cases.lu
Secure. Innovate. Lead.

CYBERSECURITY

TIPS AND TRICKS

EN


ERROR
STOP

CYBERSECURITY: TIPS AND TRICKS

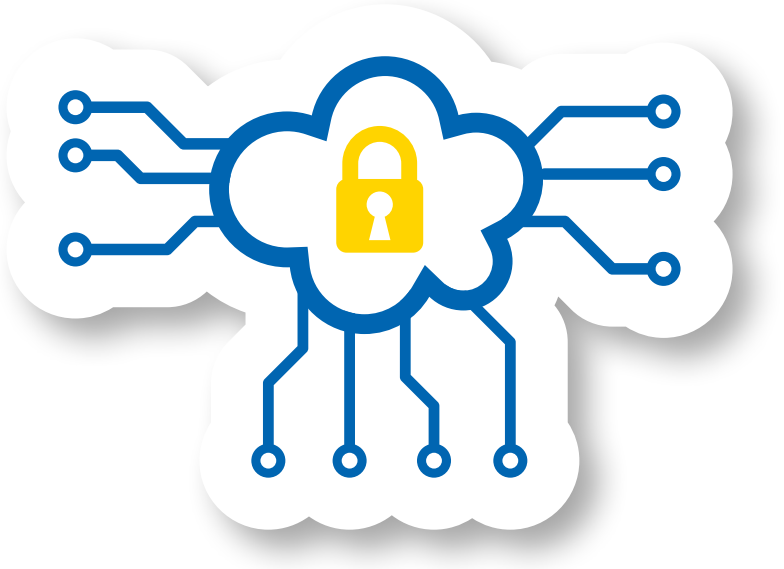
TABLE OF CONTENTS

FOREWORD

Information technology is an essential part of our society. We conduct our business and social relationships for the most part via a desktop computer or laptop, smartphone, tablet, etc. We all handle sensitive personal or professional information whose loss, theft or unavailability could have serious consequences for ourselves or others.

Do we always ensure that our electronic communications are secure and do we handle data in a responsible way?

This brochure offers some practical tips on the secure use of information technology.



HOW TO ASSESS RISK

Zero-risk situations do not exist. Security is neither a good nor a service that can be purchased. This applies to all aspects of everyday life: accidents do happen. However, we can take precautions and follow certain security measures. We can also purchase specialised insurance in order to cover certain damages.

Similarly, it is impossible to eliminate all risk in electronic communications. We can, however, minimise risk wherever possible, starting with a precise analysis of the situation.

3 factors in are important to consider, when assessing cybersecurity risk for a given situation:

- The "vulnerability" factor – i.e. a *weakness or defect* (human, technical or organisational).
- The "threat" factor – it can be an external or internal factor. *Someone or something that could exploit the vulnerability*.
- The "impact" factor – i.e. *the consequences* resulting from the threat. These consequences can be tangible and quantifiable in material terms, or intangible (psychological consequences, damage to the reputation of a person or a professional structure, etc.).

AN EXAMPLE IN DAY-TO-DAY LIFE:

You leave the key under the doormat of your home to allow someone you know to enter in your absence.

This is a "vulnerability" to the valuables in your home and/or your own safety. It could be exploited by a stranger who takes the key (i.e. "threat"), robs your house (i.e. "tangible impact") and leaves you feeling insecure (i.e. "intangible impact").

ANALOGY WITH IT SYSTEMS:

You write your password on a piece of paper near your computer, intending to pass it on to a colleague so that he can access your files in your absence. This is a “vulnerability” in the system. Effectively, someone with malicious intent may find this piece of paper, log on to your computer, appropriate confidential documents or send messages on your behalf, thereby jeopardising you or your job.

Human vulnerabilities can be prevented with a little training, organisation and vigilance and thus improve our defences and resilience.

VULNERABILITIES

HUMAN VULNERABILITIES

Humans are not infallible. A person may be fatigued or stressed, or manipulated by someone with malicious intent who exploits their fear, pity, curiosity, greed, etc. to extract or provide access to critical information.

TECHNICAL VULNERABILITIES

Software is a collection of instructions and data required for the computer to perform a task. As software is a human creation, it may contain design flaws (not impeding their proper functioning) that could represent *vulnerabilities* an attacker can exploit.

