



Australian Government  
Australian Signals Directorate

ACSC Australian  
Cyber Security  
Centre



# PERSONAL CYBER SECURITY FIRST STEPS

[cyber.gov.au](http://cyber.gov.au)

# 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 and how you can take action to protect yourself from common cyber threats.

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



**First Steps**



**Next Steps**



**Advanced Steps**

# Table of Contents

---

<b>INTRODUCTION</b> .....	1
<b>LEVEL UP YOUR CYBER SECURITY</b> .....	2
Turn On Automatic Updates .....	2
Activate Multi-Factor Authentication (MFA) .....	4
Regularly Backup Your Devices .....	5
Use Passphrases To Secure Your Important Accounts .....	6
Secure Your Mobile Device .....	7
Develop Your Cyber Secure Thinking .....	8
<b>SUMMARY CHECKLIST</b> .....	11
<b>GLOSSARY</b> .....	12

# 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**.

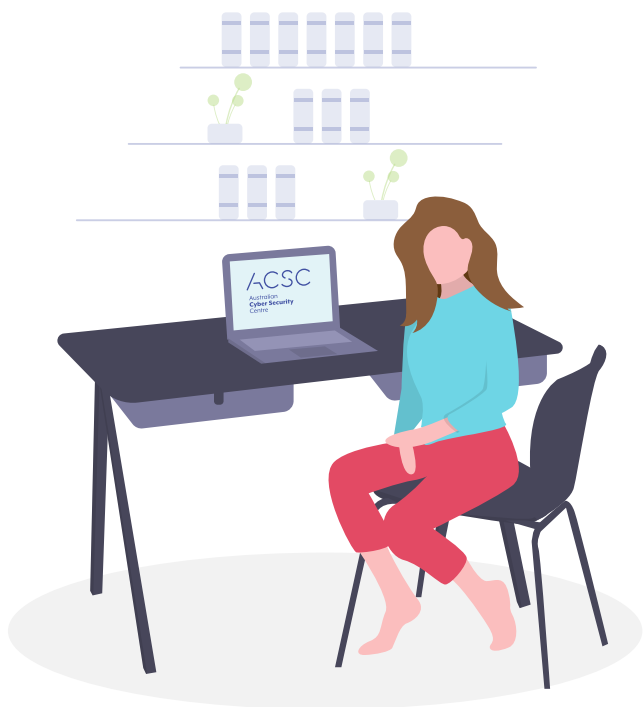
- **Malware is a blanket term for malicious software** designed to cause harm, including viruses, worms, spyware, trojans and ransomware. Cybercriminals use malware to steal your information and money, and control your devices and accounts.
- **Scams are messages sent by cybercriminals** designed to 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 and are growing in sophistication and frequency.

### How can this guide help protect me from cyber threats?

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 and how you can take action to protect yourself from common 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 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](https://cyber.gov.au).

If you think you're a victim of cybercrime report it through ACSC's ReportCyber on [cyber.gov.au](https://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](https://cyber.gov.au).

# Level Up Your 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.

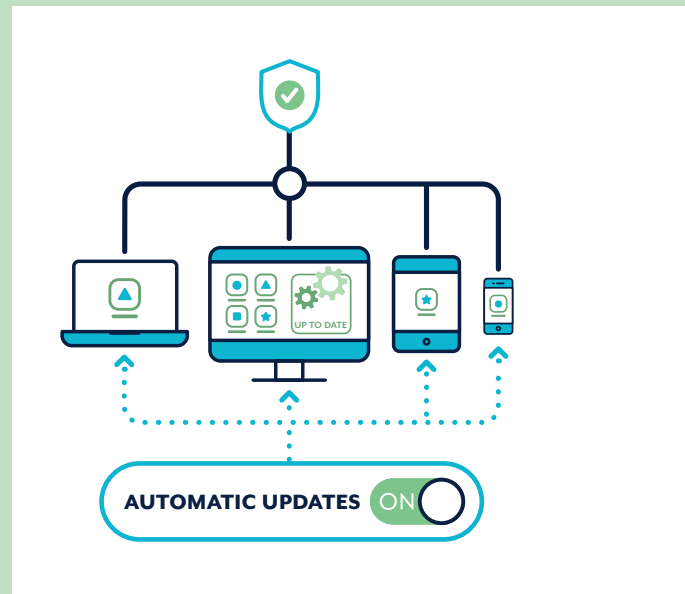
**Software updates help protect your devices** by fixing software 'bugs' (coding errors or vulnerabilities) that cybercriminals and malware can use to access your device and steal your personal data, accounts, financial information and identity.

