# Understanding cybersecurity

## What is cybersecurity?

You lock your home, secure your wallet, and keep important papers safe. Being cybersecure is keeping your digital devices, personal information, money, and online data safe.

According to the Australian Communication and Media Authority, in 2021, of all people over the age of 75:

- 76% owned a smartphone
- 41% used social media
- 81% used email

Here are some simple ways to stay safe and remain vigilant while you browse online.

# Quick facts

- A 'device' is any smartphone, tablet, laptop, desktop computer, or electronic item that connects to the internet.
- 'Online browsing' refers to internet shopping, social media, email, interacting with websites, using applications, or online banking.
- A 'hacker' or 'scammer' is a digital thief, who looks to steal your online information.
- Australians over 65 spend more than three hours a day browsing the internet.
- There are over 3 million Facebook accounts in Australia that belong to people aged 65 and over.

# Update your device, programs, and applications

Most people call applications 'apps'. Updating your device or an app can improve the way it works, change how it looks, and add new features. The most important thing is that updates fix security weaknesses.

Cybercriminals are always looking for an open door to your information. Updates are how the software or app provider closes (and locks) the door.

Always check the device or app settings and turn on automatic updates if given the choice. Check for updates regularly if you can't make them automatic.

# Back up your important information

Make a backup of your digital information. This includes your documents, photos, videos, and apps.

Creating a backup means you make a copy of that information and store it separately from the original files. If the original information gets deleted, destroyed, or corrupted, then you haven't lost it forever. You have a backup!

Save your backups to an external storage device, usually called a hard drive, or to the cloud.

# Password management

Create a strong password for every device you use and every online account that you make. Here are five tips that provide ideal password management when used together:

- Don't use personal information such as names, street names, birthdays, or postcodes. Don't use common words either.
- Use a mixture of upper-case & lower-case letters, numbers, and symbols (#, $, &).
- Your password should be at least 14 characters long. A hacker can discover a seven-character password in 31 seconds, but it would take them 438 trillion years to discover an 18-character password.
- Use a unique password for each account. Hackers can discover the email and password combination on accounts such as Facebook. Then they check if you use the same combination for your online banking.
- Do not write your passwords down or keep them with or near the device you use to log onto your accounts.

Passwords should be strong, managed properly, and kept safe whether they protect sensitive information or not.

A password manager can store your passwords securely.

Read more about password managers and how to use one.

# Multi-factor authentication

This process asks you for more than one element to get into your account. Multi-factor authentication means you:

- Log into your account with your email address and password
- Receive a secret passcode via email or text or scan your face or thumbprint
- Enter the secret passcode into the log-in screen
- Gain access to your account

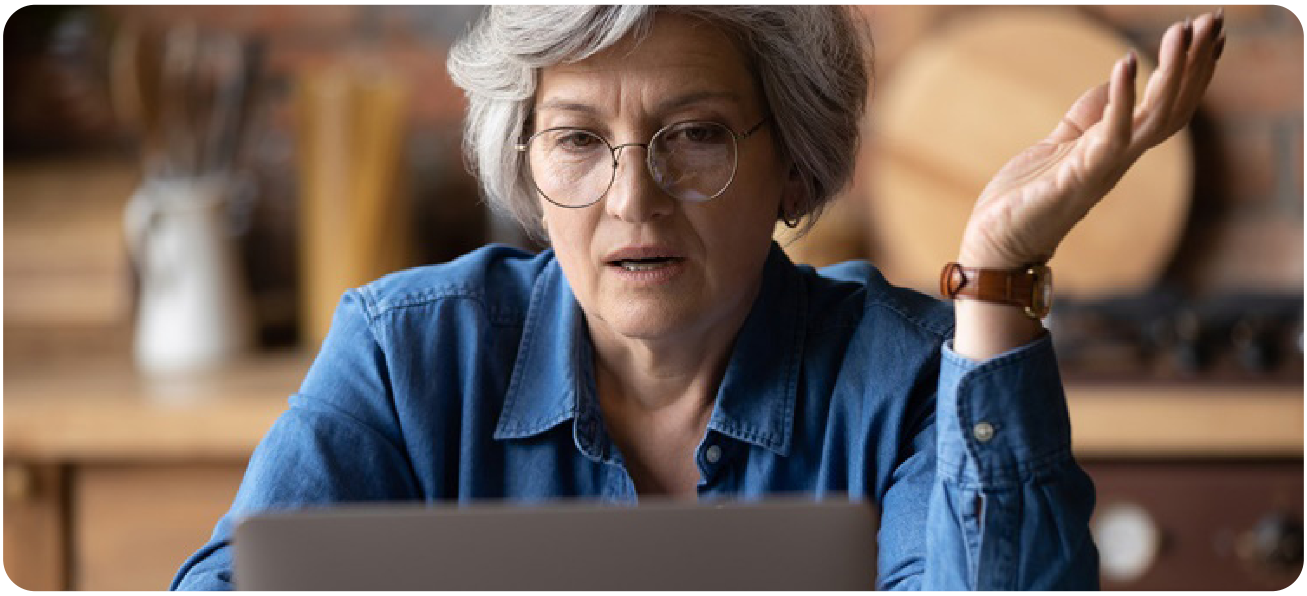
You get a new secret code every time you log-in. A hacker who knows your password, but not the secret passcode, won't be able to access your account. Use multi-factor authentication wherever you can, particularly for your most sensitive accounts like online banking, social media, and email.

