NEWSLETTER 12

SECURITY OF ONE'S OWN DEVICES: COMPUTER, TABLET AND MOBILE PHONE

The subject of Internet security can be divided into four parts: protection of devices and the home network, passwords, browsers, surfing on wifi networks.

For each of these categories, we will look at everything that should be done to achieve a minimum level of security until the system and all data transferred over the web and the network are completely protected.

1) Computer, tablet or mobile phone security

Is an antivirus installed? Does the antivirus automatically update itself every day?

If you have not yet installed an antivirus program or if you have an expired program that no longer updates, you should take action.

Uninstall your current antivirus and download one of the recommended free antivirus programs. In order to judge an antivirus in a way that everyone can understand, we must take into account at least 6 parameters before making any decisions. In fact, a good antivirus

- It must not slow down the PC too much and be light in RAM memory.

- It must stop viruses before they can act (resident active scanning).

- It must not detect too many false positives, seeing threats where there are none.

- It must not make on-demand scanning or periodic automatic scanning take too long: a modern SSD must be fully scanned in less than 2 hours.

- It must automatically update itself so it can stop new infections immediately and prevent access to vital parts of the system.

- It must be able to block undiscovered malware (0-day threats), sensing the threat only by the suspicious behaviour of certain components.

In addition to these parameters, which are all very important when it comes to antivirus, we must also consider the ease of use, the user interface, any usability problems and the presence of bugs, errors and incompatibilities.

- Is a firewall installed?

If you have Windows 7 and if you surf the Internet using a router at home, you do not need a firewall programme. If you do need one, you can download a free firewall to protect your network and block intrusions.

- Is Windows (or Mac) up-to-date and does it update automatically and regularly?

Many people neglect or forget to update Windows with the patches that Microsoft distributes every week. These updates are always security patches that cover the latest holes that allow malicious users to break into PCs from the outside and take control.

Check that the Windows Update service is active in the Control Panel.

Even Mac users should not underestimate security updates.

- Have you set up a backup plan for your data, documents and photos?

To make sure you don't lose the files you create and save on your computer, plan to back them up automatically so you have a double backup.

If you don't have too much data to back up, it can be much easier and faster to make an online backup on cloud storage services such as Dropbox and Skydrive.

- Do you keep the programmes installed on your computer up to date?

As with Windows, security updates are often released for programs.

For those who want to, there are ways to automatically update programmes and software installed on your computer.

- When downloading programmes, are you careful in the installation procedure not to install other 'recommended' software as well?

Unfortunately, many free programmes come with sponsors, so-called 'crapware', in the form of unsolicited programmes that install themselves automatically.

2) Browser security

The fact that your computer, tablet or mobile phone is protected against viruses and external intrusions does not guarantee that browsing is still safe and private. Many people may not care about privacy, but security is still paramount.

Whatever browser you use, it should be updated to the latest version and have automatic updates enabled. Browsers that are up to date and have automatic updates are certainly Chrome, Firefox, Opera and Microsoft Edge.

- When you log in with a password to a site, do you always check that the address starts with https?

HTPPS is the encrypted connection protocol and differs from normal http in that any data transmitted in https is encrypted. This means that what is written in https is unreadable to anyone, including the operators of that site.

The HTTPS Everywhere browser extension highlights secure sites and ensures that you always stay in HTTPS where available (see article Navigating in https on banking sites, online shops, Facebook with a secure connection).

- Can you recognise, by eye, dangerous sites where you have to be careful where you click?

If you still can't tell a good site from a bad one by eye, and you are always paranoid or bad-mouthed about any site other than the most popular ones, then you can install some extensions such as WOT to avoid clicking dangerous links and suspicious sites

- When you connect to a site from a computer not used only by you, do you always log out?

Always remember to log out of all accounts you use on a public computer or one shared with other people, including family members.

- Do you know the basics of online scams and fraud?

Knowing what phishing, malware and other dangers on the internet are is important for staying away from them.

- Do you protect your browser from online tracking?

As already explained, not being tracked online by websites means blocking the collection of data. This is possible via certain extensions that you can install on your browser.

The highest level of protection and privacy on the Internet is anonymous surfing. Surfing completely anonymously is not useful for everyone and cannot be done for every situation. It can be useful when you are doing something illegal (but good like downloading torrents), when you don't want to share your geographical location or when you want to spoof your IP address to access blocked sites.

Although you can surf the Internet anonymously in several ways, online privacy is only guaranteed with TOR browser.

3) Security of passwords used online

- Do you use complex passwords?

One of the most common mistakes internet users make is to use simple passwords or passwords that refer to facts or events in their personal lives. You should always choose passwords that are impossible to discover and, above all, generate a strong password for all websites, without giving anyone the chance to guess it (never use your date of birth, your favourite team or the name of your wife or dog).

- Do you use different passwords for each site?

You should never reuse the same email combination and password combo across multiple services because if a hacker manages to get into that email account, he or she will be able to breach each personal account without difficulty.

Use a programme to create and manage passwords for web accounts.

Where possible (Dropbox, Google, Gmail and Facebook), two-factor authentication can be used.

For added protection, be sure to check app permissions on Facebook and Twitter.

4) Network security

- Is your home WiFi network protected with a WPA2 key?

If not, or if you have no idea what WPA2 is, you should know that WPA stands for Wi-Fi Protected Access and that Wi-Fi Protected Access II (WPA2) and Wi-Fi Protected Access III (WPA3) are three security protocols and certification programmes developed by the Wi-Fi Alliance to protect wireless computer networks.

- Are you aware that when you connect to an open Wi-Fi network, everything you do is visible from outside your computer?

The only thing that protects password security on the internet in a public wifi network is the HTTPS protocol mentioned in the first question in point two.

- Have you checked the shared folders on your computer?

As has been demonstrated, hacking into computers and viewing the shared folders of other computers is very easy. Very often the operation is successful because people forget to exclude the sharing of folders or the entire hard disk on the computer. To use a computer in complete anonymity and connect to the network without leaving any traces, you can use an anonymous and private Linux system such as Tails.

Security is important for everyone, from the experienced technician to the computer illiterate. The level of precautions you take is up to you, but bear in mind that online security today is just as important (if not more so) than the security of your own home.

This project has been funded with support from the European Commission. This document reflects the views only of the project partners, and the Commission cannot be held responsible for any use which may be made of the information contained therein.