



# SCAMS

**Weak passwords**

- x!@\*Aj2a
- Barbra123
- weak-password

**Password length**

- At least 12 characters
- Ideally more than 16 characters
- You can use 5 or more random words
- Eg: FineCriticalAcornMinisculeAugumentations

**Use a password manager**

- 1Password
- KeePass
- Bitwarden

**Never reuse a password**

- Use a unique password for every system / application

**Two-Factor Authentication (2FA)**

- Hardware keys (safest)
- Apps (e.g. Google Authenticator)
- SMS
- Remember about generating recovery codes

**Other recommendations**

- Do not share your passwords with anybody
- .zip / .pdf / .docx protected with a weak password can be easily cracked
- Periodic / forced passwords changes are not good
- Use haveibeenpwned.com to check if your password has been leaked in a data breach
- Got an e-mail with your password / threats: „I have access to your computer” - most probably it's a scam (i.e. nobody has access to your PC)

**Recommendations**

- Verify who calls you
- Do not click links in SMS messages
- Do not install any apps recommended by strangers
- Remember about filename extensions
- Do not attach unknown USB devices to your computer
- Remember about ad blockers
- Disconnect and manually type the number you want to call
- Verify bank consultant in your mobile banking app

**Links**

- Name of the link can be different than its address
- „Padlock” / HTTPS doesn't guarantee that the site is safe
- Check if the link is safe

**Attachments**

- Be cautious when dealing with password-protected attachments
- Check if the attachment is safe
- Suspicious extensions like: .img .url .lnk .exe .hta

**Spoofing**

- Verify sender address (not its name)
- Hacked mailbox of the sender

**Phishing**

**Examples**

- Fake investments
- Fake recruitments
- Scams targeting helpdesk
- Fake bank consultant
- Free „goods”
- Delivery surcharges
- „You have a virus, install this app”

**Mail**

- Caller spoofing
- Voice cloning (deepfakes)

**Voice (Vishing)**

- Sender spoofing
- Links

**SMS**

- In car parks
- E-mails

**QR-code**

- Google, Twitter, LinkedIn, Facebook
- Deepfakes

**Advertisements**

- „Someone hacked your account”
- „Someone took a loan in your name”
- „Super profitable investment”

## Ransomware

**How does ransomware infect companies?**

- Phishing / malware
- Unpatched, vulnerable software
- Weak passwords

**Extortion**

- For „data recovery”
- For „not leaking stolen data”

## Tips for working from Home

**Pendrives**

- Permanently erase data (full format)
- Do not use for transferring confidential data
- Do not lend pendrives

**Home WiFi security**

- Set up a strong WiFi password
- Change default admin password
- Set up a guest WiFi network
- Periodically update your WiFi router (firmware updates)

**Personal e-mail**

- Do not send or forward corporate e-mails to your personal email address
- Set up a strong password and 2FA

## I think I've noticed a scam - what should I do?

- Contact your IT security / IT department
- Do not click / open any links / attachments
- Think before acting