

Ransomware

- How to detect?
 - Do you expect that email?
 - Is that email plausible?
 - Language, sender, time of day, subject, ...
 - Attachment or link to attachment?
- What when it happened anyhow?
 - Turn off workstation ASAP
 - Inform IT
 - Remember: you are a victim too
- If some information would be missing, please inform IT

Phishing

- Count red flags
 - Something you believe in
 - or someone you trust
 - Fear
 - 'Click here' to resolve
- Hover mouse over link (do not click!!)
- Copy link into Virustotal
- When in doubt: send email to IT

WiFi

- Do not connect to Open WiFi (=without password to connect to the WiFi)
- Always do 'Forget Network'

USB

- Never plug in your device in a USB wall socket
- Do not trust found USB-devices

CEO fraud

- Ask direct feedback to sender
 - Phone call using number you already have, not from the email
- Face-2-face



Passwords

- The longer the better
- Unique password for every service
- Use a company-approved password manager
- Your password compromised? Check it:
<https://haveibeenpwned.com>
- Never send passwords through email
- Never ever send username and password together
- Enable 2-step verification / multi-factor authentication with all possible services