FEDIL

Publikation

REMOTE WORKING: SAFETY AND CYBERSECURITY CAN GO HAND IN HAND

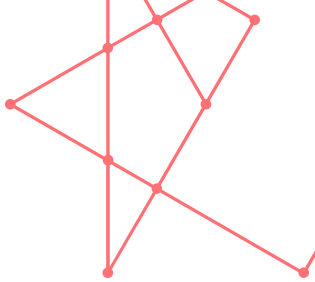
Working from home will be the only possible way to work for many people. Safety first! But cybersecurity must not be forgotten...

In this very particular situation, working remotely will be the only possible way to work for many people and a very wise choice for many others. Safety is the absolute priority for the moment. But cybersecurity has not to be forgotten if we do not want to add digital chaos to the "physical" one. We give you some basic tips to protect yourself and your information during these challenging times.

Devices

- Take extra care that devices such as USBs, phones, laptops, or tablets, are not lost or misplaced.
- Make sure that each device has the necessary updates, such as operating system updates (like iOS or Android) and software/antivirus updates.
- Ensure that your computer, laptop, or device, is used in a safe location, for example where you can keep sight of it and minimize who else can view the screen (particularly if working with sensitive personal data).
- Lock your device if you do have to leave it unattended for any reason.
- Make sure your devices are turned off, locked, or stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong. passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is stolen or misplaced.
- When a device is lost or stolen, you should take immediate steps to ensure a remote memory wipe, where possible.

Emails



• Use work email accounts rather than personal ones for work-related emails involving
personal data. If you have to use a personal email make sure contents and attachments are encrypted and avoid using personal or confidential data in subject
lines.
• Before sending an email, ensure you are sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal
data.
• Prefer sending encrypted emails every time, if possible.
Cloud and Network Access
• Do not connect to any public, unknown or unchecked networks
o Connect to the 3G or 4G networks if you have no access to a safe Wi-Fi;
o Use a VPN.
• Where possible, only use your organization's trusted networks or cloud services, and
complying with any organizational rules and procedures about the cloud or network
access, login and, data sharing.
• If you are working without a cloud or network access, ensure any locally stored data
is adequately backed up securely.
• Remote access software (like Teamviewer) should be used very carefully and only by
authorized employees. It has to be always updated, and only used in case of absolute necessity.

Special for CISO

Make sure that every mobile device used by the employees is safe and that you have the
possibility to wipe them in case of theft or loss.
Use Mobile Device Management to secure the devices used by the employees

Communicated by SECURITYMADEIN.LU