Australian Government

Act Now. Stay Secure.

How you can stay safe online

Easy Read version

Easy Read®

How to use this guide

We are the Australian Government.

We wrote this guide.

We wrote some words in **bold**.

We explain what these words mean.

There is also a list of these words on page 28.

You can ask someone you trust for support to:

- read this guide
- find more information.

This is an Easy Read summary of another guide.

It only includes the most important ideas.

You can find the other guide on our website.

www.actnowstaysecure.gov.au

What's in this guide?

About this guide

We all need to think about how we can stay safe online.

We call this **cyber** safety.

Cyber means something is to do with the internet.

This guide explains some things you can do to protect yourself online.

For example, from **cyber crime**.

Cyber crime is when criminals use the internet for crime.

For example, they might use the internet to:

- steal your personal information
- take over your online accounts or profiles.

Cyber crime can happen on any device.

This includes your:

- computer
- smartphone
- smart watch.

There are things you can do to stay safe from cyber crime.

We explain what you can do on the following pages.

Keep your accounts safe

You should think about how you can keep your online accounts safe.

Use strong and different passphrases

A **passphrase** is a stronger type of password.

It is very hard for other people to guess.

Using strong and different passphrases is one of the best ways to protect your accounts.

You should use a different passphrase for each of your online accounts.

Strong passphrases include:

- 4 or more random words
- 15 or more letters and numbers.

You can include some capital letters.

You can also use symbols such as:

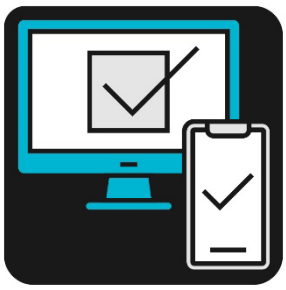
- a dash
- dollar sign
- an email @ sign.

You shouldn't use any personal information in your passphrases.

For example:

- your birthday
- the names of your family members or pets.

Add extra steps to log into your accounts



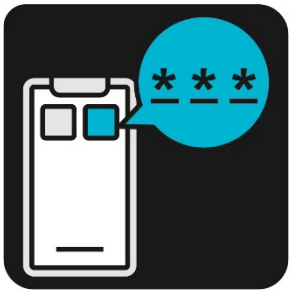
You can protect your online accounts with **multi-factor authentication (MFA)**.

MFA is when you use 2 or more different ways to log in to your account every time.

For example, you might need to enter your passphrase first.

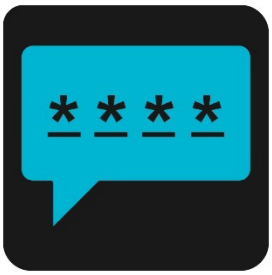
Then you enter a code that you get on your phone.

You might have the choice to:



- get an app on your phone to give you the code

- get the code in an email



- get the code in a text message.

MFA makes it harder for other people to get into your online accounts.

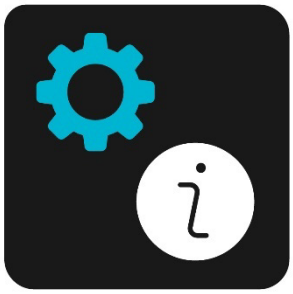
Even if they find out your passphrase.

Check your settings to protect your information

You can check that your settings are protecting your information online.

This includes settings on your:

- online accounts
- devices
- apps.



You can:

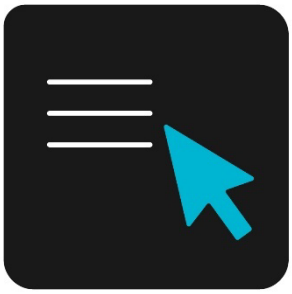
- change your settings
- choose what apps can use your information.

You might find settings on your device by:

- looking for the gear icon

  or

- typing ‘settings’ into your device’s search bar.

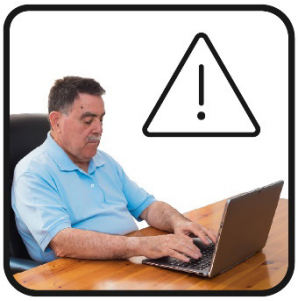


You might find settings in an app or an online account by opening up the menu.

The menu often looks like 3 straight lines.

Some of these settings can share information about:

- who you are
- where you are
- where you live.



Sharing this information online can put you at risk of cyber crimes.

Cyber criminals can use your information to pretend to be you.

For example, they might use information like:

- where you live

- the names of your family members

- the names of your pets.

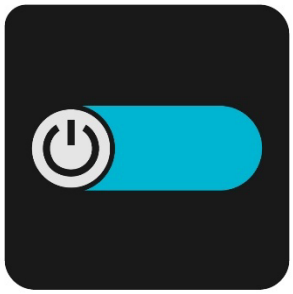
You can set your accounts so only people you know can see your social media profiles.

For example, your Facebook profile.

These settings are usually called privacy settings.

You can also control your **location settings**.

Location settings show where your device is.



You can turn location settings on or off.

You can also choose which apps can use your location settings.

You can do this for your:

- online accounts
- devices
- apps.

Some apps might also ask you if they can:

- use your camera

- see your photos.

You should only let apps you are familiar with use your camera and photos.

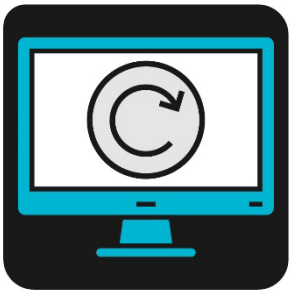
Protect your devices

You should think about how you can protect your devices to help keep you safe online.

