Informative Note

Recommendations on cybersecurity in the teleworking environment issued by the National Cryptographic Centre and the European Agency for Cybersecurity

19th March 2020

Following the previous communications issued by Andersen Tax & Legal as a result of the extraordinary situation caused by the COVID-19, we indicate a series of recommendations on cybersecurity in relation to the teleworking environment in accordance with the recent pronouncements of the National Cryptographic Centre (CNN) and the European Agency for Cybersecurity (ENISA).

The fact that many employees can provide services remotely, through the modality of teleworking from their homes, may entail certain risks in terms of cyber security and data security. In this sense, both the CNN and ENISA propose a series of measures to be considered to try to prevent and avoid these risks:

- Comply with the security protocols applicable to computer devices and equipment that the company has adopted.
- Use a secure Internet and Wi-Fi connection, protected by a sufficiently strong password combining letters, characters and numbers.
- Provide the computers you are working with with an updated antivirus system. It is also important to install all device software updates and, if possible, back up the entire system.
- Provide both mobile devices and computers with a secure password to access them or a security pattern if possible.
- Disable all wireless connections (i.e. Wi-Fi and Bluetooth) when the computers are not in use
- Avoid using the same password or key for both private or personal accounts and those of the organization for which the services are provided It is also recommended that you log off when you stop using your computer or work in an unprotected environment.
- As far as possible, avoid using your computer for both personal and professional activities, as phishing attacks related to COVID-19 are on the rise.
- Regarding the use of email, it is recommended to be wary of all messages asking to renew credentials, even when they may seem trustworthy. Therefore, it is advisable to verify the authenticity of the emails and, under no circumstances, download or open suspicious files or links.
- Make use of the cloud storage services implemented by the company.
- In the case of problems or incidents related to the security of the computers, it is necessary to contact immediately the Security Manager of the company or, if necessary, the IT Department.

In short, it is a matter of adopting simple measures whose compliance makes it possible to avoid many problems and risks in the area of cybersecurity and data security.

In any case, if any security incident occurs that puts at risk both the company's or organization's information and communication systems and databases, action should be taken in accordance with internally established security protocols and incident response plans.

You can consult the complete recommendations published by both bodies through the following links: Centro Criptográfico Nacional and Agencia Europea para la Ciberseguridad.

We hope the information is useful and of your interest. At Andersen Tax & Legal we have created a multidisciplinary team to deal with all the questions that may arise on this aspect or in relation to the COVID19 and all the professionals of the firm are at your disposal.

For more information please contact:

Isabel Martínez Moriel | Director in the area of Privacy, IT & Digital Business
isabel.martinez@andersentaxlegal.es