# What are scams?

Scam messages can be sent to you via phone, email, social media, and messaging apps.

Scammers design scam messages to look like safe messages. They use elements like tone, logos, and disclaimers from trusted organisations. These could be organisations that you may already use or know.

Scammers use these messages to get information that identifies you. This could include your bank details, credit cards, or account passwords. They can also send web links that deliver malicious software to your device when you click on them.



# An example of a scam

Scammers use language and tone to create a sense of urgency designed to make you panic. Because you panic, you have an emotional response and jump to the conclusion that you must take urgent action.

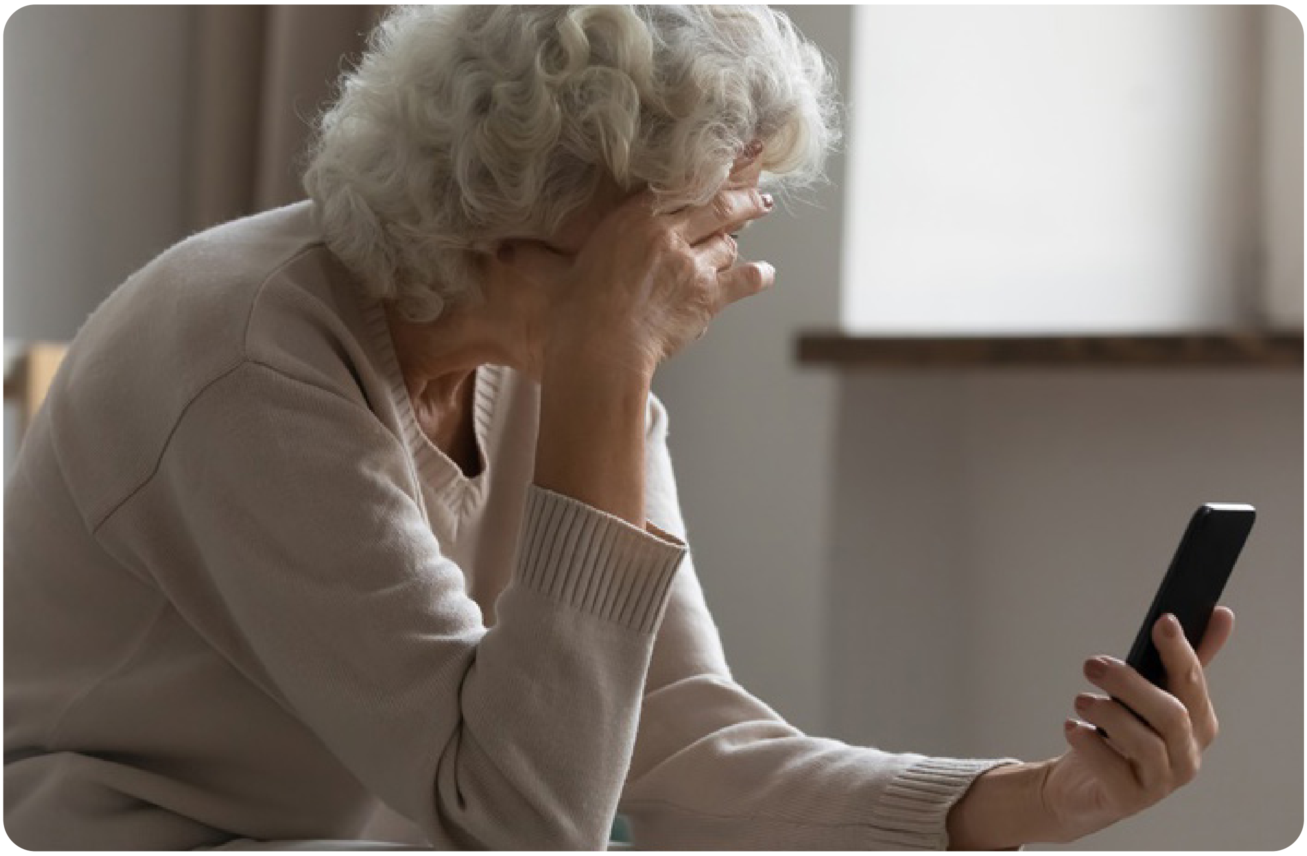
Current events and specific times of year are also useful tools for the scammer.

