



Australian Government



Act Now.
Stay Secure.

Your Online Safety Toolkit: Protecting Yourself Online

Learn simple cyber safe actions you can take every day to protect yourself online.



Table of Contents

Cybercrime affects us all	3
Install all software updates to keep your devices secure	4
Use a unique and strong passphrase on every account	5
Always set up multi-factor authentication	7
Check and update your privacy and location settings regularly	8
Be cautious when using public Wi-Fi	8
Talk about how to be cyber secure with family and friends	10
Report a cybercrime	11
Staying safe from scams	12
If you need more support	13
Glossary	14



Cybercrime affects us all

Cybercrime is real and impacts Australians every day causing financial loss, reputational damage and emotional stress. Cybercriminals are becoming smarter at targeting people. It's more important than ever to stay up to date with the best ways to keep you and your loved ones protected online.

Just as we lock our front doors and buckle our seatbelts, cyber security should be an everyday habit.

Simple actions – like always setting up multi-factor authentication, using unique and strong passphrases, and installing all software updates on your devices – make a big difference in keeping you, your family and friends safe.



Install all software updates to keep your devices secure

Installing software updates on all your internet-connected devices is one of the easiest and most effective ways to stay secure online.

Think of software updates like servicing your car – they keep things running smoothly and patch up weak spots before they cause a problem. Software updates don't just give you new features – they also fix the weaknesses that cybercriminals look for.

Be sure to turn on automatic updates where possible and install software updates when prompted – it only takes a few moments!

For a helpful how-to video on installing software updates, head to actnowstaysecure.gov.au/how-to



Use a unique and strong passphrase on every account

While you might be familiar with using passwords, many people haven't heard of using a 'passphrase'.

A passphrase is a more secure version of a password. It consists of 4 or more random words that together are over 15 characters long. It can include capital letters, symbols or numbers.

Creating unique and strong passphrases is one of the easiest and most effective ways to protect yourself online. It can be the difference between being hacked in seconds or staying secure:

Password And Time Taken to Crack

Password	Less than a second to crack
Benjamin	13 seconds to crack
Qwerty123	44 seconds to crack
Harry1995	40 mins to crack
dogfishboat	19 days to crack
cloudrushfiddlechair	Centuries to crack

Password strengths and time to crack generated by the NSW Government's Password Strength Tester tool.

Our top tip

Use a unique passphrase for every account. If one account gets hacked, the others stay safe. Password managers can help you create and store them. For a helpful how-to video on creating unique and strong passphrases, head to actnowstaysecure.gov.au/how-to.



Now it's your turn – let's create a unique and strong passphrase!

Step 1: Think of 4 random words – for example, 'crystal onion clay pretzel'.

crystal **onion** **clay** **pretzel**

Step 2: Add numbers, symbols and capital letters to further strengthen it, if required by the website or service.

cry#tal **onion** **cLay** **pret7el**

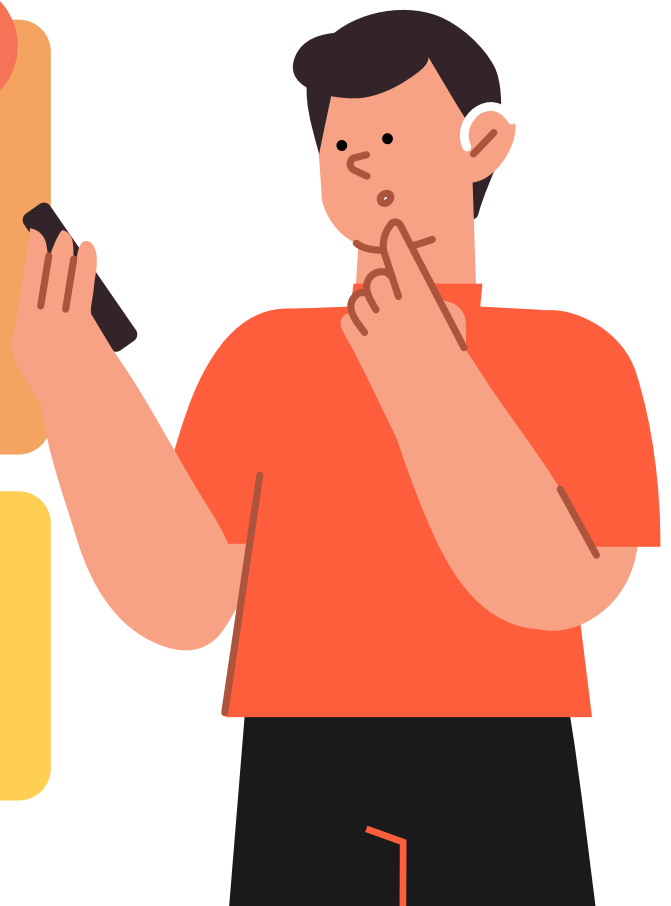
Passphrases should be easy for you to remember, but by being long and unique on every account, they are hard for cybercriminals to guess.

