Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

HOW TO USE THE INTERNET SECURELY

A GUIDE FOR SENIORS

cyber.gov.au

Introduction

Going online lets you keep in touch with friends and family, learn about topics and even play games.

Just like fastening your seatbelt before driving, you should take steps before using the internet to be more secure.

The Australian Cyber Security Centre (ACSC) wants to make sure everyone is secure when they're online. This document covers some basic cyber security practices that you can use to protect yourself when accessing the internet.

The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides 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 cyber.gov.au

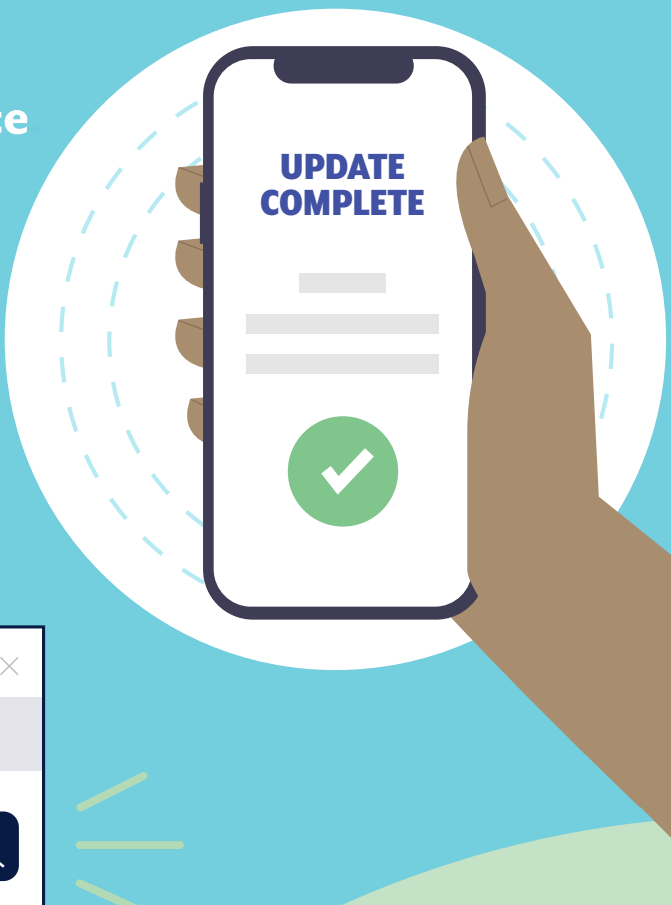
Cyber security for seniors

Tip 1: Update your device

Updating your software is like getting your car serviced. It improves your device's performance and makes it more secure.

Cybercriminals are always finding new ways to hack into devices. Setting up your device to automatically install updates can fix any weaknesses in your software and keep hackers at bay.

To find more information, search for 'Updates' on cyber.gov.au



DID YOU KNOW:
Updates may also add new features to your device and make it run faster.

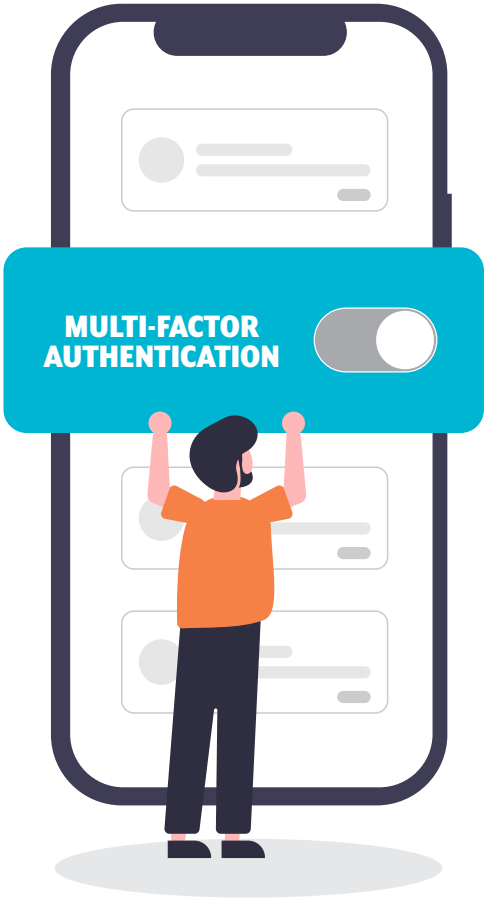
Tip 2: Turn on multi-factor authentication

Multi-factor authentication on your account is what a security screen is to your home.
It protects you from criminals who are trying to break in.

With multi-factor authentication activated, you need to give multiple pieces of information to gain access to your account. For example, you may need to enter your password and a text message code to log in to your social media profile.

