Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL CYBER SECURITY

NEXT STEPS

cyber.gov.au

Personal Cyber Security Series

The ***Personal Cyber Security: Next Steps*** guide is the second in a series of three guides 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* guide before starting this guide.

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

How can this guide help protect me from cyber threats?

The *Personal Cyber Security: Next Steps* guide is the second in a series of three guides 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* guide, and provides the next level of actionable steps and thinking to increase 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

Activate Multi-Factor Authentication (MFA) To Protect Your Accounts

Before you begin: you should read the ACSC's *Personal Cyber Security: First Steps* guide and activate multi-factor authentication (MFA) on your most important accounts (online banking and email).

Why should I activate MFA on all of my accounts?

Using MFA on your accounts makes them much harder for cybercriminals to access.

Cybercriminals might manage to steal one authentication type (such as your password), but they still need to obtain and use the other MFA method/s to successfully access your account, requiring extra time, effort and resources.

HOW CAN I ACTIVATE MFA ON ALL OF MY ACCOUNTS?

Tip: If you have a lot of accounts to secure, prioritise the following:

- Accounts that save or use your payment details (e.g. eBay, Amazon, PayPal)
- All social media accounts (e.g. Facebook, Twitter, WhatsApp)
- Any other accounts that hold personal information (e.g. myGov, Apple ID, iCloud, Uber)

The steps for activating two-factor authentication (2FA), the most common form of MFA, are different depending on the account.

For more information on how to turn on MFA for your accounts, visit cyber.gov.au/mfa

Use Passphrases To Secure Your Accounts

Before you begin: you should activate MFA on all of your accounts that support it (see page 2 for more information).

Why should I secure my accounts with unique and strong passphrases?

A passphrase is a more secure form of password. Passphrases use four or more random words as your password, and are most effective when they are long, unpredictable and unique.

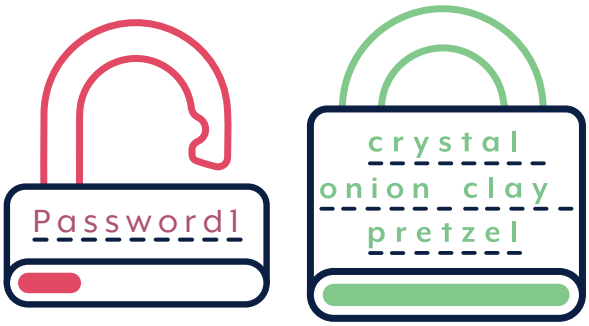
If your account does not support MFA use a unique strong passphrase as your password to protect your account.

REMEMBER: NEVER REUSE A PASSPHRASE OR PASSWORD ACROSS MULTIPLE ACCOUNTS

HOW CAN I PROTECT MY ACCOUNTS WITH UNIQUE AND STRONG PASSPHRASES?

Tip: If you have a lot of accounts to secure, prioritise the following:

- Accounts that save or use your payment details
- User accounts on your personal devices
- Social media accounts
- Any other accounts that hold personal information
- Accounts who have had their details leaked online (see the following steps)



How can I check if my account details have been leaked online?

To check if any of your account usernames and passwords have been leaked online by cybercriminals, take the following steps:

1. **Visit the *Have I Been Pwned* website** to see if account details tied to your email address/es have been leaked online in a data breach for anyone to see.

2. **If this search returns any results, immediately change your password or passphrase for those accounts** and enable MFA if possible.

3. **Make sure you haven't used the breached password or passphrase on any other accounts, if you have,** change these too and enable MFA if possible.

Ensuring your accounts have unique passphrases is vital, as reusing a passphrase allows cyber-criminals to easily take control of all of your accounts that use the same passphrase if it is leaked online.

For more advice on creating passphrases, visit cyber.gov.au/passphrases.

Use A Password Manager To Remember Your Passphrases

How can I remember the unique passphrases I've set for my accounts?

Having trouble remembering each unique passphrase you use to secure your accounts? Many people use a password manager which can securely store your passphrases.

You may choose to keep track of your passphrases in a notebook rather than a password manager. No matter how you keep track of your passphrases, ensure you have a secure storage method.

