Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Travelling with mobile devices

First published: November 2010
Last updated: March 2024

Introduction

The targeting of mobile devices used by travelling personnel, especially during overseas travel, is a real and persistent threat. Mobile devices that should be protected include, but are not limited to, corporate and personal laptops, phones, tablets and any associated removable media, such as USB drives and SD cards. The compromise of mobile devices could impact the ongoing operation and security of an organisation's business.

Generally, the risks associated with mobile devices during travel are:

- The compromise of mobile devices or removable media could give malicious actors immediate access to sensitive data. This could impact the integrity, confidentiality or operational security of an organisation's business activities.

- The compromise of mobile devices could allow malicious actors to propagate into any connected networks putting additional sensitive data at risk. This could have a long-lasting impact on the integrity and confidentiality of an organisation's business activities.

- The compromise of mobile devices belonging to personnel of enduring interest, such as an organisation's senior executives, could result in immediate or ongoing operational security or safety concerns for targeted personnel.

Securing mobile devices before travel

The following measures should be implemented before travelling personnel depart:

- If appropriate, issue travelling personnel with newly provisioned accounts, mobile devices and removable media from a pool of dedicated travel devices which are used solely for work-related activities. Further, advise travelling personnel against taking their own personal mobile devices, especially if their devices are rooted or jailbroken.

- If appropriate, apply tamper seals to key areas of mobile devices being taken, such as internal drive bays, removable media slots and other external interfaces. In addition, educate travelling personnel on associated inspection regimes to detect any attempted tampering.

- If appropriate, educate travelling personnel on emergency sanitisation procedures for mobile devices being taken.

- Record details of mobile devices and removable media being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers.

- Ensure mobile devices being taken are running a vendor supported operating system that is fully patched and securely configured and hardened (e.g. by operating in a supervised mode) with all non-essential accounts, functionality and data removed.
- Configure secure lock screen, remote locate and remote wipe capabilities of mobile devices being taken.
- Ensure all mobile devices and removable media being taken are encrypted.

Securing mobile devices during travel

The following measures should be implemented by travelling personnel during their travel:

- Never leave mobile devices, including removable media and multi-factor authentication tokens, unattended. This includes by placing them in check-in luggage or leaving them in hotel safes.
- Never store credentials (e.g. passwords and/or multi-factor authentication tokens) with mobile devices that they grant access to (e.g. in the same laptop bag).
- Never lend mobile devices or removable media to untrusted people, even if briefly.
- Never allow untrusted people to connect their mobile device or removable media to your mobile device (e.g. to charge their phone using your laptop).
- Never connect mobile devices to designated charging stations or wall outlet charging ports.
- Never use gifted or unauthorised peripherals, chargers or removable media with mobile devices. If required, purchase peripherals, chargers or removable media from established and reputable local businesses.
- Never use removable media for data transfers or backups that have not been appropriately checked for malicious code beforehand.
- Avoid reuse of removable media once used with other organisation’s systems or mobile devices.
- Avoid connecting mobile devices to open or untrusted Wi-Fi networks.
- Consider disabling any communication capabilities of mobile devices when not in use (e.g. Wi-Fi, Bluetooth, Near Field Communication and ultra-wideband).
- Consider periodically rebooting mobile devices.
- Consider using an organisation-approved virtual private network service to encrypt all communications.
- Consider using encrypted email or messaging apps for all communications.
- Report any loss, suspected compromised or unusual behaviour (including the type, date and time) for mobile devices, including removable media and multi-factor authentication tokens, to designated security personnel.
- Assume any mobile devices or removable media taken out of sight for inspection by foreign government officials, or that have been lost or stolen and later found or returned, to be potentially compromised.
- In locations where sensitive data is viewed or communicated, take additional care to reduce the chance of the mobile device screens being observed or conversations being overheard.

Securing mobile devices after travel

The following measures should be implemented after travelling personnel return:

- If appropriate, reset credentials used with mobile devices that were taken, including those used for remote access to the organisation's networks.
- If appropriate, monitor accounts for indicators of compromise. In particular, pay close attention to failed logon attempts using credentials that had recently been reset.
- Sanitise and reset mobile devices, including removable media, that were taken.
- Decommission multi-factor authentication tokens that left the physical possession of travelling personnel.
- Report if significant doubt exists as to the integrity of any mobile devices or removable media that were taken.

If at any point following travel significant doubts exist as to the integrity of a mobile device's firmware or hardware, the mobile device should be sanitised, reset and redeployed for purposes that do not pose a risk to either sensitive data or enduring personnel of interest.

The choice to decommission mobile devices for any reason should not be taken lightly given the considerable financial burden this may place on organisations.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Additional platform-specific guidance is also available from the Australian Signals Directorate to assist organisations in the secure configuration and hardening of mobile devices.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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.

Copyright

Use of the Coat of Arms

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate