Resilient Smart working: the need of cyber security is also domestic
What can users do?

1 USE SAFE AND DEDICATED PASSWORDS FOR BUSINESS DEVICES

In our homes, we have a large number of devices connected to the same network, with inadequate security protocols.

a) Do not re-use the same password for personal and business accounts.
b) Change your passwords frequently, avoiding the use of common words, important dates and personal information.
c) Use a password manager to store your passwords, to save having to remember them all the time.

2 USE SECURE AND UPDATED CONNECTIONS

Home networks are often not secure or updated connections.

a) Use the corporate VPN (Virtual Private Network).
b) Update devices with the latest security patch.
c) Avoid promiscuous usage of the company devices, limiting the use of work devices for non-professional acivities.

3 BEWARE OF PHISHING!

Attacks aimed at stealing information, personal data and passwords are increasing.

a) Do not use your personal email in the work domain. Avoid revealing financial and commercial information on social networks (including message boards/WhatsApp)
b) Be wary of links and suspicious email; avoid downloading attachments from unknown senders. Before clicking on a link move the cursor over it and check that the address is reputable.
c) Pay attention to suspicious calls from operators who may claim to be the company's technical support – they may be stealing information and passwords.

4 KEEP IN TOUCH WITH YOUR TEAM TO GUARANTEE OPERATIONAL RESILIENCE

Changing the way you relate to your work team can be confusing.

a) Don't be afraid to "disturb" your team - don't hesitate to contact them.
b) Organize at least one meeting per day with your team.
c) Choose the use of call and videocall over the use of mail and IM (Instant Messaging)

5 BACK UP YOUR DATA REGULARLY

"Perfect" security doesn't exist

a) Make and keep an up to date copy of all activities and data.
b) Back up your data: this allows you to promptly restore your operations in the event of an attack.