Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

QUICK WINS
FOR YOUR PORTABLE DEVICES

cyber.gov.au

Portable devices, such as phones, tablets and laptops, are an essential part of modern life. These portable devices are often used for banking, email and shopping – all of which involve sensitive or personal information.
While these portable devices may be small, the cyber threats associated with them are large and should not be underestimated. Secure your portable devices with these three quick wins.

Portable Device Wins

Win #1

Secure your portable device and information

By securing your portable device, you can protect your information and reduce the risk of being targeted by cybercriminals.

How can I secure my portable device?

- **Lock your portable device with a passphrase, password, PIN or biometrics.** Make it difficult to guess – your date of birth and pattern locks are easy for cybercriminals to deduce. Use a passphrase for optimal security. You might also consider using facial recognition or a fingerprint to unlock your portable device.
- **Regularly back up your files.** A backup is a copy of your most important information (e.g. photos, documents) that you have saved to an external storage device or to the cloud. Backing up is a precautionary measure so that your information can be recovered in case it is ever lost, stolen or damaged. Ideally, backups of important information should be kept on at least two other devices.
- **Encrypt your portable device.** Even though your portable device might be protected using a unique strong passphrase, cybercriminals can still access the hard drive and access your information if it's not encrypted.
- Ensure your portable device is set to **automatically lock after a short time of inactivity**, such as 5 minutes.
- If you find a random cord or USB device – **don't plug it into your portable device.** It could be infected with malware. Do not allow other people to plug their cables or devices into your portable device.
- **Treat your portable device like your wallet.** Keep it safe or with you at all times.
- Ensure you **thoroughly remove sensitive and personal information** from your portable devices before selling or disposing of them.

If possible, ensure the encryption method used on your laptop includes pre-boot authentication, which will ask for an additional password before you log on. This will keep your files encrypted even if a cybercriminal tries to bypass your device's security.

Win #2

Use secure software

Using secure software on your portable device is one of the best ways to protect yourself from being targeted by cybercriminals, as software can be malicious by design, or may contain unintentional security vulnerabilities or gaps in security that allow cybercriminals to compromise your portable device and information.

How do I ensure my software is secure?

- **Turn on automatic updates for your device and its software** to install new updates as soon as they are available. Updates help to correct security vulnerabilities that could be used by cybercriminals to access your portable device or information. If the automatic update setting is unavailable, you should regularly check for and install updates manually.
- **Check that software is made by a reputable company** before downloading and installing on your portable device.
- Always **download software from an official app store or the company's official website (if you are using a computer)**. If you access software through other means, such as pirating, this could put your portable device at risk. For example, the software may not receive security updates or it could install malware on your portable device as well.
- **Avoid software** that asks for excessive or suspicious permissions.
- Set your portable device to **require approval before software is installed.** Parental controls can also be used for this purpose.

Please note

If your hardware or software is too old it may no longer be supported and could be unable to receive updates. In these situations, the ACSC recommends upgrading your device or software to a newer version as soon as possible to stay secure.

Win #3

Wireless security

Your internet connection is a way for you to interact with the outside world, but it also provides a channel into your portable device. If your wireless connection isn't secure, someone may use it to access your personal or financial information for malicious purposes.

How can I protect myself when using Wi-Fi networks?

Public Wi-Fi 'hotspots' like cafes, airports, hotels and libraries are convenient, but they can be risky. It's easy for information sent using public Wi-Fi to be intercepted, so you need to be careful about what information you send or receive while connected. Ideally, **use cellular data** when not connected to your secure home or office Wi-Fi network. However, if you have no choice but to use public Wi-Fi, follow these suggestions to stay secure:

- **Avoid sending or receiving sensitive and personal information** while connected to public Wi-Fi networks.
- When online banking, shopping, sending emails, entering passphrases/passwords or credit card details into websites, **switch to your cellular data connection** or wait until you're on a secure home or office Wi-Fi network.
- **Always try to confirm the 'official' hotspot name** from venue staff and manually connect your device to it.
- **Do not let your device automatically connect to public Wi-Fi networks** by disabling the option in your device's Wi-Fi settings.
- **Remember to disconnect from the Wi-Fi network** and clear it from your portable device after you have finished using it.

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

ACSC Australian Cyber Security Centre