Security Tips on Remote Working

Keep your computing devices secure

- Install anti-malware software and personal firewall
- Ensure all software / firmware are patched and updated
- Enable security features to prevent unauthorised access to your devices

Secure your network

- Avoid using public Wi-Fi network
- Use secure connection (e.g. Virtual Private Network (VPN))
- Use WPA2 or WPA3 encryption for Wi-Fi connection

Protect your user accounts

- Adopt strong passwords and/or multi-factor authentication
- Do not share your personal accounts with others
- Log out remote access account when not in use

Protect your data

- Back up your important data and keep the backups in a secure, off-site location
- Adopt data encryption when storing sensitive data in storage devices or cloud storage
- Do not overshare your personal data in social networking sites

Be aware of phishing scams

- Do not click links in suspicious emails / websites
- Do not open / download email attachments from suspicious sources
- Be cautious before submitting any personal / sensitive information

Provide adequate support for remote working

- Remind employees to comply with the information security guidelines and policies of your organisation
- Ensure employees have good awareness of the IT support facilities
- Ensure the incident response plan and business continuity plan are up to date

網絡安全資訊站
www.cybersecurity.hk