Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL CYBER SECURITY

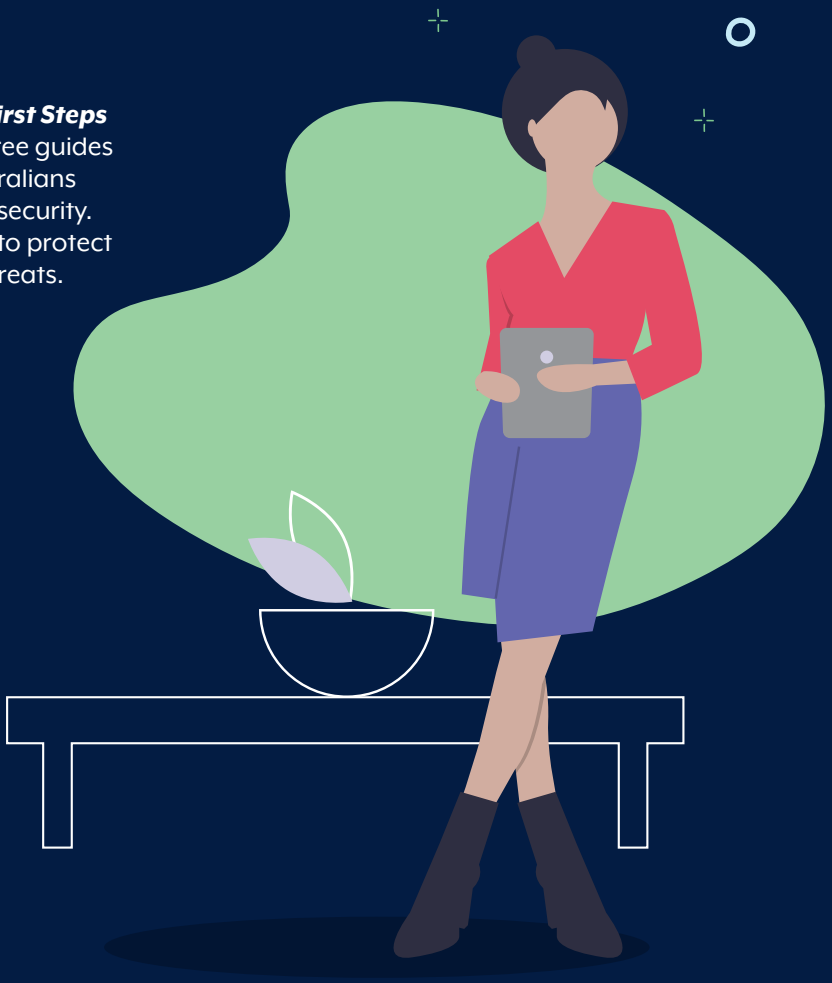
FIRST STEPS

cyber.gov.au

Personal Cyber Security Series

Personal Cyber Security Series

The ***Personal Cyber Security: First Steps*** guide is the first in a series of three guides designed to help everyday Australians understand the basics of cyber security. Learn how you can take action to protect yourself from common cyber threats.



First Steps

Next Steps

Advanced Steps

Table of Contents

Introduction

What is personal cyber security?

In an increasingly tech-driven world we use devices and accounts every day that are vulnerable to cyber threats:

- Your devices may include computers, mobile phones, tablets and other internet connected devices.
- You also may use online accounts for email, banking, shopping, social media, gaming and more.

Personal cyber security is the continuing steps you can take to protect your accounts and devices from cyber threats.

What are cyber threats?

