University of South Australia

International Travellers Cyber Security Checklist

UniSA staff travelling internationally for work, research, or vacation, have a critical responsibility to protect institutional and personal data on mobile devices. Individuals face a variety of threats when travelling and best practices start long before boarding the plane. Staff, students, and other travellers should use this checklist to prepare against the unique threats of global travel.

Contents

University of South Australia

Before you leave

Physical Security

- ☐ Be aware of national data protection laws in your home and destination countries.
- ☐ Know and follow UniSA policies for using various devices, institutional data, and institutional resources including the UniSA Information Security Policy.
- ☐ Research personal, criminal, and cyber risks in the country or region that you're visiting. A good source of information is the Australian Government provided website https://www.smartraveller.gov.au/.
- ☐ Purchase and pack privacy screen filters, portable chargers, and country specific plug adapters.
- ☐ Be aware that border and/or customs officials may search your devices multiple times and copy data therein.
- ☐ Understand that legally confiscated electronic devices may not be returned for months.

Technical Security

- ☐ Consult with Information Strategy & Technology Services (ISTS) via the IT Help Desk about special concerns regarding your technology or your destinations.
- ☐ See if low-cost, loan devices are available to mitigate the risk of losing more valuable equipment.
- ☐ Ensure your devices have full disk encryption when available and local encryption when not. For assistance in setting this up contact the IT Help Desk.
- ☐ Make sure your antivirus program is updated and performing regular scans.
- ☐ Check your mobile phone coverage and international data plan options.
- ☐ Enable VPN access. Be aware some countries block VPN. Talk to the IT Help Desk for alternatives if needed.
- ☐ Set up institutionally approved, centrally provisioned data storage. Note that this storage will only be available if you are connected with the UniSA VPN.
- ☐ Back up all data prior to travel and take only essential data with you.
- ☐ Create complex passwords, PINS, codes, and screen locks for your device.

University of South Australia

While Travelling

Physical Security

- ☐ Keep safe by carrying only necessities, keeping bags zipped, and practicing situational awareness.
- ☐ Protect mobile devices by keeping them secure, locked, and hidden from sight when not in use.
- ☐ Protect RFID-enabled devices and bank cards with RFID shielded containers.
- ☐ Report stolen devices to your native embassy or consulate and the UniSA IT Help Desk immediately.
- ☐ Protect your data by using privacy screen filters and avoiding public discussions of sensitive data.

Technical Security

- ☐ Be wary of public charging stations; use wall outlets with your own chargers or external batteries instead.
- ☐ Avoid using courtesy computers in business centres for work-related purposes.
- ☐ Disable broadcast services like Wi-Fi access points, Bluetooth devices, and GPS when not needed.
- ☐ Don’t connect to unknown resources like Wi-Fi access points and Bluetooth devices.
- ☐ Assume locally provided technology, such as wireless networks, may be vulnerable to attacks or have risky security settings.
- ☐ Use the UniSA VPN whenever possible.
- ☐ Don’t enter sensitive information while connected to wireless hotspots or unsecured networks.
- ☐ Use two-factor authentication whenever possible.
- ☐ Don’t install software updates or patches while connected to untrusted or unsecured networks.
- ☐ Choose private browsing when accessing websites.
- ☐ Clear your internet browser of history, caches, cookies, and temporary files after each use.

University of South Australia

Upon Returning

Technical Security

- ☐ Review banking and credit card statements for unauthorised transactions.
- ☐ Scan devices for unusual activities. For assistance with this contact the IT Help Desk.
- ☐ Provide feedback to the IT Help Desk on what did and did not work well.
- ☐ Re-establish normal systems and safeguards with the help of the IT Help Desk
- ☐ Resume your weekly or monthly data check and back up routines as normal.
- ☐ If you took a temporary laptop, make a copy of your data and return the laptop to the IT Help Desk for re-imaging.

University of South Australia

Geographical Locations with Elevated Risks

Some international destinations are considered hot spots for malicious cyber activity as advised by the Australian Security Intelligence Organisation (ASIO) and the Australian Cyber Security Centre (ACSC). You should be extra vigilant when travelling to these destinations and enact additional precautions prior to and during travel.

For up-to-date destination risk levels, please refer to:

https://www.smartraveller.gov.au/destinations

Additional precautions you should enact when travelling to high-risk countries include:

Before you leave

- ☐ Consider utilising a temporary 'burner' phone that only contains emergency contact details and services.
- ☐ Obtain a temporary clean laptop that contains the bare minimum of data and software required for your trip. Contact the IT Help Desk for enquiries about obtaining a spare laptop.
- ☐ Disable and place non-transparent tape over the inbuilt webcam.
- ☐ Obtain a USB Data Blocker. This is a device that prevents unintentional data exchange when your device is plugged into a computer or public charging station.

While travelling

- ☐ Never use hotel/in-room safes. Instead, always keep your devices and valuables on you.
- ☐ Never use public USB chargers or chargers provided at hotels, airports, etc.
- ☐ Avoid transporting devices in checked baggage.
- ☐ Never leave electronic devices unattended. If you must stow them, remove the battery and SIM card and keep them with you.
- ☐ Don't use public Wi-Fi networks. In some countries they're controlled by security services; in all cases they're insecure.

Upon return

- ☐ Change your password.
- ☐ Return laptop to IT for re-imaging.
- ☐ Reset burner phone to factory settings and dispose of SIM card.