Newsletter N°1/2013

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

*This campaign aims to inform RESTENA users about the use of strong passwords.*

# CAREFULLY SELECT A PASSWORD

## About passwords

A password is one of the basic information security elements and is the most commonly used authentication mode for online services.

Password and user name allow to identify yourself next to a service in order to access your mailbox, user account or other personal/protected services and resources. Their main purpose is to protect your personal access to your messages, documents and other confidential data.

It is of particular importance to select a strong password and to keep it secret such that third parties are not able to steal your identity and by this, access your confidential data.

*info:* Select a strong password to keep your data confidential and secure!

## What is a strong password?

A strong password should not be easy to guess by a third party or by an automated tool.
BUT it should be easy to remember!

A good password should be conceived with respect to the following guidelines:

- It should be composed of an unusual combination of **symbols**, **numbers** and l**etters**;
- It should be long, **at least 10** characters, better up to **16 characters**;
- **No**t have a specific **meaning** (a mix of numbers, symbols and letters);
- And it should be **easy** to **remember.**

Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Tél: +352 42 44 09 -1
Fax: +352 42 24 73

Please try to avoid the following:

- All logical sequence such ass “azerty”, “qwertz” or “asdfgh” as well as “abcdefg”, “aaaaaa”, “1234567”, ...;
- Words out of a dictionary (names of films, cities, ...);
- Words related to your private/business life (name, surname, birth date, name or birth date of family relatives, ...). Avoid also partial information of names, birth dates, ...;
- Traditional passwords a priori considered as weak are for example, “sesame”, “password”, “motdepasse”, ….

Prohibited passwords are:

**NO! :** **”Administrator”, “Administrateur”, “admin”, “password”, “restena”, “123456”, “qwertz”, “qsdfgh”, …**

## How to create a secure password?

There are different methods to build a strong password. The most common one is to choose a **sentence** or a **verse** (you can remember) and only keep the **initials** of the words. Then, **replace** some of those selected letters by **symbols** or **numbers** to increase the complexity of the password.

Some examples:

**YES! :**

Sentence 1:

*“To Be or not to Be: That is the question! by W. Shakespeare”*

Possible passwords:

"**TBontBTitq!bW.S.**" or "**TBo!=tBtitq!bW.S.**"

Sentence 2:

"Brrrr! It's damn cold this morning, -9 degrees!"

Possible passwords:

"**B!ldctm-9d!**" or "**Bidctm-9d!**"

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

## Security Recommendations for passwords

- Keep your password secret and do not share it;
- Never share your access credentials (user name or password or both) with third parties by phone, email,..., even if they insist;
- Protect your passwords, do not write them in clear anywhere it can be easily accessed;
- Do not use the same password for all your accounts. Private accounts should have different passwords from professional accounts;
- Regularly change your passwords;
- If you have a doubt about the strength or confidentiality of your password, change it.

## How do attackers get a password?

There are different attacks for collecting passwords from users. The most common ones are explained below:

### Brute-force attack

A brute-force attack is a technical method to find passwords by exhaustively testing all possible combinations of characters. By using long and complex passwords, this method is not fruitful and time-consuming too.

#### ♦ Dictionary-based attack

In a dictionary-based attack, hackers test words from a dictionary (names, cities, standard passwords, surnames, celebrities, ...) to guess a password. This attack is often used in addition to a brute-force attack to accelerate the guessing process.

The method is not successful if the password has a high randomness and does not include standard words.

To increase the probability of guessing a password, an attacker also tests replacements in words, such as:

- Replacing lower and uppercase symbols (pLaNe);
- Adding a number or symbol in front/end of word (9marc, house!);
- Replacing letters by numbers or symbols (mai5on, ho!se);

Passwords like, 'pLane12', 'marc123', … are very likely to be broken in very short time.

*info:* A password having a high randomness in letters, symbols and numbers is less affected by dictionary and brute-force attacks.

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

## Social-engineering and phishing attacks

Phishing has become one of the highest threats in the Internet. The main idea is to convince users to provide their credentials (password, credit card, PIN codes, ...) by email or fradulent websites.

In social-engineering, attackers try to exploit the "human" vulnerability. This means an attacker tries to obtain passwords by misusing the good faith or the unawareness of a user (shoulder-surfing, picture, ...).

To avoid these attacks on a best effort basis, please consider the following rules:

- Pay attention to phishing mails (e.g. fake emails from banks, postal offices, ...);
- Never provide your user credentials (password, credit card) by email, telephone or other means to third parties;
- Do not disclose your confidential data on suspicious forms on websites or in emails.

## Key logger attack

A key logger saves the key strokes from a keyboard and by this, gathers all data including passwords from a user.

The key logger is a spyware tool that is installed on a user's computer. It logs all key strokes and sends the data back to the attackers.

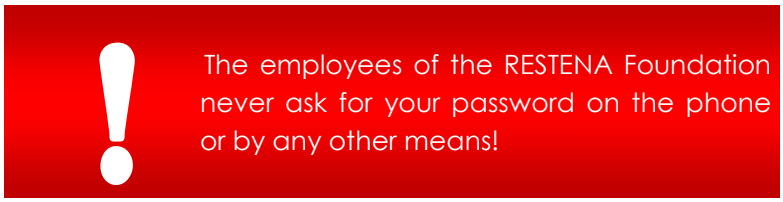
The best protection against this type of attack is to respect the following rules:

- Do not install programs on your computer without knowing their origin;
- Keep your computer updated and use the anti-virus/firewall utilities to protect against known viruses, trojan-horses and other spyware;
- Be careful when using a third party computer (hotel, cyber-café,...)! You do not know what kind of software is provided on this computer and it may have spyware or harmful programs installed.

## Responsibility

You are responsible for your user account and you should guarantee for its security on a best effort basis by using a strong password.

If an attacker succeeds to steal your password, he is not only able to access your account or to reset your password, but can misuse your identity for spreading spam or phishing emails, or to explore the resources for other fraudulent purposes (not only with direct consequences for you, but also for other users).



## How to change the RESTENA password

A password has to be changed on a regular basis or in case of a doubt about its integrity.

You can change your password whenever you like by connecting to the "Personal Profile" accessible via the RESTENA Foundation website.

*info:*

Treat your password like a tooth-brush*:

Do not share it and replace it regularly!

For more information about passwords, please contact us or visit the website of BEE-SECURE*!

This newsletter has been presented in the framework of the **SID2013**.


***The RESTENA Newsletter is a new biannual service offered by the RESTENA Foundation. To subscribe to this service, please send an email to:***

***newsletter-subscribe@restena.lu***

* BEE SECURE https://www.bee-secure.lu

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche