Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL CYBER SECURITY

ADVANCED STEPS

cyber.gov.au

Personal Cyber Security Series

Personal Cyber Security Series

The ***Personal Cyber Security: Advanced Steps*** guide is the final guide in a series of three designed to help everyday Australians further understand the basics of cyber security, and how you can take action to protect yourself from ever-evolving cyber threats.

You can access the other two guides on **cyber.gov.au**

First Steps

Next Steps

Advanced Steps

Table of Contents

Introduction

BEFORE YOU BEGIN: it is assumed that you have read and completed all steps in the *Personal Cyber Security: First Steps* and *Next Steps* guides before starting this guide.

If you haven't yet, you can access our *Personal Cyber Security: First Steps* and *Next Steps* guides on **cyber.gov.au**.

How can this guide help protect me from cyber threats?

The *Personal Cyber Security: Advanced Steps* is the final guide in a series of three designed to help everyday Australians further understand the basics of cyber security, and how you can take action to protect yourself from ever-evolving cyber threats.

This guide builds upon the steps you've taken and the cyber secure thinking you learned in the *First Steps* and *Next Steps* guides, and provides additional actionable steps and thinking to improve your cyber security to help protect you from cyber threats.

The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia. The ACSC is here to help make Australia the most secure place to connect online.

For more cyber security information, guides and advice visit the ACSC's website cyber.gov.au.

If you think you're a victim of cybercrime report it through ACSC's ReportCyber on cyber.gov.au or call our Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Keep up to date on the latest cyber threats: Sign up to the ACSC's free alert service online at cyber.gov.au.

Level Up Your Cyber Security

Use The Most Effective Multi-Factor Authentication (MFA) Methods

Before you begin: you should read the ACSC's *Personal Cyber Security: First Steps* and *Next Steps* guides and activate multi-factor authentication (MFA) on all of your accounts that offer it.

How can I increase my MFA security?

While all forms of MFA provide significant advantages over single-factor authentication (e.g. only a pass-phrase, password or PIN), some methods are more effective.

MFA is most effective when the method you use is 'something you physically have', such as security keys. You may use smartcards as MFA at work, another highly effective MFA method.

Physical tokens and authenticator apps that generate a one-time PIN or code are also effective MFA methods. Ensure you never share these codes with anyone, and beware of scam messages (phishing) that attempt to trick you into sharing these codes.

How can I implement the more effective MFA methods on my accounts?

If your account uses less effective MFA methods, such as email or SMS, you should change to a more effective method such as a security key, physical token, or authenticator app. When creating new accounts, activate the most effective MFA methods.

Tip: Prioritise changing to more effective methods of MFA on your most important accounts first. These include banking, email, social media, and accounts with access to financial or personal information.

WHAT ARE THE MOST EFFECTIVE MFA METHODS FOR HOME USERS?

Securitykeys	A small physical security key which may use a physical button, Bluetooth, Near Field Communication (NFC) and/or USB to authenticate the user.
Physical token	A small physical device that generates a one-time PIN (usually six digits) only usable for a short period of time.
Authenticator app	An app on your smartphone or tablet that generates a one-time PIN only usable for a short period of time.

If you would like more detailed information on MFA, visit cyber.gov.au/mfa.

Secure Your Accounts Using A Password Manager

Before you begin: you should read the ACSC's *Personal Cyber Security: First Steps* and *Next Steps* guides and secure all of your accounts that aren't protected with MFA using unique strong passphrases.

What is a password manager?

As detailed in the *Personal Cyber Security: Next Steps* guide, a password manager is a tool which helps you securely store and manage strong passwords and passphrases. Its two main functions are the secure storage of your existing passphrases, and assistance with generating new secure (randomly generated) passwords. Password managers are available on computers and mobile devices. Ensure that any password manager you use comes from a trusted and reputable source.

What steps can I take to secure all my accounts using a password manager?

1. **Activate MFA for your password manager to add an additional layer of security.**

   Using MFA for your password manager means that even if a cybercriminal gains access to its master password, they wouldn't be able to access the data without access to the accompanying MFA code or token.

