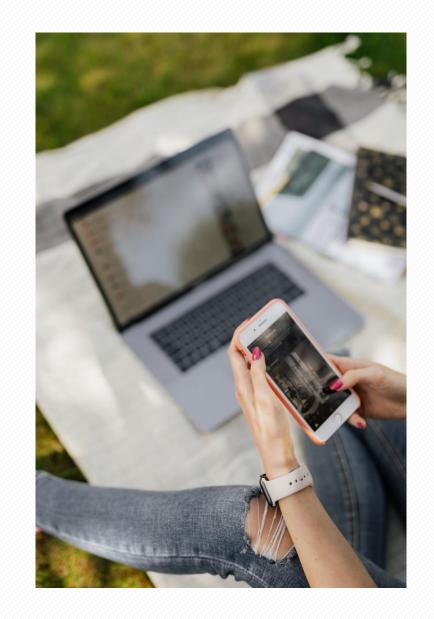
eSafety Program

Technology facilitated abuse





Acknowledgement

The Circular Head Aboriginal Corporation acknowledges and pays its respects to the traditional and continuing custodians of the lands on which we live.

Our organisation pays our respects to the Elders – past, present and emerging, and their continued cultural and spiritual relationship to the land, sky and seas.

eSafety Program

Reduced violence against women and children



In conjunction with the eSafety Commission, Circular Head Aboriginal Corporation (CHAC) is developing and rolling out culturally appropriate, place-based resources and training to address technologically-facilitated abuse as an extension of domestic and family violence.

This will enable Aboriginal and Torres Strait Islander families in our community, especially women, to identify, report and protect themselves and their children from abuse through technology.



Objectives

To increase awareness of technology-facilitated abuse and how it may be used in domestic and family violence situations.

To equip Aboriginal and Torres Strait Islander families with information on how to be safe online, and to ensure that devices and social media platforms are used safely and securely.

eSafety

Topics



eSafety Commissioner

- Who they are
- What they do



Image-based abuse



What is Technology-facilitated abuse?



Tech Tour and Tech Check-up



Reporting abuse



Seeking help & support

eSafety Commissioner

Who they are:

World's first government agency that aims to keep Australians safe online, led by Julie Inman Grant.

What they do:

Investigation of online abuse complaints and support for Australians experiencing cyberbullying, image-based abuse, and illegal and harmful online content such as child sexual abuse material, pro-terrorist content.

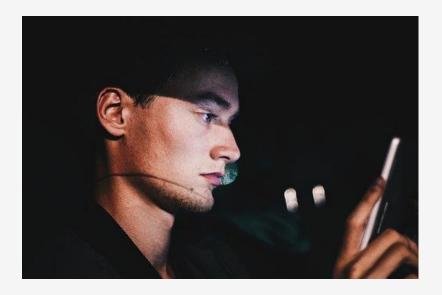
Education: free online safety webinars and face-to-face presentations.

Advice, programs and resources for educators, parents/carers, kids/young people, women, seniors, and diverse groups (Aboriginal and Torres Strait Islanders, LGBTIQ+, culturally and linguistically diverse, and people living with a disability).

What is technology-facilitated abuse?

It is a range of behaviours that involve the use of technology to:

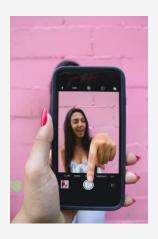
- Abuse, harass or punish
- Monitor activities
- Track location / stalk
- Control



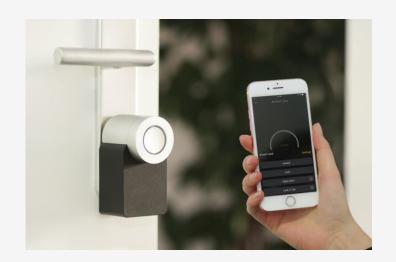
Examples of technology:

- Mobile phones
- Tablets, laptops and computers
- Wearables smartwatches, fitness bands, digital glasses, Bluetooth headphones, hearing aids and medical devices
- Automation in smart homes and in cars
- The internet, including social media and other online platforms













Examples of abuse through technology

In a domestic and family violence situation, an abusive current or former partner may misuse technology to control and punish you in the following ways:

- Bombarding you with phone calls, messages or emails
- Using social media to post abusive, embarrassing or negative comments about you
- Monitoring your devices and online accounts
- Using GPS, tracking devices, apps and cameras to track your location
- Locking you out of your devices and online accounts
- Impersonation
- Social isolation

Stalking and monitoring is a sign of serious abusive behaviour. Someone being stalked is likely to be at risk of grave physical harm.

