Safe Teleworking

TIPS AND ADVICE FOR BUSINESSES

Establish corporate policies and procedures (test them in advance if possible)

Provide a clear policy on teleworking, including guidelines on accessing corporate resources and who to contact in case of problems. Set up a clear procedure in the event of security incidents. Apply extra measures regarding documentation to the attention of middle and senior management for signature purposes, approval/feedback and information.

Secure your teleworking equipment

Implement measures such as hard disk encryption, inactivity timeouts, privacy screens, strong authentication and removable media control and encryption (e.g. USB drives). Implement a process to remotely disable access to a device that has been lost or stolen.

Secure Remote Access

Only allow your employees to connect to the corporate network through a company-provided VPN with multi-factor authentication. Ensure that remote sessions automatically time out and require re-authentication after a specified period of inactivity.

Keep device operating systems and apps updated

This will help mitigate the risk of cybercriminals exploiting unpatched vulnerabilities.

Secure your corporate communications

Enforce the use of multi-factor authentication to access corporate email accounts. Provide access to secure communication channels for employees to reach each other easily, as well as to communicate with external stakeholders.

Increase your security monitoring

Actively check unusual remote user activity and increase your alert levels for VPN-related attacks.

Raise staff awareness about the risks of teleworking

Educate employees about the company's policy on teleworking. Take the time to raise awareness of cyber threats, especially phishing and social engineering.

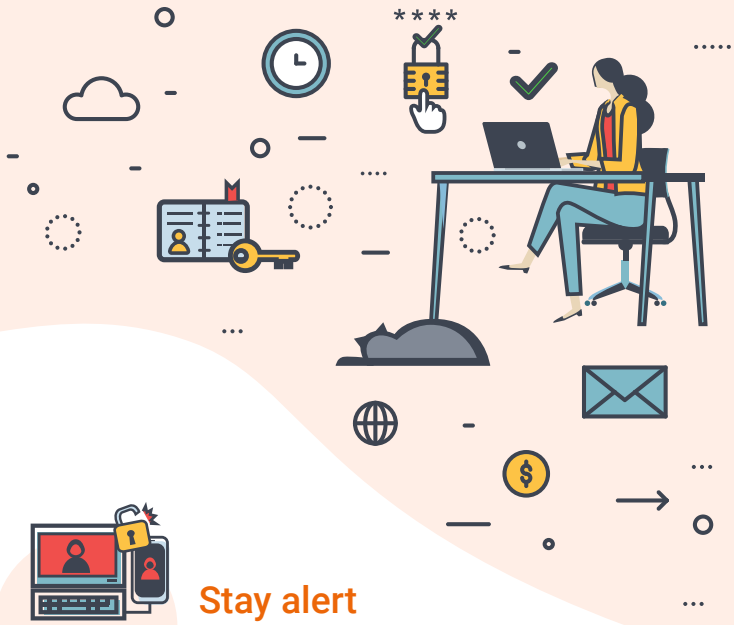
Regularly check in with the staff

Set up realistic goals, working schedules and follow-up mechanisms, being flexible where possible and taking into account personal circumstances.

EUROPOL | EC3 European Cybercrime Centre

Safe Teleworking

TIPS AND ADVICE FOR EMPLOYEES



Access company data with corporate equipment

Only use company-provided devices and software. Create strong passwords (use trusted/approved password managers if available), don't write them down, and protect them from being seen when you are typing them. Avoid work-around options, even if they seem to provide just what you need.

Stop.Think.Connect

Before starting teleworking, familiarise yourself with corporate devices, policies and procedures. Make sure you understand the equipment, the dos and don'ts of its use and where to go for help.

Secure Remote Access

Connect to the corporate network only through the corporate VPN and protect the tokens (e.g. smart card) required for the VPN connection.

Protect your teleworking equipment and environment

Do not allow family members to access your work devices. Lock or shut them down when unattended and always keep them in a secure location to prevent loss, damage or theft. Prevent shoulder surfing by using privacy screens and avoid angling screens towards windows or cameras.

Report

If you see any unusual or suspicious activity on any device you are using to telework, immediately contact your employer through the appropriate channels.

Stay alert

Watch out for any suspicious activity and requests, especially financial related ones. This could be CEO fraud! If in doubt, call the requester to double-check. Do not click on links or attachments received in unrequested emails and text messages.

Avoid giving out personal information

Never respond with personal information to messages, even if they claim to be from a legitimate business. Instead, contact the business directly to confirm their request.

Develop new routines

Discuss work plans with your direct management and team members during the teleworking period, including the distribution of tasks, deadlines and channels of communication.

Use of private devices

If using your personal device is the only option and your employer allows it, make sure your device OS and software is up-to-date, antivirus/antimalware included, and the connection is secured through a VPN approved by your company.

Keep business and leisure apart

Avoid making personal use of the teleworking device.

EUROPOL | EC3 European Cybercrime Centre