

Cyber Security Awareness

Your pocket-sized
guide to staying
cyber smart
and safe.



Deaf Children Australia.

This Cyber Security Awareness Support for Vulnerable Groups grant activity received grant funding from the Australian Government.

Contents

- 01 What is Cyber Security Awareness?
- 03 Traffic Light System
- 04 Trusted Adult
- 05 6 Golden Rules
- 07 Scam Checklist
- 08 Are you a victim of Cybercrime?
/ Reporting a Scam
- 09 Step-by-step guide if you
have been scammed



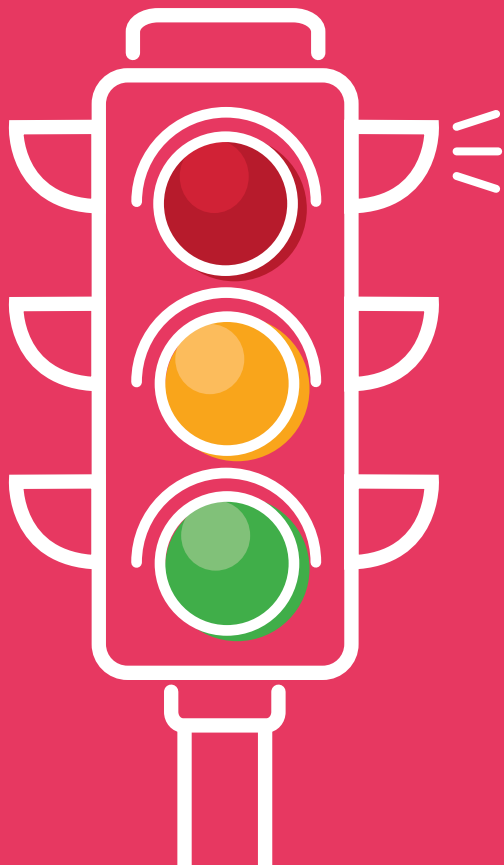
This booklet is available in alternate formats including Auslan. Scan the QR code or find the Accessible CSA Resources on our website. Please email csa@deafchildren.org.au for any assistance.

What is Cyber Security Awareness?

A stylized black icon of an eye with three short lines above it, positioned to the right of the main title text.

Being cyber secure and aware means knowing how to stay safe online.

It means protecting your personal information, so it is not stolen or misused.



Traffic Light System

Stop.

Before you click, open or respond to anything online, pause for a moment.

If something feels strange, rushed or too good to be true, stop immediately.

Think.

Ask yourself:

- Does this look real?
- Do I know who sent it?
- Is someone trying to trick me?
- Take a second to check before doing anything.

Protect.

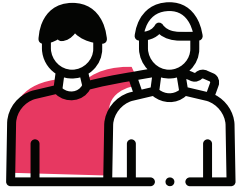
Make the safe choice:

- Tell a trusted adult.
- Don't click on any links or attachments.
- Don't share your personal information.
- Choosing the safe option helps protect you and your information.

Trusted Adult

A trusted adult is someone who:

- Keeps you safe
- Listens to you
- Helps you make safe choices



Who is a trusted adult in your life?

Is it:

- Your parent or carer
- A family member
- A teacher
- A support worker
- A coach or a mentor
- Someone who you feel safe with

6 Golden Rules



1. Be alert to the fact that scams exist.

Always be careful with unexpected messages or calls. If something feels “too good to be true,” it most likely is.

2. Know who you are dealing with.

If you only know someone online or aren't sure a business is real, check first by searching for their name or photos. Make sure they are who they say they are.

3. Do not open suspicious texts, pop-up windows, or emails. Delete them.

Delete strange texts, emails, or pop-ups. If you're unsure, search for the real contact details online, and don't use the ones in the message.

4. **Keep personal information secure.**

Keep your private info safe, like your address, documents, and passwords. Don't share too much about yourself on social media because scammers can use it against you.

5. **Keep your mobile devices computers secure.**

Use passwords, and Multi-Factor Authentication, update your devices regularly, and don't let others log in. Only use safe Wi-Fi, never do banking on public Wi-Fi.

6. **Choose your passwords carefully.**

Choose passwords that are hard to guess and different for each account. Don't tell anyone your passwords.



Scam Checklist

Not every scam has all the signs, even one is enough to be fake.

- Pressures you to act quickly
- Has a link or attachment
- Asks for personal information
- Asks for money or gift cards
- Uses scary or urgent words
- Sounds too good to be true
- Comes from an account that looks fake or new
- Comes out of nowhere
- Has spelling or grammar mistakes
- Makes your gut feeling say something feels "off"

Are you a victim of Cybercrime?



Look out for these warning signs that you may have been a victim;

- You cannot log into your account.
- You find posts or messages on your account that you did not write.
- You are missing money or notice purchases that you didn't make.
- Many strange or scam messages.
- Your device crashes or apps open by themselves.

Reporting a Scam

If you think you have been scammed, first tell a trusted adult. The website links on the back page of this booklet can help you report it with the help of your trusted adult.

A step-by-step guide if you have been scammed

Step 1

Tell a trusted adult right away.

Step 2

Do **NOT** click any links or open any attachments.

Step 3

Change your password straight away. Ask a trusted adult for help if you need it.

Step 4

Report it. Search up one of the links to help you and your trusted adult through the process of reporting a scam.

Report a cybercrime, incident or vulnerability:

Australian Government | Australian
Signals Directorate

**[https://www.cyber.gov.au/report-and-recover/
report](https://www.cyber.gov.au/report-and-recover/report)**

Report a scam:

Australian government | Scam Watch

<https://www.scamwatch.gov.au/report-a-scam>

Report online harm:

Australian Government | eSafety Commissioner

<https://www.esafety.gov.au/report>



deafchildreinaustralia.org.au

**Deaf
Children
Australia.**