Staying Cyber-Safe While Teleworking

**THREATS**

- Ransomware and spyware
- Using personal devices
- Phishing emails
- Fraudulent calls
- Connecting to unsecure networks

**Precautions**

1. Install the latest updates on your device
2. Install anti-virus software
3. Set up a strong password
4. Encrypt your device's hard drives
5. Enable two-factor authentication (2FA)
6. Always use VPN
7. Watch out for phishing emails
8. Lock your devices if left unattended

**Avoid**

- Downloading sensitive data
- Using public wi-fi
- Using personal devices
- Storing sensitive data
- Sending sensitive data via email
- Leaving devices unattended

**Tips**

- Install anti-virus software
- Set up a strong password
- Enable two-factor authentication (2FA)
- Always use a VPN
- Watch out for phishing emails
- Lock your devices if left unattended

**Withhold**

- From sending sensitive data via email

**Never**

- Store sensitive data unattended in a public place
- Leave your devices unattended
- Share your work devices with family and friends

**Protect**

- Install the latest updates on your device
- Install anti-virus software
- Set up a strong password
- Encrypt your device's hard drives
- Enable two-factor authentication (2FA)
- Always use a VPN

**Watch out for**

- Phishing emails
- Fraudulent calls
- Connecting to unsecure networks

**Lock**

- Your devices if left unattended