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