Raise your voice about online abuse

Online abuse should always be reported to the relevant platforms and depending on the level of harm, you can also report to eSafety or the police.

Social media sites all provide community rules and guidelines to follow. If you or someone you know sees something that is not respectful, you can anonymously make a report and ask the site to remove it.

TOP TIP:

When in doubt, T.H.I.N.K:

T – Is it true?

H – Is it helpful?

I – Is it inspiring?

N – Is it necessary?

K – Is it kind?

Understand what is real and what is fake online

Fake news and misinformation are becoming more common and it's getting increasingly difficult to determine truthful information.

The **S.H.A.R.E** acronym can help you to determine what is real and what is fake online:

S – Check the source.

H – Headlines don't always tell the full story.

A – Analyse the facts.

R – Images or videos could be retouched.

E – Look out for errors.

For more information on online safety, visit:
www.esafety.gov.au

ACA
AUSTRALIAN
COUNSELLING
ASSOCIATION

STAYING SAFE ONLINE

A guide for Counsellors and Psychotherapists

TIPS TO TAKE CONTROL OF YOUR ONLINE PRESENCE AND SAFETY WHETHER YOU ARE IN THE WORKPLACE OR AT HOME

Security and privacy

Regularly checking your security and privacy settings is a good idea. eSafety recommends using different passwords for each online account and signing out when you're finished.

Take a moment to check the privacy settings on all your devices and digital accounts. Social media sites have privacy settings to help you control who sees your activity, who can send you messages and connection requests.

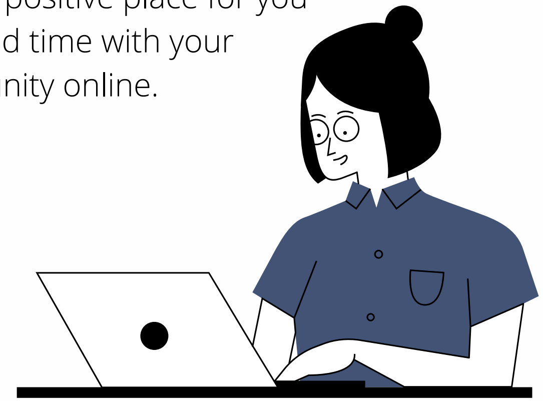
For more information on privacy settings, visit: **www.esafety.gov.au/key-issues/esafety-guide**

TOP TIP:

A strong password should include a mix of upper and lower case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.

Managing your activity

Social media sites can help you control what you can see and hear online. These conversation controls help manage your social media feeds and make them a more positive place for you to spend time with your community online.



Check your location settings

Location settings are important for map apps, social media, file sharing, connecting devices, and Bluetooth technology. You can choose when and who to share your location with. Turn these features off when you don't feel safe.

Never use public WIFI: hackers love it.

Read up about safety:
www.esafety.gov.au/women/connecting-safely/gps-location-based-services

Understand what scams may look like

Do not open suspicious emails, text messages, pop-ups windows, or click on links and attachments. Beware of any requests for your details or unusual payment requests. Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence.

Signs of a scam can include:

- a generic rather than personal greeting
- names of organisations that don't exist
- poorer quality presentation
- poorer quality grammar and spelling
- overly official or forced language.

REPORT SCAMS OR SUSPICIOUS CONTACT: SCAMWATCH.GOV.AU

ACA
AUSTRALIAN COUNSELLING ASSOCIATION