Teleworking is good, protecting data is better !

By Hamza Nassaf, Africa-Middle East CIO

In this lockdown period, many companies have resorted to teleworking to ensure business continuity. This change in working mode, which was unusual till recent days in many countries, is not without risk of cyber attack or data breach. Mazars has identified 8 key measures to limit those risks that could impact Confidentiality, Integrity and availability of data.

1. Secure Wi-Fi Network

● Secure your wireless domestic network by strengthening password (Using WPA2 instead of WEP) and if possible, not displaying its name (Hide SSID)

● Change default settings of your Wi-Fi equipment (Wi-Fi name and password, admin access) these values can be easily found on the manufacturer website

● Avoid connecting on Public Wi-Fi networks. If necessary, it is strongly recommended not to allow your device to be discoverable

2. Strengthen passwords

● Avoid using the same password for all applications accounts (Personal or Professional)

● Nowadays, passwords should be longer and more complex to withstand attacks, which are becoming increasingly dangerous. For example, a short password can be cracked instantly while a strong password, complex and composed of different characters (numbers, lowercase, uppercase, special characters) can withstand long years before being discovered by specialized software

Advice > Avoid conventional passwords (password, mypass, etc.), logical sequences (123456, qwerty, etc.) or words from dictionaries of any language

3. Ensure Antivirus update

● Make sure your antivirus is up to date and that the update is scheduled for a daily frequency, this will protect your computer even against new viruses

4. Secure remote access

● For remote access to your applications or internal networks, use VPN (Virtual Private Network) between your computer and your company's network

5. Encrypt sensitive documents

● Before sharing your sensitive documents by e-mail or by using online sharing tool, it's recommended to protect it by using a password
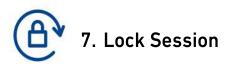
Steps to do in the Office : File Tab > Click Information > Protect document > Encrypt with password

MAZARS

6. Back up data

● Make regular backups of your data and ensure that backups location is different from original data source

Tip > Save your data to an external hard drive and place it in a safe place, or use cloud storage, this will allow you to recover your data in case of loss / theft of your computer

7. Lock Session

● It is necessary to lock your screen whenever you are absent, even for a short time

8. Last but not least, Stop Phishing !

● Given current circumstances, several applications and malicious websites have emerged exploiting coronavirus context to infect a large number of victims. Following this, it is recommended :

o Beware of emails asking to enter your password, click on a link or download an attachment to access to Corona epidemic status or update on corona vaccine research progress (use only government sources for that)
o Beware of unusual requests (password, bank transfer, sensitive paper), even from known sources
o Contact email sender by phone, in case of doubt after receiving an email from him

- In case of attack :

o Immediately change password if it has been communicated via untrusted site
o Completely disconnect computer from network if its infected
o Get in touch as soon as possible with his IT manager to inform about incident

Tips > Following indications should alert you about a potential phishing email :
Email with no Object / Multiple grammar mistakes / Lack of email personalization and greeting formulas

Did you know ?

● **94%** of malware is delivered via email*

● **3.5 Billion $**, is total losses amount** related to cyber-attacks in the world in 2019

(*) Source: Verizon Data Breach Investigations Report

(**) Source: Amount released by the FBI on his last "Internet Crime Report"

MAZARS