**New software 'bugs' are constantly being found** and exploited by cybercriminals, so 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.



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



# Personal Cyber Security: First Steps



## 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.

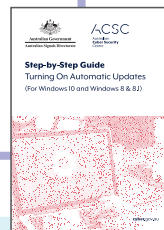
### WHAT IF MY OLDER DEVICES AND SOFTWARE DO NOT RECEIVE ANY UPDATES?

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

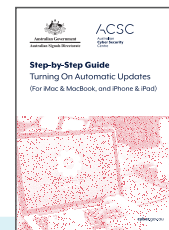
When products reach this 'end of support' stage they will no longer receive updates, leaving you vulnerable to cyber-attacks due to known software 'bugs'. Examples of products that are end of support include the Windows 7 operating system and the iPhone 6.

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, read the ACSC's *Quick Wins for End of Support* guide available at [cyber.gov.au](https://www.cyber.gov.au).



**Turning on Automatic Updates**  
(For Microsoft Windows 10 and Windows 8 & 8.1)



**Turning on Automatic Updates**  
(For iMac & MacBook, and iPhone & iPad)

For more detailed information on how to turn on automatic updates, read the ACSC's *Step-by-Step* guides available at [cyber.gov.au](https://www.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 of the following 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); and
- **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 by adding more authentication layers, requiring extra time, effort and resources to break.

**Two-factor authentication (2FA) is the most common type of MFA, requiring two different authentication types.**

#### HOW CAN I ACTIVATE 2FA TO PROTECT MY MOST IMPORTANT ACCOUNTS?

You should activate 2FA 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.

The steps for activating 2FA are different depending on the account, device or software application.

For more information on how to turn on 2FA on your important accounts, read the ACSC's *Step-by-Step* guides available at [cyber.gov.au](http://cyber.gov.au) or visit the website of your account provider.



## Regularly Backup Your Devices

### What is a backup?

A backup is a digital copy of your most important information (e.g. photos, financial information or records) 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.

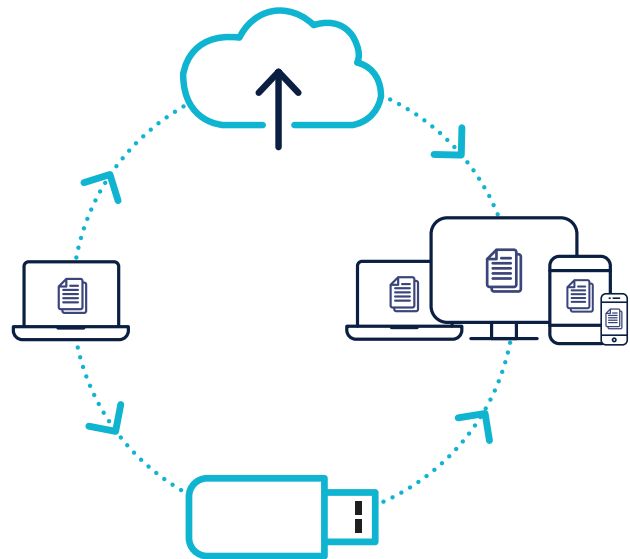
### How do I backup my devices and files?

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. Backup frequency could depend on the number of:

- **new files** you load onto your device,
- **changes** you make to files, and
- files you are **willing to lose**.

The ACSC encourages you to check your backups regularly so that you are familiar with the recovery process and ensure your backups are working properly.



For more detailed information on backing up to both external storage devices and the cloud read the ACSC's *Step-by-Step* guides available at [cyber.gov.au](https://www.cyber.gov.au):

#### FOR PC:

- *Backing Up and Restoring Your Files – For PC (To the Cloud)*
- *Backing Up and Restoring Your Files – For PC (Using an External Storage Device)*

#### FOR MAC:

- *Backing Up and Restoring Your Files – For Mac (To the Cloud)*
- *Backing Up and Restoring Your Files – For Mac (Using an External Storage Device)*

#### FOR IOS:

- *Backing Up and Restoring Your Files – For iPhone (To the Cloud)*



### Use Passphrases To Secure Your Important Accounts

Multi-factor authentication (MFA) (see page 4) 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 (see page 4), change your passwords to unique strong passphrases, starting with your:

- ✓ **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.

“Remember: Never reuse a passphrase across multiple accounts.”

For more advice on how to build strong passphrases, see the ACSC's *Creating Strong Passphrases* guidance available at [cyber.gov.au](https://www.cyber.gov.au).



### Secure Your Mobile Device

Today smartphones and tablets are used to connect, shop, work, bank, research, track our fitness and complete hundreds of other 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, 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** 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 (see page 5).

- ✓ **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.



### 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**

“Scam messages can be sent to thousands of people, or target one specific person.”

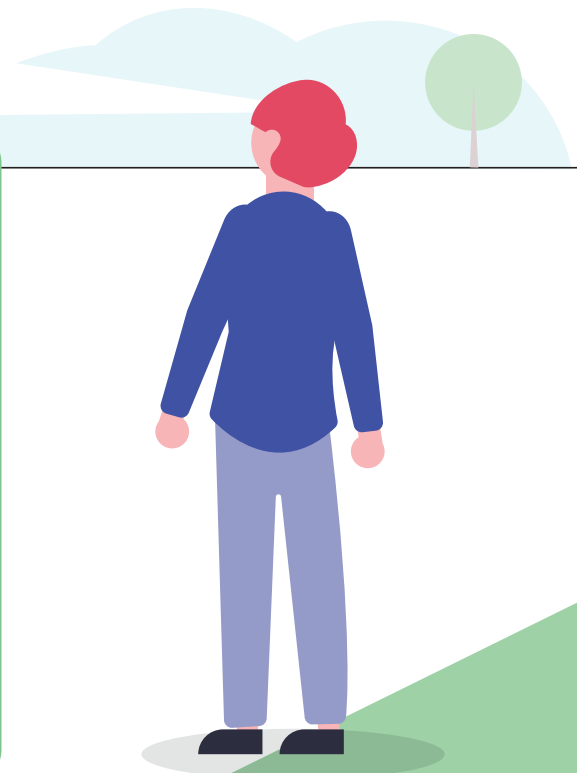
#### HOW DO I RECOGNISE SCAM MESSAGES?

**It can be difficult to recognise scam messages.**

Cybercriminals often use certain techniques 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?

To learn more about how to spot phishing or scam messages, take the quiz on ACSC's website [cyber.gov.au](https://www.cyber.gov.au).



## Personal Cyber Security: First Steps

### 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](https://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.

## Think Before You Click



- ✓ **Think before you click** on links on emails, websites and SMS.
- ✓ **Always be sceptical** of attachments you receive.
- ✓ **If your browser tells you a website is unsafe**, close it immediately.
- ✓ **Remember: No IT person, government department or business will contact you and ask for your login details.**



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

Keep up to date on the latest threats: Sign up to the ACSC's free alert service online at [cyber.gov.au](https://cyber.gov.au) which will send you an alert when we identify a new cyber threat.

### Stop And Think Before You Share On Social Media

**Think before you share online!** Cybercriminals can use information you have publicly posted on your social media account/s in their scams and cyber-attacks.

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

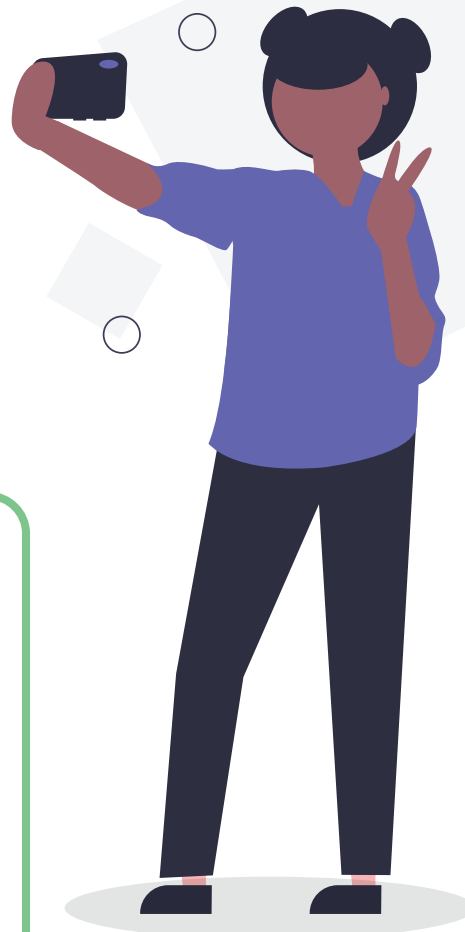
#### How can I stop and think before posting?

- **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 deduce 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](https://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.

### Copyright

© Commonwealth of Australia 2021

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](http://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](http://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](http://www.pmc.gov.au/government/commonwealth-coat-arms)).

**For more information, or to report a cyber security incident, contact us:**  
[cyber.gov.au](http://cyber.gov.au) | 1300 CYBER1 (1300 292 371)