We are products, not customers

It is a sentence launched by several social networks or Internet mastodons, such as Google, Facebook. It's part of their business strategy. And we accept their terms of use without blinking, without really taking the time to read them, to study them. Too long, too complex.

However, it is proven that Facebook acts on the psychological state of its users, by influencing the advertisements and the posts which they receive. All of this is done for commercial purposes. This helps push Facebook users to opt for specific products, specific opinions. Upstream, politicians and companies pay Facebook or Google to be featured prominently on their pages.

There are also the dangers linked to hacking, sexual crimes, theft which abound all the more, with the rise of technologies allowing to circumvent the laws: USB key hiding the IP address, untraceable mailboxes.

The dream world of Fake News.

The Internet is a great source of exchange, of communication, of knowledge. But it is not based on common laws, a shared ethics. As a user, we must above all train ourselves to face this jungle. Because all is not truth in the virtual.

On Youtube, the rise of the Youtubeur phenomenon has made it possible to launch names, to legitimize artists. But the site is full of Fake News. Like Google or Facebook, our research determines the videos that the social network will show us. On his social network page, a passionate Youtuber regrets that large Youtube channels are gradually invading space. He calls himself a craftsman of entertainment. He tries to make a living from his videos and puts a lot of time into it. But channels like the Angry Lama are factories of false information. Their goal is just to make money and not to live off their passion, like this Youtbeur. They often operate in 8 different countries, always offering the same content. But above all, they publish false information or debates treated on the angle of the sensational. And it works!

Cyber crime is also one of the dangers to which the user must be trained. Phishing or phishing allows the hacker to pretend to be an organization, a relative, in order to fool the user (bank, a relative abroad asking for money to help him ...). The goal may be to retrieve bank codes or information, or worse, money. It can also be attachments infected with a

virus that will go through an email. The virus will infect the computer, take control of it or even spy on it in order to recover confidential information (identity, banking).
A botnet is a network of computers infected with malware so that they can be controlled remotely, forcing them to send emails, spread viruses or carry out attacks without the knowledge of the real owners of the computers and without their approval.

How to fight?

The sites and social networks are all organized in a tree structure. All the addresses that are part of this tree belong to the same set. And that makes it possible to monitor a user on many different sites, to map his journey on the Internet. It is in this logic that Google and Facebook have bought other applications (Instagram, What'sApp, Youtube ...) in order to improve their tracking policy.
How can we protect ourselves? The first question is to ask what you want or not to share and publish on the Internet. Then, one of the weapons is to multiply email addresses, to avoid this tracing. It is possible to ask the site administrator to erase the content of our data. If it goes far (harassment, theft), do not hesitate to call the police. Special brigades were created there to help the victims. You can also use search engines that guarantee respect for private life and prohibit data trade (French Qwant). Finally, the European Union has created the GDPR (General Data Protection Regulation), a European body which fights against fake news and abuses on social networks.
There remains the antivirus. But, you should know that a certain number are only effective at 20 or 30%. Free antiviruses are the most problematic, because they themselves spy on and above all prevent a computer from being properly secured. For example, the latter will block updates, believing that they are dangerous elements.
You must therefore make regular copies of the contents of your computer. You must select the sites and pages that have a padlock in their addresses. These are secure sites. Be careful when synchronizing email addresses with a phone, especially with Google. This makes life easier, but also tracking and espionage. You can also use software to block cookies, spam, have your own online storage space (cloud).

François Arpin.
French Teacher
February 2020