How can I use a password manager to store my passphrases?

- Ensure that any password manager you use comes from a trusted and reputable source.
- Activate multi-factor authentication (MFA) on your password manager to best protect your stored passphrases.
- If MFA is not available, ensure that your password manager's 'master password' is your strongest password. Consider using a unique strong passphrase. Keep your 'master password' well-protected, and don't re-use it on any other account.

Tip: Every time you login to an account, add your login details (username and passphrase) to your password manager and, if needed, change any old insecure passwords into unique strong passphrases.

For more advice on passphrases and password managers, visit cyber.gov.au/passphrases

Improve Your Wi-Fi Security Habits

How can I improve my Wi-Fi security on mobile devices?

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

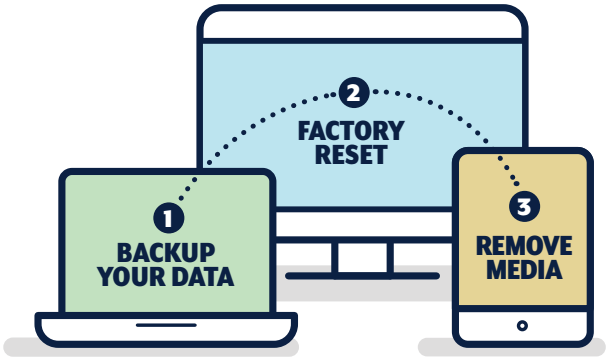
- **Disable Bluetooth and Wi-Fi when not in use**, especially if you're in a public place
- **Use cellular data** when not connected to your secure home network

How can I protect myself when using 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 need to be careful about what information you send or receive while connected.

WHEN USING PUBLIC WI-FI, FOLLOW THESE SUGGESTIONS TO STAY SECURE:

- Avoid sending or receiving sensitive information while connected to public Wi-Fi networks.
- When online banking or shopping, sending confidential emails, or 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 connection.
- 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 this option in your device's Wi-Fi settings.
- Remember to disconnect from the Wi-Fi network and clear it from your device after you have finished using it.



"Disposing of a device without taking steps to remove your data may give other people easy access to your personal information and data."

Securely Dispose Of Your Devices

Why should I take steps to securely dispose of a device?

Disposing of a device (by discarding, recycling, selling or giving it away) without taking steps to remove your data may give other people easy access to your personal information and data.

How can I securely dispose of a device?

Before disposing of your computer, phone, tablet, games console or any other smart device, you should:

1. **Create a backup of your data from the device.** Make sure you have made a backup of any important files and have transferred these to another secure device.

2. **Perform a factory reset of the device and erase all data and information.** A factory reset is designed to erase data kept in local storage and reset usernames, passwords and settings back to default. Erasing your personal information ensures that no-one gains access to it after you have disposed of the device. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.

3. **Remove any removable media (e.g. SIM cards, SD cards, USB flash drives) 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.

Protect Yourself Against Malware

What is malware?

Malware is a blanket term for malicious software designed to cause harm, such as ransomware, viruses, spyware and trojans.

MALWARE CAN:

- **Steal your bank or credit card numbers**
- **Steal your usernames and passwords**
- **Take control of or spy on your computer**

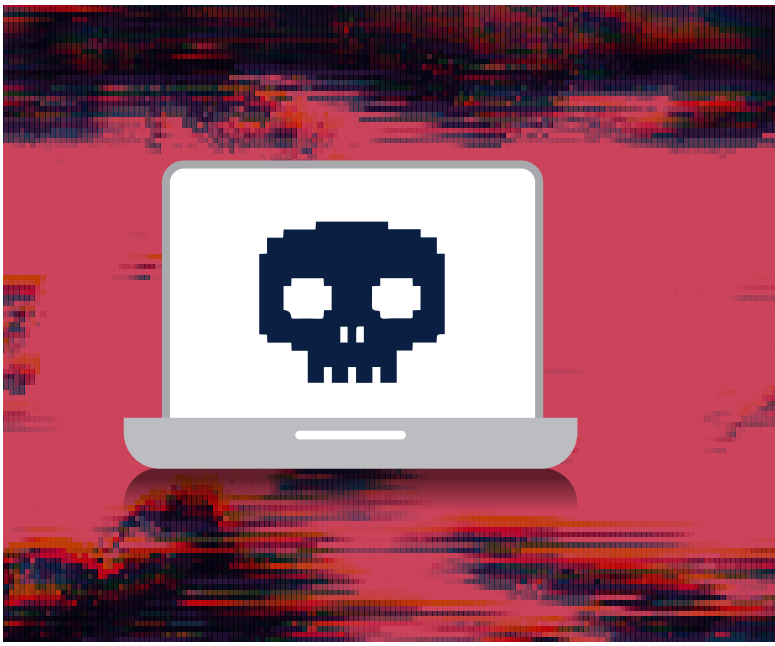
THE STEPS YOU CAN TAKE TO PROTECT YOUR DEVICES FROM MALWARE INCLUDE:

