Safely connecting in public

Reduce risk and protect your devices

When you are connecting your device in a public setting, ensure you are practising safe security habits to protect your device. When not in use, you should disable any communication capability for electronic devices, e.g. cellular data, wi-fi, bluetooth and Near Field Communication (NFC).

What should you do?

When you are travelling, set up a personal mobile hotspot rather than using public wi-fi. Cybercriminals can operate on legitimate wi-fi hotspots, or even create their own malicious hotspot and trick you into connecting.

NFC is a type of contactless, wireless technology used for sending information or making payments, such as using your smartphone to tap and pay. When not in use, disable NFC to avoid any unwanted interception.

Do not leave your bluetooth on when not in use. Only use the most recent versions and install all available patches for your bluetooth devices. Be careful what devices you pair with; only pair with devices you know and trust.

Never use chargers supplied by third parties or charge electronic devices at charging stations or USB charging outlets. Only use genuine chargers supplied with electronic devices.

Be mindful of scanning unknown QR codes – it could result in your personal contact information being used for marketing or criminal purposes. If it looks suspicious, you can run your fingers over a QR code display sign and feel whether another QR code has been stuck over the top.

For more information on connecting safely, see:
https://www.esafety.gov.au/key-issues/how-to/connect-safely

Cyber Security NSW