



Hasta



Erasmus+

Wprowadzenie



Source: Flickr

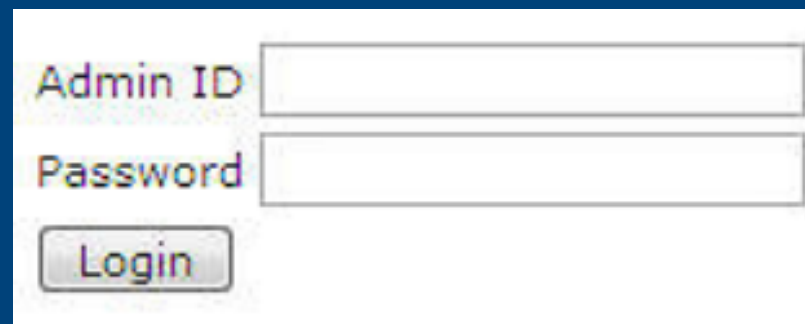
Będące kluczowym narzędziem **identyfikacji** na wielu serwisach online, hasło jest często jedyną barierą ochronną przed niechcianymi włamaniami z potencjalnie katastrofalnymi konsekwencjami.

Jednakże, jest ono narzędziem często źle zarządzanym, ponieważ wielu użytkowników nie waha się, na przykład, korzystać z bardzo prostego hasła.. Sprawia to, że jest ono łatwiejsze go odgadnięcia i złamania. Ważne jest, aby zdawać sobie sprawę z wagi haseł, i wiedzieć, jak łatwo je zabezpieczyć, zachowując je w pamięci.

Identyfikacja użytkownika

Korzystanie z komputerów często wiąże się z identyfikacją użytkowników.

Najpopularniejsza technika opiera się na parze „login / hasło”. W zależności od sytuacji identyfikator może być publiczny lub prywatny, ale często jest słabo chroniony. Hasło to narzędzie zapewniające podstawowe bezpieczeństwo.

A screenshot of a web login form. It features two input fields: the top one is labeled "Admin ID" and the bottom one is labeled "Password". Below these fields is a button labeled "Login". The labels and button text are in a blue, sans-serif font.

Source: Flickr

■ Duże ryzyko: kradzież tożsamości

Definicja z Wikipedii :

Kradzież tożsamości to **celowe wykorzystanie tożsamości innej osoby**, zwykle stosowane jako metoda uzyskania korzyści finansowej lub kredytu i innych korzyści w imieniu drugiej osoby, często na jej niekorzyść.

Kwestia:

Określenie związku między naruszeniami danych a kradzieżą tożsamości jest trudne, przede wszystkim dlatego, że ofiary kradzieży tożsamości często nie wiedzą, w jaki sposób uzyskano ich dane osobowe, a kradzież tożsamości nie zawsze jest wykrywalna przez poszczególne ofiary

A więc...

Operatorzy, którzy żądają identyfikacji, muszą wdrożyć wiele środków bezpieczeństwa do zarządzania hasłami. To bardzo ważna kwestia, ale mamy nad nią niewielką kontrolę.

➔ Korzystaj z hasła, które będzie ciężkie do odgadnięcia przez hackera

- *Unikaj podstawowych haseł, takich jak 12345, azerty, daty urodzenia, tego samego hasła co login itp.*
- *Hasło musi być długie (co najmniej 14 liter / cyfr)*
- *Musi być zróżnicowane (wielkie litery, małe litery, cyfry, specjalne znaki itp.)*
- *Poważny operator zastosuje pewne środki bezpieczeństwa, takie jak ograniczona liczba prób, captcha*



Źródło: FlickrR

Jednak...

Większość ludzi posiada wiele kont i ważne jest by mieli do nich różne hasła. W rezultacie, może być ciężko je wszystkie zapamiętać.

Zapisywanie haseł na karteczkach jest również ryzykowne.

Jak więc rozwiązać ten problem?

Istnieją trzy dodatkowe metody pozwalające zminimalizować problem z zapamiętywaniem haseł:

- Używaj „hasel zdaniowych” łatwych do zapamiętania, ale trudnych do odgadnięcia
- Używaj mieszanych metod identyfikacji
- Używaj menedżera haseł

« Hasła zdaniowe »

Zamiast konieczności zapamiętywania złożonych haseł, jak „Mç9 @ X ## Kl”, zalecamy przyjęcie „haseł zdaniowych”, łatwiejszych do zapamiętania, ale trudniejszych do złamania.

Chodzi o zachowanie kilku terminów inspirowanych elementami znanymi tylko przez użytkownika. Zamiast daty i miejsca urodzenia, moglibyśmy umieścić „Urodzony o jedenastej H27 w czwartek”. To zdanie może lub nie może być związane z używaną usługą (w nieoczywisty sposób), aby można było go zapamiętać.

Dzięki temu możliwe jest pogodzenie zalet złożonego hasła przy jednoczesnym łatwiejszym jego zapamiętywaniu!

Mieszane metody identyfikacji

Operatorzy zapewniają mieszane metody identyfikacji, w których **dodatkowy element** do hasła będzie wymagany od użytkownika. W przypadku dużych operacji identyfikacja jest często przeprowadzana za pomocą dodatkowej kontroli. W większości przypadków chodzi o wskazanie efemerycznego kodu przesyłanego przez SMS.

Złą stroną tego ulepszenia ochrony konta **jest przesyłanie dodatkowych danych** (numer telefonu w podanym przykładzie, walidacja przez e-mail, walidacja karty smart; w podobnych przypadkach mogą być również wykorzystywane dane biometryczne).

Uważaj!
podanie numeru telefonu do banku
może być uzasadnione, ale dane
biometryczne do zakupu przez Internet
już takie nie są!

Menadżer haseł



Source: Flickr

Bez względu na to, jak tworzysz swoje przepustki, pamiętanie o nich jest zawsze największym wyzwaniem! Dobrym rozwiązaniem może być użycie menedżera haseł.

Prawie wszystkie przeglądarki oferują zapamiętywanie haseł. Ta możliwość, nawet jeśli upraszcza życie, może być niebezpieczna. Niektóre przeglądarki, takie jak Firefox, domyślnie przechowują hasła w postaci zwykłego tekstu!

Jeśli naprawdę chcesz użyć tej opcji, najlepiej jest utworzyć hasło główne, które następnie uchroni dostęp do zarejestrowanych haseł.

Menadżer haseł (2)

Najlepszym rozwiązaniem jest użycie zewnętrznego menedżera haseł. Oprogramowanie to musi zostać zainstalowane na komputerze. Będzie zarządzać zapamiętywaniem haseł dla Ciebie. Najpoważniejsze oprogramowanie szyfruje hasła, które stają się dostępne tylko po podaniu hasła głównego, które jest jedynym, o którym użytkownik musi pamiętać.

Przykłady oprogramowania: Lastpass, Onepassword, Dashlane itp.

Ważne informacją, jest to, że są one bezpłatne!!.





DZIĘKUJEMY!

Czy są jakieś pytania?