The multiple layers make it harder for cybercriminals to hack in. They might manage to work out one part, like your password, but they will still need to obtain other pieces of the puzzle to access your account.

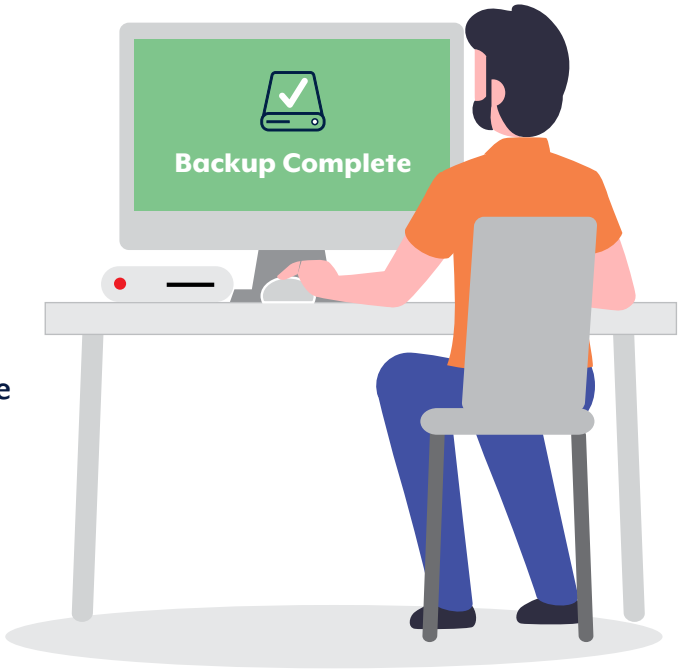
To find more information, search for 'Multi-factor authentication' or 'MFA' on cyber.gov.au



REMEMBER:

If you need help turning multi-factor authentication on, ask a friend or family member for assistance.

Tip 3: Back up your device



Performing a 'backup' is when you make a copy of your important files and put them somewhere secure. It's like photocopying precious photos to keep in a safe in case you lose the originals.

When you back up your computer, phone or tablet, copies of your files are saved online or to a separate device. Having a backup of your important files and cherished photos will provide you peace of mind.

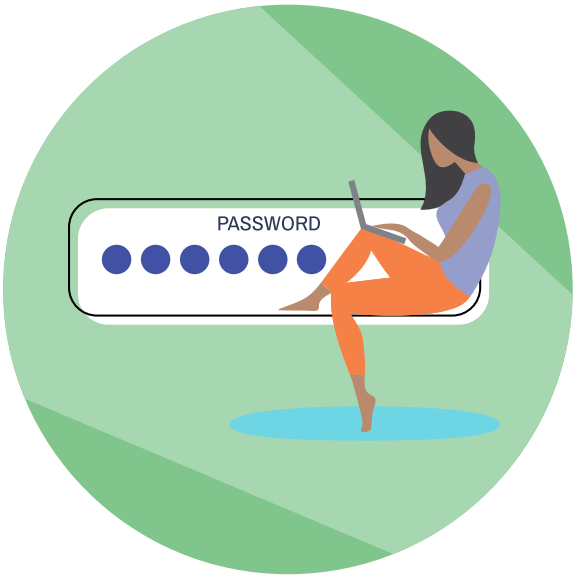
If something goes wrong with your device or you get hacked by cybercriminals, you can easily restore your files from your backups.

To find more information, search for 'Backups' on cyber.gov.au

DID YOU KNOW:

Backing up your device regularly means you'll always have access to your most up-to-date files.

