

STAY SECURE WHILE WORKING FROM HOME

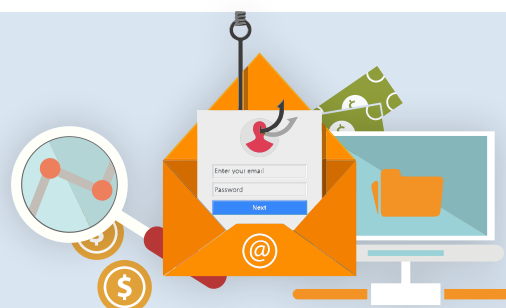
TIPS AND ADVICE FOR EMPLOYEES

ACCESS COMPANY DATA WITH CORPORATE EQUIPMENT

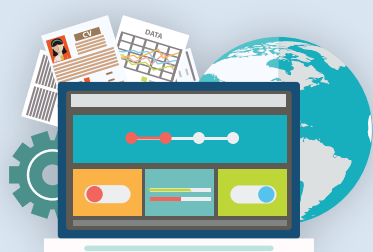


Only use company - provided devices and software. Create strong passwords (use trusted/approved password managers if available), don't write them down and protect them from being seen when you are typing them. Avoid work – around options, even if they seem to provide just what you need.

STAY ALERT



Watch out for any suspicious activity and requests in your inbox, 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.



STOP. THINK. CONNECT

Before starting to work from home, familiarize 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.

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.

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.

DEVELOP NEW ROUTINES



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



REPORT SUSPICIOUS ACTIVITY

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

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 VPN approved by your company.

PROTECT YOUR 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.



KEEP BUSINESS AND LEISURE APART

Avoid making personal use of your work from home device.