Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Quick Wins
for your Portable Devices

Mobile technology is an essential part of modern business. While these devices may be small, the cyber threats when transporting them outside of the office are huge. This guide helps small businesses understand what represents a portable device, why it is important to manage their usage and how to keep the data on portable devices secure.

Portable Devices

What?

Mobile, media, storage and other digital devices that you carry around for your work

Portable devices include:

- Portable USB or 'flash' keys
- Smartphones
- Laptops
- Personal digital assistants
- iPods
- e-readers
- External hard drives
- Memory cards
- Tablets
- Notebooks
- MP3 players

Why?

Increased risk of data breaches and attacks

When devices are portable and sharable, it can be hard to manage their contents, understand where they've been and know who has used them.

What could go wrong?

- **Data loss** – when a physical device is lost or damaged and the data cannot be retrieved.
  - **Example:** left at a café, or dropped in water
- **Data exposure** – when confidential data is exposed without consent.
  - **Example:** using an unsecured Bluetooth or WiFi connection
- **Cyber attacks or incidents** – to and from any physically or digitally connected device.
  - **Example:** unknowingly sharing documents via a USB that contains malware

Portable Devices

How?

A unified and multi-layered approach

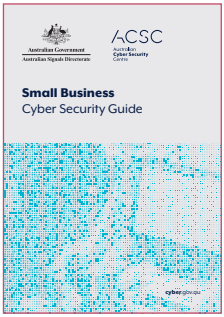
Securing portable devices is ultimately the responsibility of the device owner. However, the following measures reduce the risks associated with using portable devices.

PHONES, TABLETS & LAPTOPS	
Use password protection – pin/fingerprint	Keep devices up to date
Enable remote tracking, locking or wiping	Back up your device to a hard drive or the cloud
Only download legitimate software and apps	Use screen lock
Avoid unknown open Wi-Fi networks	Turn Bluetooth off when it is not in use

HARD DRIVES, USBS & MEMORY CARDS	
Routinely scan devices for malware with an antivirus program	Block access to physical ports
Encrypt data	Use password protection

Always keep a close eye on your device wherever you are and whatever you're doing.

For more detail on cyber security measures to help keep your business safe, refer to the **Small Business Cyber Security Guide** available at **cyber.gov.au**



For more information, or to report a cyber security incident, contact us

cyber.gov.au

call 1300 CYBER1 (1300 292 371)