Easy tips to secure your home office

Right now, many employees have home offices and try to work as normally as possible. Many have brought home monitors, mice and keyboards. Some have even brought their office chair.

But, have you thought about what you need to do to make your home office as safe and secure as your office? Mind that you are not as well protected at home as at work.

Here are some safety precautions you should consider:

You are the best protector

- Beware of scam emails, beware of scammers
  - Be cautious with messages that pretend to have been sent by someone you know, who asks you to click on something or buy something.
  - Pay extra attention to emails that appear to come from the director asking for something that violates the organization's routines. If you receive a strange email from the manager, create a new email (instead of replying to this) or call them to ask if the inquiry is genuine.
  - Be cautious with people who call you and claim to be from Support or Microsoft.
  - Be cautious with people who may take advantage of the Covid-19 situation.
- Don't give out your username and password to anyone else. If you suddenly find a Microsoft login image in a browser tab, make sure that the web page address begins with "login.microsoft.com/" (there should be no other bullets before the first slash).
- If you suspect you have clicked on something you should not, promptly notify security officers in your organization.

Secure your wireless network (WiFi)

- Use at least WPA2, or better encrypted wireless network at home
- Separate wireless networks: one for guests and another for private / work
- Have different and strong passwords on the wireless networks

(How to check your WiFi security situation:
https://www.eunis.org/blog/2020/04/09/how-to-check-your-wifi-security/)

Use a virtual private network (VPN)

- Use a VPN to access your files, services and tools at the institution from outside. This provides better security in the transfer of data between your home and the workplace
- Ask your local IT for advice on how to set up VPN in your organization

Update the software on your devices

- Keep the software on your mobile phone (Android, iOS), laptop and other mobile devices up to date. Turn on auto-update.

Do not allow guests and children to access your job equipment

- Explain to those at home that they are not allowed to use your work equipment and why.
- Guests and children may accidentally delete or modify information, and at worst infect the laptop / phone / iPad.

Use long passwords and multi-factor login

- Create long passwords with at least 12 characters, or use a passphrase of at least 16 characters.
- Enable and use multi factor login where possible.

Store your business data safely and securely

- Make sure you store the data you are working on in a location approved by your organization.
- Do not use cloud storage unless this has been clarified with the employer first.
- If you have any business paperwork at home, handle it with the same care as digital documents (especially do not throw any confidential paperwork in the normal thrash).
- Do not leave any of your work equipment unattended at places where it is easily accessible by strangers (like on the balcony or in the garden).

More information

Follow important information from the university sector and your authorities

Norway

- https://unit.no
- https://helsenorge.no/koronavirus
- https://uninett.no
- https://krono.no

Germany

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html

Other countries?

You are welcome to add useful links to information provided in your country:
https://docs.google.com/document/d/1eQXVlHcPL5sSCOl42uSWig0urA83kJSTvWo4bjZ9-Kg/edit?usp=sharing