To limit the risk associated with these technical vulnerabilities:

- your software must be up-to-date,
- your antivirus must be functional.

Keep in mind that no measure is perfect; an antivirus will not protect you against all malware and “anti-spam” filters do not filter all spam. In case of any defects or software alerts, please contact your IT department.

THREATS

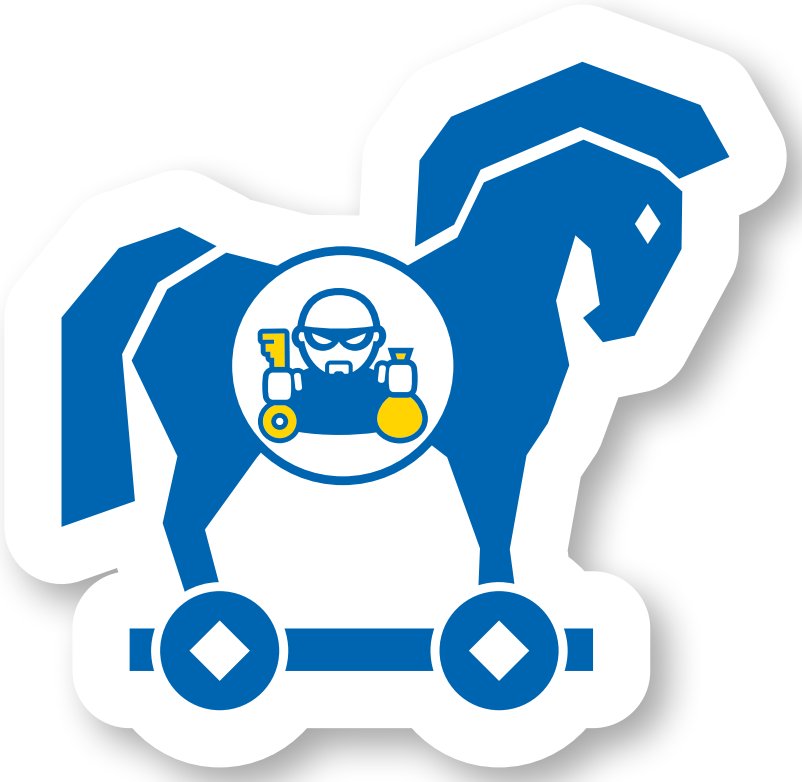
MALWARE

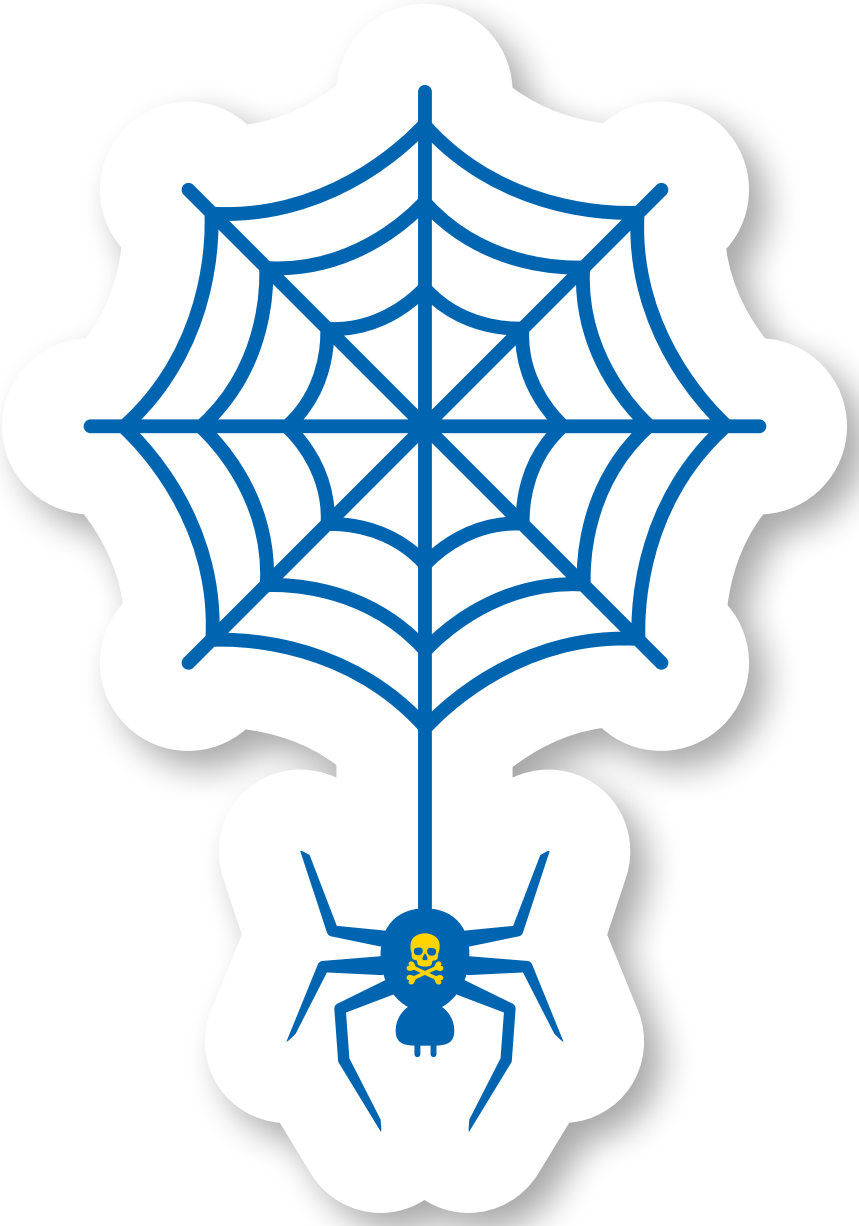
A computer cannot tell the difference between malware and legitimate software; the difference between the two is the "intent" of the programmer. As such, it is impossible to design an IT platform that is protected against malware. Today, malware is mainly used for data theft or money extorsion.

Commonly speaking, such malwares exists in the form of viruses, Trojan horses, worms, ransomware, etc.

SECURITY TIPS

- Request permission from the IT department before installing software.
- Avoid unnecessary extensions, such as plugins or toolbars.
- Update the software installed on your machine.
- Uninstall unnecessary software.
- Check antivirus messages and report any anomalies to your IT manager.





INTERNET

USING THE INTERNET

The Internet is often a source of malware. There are too many legitimate but poorly protected websites that become compromised, and are then used to infect visitors' computers. The latter generally get infected by exploiting the technical vulnerabilities of web browsers.

INTERNET FRAUD

Originally, attacks on IT systems were mainly done for fun. Nowadays, they are mostly motivated by profit.

Access to data may allow access to the victim's "wallet" through access to web-banking, virtual money and e-commerce (credit card numbers).

