

Tworzenie bezpiecznych haseł

Autor: Marek
10.10.2008.
Zmieniony 21.10.2008.

Jednym z problemów związanych z hasłami jest fakt, że użytkownicy je zapominają. Aby je pamiętać, używają oni prostych rzeczy, takich jak imię psa, imię syna czy data jego urodzenia, nazwa najbliższego miesiąca – cokolwiek, co da im wskazówkę jakie jest to hasło.

Źródło: netsecurity.about.com
Tłumaczenie: Dawid Kalinowski, Kraków

Dla ciekawskiego hakera, który w jakiś sposób uzyska dostęp do systemu Twojego komputera, odpowiada to zamknięciu drzwi na klucz i włożeniu klucza pod wycieraczkę. Nawet bez uciekania się do jakichkolwiek specjalistycznych narzędzi, haker może odkryć Twoje podstawowe dane osobowe: imię i nazwisko, imiona dzieci, datę urodzin, imiona zwierząt domowych, itp. i wypróbować je wszystkie jako potencjalne hasła.

Aby utworzyć bezpieczne hasło, które będzie łatwe do zapamiętania, postępuj według tych prostych kroków:

- Nie używaj informacji osobistych. Nigdy nie powinniśmy używać danych osobowych jako części hasła. Nie jest to żadne zabezpieczenie. Ktokolwiek może zgadnąć rzeczy takie jak Twoje nazwisko, imię zwierzaka, datę urodzenia dziecka i inne podobne szczegóły.

- Nie używaj prawdziwych słów. Istnieją narzędzia, które pomagają atakującemu odgadnąć hasło. Z dzisiejszą mocą obliczeniową, nie trzeba dużo czasu, aby spróbować każdego wyrazu w słowniku i znaleźć Twoje hasło, więc najlepiej jest, jeśli nie używa się prawdziwych słów jako hasła.

- Mieszaj różne rodzaje znaków. Możesz sprawić, że hasło będzie o wiele bardziej bezpieczne, jeżeli zmieszasz różne rodzaje znaków. Razem z małymi literami wykorzystuj duże, cyfry i nawet znaki specjalne, takie jak '&' lub '%'.

- Używaj frazy kodującej. Zamiast podejmować próby pamiętania hasła, które nie jest słowem ze słownika i zostało utworzone przy użyciu różnych rodzajów znaków, możesz używać frazy kodującej. Wymyśl zdanie lub linijkę z piosenki lub wiersza, który lubisz i utwórz hasło za pomocą pierwszej litery każdego słowa.

Na przykład, zamiast hasła "yr\$1Hes", możesz wybrać zdanie takie jak "I like to read the About.com Internet / Network Security web site" i zamienić je do następującego hasła "ilrtA!nsws". Zastępuj słowo "to"; liczbę "2"; i używaj wykrzyknika w miejsce "i"; słowo "Internet";, można wykorzystać różne rodzaje znaków i stworzyć bezpieczne hasło, które jest trudne do złamania, ale o wiele łatwiejsze do zapamiętania dla Ciebie.

- Używaj narzędzia zarządzania hasłami. Innym sposobem na bezpieczne przechowywanie i pamiętanie hasła jest użycie pewnego rodzaju narzędzia zarządzania hasłami. Narzędzia te utrzymują listę nazw użytkowników i haseł w formie zaszyfrowanej. Niektóre mogą nawet automatycznie wpisywać nazwę użytkownika i hasło na stronach internetowych i w aplikacjach.

Korzystanie z powyższych wskazówek pomoże Ci tworzyć hasła, które są bardziej bezpieczne, ale nadal należy postępować według następujących podpowiedzi:

- Używaj różnych haseł. Należy używać różnych nazw użytkownika i haseł dla każdego logowania lub dla każdej aplikacji, którym chcesz zapewnić zabezpieczenie. Tym sposobem, jeżeli jedna rzecz zostanie naruszona, reszta jest nadal bezpieczna. Innym podejściem, które jest mniej bezpieczne, ale zapewnia sprawiedliwy kompromis między bezpieczeństwem a wygodą jest korzystanie z jednej nazwy użytkownika i hasła na witrynach i aplikacjach, które nie wymagają dodatkowych zabezpieczeń, a wykorzystywanie unikalnych nazw użytkowników i haseł na stronach, takich jak strona banku lub firmy kart kredytowych.

- Zmieniaj swoje hasła. Należy zmieniać swoje hasło co najmniej raz na 30 do 60 dni. Nie należy także ponownie używać tego hasła przez co najmniej rok.

Wprowadź silniejsze hasła: zamiast polegać na tym, że każdy użytkownik komputera zrozumie i będzie postępować zgodnie z powyższymi instrukcjami, można skonfigurować polityki haseł Windows Microsoft w taki sposób, że system nie zaakceptuje hasła, nie spełniającego minimalnych wymagań.

Tłumaczenie: Dawid Kalinowski, Kraków