- **Enable automatic updates for your devices (see page 2 of the *Personal Cyber Security: First Steps* guide).**
- **Be vigilant online: be wary of opening links, emails or files from unknown sources.**
- **Activate real time protection on your Windows 10 devices.**

How do I turn on real time protection to stop malware?

Real time protection is a security feature that helps stop malware from being installed on your device.

This feature is built into Microsoft Defender, a comprehensive antimalware and threat detection program that is part of the Windows 10 security system.



Why do I need real time protection?

Prevention is better than a cure. Unlike an antimalware scan, which searches for malicious files or programs that are already on your device, real time protection will detect and stop malware before it gets to your device.

How do I activate real time protection?

Real time protection should automatically turn itself on. However, it can be temporarily switched off, so it is important to check that the feature is up and running and is actively protecting your device.

- For more information on how to activate real time protection, refer to ACSC's anti-virus guide at cyber.gov.au/acsc/view-all-content/advice/anti-virus-software.
- If you are using a different anti-malware software, ensure that it is actively protecting you against malware.

Turn On Ransomware Protection

What is ransomware?

Ransomware is a type of malware that locks down your computer or files until a ransom is paid.

The ACSC recommends you do not pay the ransom, as there is no guarantee you will regain access to your information. You may also be targeted by another attack.

Ransomware works by locking up or encrypting your files so that you can no longer use or access them. Sometimes it can even stop your devices from working. Ransoms are typically paid using an online digital currency or cryptocurrency such as Bitcoin, which is very difficult to trace.

RANSOMWARE CAN INFECT YOUR DEVICES IN THE SAME WAY AS OTHER MALWARE, INCLUDING:

- **Visiting unsafe or suspicious websites**
- **Opening links, emails or files from unknown sources**
- **Having poor security on your network or devices**

How can I protect myself from ransomware?

Ransomware protection has the ability to prevent many types of ransomware attacks from happening. In the unfortunate event of an attack, ransomware protection can also interrupt the ransomware from encrypting all your data, which minimises the extent of the damage.

Backups can also assist in recovering your data as part of the recovery process following a ransomware attack.

How can I activate ransomware protection?

For more information on turning on ransomware protection, refer to ACSC's anti-virus guidance at cyber.gov.au/acsc/view-all-content/advice/anti-virus-software.

How can I backup my devices?

In addition to installing ransomware protection, you should also back-up your information (see page 5 of the *Personal Cyber Security: First Steps* guide).

That way, even if an attack is successful, you will at least have your important information accessible elsewhere.

For more information on ransomware prevention and recovery, see the ACSC's *RansomwarePrevention* and *Ransomware Emergency Response* guides, both available at cyber.gov.au/ransomware.

Reduce Your Digital Footprint

What is my digital footprint?

As soon as you go online, you start creating a trail of information about you. This is known as your digital footprint.

Cybercriminals can use this information against you, by using it to create convincing scams that specifically target you or someone you know.

With a simple Google search, cybercriminals could find your:

- **Identifying information** (date of birth, middle or maiden name, birthplace)
- **Workplace**
- **Relationships**
- **Hobbies and interests**
- **Sporting clubs**
- **Educational background**
- **Answers to account recovery questions**

Such data could also be used to identify personal details that you have included in your passwords, PINs, or in the answers to your account recovery questions.