Other data, such as passwords, may be used to spread malware or scams. For example: those who steal Facebook passwords are stealing online identities, and thereby the confidence of the victim's group of friends.

ELECTRONIC JUNK MESSAGES

It should be noted that unwanted messages are not just e-mails. Spam can come from almost any other social media channel or instant messaging network.

SPAM

Spam is an unsolicited message that often contains advertising or misleading content.

E-mail is one of the most practical and expeditious means of communication that currently exists. It is an economical form of communication, but is often poorly secured (i.e. unencrypted) and prone to forgery. This is why they are often used to spread malicious software or carry out "social engineering" attacks (see: social engineering).

Cryptographic tools can help secure the content of electronic messages.

PHISHING

Phishing is a technique used to obtain personal information in order to commit identity theft. The technique consists of making the victim believe that they are communicating with a trusted third party – a bank, public administration, etc. – in order to obtain personal information like passwords, credit card numbers, date of birth, etc. It is a form of cyberattack based on social engineering. It can be carried out via e-mail or other means of communication. The most common targets are Apple, PayPal, Google, online banking services and tax offices.

HOW TO RECOGNISE PHISHING

A phish (e-mail used in a phishing attack) can usually be recognised by the following features:

- the e-mail indicates you need to take action quickly;
- the e-mail addresses you in an impersonal manner, often using a generic greeting such as “Dear Customer”;
- the e-mail contains a link that you must click. For your own protection, it is important that you do not click this link!

If you receive a message that fulfils one of these criteria, it is best to ignore it. If you have doubts about the veracity of the message, you can also open your web browser and manually enter the website address.

SPEARPHISHING

Phishing techniques are continuously improving, which makes malicious e-mails difficult to recognise. We also talk about "spearphishing" (targeted phishing), which is tailored to the victim. This type of targeted attack uses information collected about the targeted victim to build a credible message that is very difficult to differentiate from a legitimate message the victim might receive. Most often, this type of attack is designed to infect the victim's computer.

SECURITY TIPS

- Delete messages without opening them if they are from unknown senders or if the subject line seems strange.
- Only open attachments if they come from a reliable source. If the message is strange, contact the sender via another channel.
- Refuse to share information relating to sensitive data, even within the workplace.
- Be wary of e-mails that ask you to take action quickly.
- Do not click on links in e-mails. Visit the website in question manually by typing the address into your web browser.

Did you know?

There is a parallel economy in place in the virtual world. Cybercrime is currently considered one of the most profitable activities in the field of organised crime.

There is no reason for a user to behave recklessly even if there is nothing to hide. Similar to traffickers who plant drugs in the luggage of travellers, those with malicious intent might use your computer to send spam or host child pornography.

PHYSICAL SECURITY

Physical security goes hand in hand with information security. Access to offices can pose a large threat.

Lock your valuable items and documents in drawers. Only save sensitive data on your computer if your hard drive is encrypted.

If visitors enter your workplace, ask them about the purpose of their visit and accompany them to their desired location.

PRINTER INTERCEPTION

A risk of theft/loss of information also exists for documents lying around by the printer that are within reach of others. Make sure to pick up your copies immediately after printing. Get used to the habit of shredding (preferably using a confetti cut shredder) documents that contain sensitive information which you no longer need before throwing them in the bin.

DUMPSTER DIVING

This term literally means sifting through rubbish and is widely used by fraudsters. We all sometimes throw away letters, photos or documents without ensuring that they are destroyed. Rubbish bins often lack a padlock and remain unattended until they are collected. This waste can provide a lot of information about a person or company: names, address, bank accounts, business or private information, etc.

Destroy any documents containing sensitive information using a shredder, preferably with a confetti cut. If possible, lock the rubbish bins and dumpsters.

SECURITY TIPS

- Store paper documents in a locked cabinet.
- Make sure your computer is locked, switched off or in sleep mode when leaving the workstation or when the computer is unsupervised.
- Save electronic documents on a file server in a locked room.
- Accompany visitors to their destination and do not leave them unattended.
- Retrieve documents from the printer.
- Shred sensitive documents before throwing them away.

SOCIAL ENGINEERING

Social engineering is when an individual uses a false identity or manipulation techniques to make another person provide information it would otherwise not provide, or perform an action that it would otherwise not have done.

SECURITY TIPS

- Verify the identity of the person requesting the information and the merits of the request before sharing personal or business information online, by phone, e-mail or via the Internet. If in doubt, do not respond immediately and carry out verification in the meantime.
- Do not give in to “urgent” or threatening demands (i.e. an alleged IT provider that must “absolutely” have access to your server).
- Do not listen to any stranger who claims to want to help you.

Using two methods together naturally increases level of security of the identification. Unfortunately, the most commonly used method is still the password.

It is therefore essential to be careful when choosing it.

THE GOOD PASSWORD

Your username and password are personal access data. They must remain secret and personal.

A good password should be easy to remember but hard to guess. The password can be made more complex by increasing its length; it is recommended to use at least 12 characters, preferably around 15. If the system used imposes a maximum length, you can increase the complexity by using different character sets. For example, use lowercase letters, uppercase letters, symbols and numbers. Do not choose words that appear in a dictionary or which refer to personal information (names of your relatives, birthdays, etc.).

Use different passwords for each IT tool, account or service.

It is preferable to use mnemonics when choosing your password. Using a "phrase" password instead of a "word" password can be an advantage when the software does not impose a restriction on the password length. Example: "3 Amazonian anacondas" for your amazon.com password. If the software imposes a length restriction, choose a password comprised of the first letters of each word in a sentence.

Example: **1yco4sa12m!** (**1 y**ear **c**onsists **o**f **4 s**easons **a**nd **12 m**onths**!**).

If you have more than ten accounts that require passwords, it is advantageous to use a secure password storage application. These applications contain all of your passwords, secured under a single master password. This master password must be very strong.

SECURITY TIPS

- Choose a complex password that is easy to remember. Keep it secret and change it regularly.
- Use different passwords for each application or device.
- Use a secure password storage application.

ENCRYPTION

The encryption of communications (mathematical algorithms to make content unreadable) is the only way to ensure that your messages reach their destination without being intercepted. The message passes via the Internet, and therefore through servers, etc. that are not necessarily all trustworthy.

Simple encryption techniques exist for web pages. These are reflected in the URL of websites which begin with “https” instead of “http”.

Other encryption methods exist for other means of communication, but may be more difficult to use. Encryption of e-mails, for example, is difficult to implement.

An easy way to securely send sensitive documents by e-mail is to archive them (file format: zip, rar, etc.) and to protect the archive with a password. Simply send the archive as an attachment to the recipient and let them know the password by phone or SMS (or any other secure channel; it is important to not send it by the same channel of communication).

Encryption can also help to protect sensitive data on PCs, tablets, smartphones or backups.

BACKUPS AND ACCESS TO INFORMATION

It is vital to perform regular backups on a device that is not always connected to the machine. This will allow you to better protect yourself against hard disk malfunction or ransomware. In most cases, during an infection of this type, the backup is the only way to recover data such as holiday photos or personal documents.

Access management is an important task that requires daily monitoring. Staff departures, new arrivals and changes in staff roles must be taken into consideration, as well as the access rights for the premises and information that each person needs in order to work.

Access cards should preferably be visually neutral in appearance in order to prevent abuse in the event of theft or loss.

Access to data must be set up so that employees do not need to share passwords.

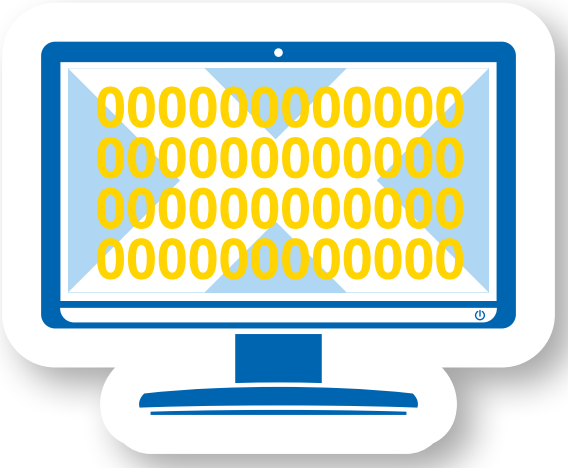
SCRAPPING

Computers accumulate sensitive data during normal use. Sensitive data is rarely disposed of properly if the computer or hard disk is scrapped, sold, given away or sent for repair.

If files are deleted from the computer, they are first sent to the recycle bin, where they remain accessible and can be recovered easily.

Similarly, when the recycle bin is emptied, the data is not actually deleted from the hard drive. What is erased is their reference in the index files, freeing up previously occupied space for other files. As long as new files are not able to take up the freed space, the data remains intact on the hard drive and can be restored with the help of specific IT tools.

To efficiently clear data from the hard drive, you must write over the entire disk surface. Certain specialised software can do so, but the operation can be long. It is quicker to destroy the disk physically.



USEFUL WEBSITES

SECURITYMADEIN.LU is the Luxembourg cybersecurity portal. It promotes cybersecurity tools, news, events and market operators in the Grand Duchy of Luxembourg.
→ **www.securitymadein.lu**

The **CASES** website provides methods and services to businesses and governments who wish to strengthen the security of their information at organisational level. It also issues alerts about threats that regularly arise and offers a helpline to answer cybersecurity-related questions and issues.
→ **www.cases.lu**
email : **info@cases.lu**

The **CERT / CSIRT** website brings together private and public emergency and response teams.
→ **www.cert.lu**

The **BEE SECURE** website promotes cybersecurity and the responsible use of new media, aimed at the general public. It is particularly addressed to young people and the Luxembourg education sector.
→ **www.bee-secure.lu**