

# Managing your emails safely

Having an email address is your gateway to the online world. It allows you to keep in touch with family and friends, and access services like online shopping and banking. It's important to keep your email account as secure as possible, using a strong passphrase and multi-factor authentication.



## Ways to access email

There are many ways to access your emails. You can do this through:

### An app






- use the email provider's app that you can download from the App Store for Apple devices or the Play Store for Android devices
- link your email account to:
  - the pre-installed mail app on your smart device
  - the Mail or Outlook app on your computer.

### Website

- log into your email provider's website from a browser on your computer or smart device.

## Email service providers

There are lots of email service providers that offer both free and paid email account options, including:

-  **Gmail** Google
-  **Outlook** Microsoft
-  **Yahoo Mail** Yahoo
-  **iCloud** Apple
-  **ProntonMail** Proton AG

Visit the Be Connected website for [step-by-step guides](#) on how to set up and use Gmail, Outlook and Yahoo.

**Tip:** You might want to set up an email account just for your banking or to use only for online shopping to help manage spam emails.

# Managing your email account

## Setting up folders and labels

Setting up folders in your inbox is a great way to keep your account organised and make it easier to locate important emails when you need them. Folders are sometimes called labels, depending on the email service you use.

## Organising and filing your emails

Your email service has handy controls that help you file emails in different ways and keep spam and junk to a minimum. When a new email arrives and you open it to read it, some controls appear at the top of the screen. You can click on these controls to:

- **Delete:** move the email to the Bin/Trash folder
- **Archive:** move the email to the archive
- **Mark as unread:** make the email appear new again
- **Labels/Folder:** label the email or move it to a folder.

## Managing spam emails

Your email service automatically detects and diverts known spam email, but some spam can still get through.

If you consider an email in your inbox to be junk or spam, you can:

- **Report spam:** tell your email provider that the email is spam
- **Block emails:** stop receiving emails from the sender
- **Unsubscribe:** stop receiving newsletters or marketing emails you subscribed to.

If you think you've unsubscribed but continue to receive unwanted spam emails, you can make a complaint to the [Australian Communications and Media Authority](#).

**Tip:** To avoid unwanted spam emails, be wary of providing your information for competitions and any pre-checked boxes to receive marketing emails when you buy products or services.

# Keep your email account secure

## Passphrases

Keep your accounts secure with strong passphrases. Passphrases are the more secure version of passwords and are made up of four or more random words.

Try thinking of a different passphrase for each of your accounts and don't recycle parts of any old ones.

When you choose your passphrase, make it:

- **Long** – at least 14 characters
- **Unpredictable** – use four or more random words with numbers, symbols, and upper and lowercase letters
- **Unique** – don't reuse your passphrases.

*E.g. Yellow So Hey Plant > Yell\*w-SOheyPl@nt!*

**Tip:** A password manager app can also help you create and store complex passphrases that are hard for others to guess or hack. You can find information on [password managers](#), and how to set them up on the Be Connected website.

## Multi-factor authentication

It's always a good idea to switch on multi-factor authentication for your accounts. Multi-factor authentication (also known as 2-step authentication) adds an extra layer of security. This means that when you log into an account with your password, you might be asked to do an extra step to confirm that it's you – like enter a code from a text message or use face recognition identification.

## Use device security

Using security software on your computer is one of the simplest ways to secure your accounts and devices. Good computer security includes installing reputable anti-spyware, anti-virus scanners and firewall software. You should also keep your online security tools and apps up to date by enabling auto-updates.

## Use a secure connection

When you need to access your accounts, send sensitive information or enter passwords, connect to a trusted internet connection, such as at home, at work or by using your own mobile data if it's available. Public Wi-Fi is not as secure as your home or work Wi-Fi.

## Account recovery options

Make sure you set up a recovery phone number or alternative email address for all of your email accounts. If you lose access to your account, or it is compromised, you can reset your password using your recovery option.

---

## Scams emails

Scam emails are designed to look like they're from legitimate organisations that you know. They may look real, using logos and a similar email address to the organisation they are impersonating. Scam emails can appear to be from your bank, internet service provider, a government agency, retailer, or even a scammer pretending to be a friend or family member. By pretending to be from someone you trust, scammers use a sense of urgency to trick you into paying money or providing personal information, such as important passwords, credit card or banking details.

These types of scams are called impersonation scams or phishing emails.

## Tips for avoiding scam emails

- Look out for the signs of a scam email. Scam emails can:
  - have a sense of urgency or use scare tactics, demanding a payment or asking you to confirm personal details
  - use generic greetings such as 'Dear customer', 'Dear user' or no greeting at all
  - ask you to click on a link or download a file, that might direct you to a fake website or contain a virus or malware.
- Always check the sender's email address is legitimate and contact the organisation directly by looking up their official website and phone number.
- Never log into your online accounts or verify details via a link in an email or click on links or open attachments in emails from unknown senders or that are suspicious.
- Delete suspicious or possible scam emails, use the 'report spam' option to classify it as unwanted email.

**Tip:** If you are unsure about an email, speak to a trusted friend or family member and contact the organisation using the phone number on their website.

Visit the Be Connected website for our free [impersonation scams guide](#) developed with Scamwatch.

---

## Take the time to discover Be Connected

Be Connected is a comprehensive website with free resources specifically designed to support older Australians to connect online safely and navigate the digital world confidently. The site is also useful for families and community organisations who want to help older community members access all the benefits of the internet.



Visit [beconnected.esafety.gov.au](https://beconnected.esafety.gov.au)



This program has been developed by the eSafety Commissioner as part of the Be Connected initiative.