Technology Facilitated Abuse



Technology facilitated abuse is a form of controlling behaviour. It occurs when someone uses technology to coerce, stalk or harass another person.

Some examples of technology-facilitated abuse include:

- Forbidding someone from having a phone or limiting who they can contact via phone or internet.
- Sending abusive texts, emails or messages via social media.
- Making continuous controlling or threatening phone calls.
- Making someone prove where they are by sending photos of their location.
- Spying on, monitoring or stalking someone through any type of surveillance device (such as a tracking system or spyware).
- Misusing banking transaction fields to send abusive messages via low-value transaction descriptions, with the sole purpose of causing distress/harm to the recipient.

Being constantly harassed or monitored can, like any other form of abuse, leave you feeling powerless and justifiably fearful for your safety. While people of all genders can experience technology facilitated abuse, there are some people who are at a greater risk.

These include:

- Women and girls
- Aboriginal and Torres Strait Islander women
- Women from culturally and linguistically diverse backgrounds
- Women living with disability
- LGBTIQA+ people

Some signs of technology-facilitated abuse[i]:

Not sure whether you're being digitally abused? Ask yourself these questions:

Gaslighting or undermining behaviour

Does anyone create self-doubt & claim their controlling behaviours such as monitoring you are normal?

Financial abuse

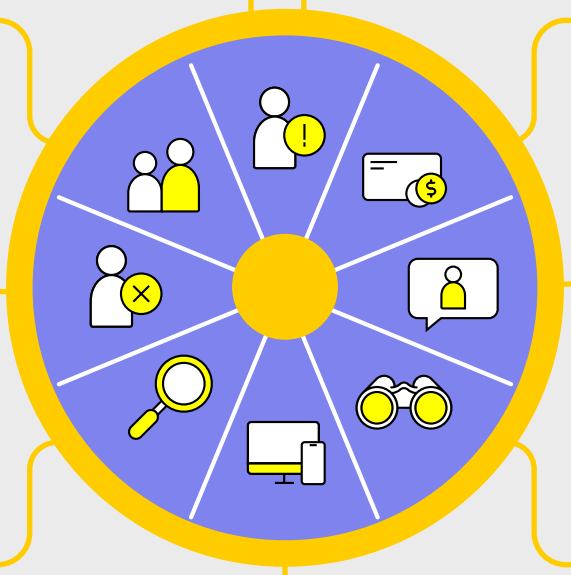
Does anyone take money out of your account without consent, limit your access to money or send you abuse in transaction descriptions?

Using children to track, control or threaten

Has anyone purchased your child a device and set it up to share the location?

Image based abuse

Has someone shared or threatened to share an intimate image or video of you without your consent?



Digital coercion

Are you being forced to share your passwords on your device or online accounts? e.g. MyGov, social media.

Using religious beliefs to cause harm

Has anyone posted an image of you without your religious or cultural clothing that you would usually wear in public?

Monitoring behaviour

Is anyone constantly calling or tracking you via:

Your phone

Your smart watch

Fitness apps

A pet's microchip

Geo-tags on social media posts

Restricting privacy

Does anyone restrict who you talk to and limit your access to devices by either damaging or destroying them?

Harassing or threatening behaviour

Does anyone in your life repeatedly message you to know:

Where you are?

Who you are with?

What are you doing?

Staying safe online[ii]:

Protect your devices

Use biometric login and change passwords and passcodes regularly on your device.

Install anti-malware protection and cover all device cameras.

Manage your security online

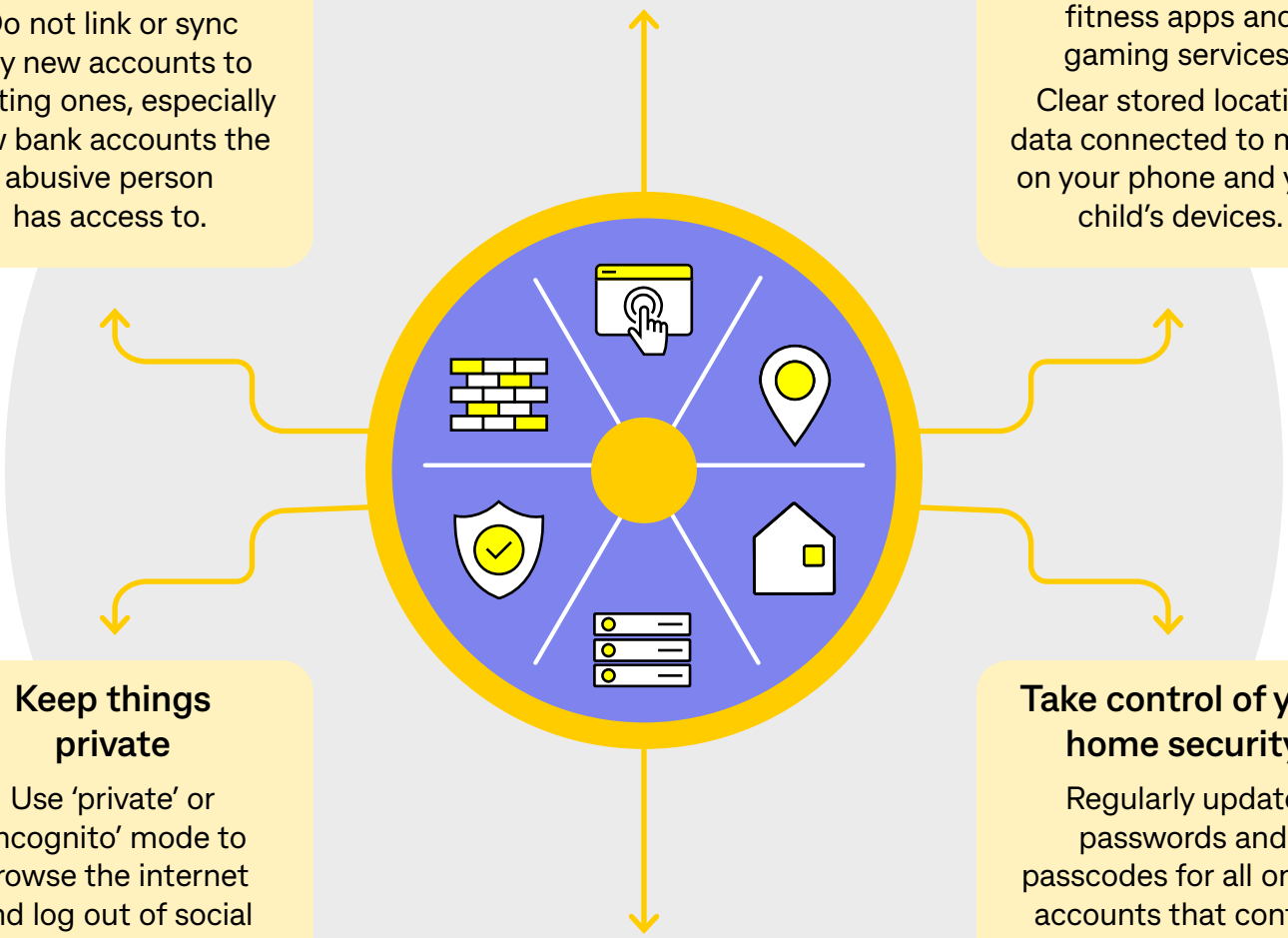
Create new accounts with strong passwords and passcodes. If possible, unlink all shared accounts and devices.

Do not link or sync any new accounts to existing ones, especially new bank accounts the abusive person has access to.

Limit ways of being tracked

Prevent or limit location tracking on devices and apps e.g. review location settings on social media, fitness apps and gaming services.

Clear stored location data connected to maps on your phone and your child's devices.



Keep things private

Use 'private' or 'incognito' mode to browse the internet and log out of social media and bank accounts after using them. Do not save your passwords or passphrases in the browser and change toll accounts such as eToll and eTag that log trips made in your vehicle.

Take control of your home security

Regularly update passwords and passcodes for all online accounts that control your household smart technologies.

Apply to Australia post for free 12-month mail redirection and check if you can provide a phone number without an address for your pet's microchip.

Manage your social media settings

Lock or restrict social media profiles from public access and limit geotagging posts.

Regularly review friend and follower lists on social media and avoid accepting requests from people you don't know.

[i] https://www.esafety.gov.au/key-topics/domestic-family-violence/coercive-control

[ii] https://www.esafety.gov.au/key-topics/domestic-family-violence/online-safety-checklist

Staying safe online[ii]

- If you are a CommBank customer and you are receiving abuse in your transactions, you can contact the CommBank Next Chapter Team on **1800 222 387** Monday - Friday, 9am-6pm, Sydney/ Melbourne time, excluding public holidays. In an emergency, always call **000**.
- If it's difficult for you to chat over the phone, CommBank customers can contact the Next Chapter Team via our online chat facility (CEBA) in the CommBank app. If you need an interpreter, you can ask for one and the CommBank Next Chapter Team will arrange one.
- For free confidential information, counselling and 24/7 support for people impacted by domestic, family or sexual violence, contact 1800RESPECT. You can contact them on **1800 737 732**, chat online via **1800RESPECT.org.au** or text **0458 737 732**.
- In a non-time critical emergency, attend your local police station or call the Police Assistance Line on **131 444** and ask if there is a specialist Domestic Violence Officer. There may also be different kinds of specialist police officers you can talk to if you are Aboriginal or Torres Strait Islander, are part of the LGBTIQA+ community or require multicultural support.
- To learn more about how you can increase your safety and privacy online, visit the Women's Technology Safety and Privacy Toolkit **https://techsafety.org.au/resources/resources-women/**.

How to get help:

If you or someone you know is experiencing technology facilitated abuse, there are free services you can access.

If you're in an emergency or if you're not feeling safe, always call **000**.

