NEWSLETTER 11

What are the dangers of the internet to know and beware of?

The dangers of the internet to be aware of, to beware of and to deal with when necessary can be encapsulated in 9 broad categories.

1) Sites with malware and viruses ready to infect your computer.

When surfing the Internet, it is very easy to click on the wrong link and open a site that loads malware onto your computer. Fortunately, if you have an up-to-date antivirus installed on your PC, this virus will almost always be stopped before it can do any damage. The biggest danger, apart from the danger of an antivirus that mistakenly lets the virus through, is not realising that you have risked an infection that could compromise the operation of your PC or the integrity of your data. It is precisely because of the lack of attention on the part of many people that ransomware viruses such as Cryptlocker, which encrypt personal files and demand ransom, have become widespread over the past year.

We know which sites are dangerous, generally those dealing with piracy, streaming sites, adult content, dating and illegal material. If you can't avoid visiting these kinds of sites, be very careful where you click because the virus can hide anywhere. You only have to click on the wrong 'Download' button to end up installing malware. And don't forget those advertising banners that tell you your PC is infected, when in fact it is not.

If in doubt, there are tools to recognise and avoid dangerous links and suspicious sites.

A key factor in recognising and avoiding sites with viruses is to use an up-to-date browser that is protected against all bugs discovered to date.

Among the most dangerous sites that may contain malware are certainly adult sites, piracy sites of any kind, almost all torrent sites (also with piracy), illegal download sites (such as films and music) and crack sites.

Ideally, if you necessarily have to visit such a site, it would be best to browse using a sandbox. In both Windows 10 and Windows 11 you can use a virtual desktop feature that is not only a security tool, but also a great way to do things on your computer without them being recorded or remembered, a bit like the incognito mode of web browsers. This tool is called the Sandbox and is intended as a zone on the computer in which everything that is done has no influence on the system and is deleted immediately after closing it. The SandBox works like a disposable virtual machine in which you can safely run anything you want; you can even open a virus or malware without worrying that it will damage your PC or steal data from your computer.

2) Online privacy always in danger

It is quite obvious that if you want to use the Internet in a participative way, i.e. by joining forums, social networks and chats, you have to sacrifice some of your privacy. On sites such as Facebook, one is obliged to give one's real name, while on other sites it is still necessary to leave an e-mail address through which one can, if one wishes, trace the owner. Basically, in normal Internet use, anonymity cannot exist, and if someone were interested in knowing who we are and had the right hacking skills and talent, they could theoretically know everything about us.

Protecting privacy online, however, does not mean preventing a hacker from spying on our lives because, unless we are being stalked by a stalker or doing things that are illegal and need to be hidden, let's just say that no one is likely to waste their time hacking into our lives. Online privacy, on the other hand, means keeping some sensitive information private, such as our credit card numbers, our passwords, where we are at any given time, what we are looking for on the internet and so on.

3) Unprotected sites

This is a danger factor that is still ignored by most people.

Websites are not all the same and are divided into secure sites, where the information you transmit is encrypted and cannot be intercepted from the outside, and normal sites that transmit in the clear. Navigaweb.net is currently an unencrypted site, which does not mean that it is not secure, but because it does not require a password to log in, it does not need to protect information. All sites where you have to enter a password must be encrypted, and this protection is recognisable by the padlock on the Internet address and the prefix https instead of http. When a site is in HTTPS and has no certificate errors, then all the information we send, including access passwords, credit card or bank account numbers, is not visible on the Internet to anyone, not even to the operator of the site to which we send this information. It goes without saying that on all sites with http and without https you should not share personal information.

If you are still using a non-https email service or such a superficial online banking service, absolutely change immediately.

4) Phishing

Amongst dangerous sites in general, a particular category is that of scam sites such as unknown and unrecommended shopping sites or, worse, fake sites that look identical to famous sites and are created to steal passwords for accounts.

Making fake sites copies of banking or shopping sites is one of the most common techniques used by hackers to steal web account passwords and is called Phishing. Phishing always works by sending a message via email, Facebook, SMS, Whatsapp, etc. The best way not to fall for this technique is to use it as an excuse to steal passwords. The best way to avoid falling into this kind of trap is to never write down passwords and important data (even via email) except on the official websites of the accounts, recognisable by the address written at the top of the browser and the HTTPS with green padlock.

Ideally, it would be better to use an email client such as Microsoft Outlook and use a spam filter to block these messages.

5) Spam

The danger of spam is much lower today than it was a few years ago.

Spam would be the whole category of junk messages, advertising, phishing and viruses or useless communications. Fortunately, today's top email services such as Gmail and Outlook.com have an effective spam filter that regulates the receipt of emails.

6) Misinformation

Although it may be part of the Spam category, misinformation on the internet has become a real danger in the last year due to the spread of fake news from hoax sites which we must learn to recognise in order not to look like imbeciles who believe anything they read on the internet or Facebook.

7) Online dating

This is one of the most serious dangers of the internet for young people.

It sounds bad to say but a responsible parent should check if their children are chatting with strangers via the internet, whatever the circumstances. You can chat with a stranger in an online game, a casual dating site, a social network, a forum and any other chat room. Whether it is for sexual, dating or purely recreational reasons, it is important not to give out too much personal information: don't tell your real age, don't say where you live, don't say what school you go to, don't give out real names of family or friends and don't give out your phone number. Online predators are very good at passing themselves off as normal kids and know how to exploit the weaknesses of teenagers like not even the best psychologists, driven, in the most serious cases, by that terrible disease that is paedophilia.

8) Cyberbullying

Chatting with strangers can be dangerous because you never know who is behind the keyboard, but chatting or messaging with known people can also be dangerous. Cyberbullying works more or less like this: if you are teased at school or by your friends, one of them may post a video or photo on Facebook or other social networking sites which may embarrass the victim.

Another case of cyberbullying can come from anonymous messages that heavily insult the victim even with threats.

Compared to the real bully, the cyberbully has the advantage that there is no control and that he can say whatever he wants without looking his victim in the face, or even anonymously, hiding behind the keyboard. In either case, it would not be so difficult, at least on a technical level. It is much more complicated, however, to defend oneself on a psychological level, which may require the help of a parent or an expert.

To begin with, however, it would be an excellent step forward to delete the account on Ask.fm, one of the sites that lends itself most to online cyberbullying.

9) Total ignorance of computer security

This is an obvious danger, so widespread that one is surprised.

Is it possible that even today the most common password in the world is 123456?

Do people think that because they have nothing to hide, no hacker is going to steal their account?

How can people still use the same password for every website?

And then there are still those who write their passwords, perhaps all different and difficult to remember, on a piece of paper that can be read by anyone?

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.