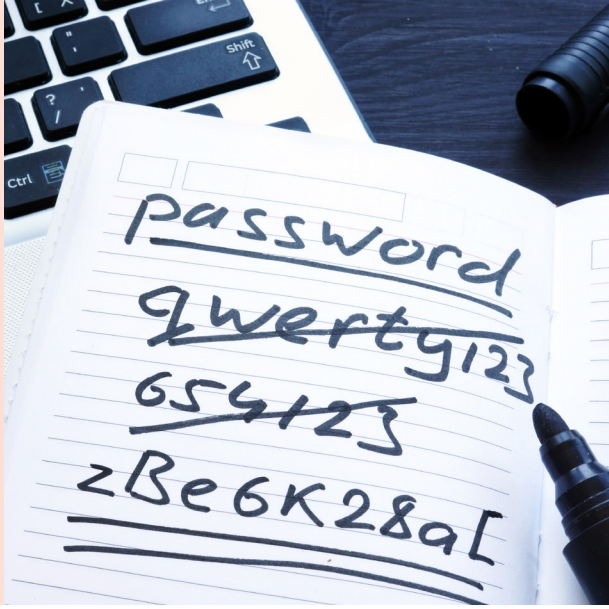
Tip sheet

CAREFULLY SELECT A PASSWORD

One of the basic elements of computer security, the password is the most commonly used authentication mode. Combined with a username, it allows you to identify yourself and to access your email, your computer account as well as all kinds of online services and resources with protected and secure access. More broadly, it plays a key role in accessing messages, documents and personal data. To preserve both the security and the confidentiality of your personal data, it is essential to choose strong passwords!



What is a strong password?

Difficult to guess by a third party and to find by automated tools while being easy to remember, a strong password is characterized by:

- an unusual combination of letters, numbers and symbols;
- a minimum of 10 characters, ideally 12 to 16 characters;
- the lack of precise meaning.

Prohibited passwords

- Logical sequences (azerty, qwertz, asdfgh, abcdefg, aaaaa, 1234567...)
- Known words or existing references, whatever the language (dictionary words, proper names, places...)
- All or part of words related to personal information (surname, first name, date of birth, registration number, telephone number, registration number...)
- 'Traditional' passwords a priori considered as weak (sesame, password, motdepasse...)

Tips for creating a strong password

1. Choose a sentence or a verse that is easy to remember.
2. Keep the initials of each word in the sentence or the verse you have chosen.
3. Replace some letters with numbers or symbols or add an extra number.

Example 1	Example 2
To Be or not to Be: That is the question! by W. Shakespeare	Brrrr! It's damn cold this morning, -9 degrees!
↓	↓
TBontBTitq!bW.S	B!Idctm-9d!
↓	↓
TBo!=tBtitq!bW.S.	Bidctm-9d!

Recommendations and responsibility

You are responsible for your computer account and must ensure its security. If a hacker succeeds in finding your password, he is not only able to access your email and computer accounts. He can also misuse the usurped account for spreading spam or phishing emails, thus exploiting the available resources for any purpose he deems useful (with implications and consequences for yourself, but also for other users).

Choose unique passwords

Do not use the same password for all your accounts and accesses, as in case of theft, the person who has stolen it will have access to... everything.

Keep your passwords secret

Do not give it to anyone under any circumstances and, above all, never give it to anyone by phone, direct mail or email, even if you are asked for it!

Protect your passwords

Do not write them down in plain text in documents or on easily accessible pieces of paper.

© Copyright Restena Foundation - November 2020 | www.restena.lu

restena
réseau · sécurité · .lu

Main attacks on passwords

Brute-force attack (by exhaustive search)

Technical method for exhaustively generating all possible combinations of character.

The more different types of characters your password contains, the more resistant it will be to attacks.

Dictionary-based attack

Technical method consisting of testing a series of words from a dictionary (names, first names, common passwords, movies, cities, etc.), often used in addition to a brute-force attack.

To increase the probability of finding (breaking) a password, automated software applies transformations to words such as:

- changing the case of certain letters (example: pLaNe);
- adding a number or symbol at the beginning or end of a word (example: 9marc, house!);
- replacing certain letters with numbers or symbols (example: mai5on, ho!se).

Passwords such as ''pLane12'' or 'marc123' are very likely to be broken in very short time.

→ Change your password as soon as you have the slightest doubt about its personal and confidential nature.

Social-engineering and phishing attack

Method leading Internet users to reveal personal or sensitive information (password, PIN code, banking information) via an electronic message or a fraudulent website.

One of the highest threats in the Internet, the phishing is based on social engineering and exploits human vulnerability, trust, credulity or ignorance of the Internet user.

Stay alert!

- Never provide your user credentials by email, phone or by any other suspicious means.
- Do not disclose any confidential data on forms received by email.

Key logger attack

Method for saving passwords and other sensitive data directly on the keyboard, in clear text form.

A spyware tool running on the computer without the user's knowledge, the key logger records all keyboard entries and sends the collected data to the hackers' networks.

Stay alert!

- Install only software on your computer that you know the origin of.
- Install and keep your anti-virus/anti-spyware softwares as well as your firewall up to date in order to protect your computer from viruses, Trojans and spyware.
- Be extremely careful when connecting to a computer that is not under your control (Internet café, hotel, etc.): you do not know what kind of software is provided and if spyware or harmful programs are installed on the machine.

Service offer

To fully benefit from the services offered by the Restena Foundation, a password is required. You can change it at any time by logging in to the online user portal at account.restena.lu.

Important: The Restena Foundation will never ask you for your password neither by phone nor by e-mail!

© Copyright Restena Foundation - November 2020 | www.restena.lu

restena
réseau · sécurité · .lu