MEMO

Protecting yourself from cyber risks when working from home

The COVID-19 epidemic and the unprecedented measures taken by the authorities in many countries around the world are forcing companies to adapt their working methods and tools. This situation, which is out of the ordinary on an international scale, offers multiple opportunities for hackers to carry out attacks against companies: it is a cyber threat that we take very seriously, and that we can combat together by adopting the right reflexes.

We have identified two of the most common types of attacks - and we are seeing an increase in recent days - and the appropriate responses:

Identity theft: these include attempts to impersonate an executive, a member of your executive Committee, or a supplier to obtain the performance of financial transactions without respecting the usual governance and procedures, under the pretext of urgency. These usurpers are very well informed and prepared, which makes their techniques very effective. These attempts can be made by phone or email. Remember that none of your group's executives would contact you directly in order to carry out confidential financial transactions without respecting the procedures in force. In any case, if you receive an unusual solicitation concerning a financial transaction or the recovery of sensitive data, systematically check with your Management and/or your financial teams.

Malicious applications and sites: claiming to disseminate information relating to COVID-19, hackers may lead you to malicious apps and / or sites that are likely to suck up your data or introduce viruses into our system: we urge you to be doubly vigilant before clicking on a link or installing an application and to limit yourself to official sources of information.
Caution and common sense are a precious help in this type of situation. We would like to draw your attention to the fact that the massive use of teleworking could lead to an increase in these fraud attempts.

In addition, you will find some good practices in terms of protecting and securing our data.

Some good practices when working remotely:

- Remember to work in a place that can be isolated and to lock your workstation after use. You may have to handle sensitive information that is not accessible to those around you.
- Only use your professional equipment for professional purposes and do not attempt to install anything on it.
- If you connect to your PC via wifi, check that it is secured by a secret key, and if this is not the case, activate encryption, disconnect and reconnect your computer.
- If other devices in your family are connected to your home network and box, make sure they are equipped with antivirus software with an up-to-date signature database, that the computers' operating systems are up to date with security patches and that the automatic update feature is enabled; and run regular virus scans on these devices to make sure that they do not risk infecting all the devices connected to your home network and box.
- Access your applications via the VPN and the protection solutions in place on the network. Remember to disconnect from the VPN session once your work is finished (after copying your files to the network zones).
- Do not connect personal equipment (printer, external disks) to your PC.
- If your PC behaves abnormally, please disconnect your PC from the network; Do not connect to the VPN any more and ask for assistance in order to have the status of your computer checked.
- Do not click on any links or attachments from unverified individuals.
- Be suspicious of any emails referencing the Coronavirus or COVID-19 even if they appear to be coming from a trusted source (HR, government agency) as these could be phishing emails.
- Completely avoid use of any personal social media accounts or internet websites (including email) on your work from home device. This is a common target right now as a way to infiltrate into a corporate system.