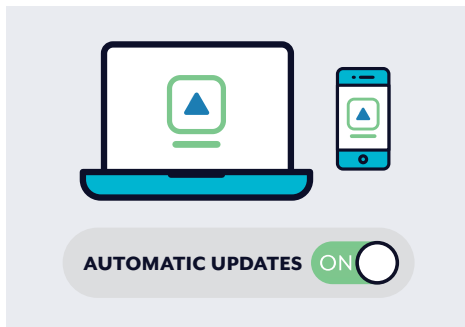# TOP TIPS FOR CYBER SECURITY
PRACTICAL WAYS TO PROTECT YOURSELF ONLINE
cyber.gov.au/learn

Update your apps and devices

Updating your apps and devices can fix issues and address new security concerns or weaknesses that hackers could use to access your devices or accounts. They can also add new features.

Turn on multi-factor authentication (MFA)

MFA means having more than one check in place to prove your identity on an account. For example, you may need a code from a text message and your passphrase. It makes it much harder for cybercriminals to access your accounts.

Set up and perform regular backups

A backup is a digital copy of your most important information either to an external storage device or a server on the internet like the cloud. It means you can restore your files if something goes wrong.
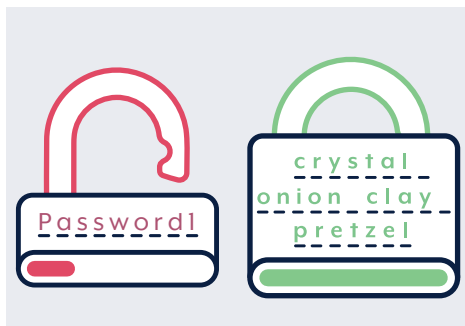
Set up secure passphrases

When MFA is not available, use a passphrase to secure your account. A passphrase is a strong type of password that uses four or more random words. This makes them hard for cybercriminals to guess but easy for you to remember.
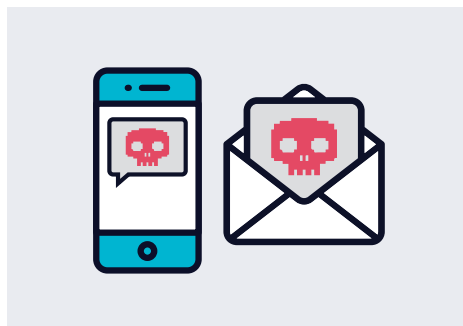
Recognise and report scams

Criminals often use email, SMS, phone calls and social media to scam people. They usually do this by contacting you and pretending to be an individual or organisation you know and trust.

Always be alert when clicking on attachments or links within emails or messages.

Level up your cyber security by...

- Thinking about what you post online.
- Signing up to our free alert service to receive alerts on new threats
- Talking about cyber security with your family and friends.
- Avoiding public Wi-Fi when you're banking or shopping online.
- Reporting cyber attacks and incidents to keep Australia secure.

Find out more at **cyber.gov.au/learn**

Do you have some feedback on this product? Go to **cyber.gov.au** and let us know.