For example, your phone or smart watch.

This is important for devices that connect to the internet.

Update your devices



You can update your devices to keep them safe online.

For example, your phone and laptop.

Your device might call this a software update.

Updates help a device protect itself from cyber crime.

You can set a device to update on its own.

You can learn more about how to update your devices on our website.

www.actnowstaysecure.gov.au/cyber-safe-actions

Public Wi-Fi networks

You should be careful when you use **public Wi-Fi**.

Public Wi-Fi is free wireless internet that you can use in public places.

For example, in a:

- cafe
- airport
- hotel.

You should be careful about what information you enter into a website using public Wi-Fi.

For example, your:

- bank details
- email accounts
- social media profiles.

Some cyber criminals can use public Wi-Fi to:

- see what you're doing online
- steal your information.

This is because:

- anyone can use it

- it is harder to protect your devices.

You can learn how to stay safe using public Wi-Fi on our website.

www.actnowstaysecure.gov.au/cyber-safe-actions

Scams

We call it a **scam** when someone tries to:

- trick you
- take your money.

A **scammer** is someone who does scams.

Scammers might try to trick you through:

- a text message or phone call
- an email
- social media
- a website.

They might seem friendly.

But they might trick you into giving them your information.

They can use this to:

- get into your online accounts

- pretend to be you

- steal your money.

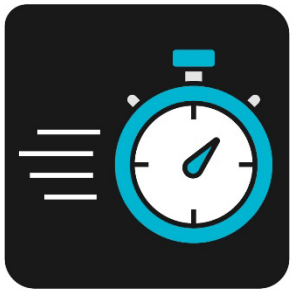
Scammers might also:

- create fake accounts to trick you

- share links and ads for you to click on.

How to spot a scam

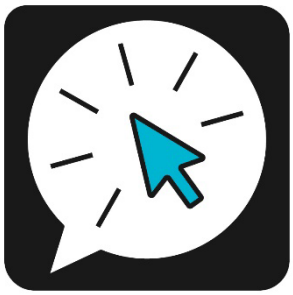
It might be a scam if it:



- asks you to do something quickly

- offers you lots of money

- asks you for money



- asks you to click on a link.

Scammers might also pretend to be an organisation you know and trust.

For example, your bank.

Scammers do this so you will share your personal information with them.

You should stop talking to the person if you think they are a scammer.

You should check that the person is who they say they are.

You can contact the person or organisation using details you trust and have found yourself.

Act quickly to protect yourself if something feels wrong.

Reporting a scam

Scamwatch helps Australians:

- understand scams
- report scams.

Scamwatch also helps Australians who have experienced scams.

You can report a scam on the Scamwatch website.

www.scamwatch.gov.au/report-a-scam

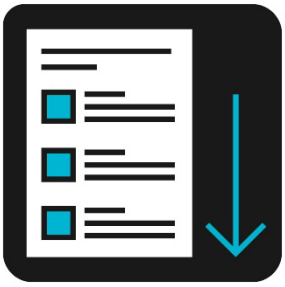
Speak up

You should speak up about how others can protect themselves online.

This includes:

- reporting cyber crime

- sharing what you know with family and friends.



We will explain how you can speak up on the following pages.

Report cyber crime

Reporting cyber crime helps the government:

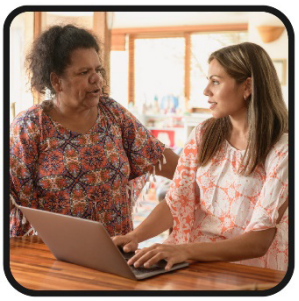
- learn how cyber criminals try to attack people

- protect more people.

You can report cyber crime on the ReportCyber website.

www.cyber.gov.au/report

Talk to family and friends about staying safe online



You should share your tips about staying safe online with your family and friends.

You can learn from them as well.

You can protect yourself and the people around you by sharing what you know about staying safe online.

This is also important if you share devices with others.

Word list

This list explains what the **bold** words in this guide mean.

Cyber

Cyber means something is to do with the internet.

Cyber crime

Cyber crime is when criminals use the internet for crime.

For example, they might use the internet to:

- steal your personal information
- take over your online accounts.

Location settings

Location settings show where your device is.

Multi-factor authentication (MFA)

MFA is when you use 2 or more different ways to log in to your account every time.

Passphrase

A passphrase is a stronger type of password.

It is very hard for other people to guess.

Public Wi-Fi

Public Wi-Fi is free wireless internet that you can use in public places.

Scams

We call it a scam when someone tries to:

- trick you
- take your money.

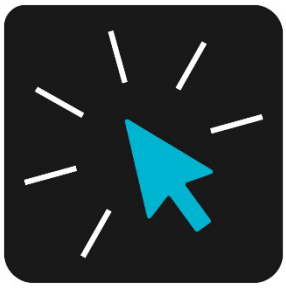
Scammers

A scammer is someone who does scams.

Contact us

You can call the Australian Cyber Security Hotline.

1300 292 371



You can visit our website.

www.actnowstaysecure.gov.au

You can report cyber crime on the ReportCyber website.

www.cyber.gov.au/report

The Information Access Group created this Easy Read document using stock photography and custom images.
The images may not be reused without permission.
For any enquiries about the images, please visit www.informationaccessgroup.com. Quote job number 6342.