Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Security tips for travelling checklist

When travelling, you may be more vulnerable to a cyber attack. Cybercriminals will target anyone to steal information or money. Whether you're going interstate or overseas, make sure to secure your devices.

Following this checklist will help improve your security. You can also refer to the full guide on cyber.gov.au

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.

For help if you have been compromised, visit cyber.gov.au/report-and-recover

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.

More information

For more tips on how to secure your devices, visit cyber.gov.au/protect-yourself

For more travel advice, search 'cyber security' on smartraveller.gov.au