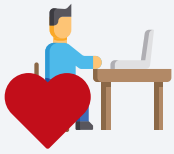
The Independent Solution Provider for Smart Digital Transformation

Working from home safely



Healthy work environment

- Take care of proper ergonomics. (Proper chair, desk height, monitor usage etc)
- Remember to take regular breaks to stretch.
- Your surroundings are important, organise it to work for you.

Working securely from home

- Ensure your printed documents are handled or disposed of properly.
- Even working from home, you should lock your workstation.
- Don't use a private laptop for work or vice-versa if you can avoid it.

Your home network

- Make sure your network is safe.
- Change default names and passwords of your WIFI network.
- Wireless networks come with encryption options. Use WPA2, this is the current standard.
- Check that your firewall is running. As a bare minimum you need to use the firewall on your workstation.

Secure connection

- Only use safe websites and services. (Think about HTTPS and check the URL's)
- Use VPN if possible. Often it is provided by the company.

Cloud

- Only use cloud services approved by the company.
- Use two or multi factor authentication where ever possible.

Hardware safety

- How does your printer connect? The safest way is to connect to your workstation directly.
- Check the security settings of your printer. (The manual usually shows an easy way to update the settings and improve security)
- Using private hardware for business purposes is not advisable as it usually does not comply with the company security standards.
- Don't use company hardware for private purposes either. Privately used cloud services provide yet another possible angle of attack.

Software safety

- Make sure your operating system (Windows, MacOS etc) is patched: all security updates should be installed.
- Keep the business software safe, don't skip updates.
- Always use anti virus software.
- Don't forget the updates for any software you installed yourself.

Security Awareness is extremely important, now more than ever

Always check the complete email address of the sender.

If you do not trust the email 100%, don't open any attachments.

Don't click on any hyperlinks if you can't trust the email.

Always notify your IT department of any suspicious emails.

ATS Enterprise Security is an expert division of ATS Global B.V. , A. Hofmanweg 5a, 2031 BH Haarlem, P.O. Box 4993, 2003 EZ Haarlem, +31 (0)23 – 751 12 00, www.ats-global.com/enterprise-security/