



10 cybersecurity tips for teleworking :

#1 - Separate your professional and personal usage of IT equipment, if possible

The professional activity must be carried out on your professional equipment, if you have any, because it is complicated for IT departments to secure a personal computer. Regarding your personal activity, it must be done only on your personal equipment. Otherwise, there is a risk of generating security breaches that could be detrimental to your business.

#2 - Apply security and software updates to all your connected equipment (PCs, tablets, telephones, etc.) as soon as they are available.

This allows to correct security flaws that could be used by hackers to penetrate your connected equipment and use it to attack your company's network through your accesses.

#3 - Check that all your connected equipment (PCs, phones, tablets, etc.) is well protected by an antivirus.

Make sure that the antivirus is up to date, and carry out a complete analysis (scan) of your equipment. If a piece of equipment cannot have an antivirus software, avoid using it as much as possible to access your company's network.

#4 - Strengthen the security of your passwords

Use complex and different passwords on all the equipment and services you access, whether personal or professional. The majority of attacks are due to overly simple or reused passwords. Don't use your children's/boyfriend's/wife's/dog's name as a password, and don't write down your passwords Post-it® or Sticky Notes! When in doubt, or even as a precaution, change your password on a regular basis and enable dual authentication whenever possible.



Rue Wangari Maathai
57140 Norroy-Le-Veneur
France



0811 030 767



contact@steel-pc.fr



www.steel-pc.fr



facebook/SteelPCNews



twitter/SteelPCNews



#5 - Secure your Wi-Fi connection

Teleworking is generally done on your personal Wi-Fi connection. It is therefore essential to secure it well to avoid any intrusion on your network that could be used to attack your company. Use a long and complex password (see above) and make sure that you use the encryption of your WPA2 connection. Also remember to regularly update your router by restarting it or from its administration interface. Do not connect to open or public networks, as they are often used to launch attacks against your company. If you have no choice but to work from a public network, use a VPN (Virtual Private Network) to connect to your company's network.

#6 - Back up your work on a regular basis


Backing up is the only way to recover your data in case of cyberattacks, but also in case of failure or loss of your equipment. If possible, regularly back up your work on the company's network, but also externally (e.g. on a USB device or external hard drive) that you unplug once the backup has been made.

#7 - Beware of suspicious messages (email, SMS, chat...)

This could be a phishing attack aimed at stealing confidential information (passwords), a virus sent by attachment, a link that would lead you to a trapped site, or an attempt to scam false transfer orders. In the event of a suspicious behaviour (even if minor), immediately inform your IT department.

#8 - Install only official applications and avoid suspicious sites

Only install new applications on your professional equipment after approval from your IT support. On your personal equipment used for teleworking, only install applications from official sites or stores (e.g. Apple App Store, Google Play Store) to limit the risk of installing an application that is trapped to hack your equipment. Besides, avoid suspicious or fraudulent websites (downloading, video, illegal streaming) that could also trap your equipment.

 Rue Wangari Maathai
57140 Norroy-Le-Veneur
France

 0811 030 767

 contact@steel-pc.fr

 www.steel-pc.fr

 [facebook/SteelPCNews](https://www.facebook.com/SteelPCNews)

 [twitter/SteelPCNews](https://twitter.com/SteelPCNews)



#9 - Be vigilant when working in a public place

Whether on the train, in a café or in a coworking place, never leave your equipment unattended. Lock your PC when you are not using it (this also applies when you are working on company premises!). Hide your camera when not in use. Also, note that the likelihood of spilling your drink or any other harmful liquid on your computer is greater when you work in a café or in your kitchen.

#10 - Get informed and get trained!

Knowledgeable users are often the best mean to avoid or even detect cyberattacks. Training is therefore the best protection against cyberattacks. If in doubt, ask your IT department for advice. Your IT department should give clear instructions to be followed by all company employees.



Rue Wangari Maathai
57140 Norroy-Le-Veneur
France



0811 030 767



contact@steel-pc.fr



www.steel-pc.fr



[facebook/SteelPCNews](https://www.facebook.com/SteelPCNews)



[twitter/SteelPCNews](https://twitter.com/SteelPCNews)