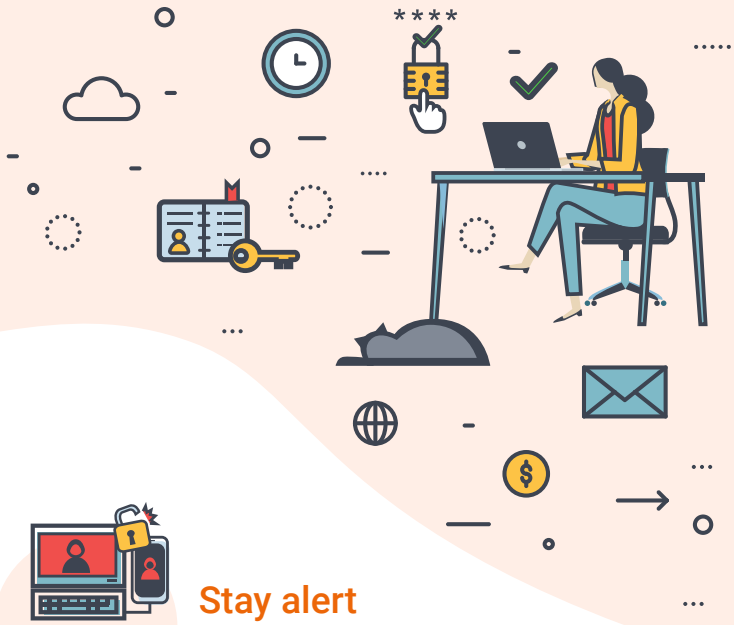
Safe Teleworking

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