Tip 4: Use a passphrase

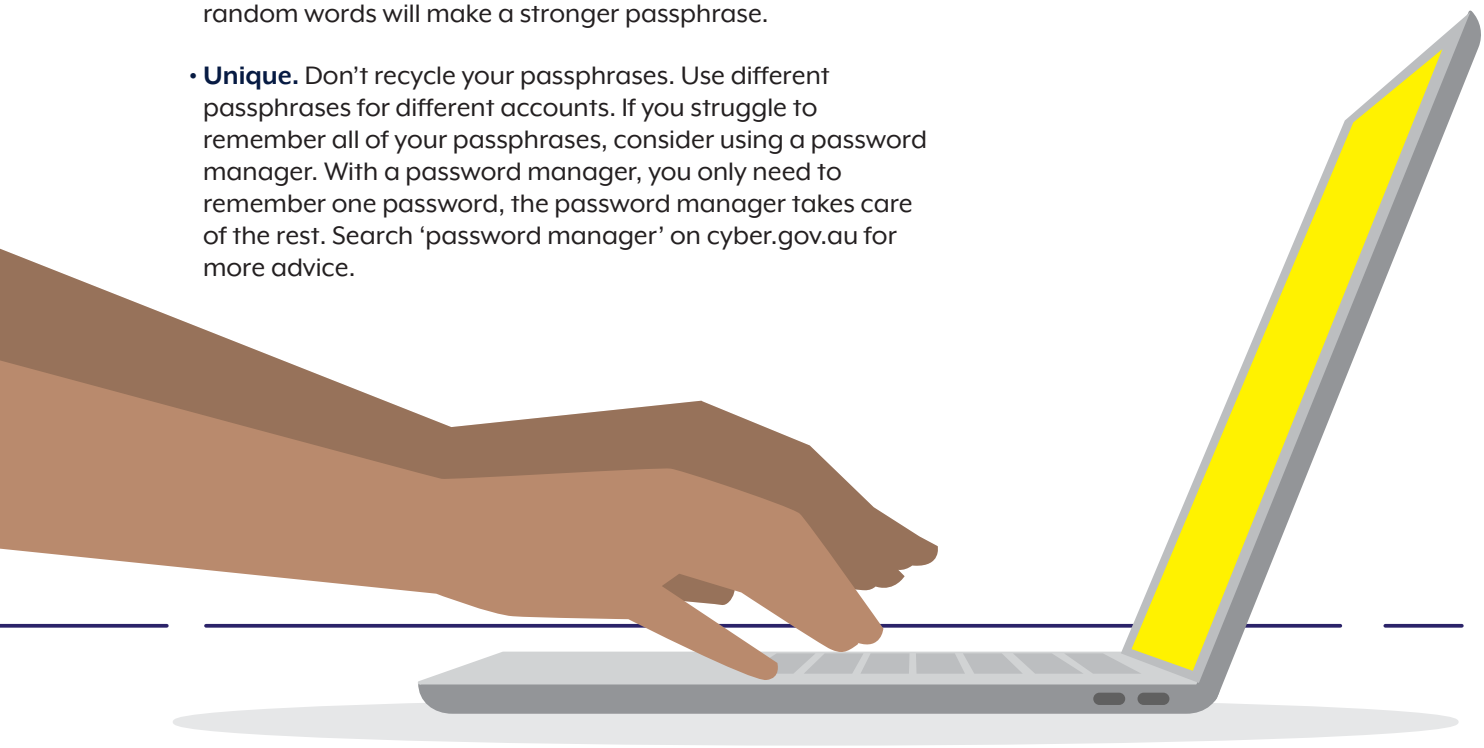


If a password puts a padlock on your account, a passphrase gives its own security system! They're stronger and more secure versions of passwords.

When you can't turn on MFA, use a passphrase to secure your account. Passphrases use four or more random words as your password. This makes them hard for cybercriminals to guess but easy for you to remember.

When you create a passphrase, make it:

- **Long.** The longer, the better. Aim for at least 14 characters in length. Four or more random words that you will remember is great.
  For example, 'purple duck potato boat'.
- **Unpredictable.** The less predictable your passphrase, the better. Sentences can make great passphrases, but they're easier to guess. A mix of four or more random words will make a stronger passphrase.
- **Unique.** Don't recycle your passphrases. Use different passphrases for different accounts. 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.



Learn more about creating secure passphrases by searching 'Passphrases' on cyber.gov.au

Tip 5: Recognise and report scams

The faster you report a scam, the quicker we can act.

If you believe that someone is attempting to use the internet to scam you, it's better to be proactive and cautious than risk being taken advantage of.

If it sounds too good to be true, it probably is. While a message might say you've won a prize or that your computer contains a virus, that message is not unique to you.

It might be coming from a scammer and they want to take advantage of you.

Remember, scammers will often pretend to be a person or organisation you trust. Be suspicious if you receive a message that looks like it's from someone you trust but they're using a new phone number, email address or social media profile. Before you respond, verify that the person or organisation messaging you really is who they say they are by contacting them through a channel you can rely on. For example, if you receive a text message that looks like it's from one of your children, but it comes from a new number, don't respond. Send them a message on social media to check that they really have changed their phone number first.

DID YOU KNOW:

Cybercriminals are crafty and might use a familiar name and email address. Be cautious if:

- **you're asked to urgently pay a bill.**
- **you're asked to change your details or password.**
- **you're asked to click on a link or open an attachment.**

Conclusion

Now that you're armed with the knowledge to use the internet more securely, you can browse with confidence and continue enjoying your time online.

Just remember, cybercriminals are always coming up with new ways to target people.

It never hurts to brush up on your cyber security know-how from time to time and learn new ways to stay secure.

Bonus tips

Want to learn more ways of staying secure online? Check out the following tips.

Think about what you post.

Think carefully about the information you share online and who will see it. Only accept friend requests from people you know in real life.

Get alerts on new threats.

