Alliances MANAGEMENT

Coronavirus & Working from Home: Part 7

Ensuring the Security of Data & Devices: Protecting Company and Client Information

by Jean-Pierre Lacoustille & Sébastien Valette

Even in normal times, companies that allow their employees to work remotely should perform risk assessments of their remote workers' computing setups, as this is essential to protect company and client information. For companies without such processes in place, now is a good time to implement them.

As general guidance, companies should consider the following:

- Agreed security measures and tips should be incorporated into a company's official employee and cybersecurity policies.
- Dedicated training sessions should be held for new staff.
- Companywide security awareness trainings should be scheduled, especially when companies update their security policies.
- Newly remote workers should be given a quick refresher course about how the company's official cybersecurity policies translate into a remote environment.

This is Part 7 of our series *Coronavirus & Working from Home*.

It includes insights from Alliances Management staff, who have worked remotely since the company's inception in 2006.

The entire eight-part series can be viewed on our website.

Secure devices

Companies' IT and security managers should establish clear policies about how employees should connect to the company's systems (and specifically to which parts of the systems depending on the level of sensitivity of the

data). This policy should define which devices are allowed to access which systems and information. It is usually best for employees to use company-issued equipment only, whenever possible, be it laptops or wireless devices, for the following reasons:

- As they will have configured it by themselves, IT personnel will be able to better manage and monitor company-issued equipment.
- Security protocols enforced by professional software and technology are typically stronger than what is usually installed on personal devices — it's best to use evaluated and certified tools such as encryption software, antivirus software and firewalls.
- It is probably not a good idea to use the same computer that the kids use to play online games.

Once you're working on an approved device, consider the following security issues and best practices.

Digital security while working remotely

- Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection, for example use a VPN IPsec solution or activate point-to-point encryption on your home box.
- Keep work data on work computers, as opposed to transferring data via USB drives or Bluetooth from or to other personal devices, typically for using a home printer or any other practical reason.
- Use secured online backup systems (with proper encryption activated), as opposed to using your own local backup disk or non-controlled online solution.
- Encrypt any sensitive data sent through emails or stored on your device. Many user-friendly tools exist for this.
- Do not use random thumb drives, but rather, dedicated professional USB drives with proper labels, for any sensitive data transfers between computers.
- Install security software and ensure software updates and operating system updates are turned on.
- Use Virtual environment and/or VPN IPsec solution to access the company network.
- Use strong passwords and two-factor authentication for enhanced protection.

Password security

Many employees take the easy route when it comes to defining passwords. They want something that is easy to remember, so they select passwords that are simpler and apply them to numerous systems. IT departments should, rather, insist that for all company hardware and online access, staff adhere to a well-defined and strong password policy. The following are considered best practices for passwords:

- Never write down your passwords. If passwords must be written down, then they must be secured in a safe or a locked file cabinet.
- Never send a password through a non-encrypted email or messaging platform (e.g. Skype).
- Never include a password in a non-encrypted document.
- Never tell anyone your password.
- Never hint at the format of your password.
- Never use the “Remember Password” feature of applications like web browsers and email clients.
- Report any suspicion of your password being compromised to your company’s IT and security managers.
- Only change your password if your company’s IT department explicitly instructs you to do so. Beware of emails asking you to enter or change your password, even if they look official.
- Be aware of anyone who can see you type your password.

Physical security while working remotely

Workers who print documents or possess other confidential client information should take additional steps to physically secure that information in their homes:

- Lock your doors as soon as you leave your work area.
- Store any printed documents in a lockable filing cabinet.
- Equip your home office with a cross-cut paper shredder (at least ‘DIN3’ compliant) to destroy any confidential printed information as soon as it can be disposed of.
- When traveling, always take your computer with you and never leave it alone such as in your car while going shopping.

About Alliances Management

Alliances Management is a consulting, association management, and strategic staffing firm that delivers top-quality project management, operations, and administrative services. Visit us at www.am.consulting or on LinkedIn.

Finally, social engineering is a particular risk that could give rise to successful attacks from hackers if employees are not properly warned. It consists of luring unsuspecting workers into retrieving confidential data from them. In order to avoid this, proper training of remote workers about such techniques (e.g. phishing) and ways to avoid being tricked should be a key facet of your company’s overall security practices. It will also allow them to be conscious of security risks and to take ownership of the more global security measures enforced by the company to apply them in the best way possible.