# Brief computer survival guide for beginners

## *Warning*

**These brief reminders of the minimal rules of computer hygiene will not make the reader an « *expert* », but rather a respectable beginner.**

*Understand the concept of security*

Security may be summarized in 5 phases:

- anticipate the risk ;
- identify the threat,
- react to said threat,
- fix and stop the incident from spreading and
- avoid its recurrence.

*Master the common vocabulary used by protection tools*

The term "*anti-malware*" is gradually taking over the term "*anti-virus*".

A malware is a malicious software that is not limited to viruses.

Furthermore, the software programs do not all have the same end purpose: The essence of a "*virus*" is to ensure it can be propagated, the "*spyware*" has for vocation to spy, the "*root kit*" gives a third party fraudulent access to the machine, the Trojan horse is a software that contains an illegitimate program.

Different evils require different remedies and we then speak of "*anti-virus*", "*anti-spyware*", or even *"anti-root kit*". These programs are all anti-malware.


*Why was I infected ?*

The answer probably deserves some tact, but most of the time, the user contributes directly to his or her own misfortune.

For example, if I do not click the link that will allow me to download the screen background of Pan-pan, Disney's famous rabbit, the file will not be executed and my computer will not be infected.

**Rule n° 1: When in doubt, I do not click**

(in other words, if I do not know the person, I do not open the door).

In the same way, when I download free software (or "*freeware*") from a download platform, nothing guarantees the harmlessness of the software.

By default, it is advised to download the program from the official website of the software vendor.

**Rule n° 2: I do not download just anything from anywhere**

(in other words, if I find a chocolate pastry on the ground, I do not eat it).

As such, I have a friend who is a specialist and tells me that 80% of anti-viruses do not work and that an anti-virus only gives me a clear conscience.

My friend is an expert as you will have guessed: I always use an anti-virus.

**Rule n° 3: I always install an anti-virus**

(in other words, I am really pleased that there is a door separating me from the man on the other side).

*"I do not understand, it was working very well before the update (UPD)... ...frankly, I wonder if it is really worth updating the software!"*

First of all, all computer users are potential victims of Murphy's Law: "*Anything that can go wrong will go wrong* ".

But, this law should not prevent you from following your tendency to do the right thing and so proceed with the software updates.

Software updates mean updating the operating system and the software installed on the machine.

Updates allow you to shield yourself from any detected security vulnerabilities.

**Rule n° 4: I always run software updates of the operation systems and installed software**

(in other words, I seal the crack on the hull of the boat before setting out to sea even if I know how to swim)

*My anti-virus is the best in the world (in fact that is what can be read on the Internet) it is up-to-date and yet there are still some stuff that gets through"* (in other words, my patience has reached its limits).

An anti-virus only protects against the threats that it recognises. The software update collects new virus signatures in order to allow the anti-virus to accomplish its task.

Unfortunately, a virus may sometimes be an impatient evil, which may not always have the decency to wait until the anti-virus is up-to-date.

**Rule n° 5: Each week, I run a complete scan (the one that takes a long time) in order to ensure that malwares are not installed before the software update**

Nothing stops me from continuing to do other tasks while the scan runs (apparently some users may feel obliged to watch the progress of the scan file by file in case they miss a hidden truth concealed therein).

A friend of mine who is an expert told me that we must *"partition".* (in other words, I pretended to understand to save face).

At first, it is advised to classify one's data (everyday, important, utmost important). It is a question of sensitivity.

The question could be expressed as follows: if I lose that data, what will it cost (in terms of time, money, tears, and regrets)?

To invest in an external hard drive may reveal itself to be judicious in a certain number of situations: thus, data are duplicated and placed in a secure place (physical even logical if encrypted).

Another question to ask oneself is: "*if I lose everything, who do I blame?"*

It is important to configure a machine with at least as many sessions as there are users and to never work with an administrator account:

- even if you are the "*master*" of the computer;
- unless you are an expert.

For the most sensitive files, there are encrypted containers described in detail on the Agence nationale de la sécurité des systèmes d'information (ANSSI) website.

*Health reflex*

As important as the rule of the five servings of fruits and vegetables per day, there are five elementary principles to be observed by the computer user:

- use passwords;
- lock the user session;
- prevent the restarting by external peripherals (such as, CD, memory sticks...);
- switch off the computer when it is not in use;
- encrypt the hard drive.

**Rule n° 6: 1234 and abcd are not passwords**

An expert password:

- contains a minimum of 12 characters including letters, numbers, and special characters;
- does not use words taken from a dictionary;
- may sometimes be a phrase that is easy to remember (passphrase).

When the user is afraid to forget his or her password, he or she does not stick the password on his or her screen or inside his or her desk drawer : the user uses a digital safe for passwords allowing him or her to store the totality of the passwords in one file.

*...and mailboxes?*

According to certain historians, Pandora had a mailbox...

It should be known that 75% of traffic on the Internet is comprised of emails and that 80% of these are spam.

Furthermore, messaging is a vector to propagate digital insecurity.

Quick reminder: an email is a text file. Consequently, an attachment (except when you are sure of the sender) is an enemy.

So, when I click an attachment, I execute a file that often contains malware.

**Rule n° 7: I do not click unless I am absolutely sure**

(in other words, if I want a gift inside, I can fall back on a famous egg with a surprise inside).

Furthermore, I may sometimes give in to office humour during my spare time and send my colleagues links to funny websites.

First of all, we must fight against the dark side of the forces and not succumb to the sirens of cumbersomeness.

Then (in other words, it is already too late), we must take care to not send unverified images or links.

Finally, sending mails to a huge list of recipients in carbon copy (CC) is to be avoided. By using BCC (blind carbon copy), you are respecting the privacy of your contacts and fighting against spam.

*« I am back from a seminar in Hong Kong, I brought back some fantastic goodies. »*

Except if their ornamental value is proven, you have no valid reason to keep them.

As for plugging them into the USB port of a machine (professional or personal) that amounts to sabotage.

This is valid for the (super) memory stick 64Go as well as the cup-heater or the mini-fan whose gaudy colours and doubtful design are a call for caution just by themselves.

**Rule n° 8: I do not connect anything to my computer that has not been previously verified or is not from a reliable source**

*And the winner is?*

We all have a friend who has a telephone or a computer with a bitten into apple logo on it.

This friend lives with the certitude that malwares are stopped by the simple glow of his or her super machine.

With all the tact that such a situation requires, it is your role as a friend to invite him or her to protect his or her equipment that has no more reason to be impermeable to malware than others.

All operating systems have flaws and are potential targets. Therefore, computer hygiene necessitates vigilance regardless of the equipment used.

**To conclude, all experts have, basically, a certain form of tenderness for the beginner who seeks to rise. Do not hesitate to ask them for advice.**