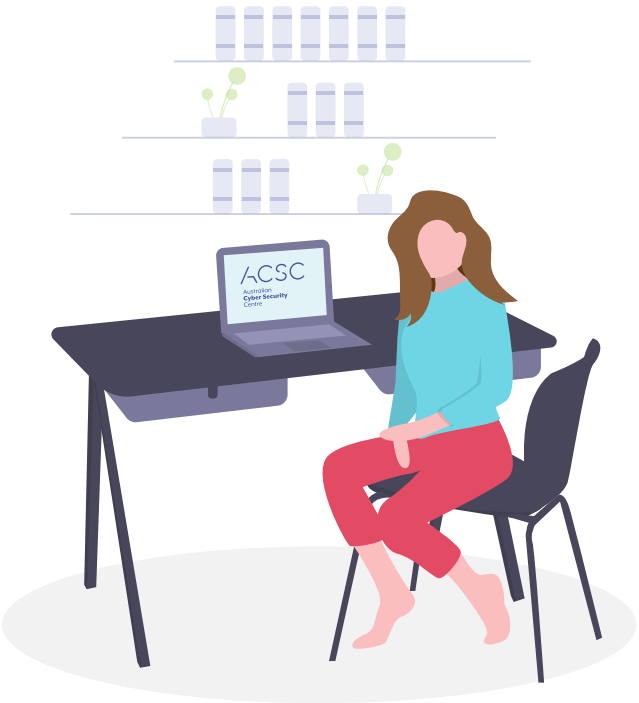
The main cyber threats affecting everyday Australians are **scams and malware**.

- **Malware is a blanket term used to describe malicious software** designed to cause harm. This can include viruses, worms, spyware, trojans and ransomware.
  Cybercriminals use malware to steal your information and money, and control your devices and accounts.
- **Scams are messages sent by cybercriminals** designed to manipulate you into giving up sensitive information, or to activate malware on your device.

These attacks can have significant personal and financial impact on victims. They are also growing in sophistication and frequency.

How can this guide help protect me from cyber threats?

If you are learning about cyber security for the first time, or are keeping yourself up to date, this guide is an excellent place to start. The Personal Cyber Security: First Steps guide is the first in a series of three guides designed to help you understand the basics of cyber security.



Turn on automatic updates

What are updates?

An update is an improved version of software (programs, apps and operating systems) you have installed on your computer and mobile devices.

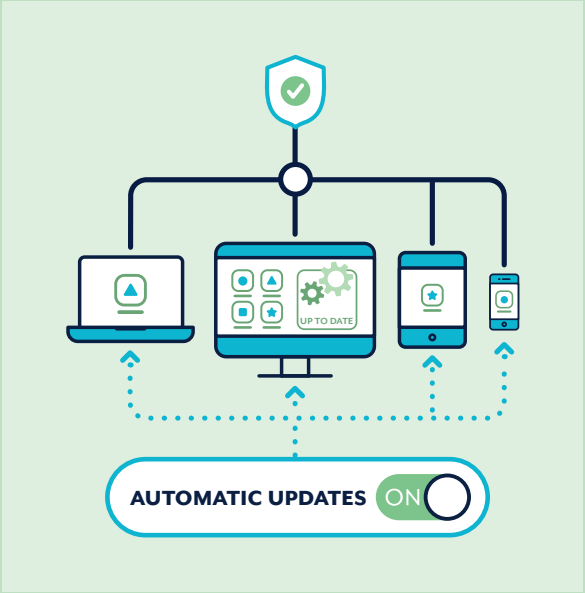
- **Software updates help protect your devices** by fixing software 'bugs' (coding errors or vulnerabilities). Cybercriminals and malware can use these 'bugs' to access your device and steal your personal data, accounts, financial information and identity.
- **New software 'bugs' are constantly being found** and exploited by cybercriminals. Updating the software on your devices helps protect you from cyber-attacks.

How do I set up automatic updates?

Automatic updates are a default or 'set and forget' setting that installs new updates as soon as they are available.

- **Turn on and confirm automatic updates** on all software and devices.
- **How you turn on automatic updates can differ** depending on the software and the device.
- **Set a convenient time for automatic updates** if possible, such as when you're asleep or not typically using your device.

Your device must be powered on, plugged into power and have unused storage space.



Tip: If you receive a prompt to update your device's software you should do so as soon as possible.

More detailed information on how to turn on automatic updates can be found by searching 'Updates' on cyber.gov.au

What if the automatic update setting is unavailable?

If the automatic update setting is unavailable, you should regularly check for and install new updates through your software or device's settings menu.

What if my older device and software do not receive any updates?

If your device, operating system or software is too old, it may no longer be supported by the manufacturer or developer.

