Hasła – sposoby ich tworzenia i przechowywania

W podręczniku często poruszany jest problem dotyczący tworzenia i przechowywania haseł. Zagadnienia związane z hasłami były w czasie pisania podręcznika tematem kilku rozmów. Wnioski z nich przedstawiono poniżej. Są to pomysły różnych osób – na początku podano informację o statusie zawodowym pomysłodawcy.

Programista, specjalista od baz danych

Aby logować się na stronach internetowych, należy utworzyć hasło. Powinno być ono na tyle proste, aby można je było bez trudu zapamiętać, i jednocześnie na tyle skomplikowane, aby nie dało się go złamać.

Długość hasła ma znaczący wpływ na bezpieczeństwo konta. Wiele formularzy wymusza użycie określonej ilości znaków w haśle.

Hasło może składać się z jednego wyrazu (np. zamczysko) lub krótkiego zdania (np. moje ulubione zamczysko). Poddając je odpowiednim modyfikacjom, otrzymamy trudny do złamania ciąg znaków.

Hasło „zamczysko” można zmodyfikować następująco:

- pierwszą i ostatnią literę zmieniamy na wielką – **ZamczyskO**
  (albo co drugą lub co trzecią literę w słowie zmieniamy na wielką – **ZaMcZySkO**)
- litery „a” zastępujemy znakiem „@” – **Z@McZySkO**
- zamiast litery „O” wpisujemy zero „0” – **Z@McZySk0**

Hasło składające się z krótkiego zdania można zmienić następująco:

- każdy wyraz w zdaniu piszemy wielką literą – **Moje Ulubione Zamczysko**
- każdy wyraz oddzielamy kropką, przecinkiem, myślnikiem, podkreślnikiem lub dowolnym stałym znakiem – **Moje_Ulubione_Zamczysko**
- litery „o” zamieniamy na zera „0”, litery „e” na cyfrę „3” – **M0j3_Ulubi0n3_Zamczysk0**

Oczywiście należy stworzyć swój własny system modyfikacji haseł.

Jak przechowywać hasła? Wszelkiego rodzaju hasła należy odpowiednio zabezpieczyć. Można na przykład gromadzić je w pliku programu Word. Taki plik należy zapisać z zaznaczoną opcją zabezpieczenia dokumentu hasłem przed odczytem.

Innym sposobem może być zapisywanie haseł w zwykłym pliku tekstowym a następnie spakowanie go programem pakującym (np. WinRar) również z zaznaczoną opcją rozpakowania po podaniu hasła.

Oficer Wojska Polskiego

Hasła powinny być traktowane jak bielizna osobista. Należy je często zmieniać i używać tylko swoje.

Jest wiele miejsc w sieci globalnej i lokalnej, gdzie należy zmieniać hasła lub wręcz oprogramowanie wymusza takie działanie. Trzeba wtedy mieć swój unikalny sposób na ich tworzenie. Hasła muszą być łatwe do przypomnienia dla jego autora, ale nie mogą zawierać elementów, które w powiązaniu z autorem będą łatwe do odgadnięcia dla innych.

Jak przechowywać hasła? Najlepiej nigdzie, czyli we własnej pamięci, a jeśli muszą być znane kilku upoważnionym osobom, to należy postępować zgodnie z ustaloną wcześniej odpowiednią procedurą.

Specjalista do spraw systemów informatycznych w zarządzaniu w firmie energetycznej

Wiele serwerów, gdzie zakłada się różne konta podaje możliwe sposoby konstruowania haseł (liczba znaków, wielkość liter, dopuszczalne lub konieczne znaki). Użytkownicy muszą się dostosować – muszą wymyślić treść hasła. Może nim być dziwne zdanie, które zapamiętamy a nikt inny go nie zna. Możemy się posłużyć zdaniem z języka, który nie jest powszechnie używany, na przykład z języka Hobbitów lub plemienia Nawahów.

Kategorycznie nie należy używać kompilacji własnych imion, nazwisk i dat urodzenia. Jest to zbyt łatwe do odgadnięcia. **Pod żadnym pozorem nie wolno** używać fragmentów *Lorem ipsum* zwłaszcza w serwisach internetowych. Na tym generowanym tekście ćwiczą nie tylko drukarze, ale i hakerzy przy konstruowaniu oprogramowania szpiegowskiego.

Jak przechowywać hasła? Najlepiej we własnej pamięci. Tak należy hasła konstruować, aby można je było sobie przypomnieć. Więcej haseł można „schować" w programie do przechowywania haseł, na przykład w Password Manager. Ma to jednak tę wadę, że i tak trzeba zapamiętać hasło do programu od przechowywania haseł i sobie je wcześniej wymyślić.

Nauczyciel informatyki, administrator szkolnej sieci i ABI w szkole (Administrator bezpieczeństwa Informacji)

Loginy i hasła do kont uczniowskich w szkolnej sieci i do dziennika internetowego najczęściej są generowane przez system a po pierwszym uruchomieniu uczeń może je zmienić zgodnie z sugestiami administratora lub we własny sposób. Tej kwestii jest poświęcony czas na lekcji. Każdy uczeń wie, jak się konstruuje hasła i ma świadomość, że od tego zależy bezpieczeństwo wykonanych przez niego prac. Przy otrzymywaniu danych konta należy zwrócić uwagę na zapis w regulaminie pracowni szkolnej, że uczeń odpowiada za to, czy nie zgubił hasła, nie umożliwił komuś wejścia na jego profil i dokonania tam niewłaściwych zmian. Od właściciela loginu i hasła zależy, jak te dane przechować, aby codziennie móc uruchomić komputer w szkolnej pracowni lub bibliotece i zobaczyć swoje oceny w internetowym dzienniku.

Co z hasłami o dużym znaczeniu? W szkole dostęp do profilu administratora jest zabezpieczony bardzo długim hasłem złożonym z liter wielkich i małych, cyfr i znaków specjalnych. Jego treść wynika z fantazji autora hasła i na pewno nie kojarzy się nikomu z tą osobą. Hasło jest zmieniane niesystematycznie. Ponieważ wszelkie tego typu dane muszą być znane dyrektorowi na wypadek sytuacji awaryjnej, sposób wejścia na profil administratora jest opisany na papierze, w jednym egzemplarzu, umieszczony w zaklejonej kopercie i schowany w sejfie, w gabinecie dyrektora.

Jak ułożyć bezpieczne hasło? Najlepiej trochę poczytać na ten temat i wymyślić własny, unikalny „patent" na tworzenie haseł. Tego sposobu nikomu nie ujawniać. Nie stosować haseł zaproponowanych w przykładach i umieszczonych na tak zwanych listach bezpiecznych haseł, choćby wydawały się nie do odgadnięcia, na przykład:

IdzieGrzsPrzezWiesWorekPi@skuNiesie@PrzezDziurePiasekCiurkiemSypieSieZ@Grzesiem2011