Our top tip



Don't use personal information like your birthday or pet's name as part of your passphrase. Cybercriminals may be able to find this information online – for example, on your social media accounts.

Well done! You now have a unique and strong passphrase. Repeat these steps to create different passphrases for each of your online accounts.



Always set up multi-factor authentication

Multi-factor authentication (MFA) is one of the best ways to protect your online accounts as it adds an extra layer of security. Put simply, it requires 2 or more ways to verify your identity to log in to your online accounts, such as banking, government services and social media.

For example, after you enter your password or passphrase on an account you may get a code from an authenticator app, email or text message that you will need to enter to log in. It provides a second layer of security – which comes in handy if a cybercriminal has managed to get your password.

You should review all your online accounts and set up MFA, where available.

For a helpful how-to video on setting up MFA, head to actnowstaysecure.gov.au/how-to



Check and update your privacy and location settings regularly

Did you know that information you share on public internet forums and social media, or through your device settings, can put you at risk of becoming a victim of cybercrime?

Cybercriminals can use your personal information to impersonate you and access your online accounts. For example, the name of a family member, pet or your suburb (when you check in or tag a photo at a location).

Our top tip

Turn off access to your location, photo and camera in your device and app settings where it is not needed.



If you don't regularly review your privacy and location settings, you may be at risk of oversharing online. Use our Oversharing Risk Indicator tool to find out and learn how you can improve.

Oversharing Risk Indicator



Ready to rate your online habits? Use our Oversharing Risk Indicator tool at actnowstaysecure.gov.au/oversharing-risk-indicator

Be cautious when using public Wi-Fi

Lots of people find themselves needing to use public Wi-Fi, whether on holiday, at the airport, at a café, or if they've run out of data.

Many people don't realise that these public networks are often not secure and are an easy way for cybercriminals to target you.

When using public Wi-Fi it's best not to access any sensitive or personal information, or log in to online banking, social media or email accounts.

Cybercriminals could easily access any information you enter while using public Wi-Fi – so it's best to play it safe.



Talk about how to be cyber secure with family and friends

Talking regularly about online security is a great way to ensure that you and those around you have the most up-to-date information. A quick conversation can make a big difference for you and your loved ones!

Be the difference.

With only 1 in 10 Australians regularly talking about how to stay safe online, you can make a difference and help take care of your family and friends by starting the conversation.³



Report a cybercrime

Reporting cybercrimes helps to protect Australians, no matter how small the crime may seem.

Common cybercrimes include:



Cyber attacks



Identity theft



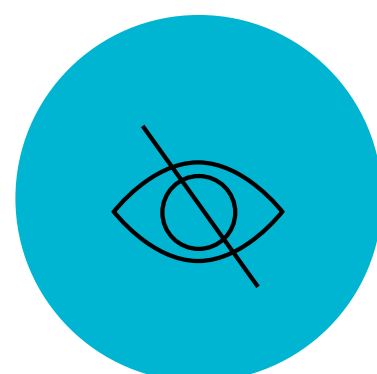
Scams



Fraud



Deliberate data
breaches



Sharing of offensive and
illegal content

Reporting cybercrimes helps the Australian Government:

- identify new trends
- collate data
- alert the community
- help you recover from the incident.

You can report a cybercrime at [cyber.gov.au/report](https://www.cyber.gov.au/report)

Staying safe from scams

Scams are getting more sophisticated and harder to detect. Take a moment to check who you're dealing with and never share personal details unless you're sure. Scammers may contact you by phone call, text, email or social media. They may also create fake websites that look real.

Stop

Scammers will try to get you to act quickly. Take a moment before giving your money or personal information to anyone.

