Passwords

Introduction

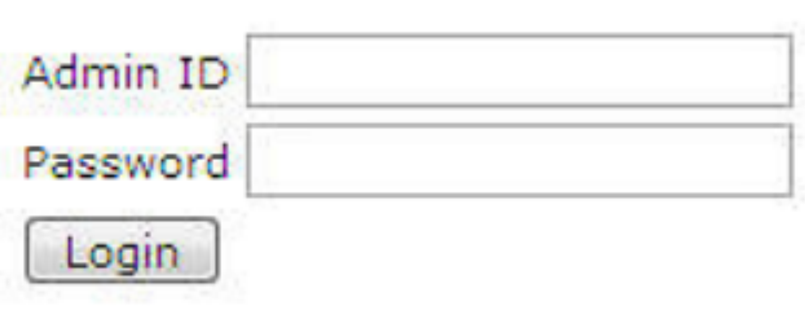
Source: FlickR

A key tool for **identification** on the various online services, the password is often the only protective barrier against unwanted intrusions with potentially disastrous consequences.

However, it is often a poorly managed tool, as many users do not hesitate, for example, to use very basic passwords. They are, then, easier to guess and hack. It is important to be aware of what is at stake with passwords and to know how to easily secure them while keeping them in memory.

Identification of the user

The use of computers often involves identifying Internet users. The most common technique is based on the "login/password" pair. Depending on the situation, the identifier may be public or private, but is often poorly protected. The password is the tool that ensures the essential security.



Source: FlickR

Major risk: identity theft

Wikipedia's definition:
Identity theft is the **deliberate use of someone else's identity**, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

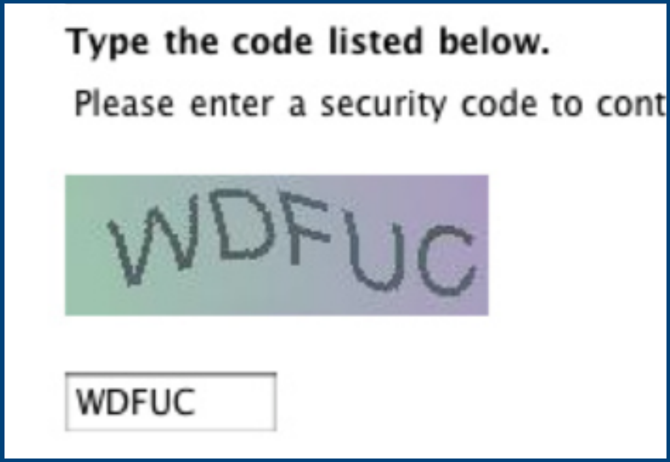
Issue:
Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and identity theft is not always detectable by the individual victims

So...

Operators who request identification must implement numerous security measures to manage passwords. This is a very important issue, but one over which we have little control.

➔ Use a password that is not easily guessed by a hacker

- *Avoid basic passwords such as 12345, azerty, birthdate, same password than login etc.*
- *The password needs to be long (at least 14 letters/digits)*
- *It needs to be diversified (capital letters, lower cases, digits, special caracters etc.)*
- *A serious operator will implement some safety measure such as limited number of attempts, captcha*



Type the code listed below.

Please enter a security code to cont

WDFUC

Source: FlickR

But…

Most people have many accounts and it is fundamental to diversify your passwords. As a result, it is complicated to memorize them all. Keeping passwords on a post-it is also risky.

So how to tackle this issue?

To limit this memorization problem, three complementary methods are available:

- Use “sentence passwords” easy to remember but hard to guess
- Use mixed identification methods
- Use a password manager

« Sentence passwords »

Rather than having to remember complex passwords like "Mç9@X##Kl", we advise you to adopt “sentence passwords”, easier to remember but more complicated to hack.

It is about retaining several terms inspired by elements known only by the user. Instead of the date and place of birth, we could put a "Born at eleven H27 on a Thursday". This sentence may or may not be related to the service used (in a non-obvious way) so that it can be remembered.

This makes it possible to reconcile the advantages of a complex password while memorizing it more easily !

Mixed identification methods

Operators provide mixed identification methods where an **additional element** to the password will be requested from the user. For large operations, identification is often done with an additional check. Most of the time, it is a question of indicating an ephemeral code transmitted by SMS.

The bad point of this improvement in account protection is the **transmission of additional data** (telephone number in the example given, validation by e-mail, validation of a smart card; biometric data can also be used in similar cases).

Pay attention !
giving your phone number to your bank can be justified but biometric data for an internet purchase is not!

Passwords managers

Source: FlickR

No matter how you create your pass pots, remembering them is always the biggest challenge! A good solution may be to use a password manager.

Almost all browsers offer to remember your passwords. This possibility, even if it simplifies life, can be dangerous. Some browsers, like Firefox, keep passwords by default and in plain text!
If you really want to use this option, the best is to create a master password. It will then protect access to registered passwords.

Passwords managers (2)

The best solution is to use an external password manager. This software must be installed on your computer. It will manage the memorization of your passwords for you. The most serious softwares encrypt passwords which only become accessible by giving the master password which is therefore the only one the user must remember.

Software examples: Lastpass, Onepassword, Dashlane etc.

Important point to be noted, they are free of charge!

THANKS!

Any questions?