When products reach this 'end of support' stage they will no longer receive updates. This can leave you vulnerable to cyber-attacks. Examples of products that are end of support include Windows 7 operating system and the iPhone 7.

If your device, operating system or software has reached end of support, the ACSC recommends upgrading as soon as possible to stay secure.

For more information, search 'End of support' on cyber.gov.au

Activate multi-factor authentication (MFA)

What is MFA?

You can use multi-factor authentication (MFA) to improve the security of your most important accounts. MFA requires you to produce a combination of two or more authentication types before granting access to an account.

- **Something you know** (e.g. a PIN, password or passphrase)
- **Something you have** (e.g. a smartcard, physical token, authenticator app, SMS or email)
- **Something you are** (e.g. a fingerprint, facial recognition or iris scan)

MFA makes it harder for cybercriminals to gain initial access to your account. It adds more authentication layers, requiring extra time, effort and resources to break.

How can I activate MFA to protect my most important accounts?

The steps for activating MFA are different depending on the account, device or software application. You should activate MFA now, starting with your important accounts:

- All online banking and financial accounts (e.g. your bank, PayPal)
- All email accounts (e.g. Gmail, Outlook, Hotmail, Yahoo!)

If you have a lot of email accounts, prioritise those that are linked to your online banking or other important services.

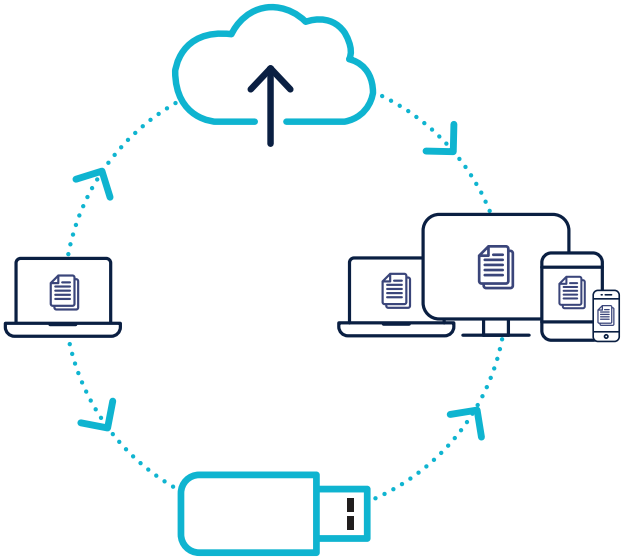
You can read more on how to turn on multi-factor authentication by searching 'Multi-factor authentication' or 'MFA' on cyber.gov.au

Regularly back up your devices

What is a backup?

A backup is a digital copy of your information. This can include things like photos, financial information or records that you have saved to an external storage device, or to the cloud.

Backing up your information is a precautionary measure so that it can be recovered if it is ever lost, stolen or damaged.



How do I back up my devices and files?

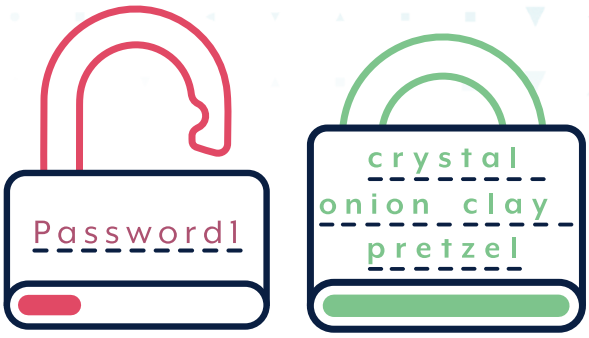
You should regularly back up your files and devices. What that looks like, whether it is daily, weekly or monthly, is ultimately up to you. How many times you back up could depend on the number of:

- new files you load onto your device,
- changes you make to files.

Tip: Check your backups regularly so that you are familiar with the recovery process. Always make sure your backups are working properly.

More detailed information on how to back up your information can be found by searching 'Backups' on cyber.gov.au

Use passphrases to secure your important accounts



Multi-factor authentication (MFA) is one of the most effective ways to protect your accounts from cybercriminals. **If MFA is not available**, a unique strong passphrase can better protect your account compared to a simple password.

What is a passphrase?

