CIRCULAR HEAD ABORIGINAL CORP,
1O King St, Smithton TAS 7330
Phone: (03) 6452 1287
Web: chac.com.au

Session notes

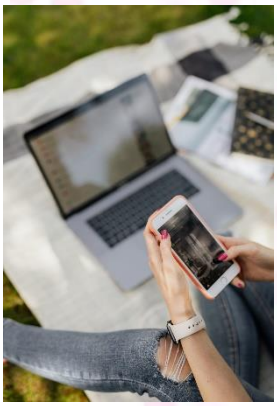
eSafety

Technology-facilitated abuse

Australian Government | eSafetyCommissioner

Supported by ***eSafety Dedicated Project Officer Grants Program-an Australian Government initiative.***

Technology-facilitated abuse



Topics

1. eSafety Commissioner: who they are, and what they do
2. What is technology-facilitated abuse?
3. Red flags to look out for
4. Image-based abuse
5. Online safety tips
6. Help and 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, and 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, threaten or humiliate
- Monitor activities
- Impersonate someone
- Track location or stalk
- Isolate someone.

Technology includes:

- Mobile phones
- Tablets, laptops and computers
- Wearables – smartwatches, fitness bands, digital glasses, Bluetooth headphones, body-mounted action cameras (Go Pros), hearing, medical devices and 'smart collars' for pets
- Smart toys with inbuilt cameras and microphones
- Automation in smart homes and in cars
- The internet, including social media and other online platforms.

Examples of abuse through technology

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

- Bombarding you with phone calls, messages or emails to abuse or threaten you
- Using social media to post abusive, embarrassing or negative comments about you
- Constantly calling and texting, demanding to know where you are
- Monitoring your devices and online accounts to see who you are talking to
- Using GPS, tracking devices, apps and cameras to track your location
- Logging in, and changing your passwords or pin numbers to lock you out of your devices and online accounts
- Impersonation: creating a fake account to harass you, or to post negative comments about you online
- Social isolation: taking away or destroying your devices to limit your communication with your family and friends.

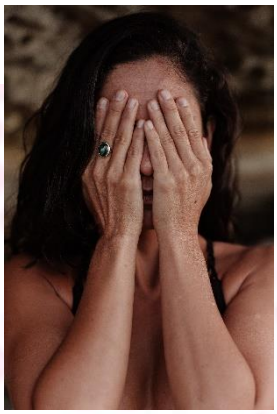
Stalking and monitoring is a sign of serious abusive behaviour. Someone being stalked is likely to be at risk of grave physical harm.

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’ but not by you, emails sent but not by you
- Unusual financial transactions
- Unfamiliar apps on your devices
- You receive messages from people you don’t know.

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.

Sexual extortion (Sextortion)

If someone is blackmailing you by threatening to share your intimate images unless you send them money, more intimate images, or give in to other demands, stop all contact with them. Take screenshots of the threats, then block them. Report them to the website or social media service. You can also report to eSafety. Call the Police on Triple Zero (000) if you are in immediate danger.

Reporting to eSafety

The eSafety Office can help to get intimate images or videos removed. In some cases, they can take action against the person who shared (or threatened to share) the images. This may include issuing a formal warning, giving an infringement notice, and seeking a civil penalty order from a court.

If you wish to report the abuse to the website, social media service, the police, or to take legal action, you may need to collect evidence before the content is removed. You can take screenshots or photos of the content on the web page.

Record the webpage addresses, social media name, and profiles/usernames of the people who shared the images or videos. You should seek guidance from eSafety before collecting evidence if the person in the image is under 18 years of age because it may be unlawful to possess, create or share sexualised images of people under 18.

Visit www.esafety.gov.au/report for more information and support.

Has this happened to someone you know?

You can support them by:

- Letting them know that it is not their fault, and that they are not alone
- Assisting them to report to eSafety
- Encouraging them to seek counselling and support from 1800RESPECT (1800 737 732) or Lifeline (13 11 14) or www.lifeline.org.au

Online safety tips

- Trust your instincts
- Be alert to tracking devices and apps
- Never leave your devices unattended and use a PIN number or password to lock them
- 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. Passwords should be hard to guess and you should have a different one for each online account or device
- 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 or close the window
- Remove unknown apps from your devices.

Help and support

esafety.gov.au/women

- For information, help and support
- Learn how to keep you family safe from online harms.

esafety.gov.au/report

- Learn how to identify and report abuse through technology
- For help in removal of intimate images

1800respect.org.au or call **1800RESPECT (1800 737 732)**

- For free confidential counselling, support and safety planning. They can also connect you to other services in your area.

Police assistance line

- Call 131 444 if it is not an emergency.

Triple Zero (000)

- If you or someone you know feels unsafe or you are ever in immediate danger.

References

- esafety.gov.au/women
- dvrcv.org.au/knowledge-centre/technology-and-family-violence