Zadbaj o silne hasła do kont. Zniwelujesz zagrożenie cyberatakiem i ochronisz swoje dane, pieniądze

W cyberprzestrzeni coraz częściej przechowujemy wiele cennych informacji – prywatnych i nie tylko. Od nas zależy, czy odpowiednio je zabezpieczymy. Wydział Promocji Polityki Cyfrowej Kancelarii Prezesa Rady Ministrów (KPRM) przypomina, że internetowi przestępcy atakują nie tylko duże przedsiębiorstwa, lecz także zwykłych ludzi. Eksperci namawiają do stosowania silnych haseł do kont bankowych, poczty elektronicznej, na portalach społecznościowych, a także w telefonie czy w komputerze, by nikt ich nie przejął, nie ukradł tożsamości, nie pozbawił oszczędności bądź nie miał dostępu do naszych prywatnych danych. Jak zatem powinniśmy tworzyć kody zabezpieczające?

Mankamenty haseł

Cyfryzacja KPRM podaje, że część cyberataków uderza właśnie w hasła użytkowników, dlatego należy wystrzegać się najpowszechniejszych błędów, a więc unikać prostych haseł i nie używać tego samego kodu zabezpieczającego do różnych kont. Wskazane jest tworzenie unikatowych haseł dla każdej witryny.

Jakich jeszcze błędów nie powinniśmy popełniać? Nie zabezpieczajmy dostępu do swoich danych

najpopularniejszymi hasłami lub oczywistymi wyrażeniami, typu: „hasło”, „123456”, „qwerty”, „piłka nożna”, „wpuscmnie”, ani imieniem własnym bądź kogoś z bliskiego otoczenia, bądź ulubionego zwierzaka. Ta sama zasada dotyczy też danych osobowych, które łatwo zdobyć, takich jak: data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania lub domu.

Niewskazane jest stosowanie wyrażeń identycznych z nazwą użytkownika, lub nawet jej częścią, oraz sekwencji kolejnych liter, liczb lub innych znaków, np. „abcde”, „12345”, „QWERTY”, jak również dwóch lub trzech kolejno powtarzających się ciągów znaków, np. „bbbb2bbb”.

Ponadto odradza się używanie pojedynczego wyrazu dowolnego języka, pisanego normalnie lub wspak, nie wystarczy też, że poprzedzimy lub zakończymy go znakiem specjalnym lub cyfrą.

W komunikacie zwrócono uwagę, by przy zmianie hasła do istniejącego konta nie użyć tego samego sformułowania, co poprzednio lub po niewielkiej modyfikacji, np. zmiana z „hasło1” na „hasło2”.

Cyberklucz

Cyfryzacja KPRM przypomina: „Hasła są jak klucze do sejfu lub domu”. Trzeba dbać, żeby nie dostały się w niepowołane ręce.

Dlatego radzi, aby tworzyć dłuższe hasła, składające się z 12 lub 14 znaków, które będą zawierały co najmniej jeden znak z każdej z następujących grup: małe litery, duże litery, liczby, znaki specjalne.

Konstruując unikatowe hasło, można, jak podpowiadają specjaliści, wykorzystać frazy, wybrać np. łatwy do zapamiętania cytat z piosenki i użyć pierwszych liter poszczególnych słów. Poleca się zastępowanie liter bądź wyrazów liczbami i symbolami.

Podano przykłady: „Mam dwadzieścia lat” można zamienić na M@m2dzie$ciAl4T, a „Mam psa” na M@m%p$@.

Można stosować też metodę łączenia trzech losowych słów, np. „kawatramwajryba”, byleby nie były zbyt proste do odgadnięcia.

Podkreślono, że zabezpieczeń nie powinno się zapisywać na papierze, przesyłać np. w mailu albo wpisywać haseł, gdy ktoś to widzi, bo nawet bardzo silne kody mogą w takich przypadkach okazać się bezużyteczne.

Cyfryzacja KPRM ostrzega przed podszywającymi się np. pod pracowników pomocy technicznej hakerami, którzy próbują wyłudzić dane użytkownika i hasła. Jak zaznaczono: „Wiarygodne witryny i organizacje nigdy nie poproszą o nazwę użytkownika i hasło w wiadomości e-mail lub przez telefon”.

Hasło powinniśmy bezzwłocznie zmienić, jeśli doszło do jego naruszenia lub nawet jeśli tylko przypuszczamy, że ktoś mógł je wykraść.

Nie należy również wpisywać hasła, gdy korzystamy z cudzego komputera.

Aby dane były bezpieczniejsze, potrzebne jest nie tylko silne hasło, lecz także stosowanie dwuetapowej weryfikacji.

Dodatkowe informacje o zabezpieczaniu danych w cyberprzestrzeni można znaleźć w poradniku „Jak chronić się przed cyberatakami”.

Źródła: PAP, Cyfryzacja KPRM.