A passphrase uses four or more random words as your password.

For example: 'crystal onion clay pretzel'.

- **Passphrases are more secure** than simple passwords.
- Passphrases are **hard for cybercriminals** to crack, but **easy for you** to remember.

How can I create a passphrase?

Create passphrases that are:

- **Long:** at least 14 characters long, using four or more random words. The longer your passphrase the more secure it is.
- **Unpredictable:** use a random mix of four or more unrelated words. No famous phrases, quotes or lyrics.
- **Unique:** not re-used across multiple accounts.

If a website or service requires a complex password including symbols, capital letters, or numbers, you can include these in your passphrase. Your passphrase should still be long, unpredictable and unique for the best security.

Which accounts should I secure with a passphrase?

If your most important accounts are not protected with MFA, change your passwords to unique strong passphrases, starting with:

- Online banking and financial accounts
- Email accounts

If you have a lot of email accounts, prioritise those that are linked to your online banking or other important services.

You can typically change your password to a unique strong passphrase through your account settings menu.

Tip: If you struggle to remember all of your passphrases, consider using a password manager. With a password manager, you only need to remember one password, the password manager takes care of the rest. Search 'password manager' on cyber.gov.au for more advice.

More detailed information on how to create secure passphrases can be found by searching 'Passphrases' on cyber.gov.au

Secure your mobile device

Today smartphones and tablets are used in everyday life. We use them to connect, shop, work, bank, track our fitness and complete hundreds of tasks at any time, and from any location.

What can happen if my mobile device is compromised, lost or stolen?

- It may be used by cybercriminals to steal your money or identity. They do this by using information stored on your device, including social media and email accounts.
- You may lose irreplaceable data like photos, notes or messages (if it is not backed up).
- A cybercriminal may use your phone number to scam other people.

How do I secure my mobile device?

Device security:

- **Lock** your device with a passphrase, password, PIN or passcode. Make it difficult to guess – your date of birth and pattern locks are easy for cybercriminals to deduce. Use a passphrase for optimal security (see page 6). You might also consider using facial recognition or a fingerprint to unlock your device.
- **Ensure** your device is set to automatically lock after a short time of inactivity.
- **Don't** charge your device at a public charging station and avoid chargers from third parties.
- **Treat** your phone like your wallet. Keep it safe and with you at all times.

Software and app security:

- **Use** your device's automatic update feature to install new application and operating system updates as soon as they are available.
- **Set** the device to require a passphrase/ password before applications are installed. Parental controls can also be used for this purpose.
- **Check** the privacy permissions carefully when installing new apps on your device, particularly for free apps. Only install apps from reputable vendors.

Data security:

- **Enable** the remote locking and wiping functions, if your device supports them.
- **Ensure** you thoroughly remove personal data from your device before selling or disposing of it.

Connectivity security:

- **Turn** off Bluetooth and Wi-Fi when you are not using them.
- **Ensure** your device does not automatically connect to new Wi-Fi networks.

More detailed information on how to sure your mobile can be found by searching 'Secure your mobile phone' on cyber.gov.au

Develop your cyber secure thinking

Personal cyber security is not just about changing settings, it's also about changing your thinking and behaviours.

Watch out for cyber scams

Cybercriminals are known to use email, messages,social media or phone calls to try and scam Australians. They might pretend to be an individual or organisation you think you know, or think you should trust.