Videos

How does technology-facilitated abuse fit within the overall pattern of domestic and family violence?

https://vimeo.com/271579285/2f5ce57b93

Facts and figures: technology-facilitated abuse

https://vimeo.com/270304304/f82b9fe12b

Red flags to look out for

- He seems to know where you are at all times
- He checks your phone logs, text messages and web browser history
- He has requested your passwords or PIN numbers
- He seems to know what you are doing online
- Your passwords and PIN numbers no longer work
- Your devices take longer to load
- There is a spike in your internet data use
- He has gifted you or your children a new phone, tablet or laptop
- He has set up security systems and cameras around the home
- He has installed a GPS tracker in your car
- A fake social media account has been set up in your name
- Unusual online activity such as emails marked 'read' or 'sent' but not by you
- Unusual financial transactions
- Unfamiliar apps on your devices

Tech Tour

https://www.esafety.gov.au/key-issues/domestic-family-violence/safety-quiz-interactive-tour/technology-tour

Tech check-up

https://www.esafety.gov.au/key-issues/domestic-family-violence/safety-quiz-interactive-tour/technology-checkup-quiz

Image-based abuse

Image-based abuse is when someone **takes**, **shares**, or **threatens** to share intimate images or videos of you without your permission. The images or videos could be real or altered, for example using Photoshop.

An intimate image or video is one that shows:

- A person's private parts (whether bare or covered by underwear)
- Private activity, for example a person undressing, using the toilet, showering, bathing or engaged in sexual activity
- A person without attire of religious of cultural significance if they would normally wear such attire in public, for example a Muslim woman photographed without her hijab.

This includes images that were taken with and without your consent.

https://vimeo.com/372982207

Reporting abuse

https://forms.esafety.gov.au/Infiniti/Produce/wizard/deob7c64

www.esafety.gov.au/media/reporting-abuse-facebook

How to take screenshots

www.esafety.gov.au/media/taking-screenshot-android

www.esafety.gov.au/media/taking-screenshot-apple-device

Help and Support

- Visit <u>www.esafety.gov.au/women</u> and <u>www.esafety.gov.au/report</u>
- ✓ For information , help and support
- ✓ Learn how to identify and report abuse through technology
- ✓ For help in removal of intimate images
- ✓ Learn how to keep you family safe from online harms
- Visit <u>1800respect.org.au</u>
- Call 1800RESPECT (1800 737 732)
- ✓ For confidential counselling, support and safety planning.

Call the Police Assistance Line on 131 444 if it is not an emergency

Call Triple Zero (000) if you are ever in immediate danger

Safety tips

- Trust your instincts
- Be alert to tracking devices and apps
- Use a safe device (a new phone, a friend's phone or a library computer) to seek help and information
- Change your password and PIN numbers often, and do not share them
- Update your privacy and security settings on your devices and online accounts
- Turn off location settings on devices and apps if safe to do so
- Install antivirus/ malware protection on your devices and maintain software updates
- Learn how to block unwanted contacts
- Always sign out or log out of online accounts, don't just exit / close the window.

References

www.esafety.gov.au/women

www.esafety.gov.au/iba

www.esafety.gov.au/key-issues/domestic-family-violence

www.esafety.gov.au/report

National Plan to reduce Violence Against Women and their Children 2010-2022: www.dss.gov.au/women-publications-articles-reducing-violence/fourth-action-plan

www.techsafety.org.au/wp-content/uploads/2019/06/4317-Wesnet-2018-Listening-Session-Report-24pp-A4-WEB-SPREADS.pdf