2. **Ensure that your password managers' master password is your strongest password.**

   Use a unique strong passphrase as your master password.

3. **Generate long and secure passwords using your password manager.**

   Use your password manager to generate strong and long randomised passwords to further secure your accounts. Password managers can quickly generate passwords tailored to your criteria (e.g. you could create 50 character passwords with upper and lowercase letters, numbers, and special characters for every account).

4. **Add accounts to your password manager.**

   Every time you login to an existing account that is not in your password manager, change the password into a strong randomly generated password and store it using your password manager.

5. **Use your password manager to fill in the password fields when logging in for you.**

   For ease of use, password managers typically have browser extensions (always check for authenticity before installing these) to auto-fill login pages with your saved username and password, and the option to copy-paste your credentials into login fields. This can be used to streamline logging into accounts with long secure passwords (e.g. a randomly generated 50-character complex password).

Improve Your Wi-Fi Router Security

What is a Wi-Fi router?

A home Wi-Fi router is a small electronic box that typically combines router and modem functions to create an internet-connected network for the devices in your home.

Here we refer to the device simply as a router.

How can I improve my router security?

1. **Change your router's default username and password**

   Use the information contained in your router's user manual to access your router settings. If you can't find the user manual a quick internet search of your router model should typically provide you with access to a copy. Some routers have a sticker on the device that also provides your router's IP address and default login details.

   a) **Open a web browser and type into the address bar your router's IP address.** Your router's IP address will typically start with "192.168.#.#" or "10.0.#.#" (where # represents different numbers), check your user manual for the exact IP address.

   b) **Enter the router's username and password when prompted.** In your user manual you should also be able to find the default username and password which you will need when logging in to your router.

   c) **Change the password on your device** using the router settings to a unique strong passphrase.

   d) **Where possible, also change the default administrator username** (typically 'admin' or 'administrator') to something hard to guess.

Your router's default administrator username and password may be publicly available online, making it easy for cybercriminals to access if you don't change its default username and password.

2. Change your default Wi-Fi name and password

- **Change your Wi-Fi name** (also known as SSID) from the default set by the router manufacturer to something that doesn't contain identifiable information. You can do this in the router's settings menu.
- **Ensure your Wi-Fi password** provided by your internet service provider or router manufacturer is long and hard to guess. If not, change it to a unique strong passphrase.

In many cases a cybercriminal can use your router's default Wi-Fi network name to easily determine the make and model of the router you are using and use this information to gain access to your router.

Also, if your Wi-Fi password is weak it can be trivial for cybercriminals to break. For more information on creating strong passwords, visit cyber.gov.au/passphrases.

3. Use the strongest Wi-Fi encryption

- **You should change your Wi-Fi encryption** protocol used by your router to WPA3 or WPA2 (if WPA3 isn't supported) in the settings menu.

It is possible for anyone within range of your router to intercept your internet activities if your Wi-Fi is unencrypted or using an outdated encryption protocol.

You should use the strongest encryption protocol provided by your router, which is currently WPA3 (introduced in 2018) or WPA2 (if your router or devices don't support WPA3). If your router does not support WPA2 (as a minimum), you should consider replacing it.

4. Update your router to use the latest firmware

Firmware is the software on your router that determines the functions it can perform. Just like new software updates for your computer, new firmware for your router will provide improved features and security.

- **To find out which version of firmware is installed** on your router log in to the device and check its settings.
- **Then go to the manufacturer's website,** it will tell you if there's a more recent version of firmware for your device and allow you to download it.
- **Install the updated firmware.** Be careful when you do this because a failed update can render your device unusable and disconnect all your devices from the internet. Make sure you follow the instructions in your device's manual and select the correct firmware upgrade version for your model of router.
- **If you don't feel confident to updating your router firmware,** you could contact a reputable computer technician for assistance. You could also think about replacing your router.

5. Disable remote management and Universal Plug and Play (UPnP)

- **Ensure both remote management and Universal Plug and Play (UPnP) are disabled** in your router's settings.