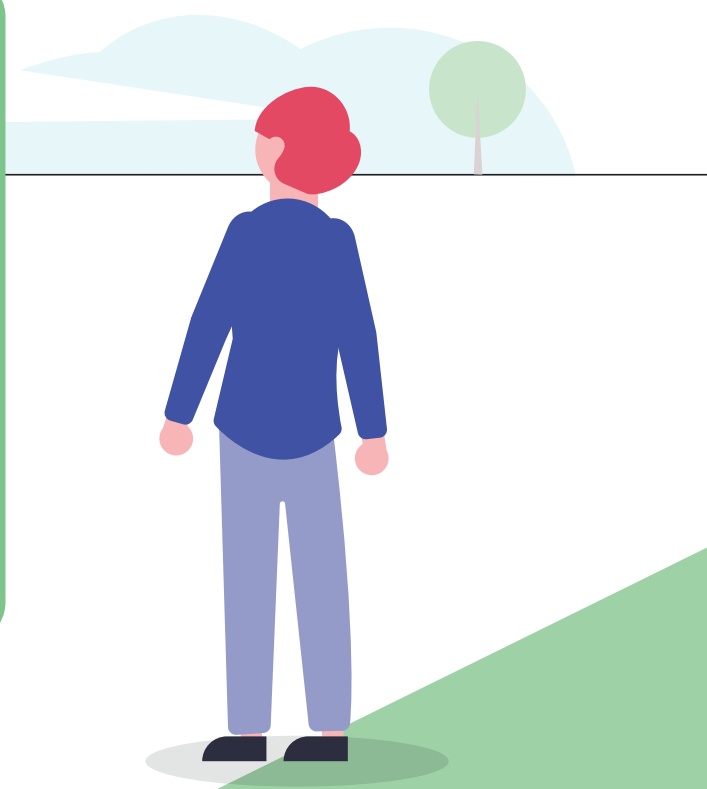
Their messages and calls attempt to trick you into performing specific actions, such as:

- Revealing bank account details, passwords, and credit card numbers
- Giving remote access to your computer
- Opening an attachment, which may contain malware
- Sending money or gift cards

How do I recognise scam messages?

It can be difficult to recognise scam messages. Cybercriminals often use certain methods to trick you. Their messages might include:

- **Authority**: is the message claiming to be from someone official, such as your bank?
- **Urgency**: are you told there is a problem, or that you have a limited time to respond or pay?
- **Emotion**: does the message make you panic, hopeful or curious?
- **Scarcity**: is the message offering something in short supply, or promising a good deal?
- **Current events**: is the message about a current news story or big event?



Learn how to spot phishing or scam messages by visiting 'Learn the basics' on cyber.gov.au

What should I do if I get a scam message?

If you receive a scam message or phone call, you should ignore, delete or report it to ACCC's Scamwatch at scamwatch.gov.au

You can also contact the ACSC's Cyber Security Hotline on **1300 CYBER1** (1300 292 371) if you are concerned about your cyber security.

If you've engaged with a scam and think your bank accounts, credit or debit cards may be at risk, contact your financial institution immediately. They may be able to close your account or stop a transaction.

What if I'm unsure if a message is a scam?

If you think a message or call might truly be from an organisation you trust (such as your bank) find a contact method you can trust. Search for the official website, phone their advertised phone number, or visit a physical store or branch. Do not use the links or contact details in the message you have been sent or given over the phone as these could be fraudulent.

Tip:
Think Before You Click

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

You can also keep up to date on the latest threats by subscribing to ACSC's free alert service. Search 'Subscribe to the ACSC alert service' on cyber.gov.au
We will send you an alert when we identify a new cyber threat.

