Safer online banking and payments

Get Online Week

a campaign by Good Things

Online banking and payments make managing your money easy.

You can pay bills, transfer money and access your accounts anytime, anywhere. By following some simple steps, you can reduce risks and protect your personal information.

Choose strong and unique passwords

Strong passwords make it harder for criminals to steal your money.

Make your passwords hard to guess. Avoid using birthdays, street names, children's names, common words like 'password' and sequences like '1234'.

> **Top tip:** Consider using more complex 'passphrases' instead of words. This is where you combine three words together.

Make sure your passwords are different for every online account you have. This way if a criminal gets one of your passwords, they don't get access to everything.

> **Top tip:** Update important passwords every 3-6 months or if you notice any suspicious activity.

Two factor authentication

Two factor verification is a second step after your password when you log in to online accounts. It checks that it really is you trying to log in.

The second step can be adding a pin number or one time code sent to your mobile phone or email, a scan of your fingerprint, or a scan of your face.

> **Top tip:** Set up two factor verification on all your important online accounts, like your bank account.

Avoid using public WiFi

Public WiFi networks may be convenient and free, but are less safe to use for tasks like online banking and payments. Criminals can watch what you are doing

when connected to public WiFi and collect your personal information.

> **Top tip:** Use your mobile data instead of public WiFi to access your bank account or make payments on the go.

Check notifications

Security notifications alert you to new log ins or payments from your online banking account. They can be a pop up message, text message or email. If you get an unexpected security notification or suspect fraudulent activity, change your online banking password and contact your bank immediately.

> **Top tip:** Go to your online bank account settings and turn on notifications and security alerts.

Watch out for scam emails and texts

Criminals can try to trick you by sending fake email or text messages pretending to be your bank. They will often sound very urgent and ask you to click a link to update your information. Clicking this link is how they will start to steal your information like passwords.

> **Top tip:** Do not click on links in emails or text messages that you are not expecting.

If you get a message from your bank, credit card or payment app, check it is real before you do anything. Go to the official website and use those contact details to check.

> **Top tip:** Visit scamwatch.gov.au for useful information on how to recognise and stay safe from scams.

Banks will never ask you:

- For your online banking password
- To log in to your account from a link in an email or text message
- For remote access to your computer, smartphone or tablet.

Keep learning

Keep learning how to stay safer online on the Be Connected and Good Things websites

Visit **beconnected.esafety.gov.au** and **goodthingsaustralia.org/learn** to get started.

Bendigo Bank

Our thanks to our Principal Financial Inclusion Partner Bendigo Bank for their collaboration on these tips.

Get Online Week

a campaign by Good Things