Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Security tips for travelling

Content Complexity
SIMPLE

cyber.gov.au

For more cyber security advice

For more information on how to improve your cyber security when travelling, see our other guides at **cyber.gov.au**

Personal cyber security series

Secure your mobile phone

Protect yourself: Multi-factor authentication

Table of Contents

Security tips for travelling

When travelling, you may be more vulnerable to a cyber attack. Your electronic devices contain personal data and using public networks can be a risk. Cybercriminals will target anyone to steal information or money.

Whether you're going interstate or overseas, make sure to secure your devices. Especially if you have access to sensitive data on them, such as identity documents or work files.

Follow the basic tips in this guide or learn more by searching 'travelling with mobile devices' on cyber.gov.au

Before you travel

Travelling can be a stressful experience. Secure your data, accounts and devices before you leave to help reduce the chance of a compromise.

Safeguard your data

Create a backup of your data that you can keep secure at home. Also, leave behind any information or devices you don't need. This limits how much data is at risk if someone steals or compromises your devices. To learn more, visit cyber.gov.au/backups

Secure your accounts

Turn on multi-factor authentication (MFA) for your accounts. MFA is when you need 2 or more steps to verify your identity before you can log in. For example, using your login details as well as an authentication code. To learn more, visit cyber.gov.au/mfa

Avoid using SMS as an MFA method as it is less secure. Also be aware you need to enable international roaming to get SMS overseas.

Where MFA isn't an option or you need to disable it before travel, use a strong password such as a passphrase. A passphrase is a string of random words like 'crystal clay onion pretzel'. It should be long, unpredictable, unique and should not include personal details. To learn more, visit cyber.gov.au/passphrases

Secure your devices

Secure your devices with a PIN or passphrase. Make it hard to guess and don't include personal details such as your date of birth. Make sure your devices are set to lock automatically after a short time (less than 5 minutes).

For more security use biometrics if your device supports it, such as your fingerprint. But check the laws of where you are travelling. Some countries may force you to unlock your device if you use biometrics. To avoid this, you can disable biometrics and use a PIN or passphrase instead. To get travel advice for your destination, visit smartraveller.gov.au/destinations

For more protection against unwanted access, encrypt your devices. It means if a device was compromised your data stays secure. If you do encrypt your devices, make sure to back up your recovery keys. If you lose the keys, you won't be able to use your device until you factory reset it or reinstall the operating system.

To learn more, search 'how to secure your device' on cyber.gov.au

Keep devices and software up to date

Update any devices you are travelling with so they have the latest security. Check automatic updates are on and install updates as soon as possible. The longer you leave it, the more vulnerable you could be to a cyber attack. To learn more, visit cyber.gov.au/updates

Protect against malware

Confirm you have installed antivirus software and that it is working. Your devices may already have it installed by default.

If you decide to use third-party antivirus software, make sure to research and choose a reputable provider. To learn more, search 'antivirus software' on cyber.gov.au

Limit what you bring

Consider using a device that is only for travel, such as a burner phone (a cheap phone you can dispose of). This should not have any personal data on it, including accounts or password managers. If someone gains unauthorised access to your device, there is less sensitive data at risk.

While you travel

Remember to stay vigilant with your security while on your trip with the following tips. This is the period you will be most vulnerable to cyber threats.

Lock and secure your devices

Lock your devices whenever you leave them unattended. Even if it is only for a short period. Make sure your devices are set to automatically lock after a short time (less than 5 minutes).

Try not to leave your devices in your room when you go out, even if there is a hotel safe. When in transit, always keep your devices on you or in sight.

Be wary of public devices

Avoid using public devices such as computers in a hotel business centre. These devices could have malware installed and using them can put your accounts at risk.

If you must use a public device, try not to log into your accounts or input personal information. If you do log in, don't save your login details and remember to log out when done.

Use trusted peripherals

Never use someone else's peripherals such as chargers, cables and other removable devices. Public charging stations and ports could also put your data at risk. Buy peripherals from reputable stores if you need them.

Avoid using portable storage devices such as USB drives. These are easy to lose, steal or infect with malware. Use more secure methods of file transfer and storage such as cloud services.

Be aware of your surroundings

Avoid accessing sensitive information in public spaces such as airports and hotel lounges. You could expose information to anyone passing by. Wait until you are in a more private location or consider using a privacy screen protector.