Sign up for our free alert service. This will let you know whenever we find a new cyber threat.

This will also give you advice on what to do if an attack happens.

Talk about cyber security with family and friends.

Now that you've been skilled up in cyber security, share what you've learnt with your family and friends. Your knowledge could help them out of a tricky situation down the track!

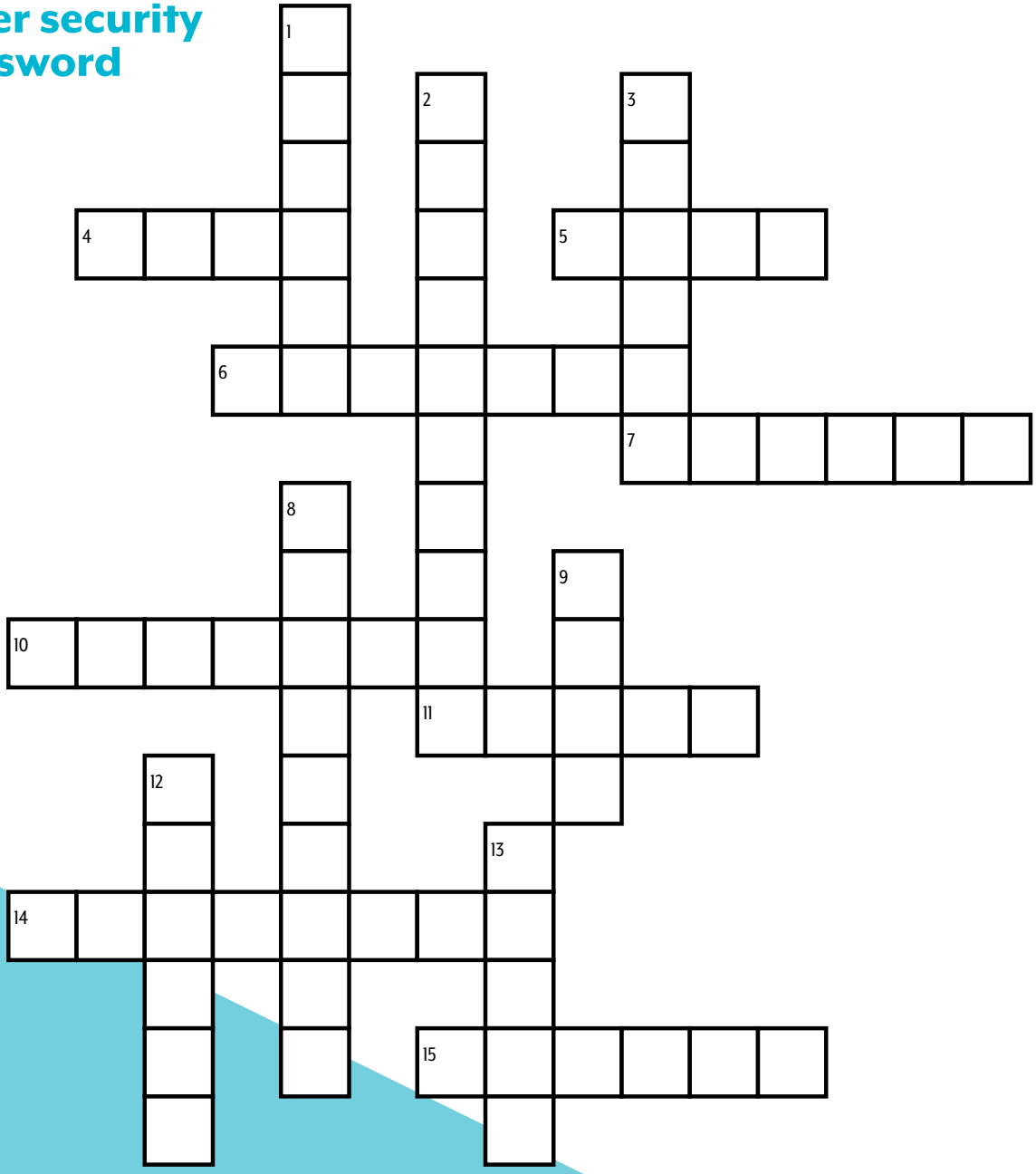
Avoid public Wi-Fi when you're banking or shopping online.

Public Wi-Fi is great for watching videos or reading websites but keep any online activity involving money for your home internet connection. Public Wi-Fi can be risky.

Report cyber crimes and incidents to keep Australia secure.

If you think you've been a victim of a cybercrime, act quickly. More advice is at cyber.gov.au

Cyber security crossword



DOWN

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

ACROSS

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Supplemental guides

For further information please check out our *Personal Cyber Security* series: 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 all three guides on **cyber.gov.au**

Crossword Answers:

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Notes

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