać dostęp za pośrednictwem własnej zakładki lub wpisując prawidłowy adres usługi samodzielnie.

Zobacz też:

Rozwiązania zabezpieczające firmy Microsoft — pomoc i materiały

SUBSKRYBUJ KANAŁY INFORMACYJNE RSS

Potrzebna dalsza pomoc?

Jak możemy Ci pomóc?

Dołącz do dyskusji

ZAPYTAJ SPOŁECZNOŚĆ >

Uzyskaj pomoc techniczną

KONTAKT Z NAMI >

Czy te informacje były pomocne? Tak Nie