This information could be used by cybercriminals to access your accounts and devices.

How can I reduce my digital footprint?

Protecting your identity online can go a long way in reducing the chances of being targeted by cybercriminals.

TO REDUCE YOUR DIGITAL FOOTPRINT:

- Increase your privacy settings on social media sites.
- Consider using an adblocker that can block tracking pixels and social media icons.
- Do not post your personal contact details (such as email address and phone number) online. Remove this information if already posted online.
- Avoid sharing information online that may identify you, or could be answers to your account recovery questions (e.g. your birthplace, or where you went to school). Remove this information if already posted online.
- Delete or deactivate any online accounts that you no longer use.
- Use a search engine to look up your name and review both the image and text results. If you find a result that reveals too much personal information, either take it down yourself or ask the person or company who posted it to delete it.

For more information about how to manage your information online, visit the Office of the Australian Information Commissioner at oaic.gov.au

Extend Your Cyber Secure Thinking

Secure Your Apps And Browser Extensions:

When using apps and browser extensions on your devices, use the following cyber secure behaviours and thinking:

- **Turn on automatic app updates**, and always update your apps and browser extensions as soon as possible for the latest security protection.
- **Check that your apps and browser extensions are made by reputable publishers** and ask for permissions that are appropriate for their intended use.
- **Uninstall apps and browser extensions** you don't need or use anymore.
- **Always download apps and browser extensions from an official store** such as Apple's App Store or Google Play for Android.

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

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

Summary Checklist

Have you completed everything in this guide?

Use this handy checklist to track your progress:

- **I have activated multi-factor authentication to protect all of my accounts, starting with:**
  - Accounts that save or use my payment details (e.g. eBay, Amazon, PayPal)
  - All social media accounts (e.g. Facebook, Twitter, WhatsApp)
  - Any other accounts that hold personal information (e.g. myGov, Apple ID, iCloud, Uber)
- **I have used unique strong passphrases to secure my accounts that aren't protected by MFA, starting with:**
  - Accounts that save or use my payment details
  - User accounts on my personal devices
  - Social media accounts
  - Any other accounts that hold personal information
  - Accounts who have had their details leaked online
- **I use a password manager to remember all of my passphrases.**
- **I have improved my Wi-Fi security habits.**
- **I have turned on real time protection to stop malware.**
- **I have turned on ransomware protection to defend against ransomware.**
- **I have reduced my digital footprint across all social media accounts (e.g. Facebook, Twitter, Instagram).**
- **I practice cyber secure thinking to secure my apps and browser extensions.**

Glossary

Anti-malware
A software program designed to protect a user's computer or network against malware. Also known as antivirus.

Account recovery
A process in which a set of questions or other 'proofs of identity' are used to recover or regain access to an account or to change an account passphrase/password.

Backup
A copy of device data stored elsewhere so that it may be used to restore the original.

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

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

Cryptocurrency
A type of digital currency that uses encryption techniques for security and anti-counterfeiting measures.

Cybercriminal
An individual who illegally accesses a computer system to damage or steal information.

Device
A computing or communications device. For example, a computer, laptop, mobile phone or tablet.

Digital footprint
The unique set of a user's traceable activities, actions, contributions and communications on the internet or digital devices.

Encryption
The process of making data unreadable for the purpose of preventing those without the encryption key (password) from gaining access to its contents.

Factory reset
Restores a device to its original manufacturer settings.

Hotspot
An area where wireless internet access is available to the general public.

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

Spyware
A program designed to covertly gather information about a user's activity on their device.

Trojan
A type of malware that is often disguised as legitimate software, used by cybercriminals to gain access to users' systems.

Virus
A type of malware that spreads on its own by attaching itself to other software, or copying itself across devices and networks.

NEXT GUIDE IN THE PERSONAL CYBER SECURITY SERIES

Now that you have completed the ACSC's *Personal Cyber Security: Next Steps* you should begin the *Personal Cyber Security: Advanced Steps*, available on **cyber.gov.au**.

The *Personal Cyber Security: Advanced Steps* outlines the actions you can take now to further increase your cyber security.

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

© Commonwealth of Australia 2023
With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

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