Remote management on your modem or router can allow you to make changes to your internet connection, including passwords, by logging into your device via the internet.

UPnP allows devices on your network to automatically discover and communicate with each other using your Wi-Fi network at home or from another location using remote access, without needing authentication.

Disabling remote management and UPnP can increase your security from remote attackers.

Please note, PC and console games with online functionality may report network errors if UPnP is disabled. If this occurs, set up manual port forwarding in your router's settings.

6. Enable Guest Wi-Fi

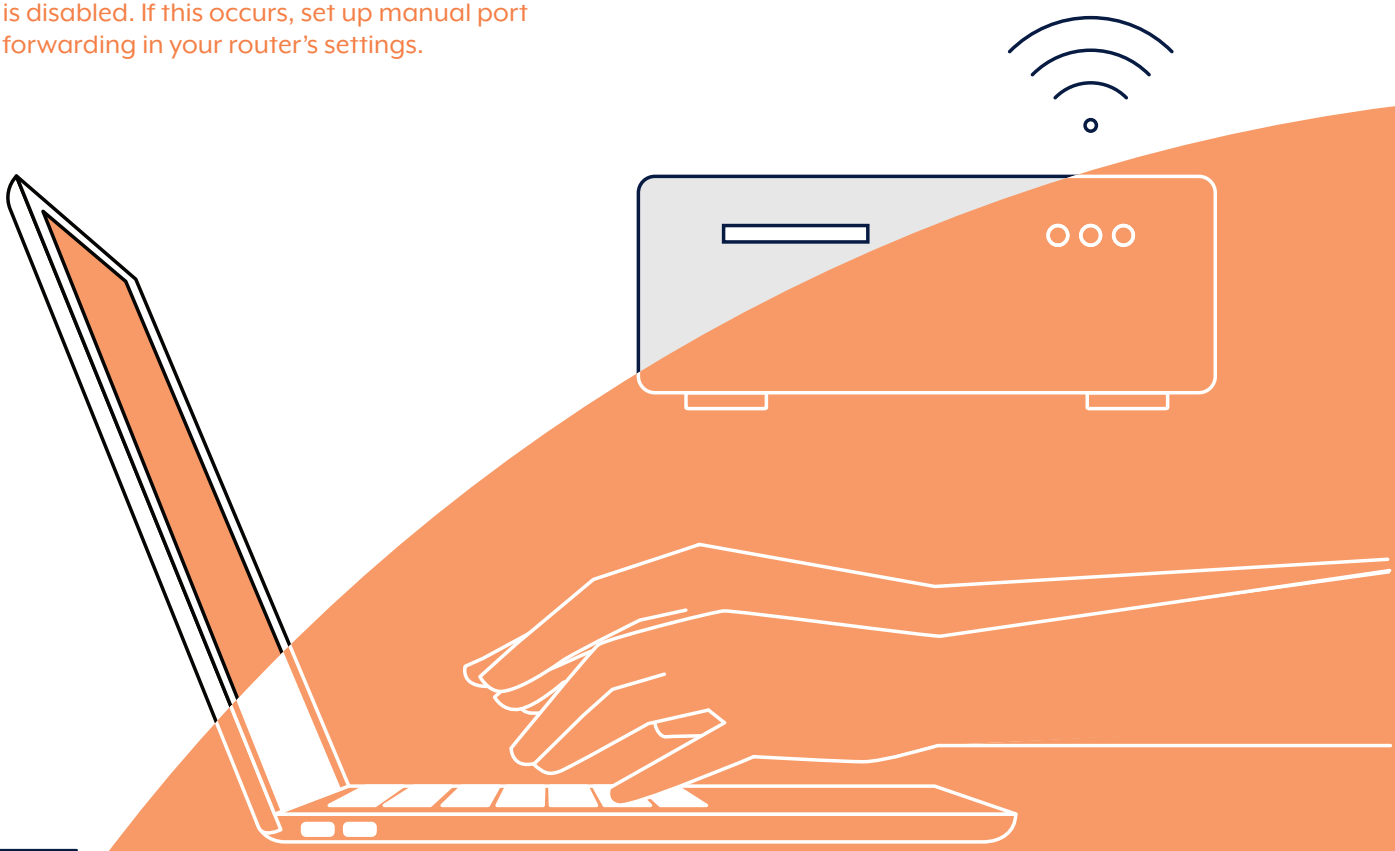
- **Consider enabling the 'Guest' Wi-Fi feature** in your router's settings.

