International Travel – Cyber Safety Tips

Security warnings

Never ignore a security warning such as 'certificate can't be verified, or this is from an 'untrusted service'.

Never install or download certificates or software from untrusted locations (public Wi-Fi). This will minimise your risk of a third party having visibility of your data.

Avoid using a plug in memory stick

Malware can infect your computer using a plug in memory stick. Leaving infected memory sticks around is a known tactic used by cyber attackers. Leave them where you see them

Memory sticks can easily be lost or stolen which means sensitive information may be compromised

Avoid public charging kiosks

Charging kiosks at airports and public events may transfer data or install malware on devices that connect to them. A plug in wall charger or a portable charger is a far safer option.

Beware of Public Wi-Fi

Public Wi-Fi at airports or hotels uses an unprotected network connection. This means it is not a secure connection and your data can be accessible to scammers. This includes Public Wi-Fi at airports and hotels accessed with a security code. We do not recommend public Wi-Fi to access anything that requires you to log such as banking or shopping applications. It's best used only to browse the web such as sports and news sites.

The Wi-Fi link you choose may not be legitimate (even if the name is the one you think you are after).

Be mindful of social media posts

Be careful what you post on social media. It's best to hold off sharing your journey until you are home.

Hotspot for a secure internet connection

RMIT recommends the use of your RMIT mobile device as a portable Wi-Fi hotspot. Connect your device to the internet via your smartphone's data connection (avoid large downloads). Refer 'Get connected' – Hotspot set up

Protect your devices & data

Keep your devices password protected, use multi-factor authentication or a biometric lock.

Devices left in your hotel should be locked in the room safe.

Never let a stranger 'borrow' your device or leave them unattended in public. It takes seconds for a hacker to install malware or grab and run.

Use HTTPS websites which encrypt any data you enter. These are safer than HTTP websites which do not encrypt data.

Don't install certificates or any executable files.

Update your phone operating software before you depart. Minimising the risk of malware by deferring updates while travelling and only ever download apps from Apple Apps Store or Google Play store.

Cover your screens when putting in passwords and usernames. You never know who may be able to view video surveillance of public areas

Restrict iPhone airdrop settings

If you are using an Apple device, ensure your Airdrop settings are set to "Contacts Only"

Disable Bluetooth and Wi-Fi auto connect on your devices when not in use

Be sure to adjust your phone settings and protect any access to your device. Cyber hackers often set up phony networks to capture data from anyone who connects to them

Disconnect from MyDesktop connection upon completion

Use RMIT's MyDestop application (https://mydesktop.rmit.edu.au) when working in a public place (or accessing any other RMIT files on a public PC, be sure to terminate your connection upon completion. Shared computers may be susceptible to security risks.

Do not connect your phone to your rental car

Bluetooth connectivity is in many rental cars and may leave your device vulnerable to hackers. Personal information, such as your contact list may be retained even after a connection has been terminated.