Information Security Guide for Small and Medium Enterprises

Security Tips for Remote Working

Government Computer Emergency Response Team Hong Kong

Hong Kong Computer Emergency Response Team Coordination Centre

Hong Kong Police Force

For details, please visit :

www.cybersecurity.hk

Secure Your Computing Devices and Remote Working Environment

- Install personal firewall; install anti-malware software and perform regular scanning
- Ensure all software / firmware patches are updated
- Ensure the working environment is free from peeping

Secure Your Network

- Use secure connection (e.g. Virtual Private Network (VPN)) to access sensitive information of the organisation
- Enforce WPA2 or WPA3 encryption for Wi-Fi network

Protect Your User Accounts

- Adopt strong passwords and/or multi-factor authentication
- Do not share your accounts in working devices
- Log out remote access account immediately after use

Protect Your Data

- Back up important data regularly; keep the backups in a secure off-site location
- Encrypt sensitive data when storing in storage devices or cloud storage

Be Aware of Phishing Scams

- Do not click links or open email attachment in unknown emails / websites
- Be cautious when submitting any personal / sensitive information

Provide Adequate Support for Remote Working

- Educate staff to observe corporate information security policy for remote working; and raise their security awareness
- Ensure the incident response plan and business continuity plan are up-to-date