Visitors can use Guest Wi-Fi for internet access in your home, but won't have your Wi-Fi passphrase/password or access to your main Wi-Fi network.

Should I upgrade my old router?

Manufacturers often classify old devices as 'legacy' models and no longer develop firmware upgrades for them, which can leave you exposed to known security vulnerabilities.

Upgrading to a current router model will offer you significant benefits such as additional features and configuration options, the latest encryption, and faster data transfer speeds.



Secure Your Internet Of Things (IoT) Devices

What is an Internet of Things (IoT) device?

An IoT device is an everyday item that has had internet connectivity added to it. Examples of IoT devices include smart fridges, smart televisions, baby monitors and security cameras. IoT devices within homes and businesses generally use Wi-Fi or cellular networks to connect to the internet.

Why do I need to secure my IoT devices?

Many IoT devices commonly found in Australian homes and businesses have not been designed with security in mind. If your IoT devices have known unpatched security vulnerabilities, it can allow cybercriminals to access your device, network and personal data for malicious purposes.

What can I do before purchasing an IoT device?

You should research IoT devices before making a purchase, as manufacturers provide varying levels of security. Things to consider include:

1. **Is the device made by a well-known reputable company and sold by a well-known reputable store?** Well-known reputable companies are more likely to produce devices with security in mind. Well-known reputable stores are more likely to have a stricter supply chain, ensuring the device gets to you as intended by the manufacturer.
2. **Is it possible to change the password?** If the device is shipped with a weak default password, it is important you are able to change it. Weak default passwords are an easy way for cybercriminals to attack a device.
3. **Does the manufacturer provide updates?** It is important that companies offer updates to fix security vulnerabilities as they are discovered.
4. **What data will the device collect and who will the data be shared with?** This information should be readily available on the manufacturer's website or in their privacy policy. Also consider the information that is collected by the IoT device's online or mobile app.
5. **Does the device do only what you want it to do?** Extra IoT device capabilities that you don't need or won't use (such as connecting to the internet) can increase the device's vulnerability to attacks and reduce your security.

How should I set up an IoT device?

Keep in mind a few simple questions while setting up your device, to help you keep your network and data more secure.

1. **Does the device need to be connected to the internet?** If you're not going to use the device's features that require internet connectivity, then you should consider whether it needs to be connected. Devices that are not connected to the internet are much less likely to be compromised.
2. **Is the device in a secure location?** Installing your device in a secure location can reduce the risk of physical compromise.
3. **Do I change the default username and password?** If your device is not equipped with a unique strong passphrase or password, then you need to change it. Default usernames and passwords are collected and posted online, leaving your device vulnerable to cybercriminals.
4. **Is my Wi-Fi network set up securely, and does it have a secure password?** Secure your Wi-Fi network and router (see page 4) to make it harder for attackers to access your device and network.

5. **Add device to your Guest Wi-Fi network.** Consider enabling Guest Wi-Fi on your router (see page 6) and add your device to that network to isolate it from the devices on your main network. Keep in mind that some IoT devices require your mobile devices to also be connected to the same network to communicate.
6. **Are unnecessary features turned off?** If your device has unwanted or unnecessary features (such as cameras or microphones), these should be disabled where possible.

How can I maintain my IoT devices?

There are some important things to remember once your IoT device is set up and in use. These include:

1. **Reboot your devices regularly.** If the IoT device starts to become slow or inoperable, it may mean that malware is present. Some malware is stored in memory and can be easily removed by a device reboot. If the device continues to be slow or inoperable after a reboot, try a factory reset.
2. **Apply regular updates.** Some devices apply updates automatically. For those that don't, regularly check with the manufacturer and apply updates when they become available. When updates are no longer available for your device, consider upgrading to a newer device as soon as possible to reduce security risks to your network.
3. **Turn off your device when it is not in use.** Leaving unused and unmonitored devices powered on and connected to your network for extended periods can increase the likelihood of your devices being attacked.
4. **Watch for a significant increase in your monthly internet usage or bill.** Significant increases can indicate that your device has been compromised with malware. Performing a factory reset or changing the passphrase/password on your IoT device may remove the malware.

How can I dispose of an IoT device?

Disposing of a device (by discarding or selling it) may give other people easy access to your personal information or data. Ways to prevent this include:

1. **Erase all data and personal information.** Erasing your personal information ensures that no one gains access to it after you have disposed of the device. The manufacturer should provide a method for how to erase your data and personal information from both the device and associated applications.
2. **Perform a factory reset of the device.** A factory reset is designed to erase data kept in local storage and reset passphrases/passwords, usernames and settings back to default. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.
3. **Disassociate the device from mobile phones and other devices.** Make sure you check your other devices and remove any pairing with the device you are disposing of. Remove any permissions granted to the mobile applications that are no longer needed.
4. **Remove any removable media (e.g. USB flash drives, memory cards etc.) attached to the device.** Removable media may contain personal data that is not deleted in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.

Encrypt Your Computer's Hard Drive

Why should I encrypt my computer's hard drive?

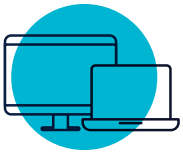
Performing a full-disk encryption means the entire contents of your computer's hard drive are encrypted, and can only be accessed with a passphrase or password. Even though your device itself might be password protected using a unique strong passphrase, cybercriminals can still access the hard drive and steal your data if it is not encrypted.

How can I encrypt my computer's hard drive?

You should take care when encrypting your hard drive – if you lose access to the encryption or recovery keys, you will not be able to use the device and will have to wipe everything and start again.

- Check whether disk encryption is enabled on your devices, and turn it on if it is not. Most modern operating systems have some form of disk encryption built in.

Desktop or Laptop Computers



- On Apple macOS, disk encryption is known as FileVault, and can be enabled in the Security & Privacy section of the System Preferences. When enabled, your login passphrase/password is used to encrypt the hard drive, and any new files that are created are automatically encrypted as they are saved to your disk.

- On Microsoft Windows 10 disk encryption is less straightforward. There is an included encryption tool called BitLocker that is available to users with all versions except Windows 10 Home. Windows 10 Home has a built-in Device Encryption tool, but it is only available to devices that meet certain hardware specifications. Microsoft's website contains information about both of these tools and how they can be configured.

If your device does not meet the hardware requirements, there are free and open source third party tools available that will allow you to enjoy the same level of protection as the built-in methods.

Mobile devices

- 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.

Enhance Your Cyber Secure Thinking

Take Control Of Your Mailboxes:

Don't let your mail accumulate in both your home and email mailboxes. This prevents cybercriminals stealing your emails and physical mail and using it for socially engineered scams or accessing your accounts.

- **Periodically clean out your email inbox** of sensitive personal information and documents (such as copies of IDs, loan and job application documentation). This prevents cybercriminals from stealing this sensitive information if your email account is ever compromised. To do this:

  1. **Archive your emails** in a passphrase protected zip-file (and create a backup),

  2. **Delete the emails from your account** (and the deleted items/trash folders).

- **Don't let your mail accumulate** in your mailbox at home.

- **Destroy mail or documents** containing personal information and account details before disposal (e.g. bank statements, bills, and address labels).

Learn More About Cyber Security:

Staying cyber secure will always be an ongoing learning process as cybercriminals are innovative in their attacks and scams.

- **Get alerts on new threats:** Sign up to our free alert service online at **cyber.gov.au**. This service will send you an alert when we identify a new cyber threat. It will also help you through what to do if an attack happens and how to report new incidents.

- **Talk about cyber security.** Share these messages with your family and friends and encourage them to visit our website **cyber.gov.au**.

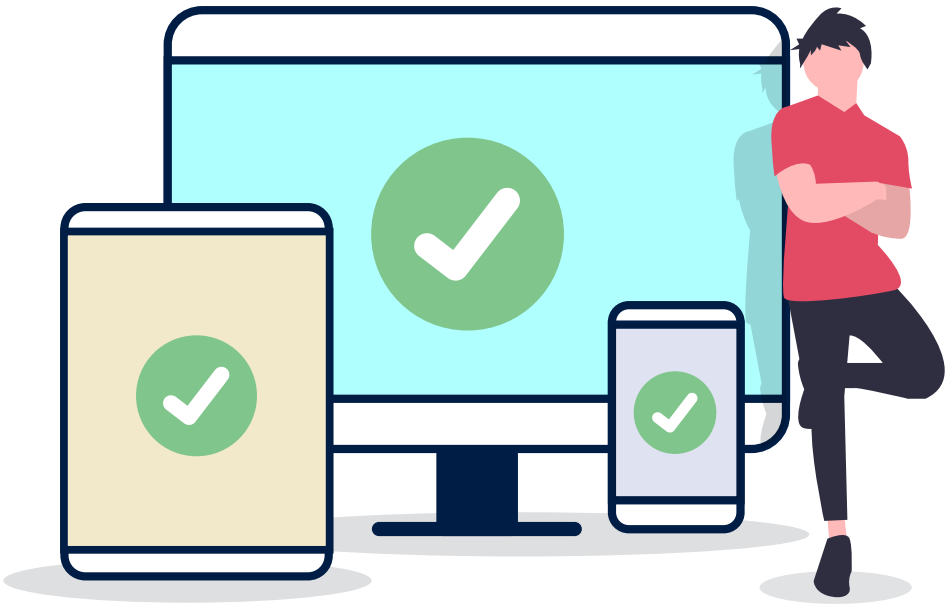
- **Report cyber security incidents** to keep Australia secure. You can report a cybercrime incident using the ACSC's ReportCyber tool on **cyber.gov.au**.

Summary Checklist

Have you completed everything in this guide?

Use this handy checklist to track your progress:

- **I have implemented the most effective MFA methods on all my accounts**
- **I have secured my accounts using a password manager**
- **I have improved my Wi-Fi router security by**:
  - Changing my router's default username and password
  - Changing my default Wi-Fi username and password
  - Changing to the strongest Wi-Fi encryption (WPA3 or WPA2)
  - Updating my router's firmware
  - Disabling remote management and UPnP on my router
  - Enabling Guest Wi-Fi
- **I ensure I secure my IoT devices:**
  - Before purchasing an IoT device
  - When setting up an IoT device
  - When maintaining an IoT device
  - When disposing of an IoT device
- **I have encrypted my computer's hard drive**
- **I have extended my cyber secure thinking by ensuring I am:**
  - Taking control of my mailboxes
  - Continuing to learn more about cyber security



Glossary

Authenticator app
An app used to confirm the identity of a computer user to allow access and control used within multi-factor authentication.

Browser extensions
An internet browser add-on (e.g. Google Chrome, Firefox) that provides additional features, functionality, or appearances.

Cellular network
The internet connection provided by a SIM card, such as 4G or 5G.

Encryption
The process of making data unreadable by others for the purpose of preventing others from gaining access to its contents.

Internet of Things (IoT)
The network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to connect to the internet and collect and exchange data.

IP address
Short for Internet Protocol. A code made up of a string of numbers that identifies a particular computer on the internet. Every computer requires an IP address to connect to the internet.

Near Field Communication (NFC)
Short-range, wireless communication between two compatible devices, allowing them to share data. Examples include Apple Pay and Google Pay.

Network
A collection of computers, servers, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

Software
Commonly referred to as programs, collection of instructions that enable the user to interact with a computer, its hardware or perform tasks.

Universal Plug and Play (UPnP)
Allows devices on a network to automatically find and communicate with each other.

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