Safe remote working

Help protect yourself and others

If you are working remotely, it is important that you have secure work practices at all times.

What should you do?

- Don't use public wi-fi.
- Conceal any personal or sensitive information in view during video calls.
- Cover or unplug webcams when you're not using them.
- Change your default home wi-fi password to a strong passphrase.
- Don't let family or friends use your work device.
- Always lock your screen when taking a break.
- Don't follow links or open attachments from untrusted sources.
- Avoid using free charging stations at airports, hotels and shopping centres. Public USB ports may be tampered with and can spread malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead.
- Disable any bluetooth, NFC, wi-fi, cellular and other connectivity functions when not in use.
- Always have the contact details of your IT team ready in case of an emergency and report any cyber incidents.

For a step-by-step guide on how to secure your home wi-fi, visit: https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-resources/cyber-security-awareness-resources

Cyber Security NSW