Back up your data

Make sure to back up your data often while travelling. If something happens to your device, you can restore important data such as photos and files. Create backups using a secure cloud service or an external storage device. You can turn on automatic backups to reduce the risk. To learn more about, visit cyber.gov.au/backups

Limit the information you post

Be careful of sharing your location and personal information on social media. This includes details such as your flight number, hotel check-in or photo metadata. Someone could use this information to target you. To learn more, search 'secure your social media' on cyber.gov.au

Manage your device connections

Public networks are convenient but can also be unsecure. Cybercriminals will target public networks to gain access to your sensitive information. If you are working in public spaces such as an airport or café, avoid using their Wi-Fi or use a VPN. Before using a VPN, check local laws to make sure it is legal in your current location.

Only use trusted networks such as your mobile data and personal hotspot. Where this isn't an option, think twice about what you share or access on a public network.

Consider turning off Wi-Fi, Bluetooth and near-field communication (NFC) on your devices when not in use. Cybercriminals could use these to hack your device or make unauthorised transactions.

To learn more, search 'public Wi-Fi and hotspots' on cyber.gov.au

Check for signs of compromise

While travelling you should be alert for signs of compromise, such as:

- devices or apps keep crashing
- suspicious adverts or pop-ups
- unexpected activity on your accounts
- unknown emails in your sent folder
- excessive battery or data usage when using your device
- devices are hot to the touch when idle.

If you believe you may have been compromised and need advice, visit cyber.gov.au/report-and-recover

Case study: Identity theft from using public Wi-Fi

A NSW man owed over $7000 in fees to a company for gift cards and subscriptions he didn't buy. The recipients for these purchases went to unknown email addresses.

After investigating, he found several inquiries on his credit report. These happened around the same time as the sale of the gift cards and subscriptions. The first inquiry happened not long after he had used his laptop on a trip.

When connected to the public airport Wi-Fi, he had sent his ID documents to his parents. These included his passport and birth certificate. Using the airport Wi-Fi may have let cybercriminals access his IDs and steal his identity.

After you travel

When you have returned home, you should still be alert to the possibility of a compromise. To further secure your devices, consider:

- changing the PINs and passwords for your devices and accounts
- disposing of your burner phone if you used one, including any SIM cards, eSIMs or microSD cards
- wiping any removable storage used when travelling, such as USB drives or SD cards.

Recover from a suspected incident

It is important to act as soon as you believe someone has access to your accounts or devices. Log out of the compromised device and don't use it to change your passwords.

Find out if you have been hacked and report the incident below. If you need more help, you can call our cyber security hotline on 1300 CYBER1 (1300 292 371).

Have you been hacked?

Find out what to do if you think you're the victim of a cybercrime. Visit cyber.gov.au/have-you-been-hacked

Report and recover

Respond to cyber threats and take steps to protect yourself from further harm. Visit cyber.gov.au/report-and-recover

Security tips for travelling checklist

Before you travel

- [ ] Create a backup of your data.
- [ ] Leave behind devices and information you don't need.
- [ ] Use multi-factor authentication (MFA) or a passphrase for each account. **Note:** You need international roaming if using SMS as an MFA method.
- [ ] Secure your devices with a PIN, passphrase or biometrics.
- [ ] Check automatic updates are on and install updates as soon as possible.
- [ ] Check you have antivirus software on your devices and that it is working.
- [ ] Consider encrypting your devices and back up the recovery keys.

Signs you may be compromised

- Devices or apps keep crashing.
- Suspicious adverts or pop-ups.
- Unexpected activity on your accounts.
- Unknown emails in your sent folder.
- Excessive battery or data usage when using your device
- Devices are hot to the touch when idle.

While you travel

- [ ] Lock your devices whenever you leave them unattended.
- [ ] Try not to leave your devices in your room when you go out and always keep your devices on you or in sight when in transit.
- [ ] Make sure your devices are set to automatically lock in under 5 minutes.
- [ ] Never use someone else's chargers, cables and other removable devices.
- [ ] Avoid logging into your accounts or saving your personal details on public devices.
- [ ] Be careful of accessing sensitive information in public spaces.
- [ ] Back up your data often to a secure cloud service or external storage device.
- [ ] Don't share your location or personal information on social media, including your flight and hotel details.
- [ ] Only use trusted networks such as mobile data and personal hotspot.
- [ ] Where you must use a public network, think twice about what you share or access.
- [ ] Consider turning off Wi-Fi, Bluetooth and Near-Field Communication when not in use.

After you travel

- [ ] Consider changing your PINs and passwords.
- [ ] Consider disposing of your burner phone if you used one, including SIM or microSD cards.
- [ ] Consider wiping any removable storage you used, such as USB drives and SD cards.

Notes

Notes

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre