REPORT CYBER-ATTACKS AND INCIDENTS TO KEEP AUSTRALIA SECURE.

SIGN UP

To our free alert service

cyber.gov.au/acsc/register

REPORT

Cybercrime to REPORTCYBER:

cyber.gov.au/report

CONTACT

Call 1300 CYBER1 or

visit **cyber.gov.au**

FOLLOW US

ACSC Australian Cyber Security Centre

5. WATCH OUT FOR SCAMS

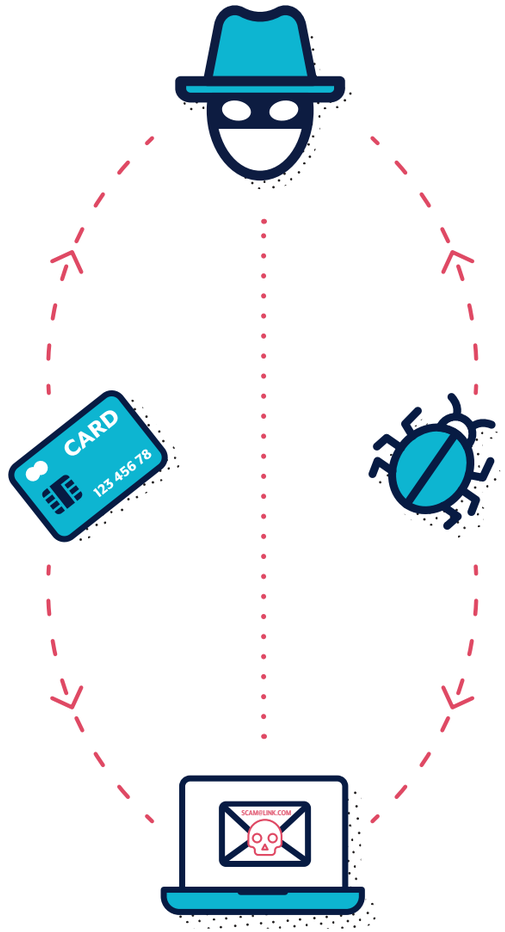
Cybercriminals use email, SMS, phone calls and social media to trick you into opening an attachment, visiting a website, revealing account login details, revealing sensitive information or transferring money or gift cards. These messages are made to appear as if they were sent from individuals or organisations you think you know, or you think you should trust.

To spot scam messages, stop and think:

- **Authority:** Is the message claiming to be from someone official?
- **Urgency:** Are you told you have a limited time to respond?
- **Emotion:** Does the message make you panic, fearful, hopeful or curious?
- **Scarcity:** Is the message offering something in short supply?
- **Current events:** Is this message related to current news stories, big events or specific times of year (like tax reporting)?

To check if a message is legitimate:

- Go back to something you can trust. Visit the official website, log in to your account, or phone their advertised phone number. Don't use the links or contact details in the message you have been sent or given over the phone.
- Check to see if the official source has already told you what they will never ask you. For example, your bank may have told you that they will never ask for your password.



For more information on spotting scam messages, see the Australian Cyber Security Centre (ACSC)'s Detecting Socially Engineered Messages publication, and stay informed by signing up to the ACSC's Alert Service on **cyber.gov.au**

EASY STEPS

TO SECURE YOUR DEVICES AND ACCOUNTS

REDUCE THE RISK OF BEING TARGETED BY CYBERCRIMINALS BY FOLLOWING THESE STEPS

ACSC Australian Cyber Security Centre

cyber.gov.au

1. UPDATE YOUR DEVICES

Cybercriminals hack devices using known weaknesses in systems or apps. Updates have security upgrades to fix these weaknesses. Turn on automatic updates so that this happens without your input.

Turn on automatic updates on all your devices:

- Mobile phone
- Laptop
- Desktop

Regularly check for updates for your:

- Apps
- Programs
- Smart devices

2. ACTIVATE MULTI-FACTOR AUTHENTICATION (MFA)

MFA improves your security by increasing the difficulty for cybercriminals to access your files or account.

Activate MFA, starting with your most important accounts:

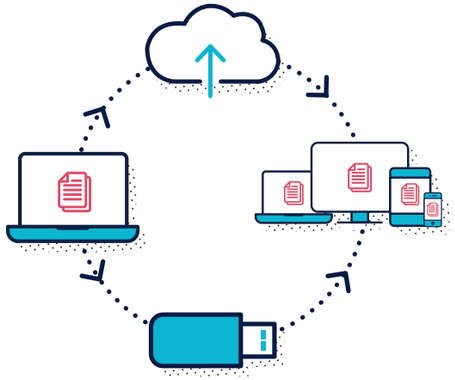
- Email accounts
- Online banking and accounts with stored payment details
- Social media

3. BACKUP YOUR DEVICES

A backup is a digital copy of the information stored on your device, such as photos, documents, videos, and data from applications. It can be saved to an external storage device or to the cloud. Backing up means you can restore your files in case your device is ever lost, stolen, or damaged.

Regularly backup your devices:

- Mobile phone
- Laptop
- Desktop
- Tablet



4. SET SECURE PASSPHRASES

In cases where MFA is not available, a secure passphrase can often be the only thing protecting your information and accounts from criminals.

A passphrase uses four or more random words as your password. Change your passwords to passphrases, making sure they are:

- Long: The longer your passphrase, the better. Make it at least 14 characters in length
- Unpredictable: Use a random mix of unrelated words
- Unique: Do not re-use passphrases on multiple accounts