How to: Be secure at home

The basics when working from home

A wide threat landscape

Working from home involves more risks than we are accustomed to in the office. In times of dynamic change between home and office, we must remain especially vigilant.

In general

- Use professional devices only for work and vice versa
- Be aware of your surroundings – could spectators or eavesdroppers see or hear confidential information (e.g., through a window)?
- Lock or shut down your computer during breaks, even at home

Your router

- Change your router password from the factory password to something secure
- Update the firmware of your router and keep it updated
- Set up a guest network for visitors and other devices

Smart devices

- Voice activated devices like smart-speakers or smart-TVs are always listening – keep them out of range or turned off
- Check the data privacy settings of your smart devices
- Please note: Don’t log into your smart home from public Wi-Fi

How can I handle data with care, especially at home?

Documents, devices and classified information generally face a greater **risk of being exposed** to third parties once they are outside the office.

When working from home ...

Don’t throw away classified documents in your private garbage or recycling bin. Instead, shred the documents. Sensitive documents can be brought and disposed of at the office.

Your private printer shall not store, print, or scan jobs locally. If necessary, it should be connected via USB, local LAN or encrypted Wi-Fi. Don't print strictly confidential documents at home.

Never store or use company information on private storage media (e.g., Cloud solutions, personal devices, and USB Sticks.)

Further Information

Looking for more examples and information on this topic?
Ask your organization for additional guidance.

Join or create a Security Community
Become a member of your internal group or get connected with other colleagues interested in cybersecurity by creating a new group.