Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

SECURE YOUR MOBILE PHONE

cyber.gov.au

Secure your mobile phone

For more cyber security advice

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

Personal Cyber Security Series

Table of Contents

Protect your phone or tablet from cybercriminals.

If your phone is lost or compromised, your information could be at risk. Protecting your mobile phone is just as important as protecting your computer or your wallet. If someone gets access to your phone, they could also get easy access to:

- your email and social media accounts
- your messages and contacts
- your photos, videos and notes
- your banking or financial details
- any apps you use and the data you store in them
- your browser history.

Follow these steps to secure your phone and protect your information. Most of these steps are free and easy to do, and can also be used to secure your tablet.

Keep your phone locked and physically secure

- **Lock your phone with a passphrase, password, PIN or biometrics.** Make it difficult to guess – simple patterns or your date of birth are too easy. You should consider using facial recognition or a fingerprint to unlock your device if it has this option. This way, people can't watch what you use for your password or PIN.
- Ensure your phone is set to **automatically lock after a short time of inactivity**, such as five minutes. The shorter the better.
- **Treat your phone like your wallet**. Keep it safe or with you at all times.
- **Encrypt the data on your phone**. Even though your phone might be locked, someone could still access your phone's onboard data storage and your information if it is not encrypted. Recent versions of Apple iOS or Google Android now also have encryption options available. Encryption of some form has been included in mobile devices from iOS 3.0 and Android 4.0, and most devices will now ship with encryption turned on by default. This uses your normal PIN or screen lock passphrase/ password to protect your data.
- **Use your phone's remote tracking features** (such as Apple's Find my iPhone or Google's Find your phone) to help find your phone or remotely erase the contents if it is lost or stolen.

Regularly back up your phone

Backing up the data on your phone is important and should be done regularly. This will help you recover your data if your phone is ever lost, stolen or damaged. Backups of important information should be kept on at least two other devices. For more information, read our advice for backups available at cyber.gov.au/backups.

Update your phone's software

Turn on automatic updates for your phone's operating system and apps to install new updates as soon as they are available. This is often done through your phone's settings menu. Updates help to correct security vulnerabilities that could be used by cybercriminals to access your phone or information. Your phone may need to be connected to Wi-Fi and a charger to install the updates. If you need help, the ACSC has published guidance on how to update your phone, available at cyber.gov.au/updates.

If your phone or operating system is too old it may no longer receive updates. This could put your device and information at risk. Upgrade to a newer phone or operating system as soon as possible to stay secure. Examples of phones that no longer receive updates include the **iPhone 7** and **Google Pixel 2**.

Use secure and reputable apps

- **Check that apps are made by a reputable company** before downloading and installing on your phone. Only download apps from an official app store.
- Review the permissions and settings on your apps and **remove apps that asks for excessive or suspicious permissions**. For example, apps that request access to your photos or microphone where it is not required. App permissions can be viewed in your settings menu.
- Set your phone to **require approval before apps are installed**. Parental controls can also be used for this purpose.
- **Remove apps when you no longer need them.**

Be careful using free or public Wi-Fi

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 should be careful about what information you send or receive while connected.

- Where possible, **use cellular data** when not connected to your own Wi-Fi network.
- **Do not let your device automatically connect to public Wi-Fi networks**. You can turn this off in your phone's Wi-Fi settings.
- If you have to use a public Wi-Fi network, **know that the information you send or receive while connected may not be private**. This can include sensitive emails or messages, as well as passwords, credit card details, and online banking information. Attackers could also intercept your connection and send you to malicious webpages.
- To keep your information and device secure, **consider using a VPN** on your phone when using public Wi-Fi. Otherwise, use your cellular data connection or wait until you're on a trusted Wi-Fi network.
- **Always try to confirm the official hotspot name** from venue staff before connecting to it.
- **Remember to disconnect from any public Wi-Fi networks** and clear them from your phone after you have finished using them.

Watch out for scams and phishing attempts

Look out for suspicious calls, emails and messages. These could be attempts to steal your money or access your device and information. Scams might pressure you to take urgent action or claim that there's a problem with your device or account. For more information or to test your ability to spot scams, read our advice on recognising and reporting scams at cyber.gov.au/learn/scams.

Stay vigilant of emails and messages that ask you to open a link or attachment.

If you're unsure whether a call, email or message is real, **contact the person or business through another method**. For example, if you receive a suspicious message about a parcel delivery, contact the courier through their official website or call centre. Do not use the links or contact details you have been provided in the message as these could be fraudulent.

Reset your phone before selling it

Make sure you **remove all personal information from your phone** before selling or giving it away. For example, by doing a factory reset. This will wipe your information and restore the device to its original settings.

For more advice, read the ACSC's guide on how to dispose of your device securely, available at cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/how-dispose-your-device-securely.

Protect your phone in public spaces

If you find or receive a random cord or USB device – **don't plug it into your phone**. It could be infected with malware.

Turn off Bluetooth and Wi-Fi when you are not using them.

Be cautious with QR codes. Cybercriminals can generate codes that cause your phone to visit a harmful website, install a malicious app or join an untrustworthy Wi-Fi network. Only scan QR codes located in prominent positions in a business as these are more likely to be legitimate. Check with a staff member if you are unsure. While scanning a QR code, look for prompts on your smartphone indicating actions that the QR code will perform.

If you're going overseas, **visit the Smartraveller website** at smartraveller.gov.au for advice on keeping your electronic devices secure when travelling.

Review your phone's security features

Most phone companies provide simple security guidance on their website. For example, Apple's security and privacy advice for iPhones and Google's security tips for Android devices. **Read through this security guidance** every few months, or when you get a new device, to make sure you're protected.

Case study

Marie from WA once lost her mobile phone, which was unlocked and not protected by a PIN or password. **Marie kept all of her account passwords in a notes app on her phone, giving the thief easy access to her online accounts**. She also had photos on her phone of her driver's licence.

While the phone was returned a few hours later, Marie did not realise until the next day that the thief had transferred all of her money to a cryptocurrency website, losing close to $4000.

Protect your phone with a PIN, password or biometrics. Make sure your phone automatically locks when you are not using it. You should not store account passwords, PINs, or identity documents on your phone without additional protection. For example, store them in a password manager that requires a password or facial recognition to grant access.

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

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

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