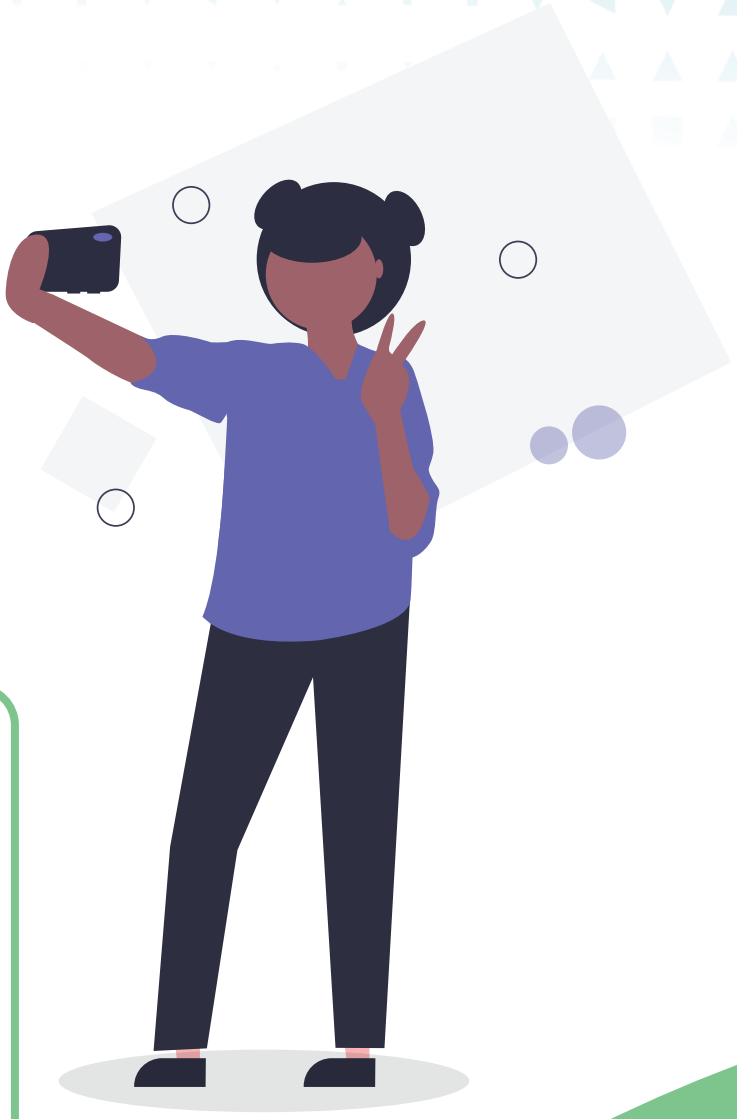
Stop and think before you share on social media

Cybercriminals can use information you have publicly posted on your social media account/s in their scams and cyber-attacks.

Remember information on the internet is permanent and you can never fully remove what has been posted.

How can I stop and think before posting?

- **Think:** How could a cybercriminal use this information to target me or my accounts?
- **Think:** Would I be comfortable showing this information or image to a complete stranger offline?



What information should I avoid sharing?

Avoid sharing information (including photos) online that cybercriminals can use to identify you, manipulate you through a scam or guess your account recovery questions. This may include your:

- Birthplace and date of birth.
- Address and phone number.
- Employer and work history.
- Where you went to school.
- Any other personal information that can be used to target you.

Summary Checklist

Have you completed everything in this guide?

Use this handy checklist to track your progress:

- **I have turned on automatic updates for all my devices:**
  - Computer (desktop and laptop)
  - Mobile phone
  - Tablet
- **I have activated multi-factor authentication on my most important accounts:**
  - All my online banking and financial accounts (e.g. your bank, PayPal)
  - All my email accounts (e.g. Gmail, Outlook, Hotmail, Yahoo!)
- **I regularly back up my devices:**
  - Computer (desktop and laptop)
  - Mobile phone
  - Tablet
- **I use unique strong passphrases on my most important accounts that aren't protected by MFA:**
  - Online banking and financial accounts
  - Email accounts
- **I have secured my mobile devices:**
  - Laptop
  - Mobile phone
  - Tablet
- **I use cyber secure thinking every day:**
  - I can recognise scam messages
  - I know what to do if I receive a scam message
  - I know how to check if a message is a scam if I'm unsure
  - I think before I click on links and attachments
  - I think before I share anything on social media
- **I know where to get help if I'm a victim of cybercrime or a scam**

Glossary

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

App
Also referred to as a mobile application, an app is a term for software that is commonly used for a smartphone or tablet.

Attachment
A file sent with an email message.

Authenticator app
An app used to confirm the identity of a computer user to allow access through multi-factor authentication (MFA).

Cloud
A network of remote servers that provide massive, distributed storage and processing power.

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

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

End of support
End of support refers to a situation in which a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for previous versions.

Malware
Malicious software used to gain unauthorised access and control of a user's computer, steal information and disrupt or disable networks.

Operating system
Software installed on a computer's hard drive that enables computer hardware to communicate with and run computer programs. Examples: Microsoft Windows, Apple macOS, iOS, Android.

Physical token
A physical device that can usually fit on a keyring, which generates a security code used to confirm the identity of a computer user using MFA.

Remote access
Gain access and control over devices and networks from an offsite location.

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

Next guide in the Personal Cyber Security Series.

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

The *Personal Cyber Security: Next Steps* guide 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.

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