Example: You receive an email that appears to be from the ATO. The email warns you that something was wrong with your recently filed tax return. You must now click a link and offer more information to avoid prosecution. The email looks legitimate, but the scammer will use that information to steal your identity.

# Tips to avoid a scam

Always stop and consider these tips:

- Hover over links and see whether they have the right address to take you to an official website. If in doubt, do not click the link.
- Never log into an account directly from a link provided in a message. Visit the official website instead. Type the web address into your browser or Google or try and log-in via a saved shortcut on your browser.
- Phone the official advertised phone number of the organisation and double check if they sent the message.
- Find out whether the organisations you use will ever ask for your password or personal information in their communications.
- Keep your knowledge on scams up to date and find resources via the Australian Government Cybersecurity website: www.cyber.gov.au

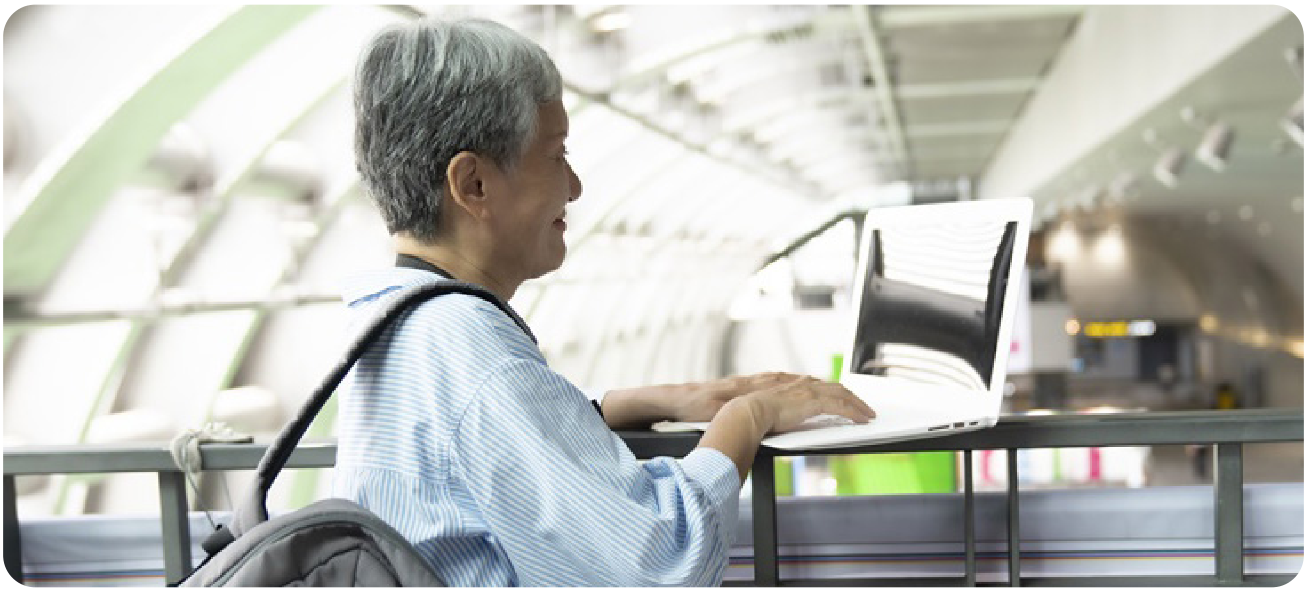


# Avoid free or public Wi-Fi

Wi-Fi is a wireless way to access the internet using your devices. If you have access to the internet outside of your house, you are either using a mobile phone network (via the SIM in your phone) or you're using Wi-Fi.

Free Wi-Fi is sometimes provided by a place, like the airport, or a shop. Not all Wi-Fi is safe though. A public network, like the one provided at certain airports, doesn't require a password and is therefore susceptible to hackers. If you don't trust the Wi-Fi network, it's best not to access it.

You could also use a VPN (Virtual Private Network) when accessing free public Wi-Fi if you're confident with technology.



## Contact us

**Website:** liveup.org.au
**Email:** support@liveup.org.au
**Phone:** 1800 951 971
**Facebook:** facebook.com/LiveUpAus

LiveUp is a healthy ageing initiative funded by the Australian Government Department of Health and Aged Care.