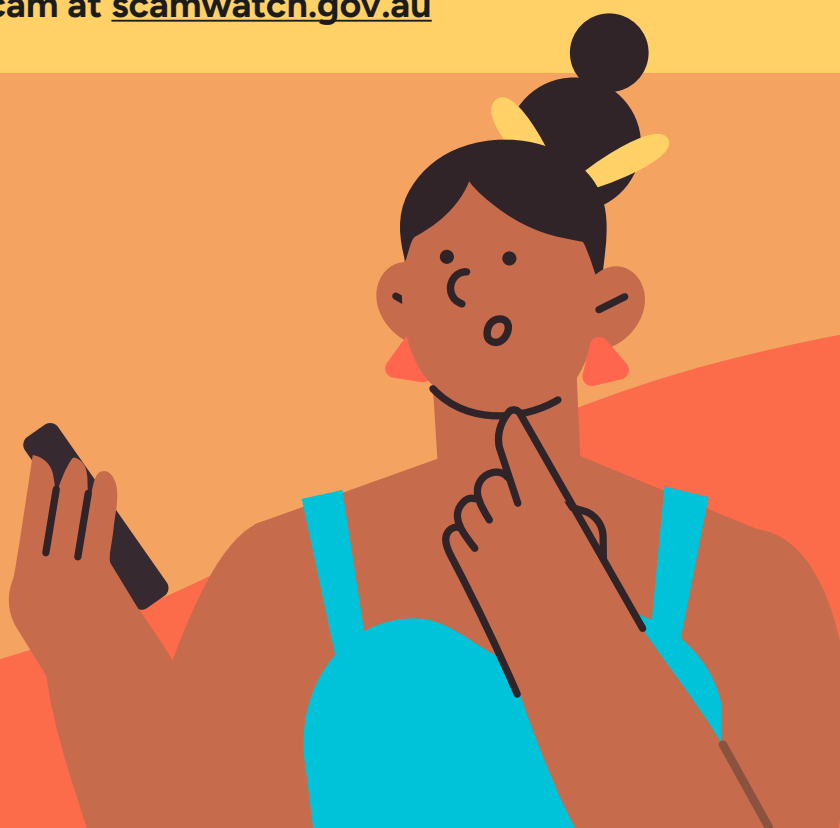
Check

It's important to confirm who you're really communicating with. Always check by contacting the person or organisation using details from the organisation's official website or app.

Protect

Act quickly if something feels wrong. Call your bank if you have transferred money.

Find out more about what to do if you've been scammed and report a scam at [scamwatch.gov.au](https://www.scamwatch.gov.au)



If you need more support

Well done! Combining these steps means you've strengthened your cyber security and are now better protected online.

The Australian Government has a variety of resources to help those who might need more support to stay secure online, including:

- Cyber security tutorials with Auslan translation
- An Easy Read document explaining how to be cyber secure.

Type 'actnowstaysecure.gov.au/accessible' in your internet browser to find these resources.



References

¹Scamwatch Targeting Scams Report 2024

²Australian Signals Directorate's Australian Cyber Security Centre Annual Cyber Threat Report 2024–2025

³Act Now. Stay Secure. Phase 4 Campaign Extension Report 2025

Glossary of Terms

Cyber security - Cyber security means keeping yourself safe on the internet.

Cybercrime - Cybercrime is when criminals use the internet for crime. For example, they might steal your information or take over your online accounts.

Cybercriminal - A cybercriminal is a person who uses the internet to commit crimes. They may try to trick you, steal your money, or get into your accounts.

Online account - An online account is a personal account you use on the internet. For example, for email, banking, social media, or government services.

Multi-factor authentication (MFA) - Multi-factor authentication, or MFA, means using 2 or more ways to log in to an account. For example, using a passphrase and then entering a code sent to your phone.

Authenticator app - An authenticator app is an app on your device that gives you a login code. You use this code as an extra step when logging in to an account.

Passphrase - A passphrase is a stronger type of password. It uses 4 or more random words and contains at least 15 characters.

Password manager - A password manager is a tool that helps you create and store passphrases. It helps you remember your passphrases so you do not have to write them down.

Software update - A software update helps keep your device safe online. It fixes problems and helps protect your device from cybercrime.

Automatic updates - Automatic updates mean your device updates itself without you having to do anything. This helps your device stay safe all the time.

Data breach - A data breach occurs when sensitive or personal information, that is held by an organisation, is accessed, disclosed or exposed without your permission. A data breach is often the result of a cyber attack.



Australian Government



Act Now.
Stay Secure.

Learn more ways to protect
yourself online at

actnowstaysecure.gov.au

