



What is tech abuse?

People can use technology as a type of domestic and family violence. This is called technology-facilitated abuse or tech abuse.

For example, your partner or ex-partner might use technology to:

- monitor you
- stalk you
- harass or scare you
- pretend to be you or someone else.

Examples of tech abuse

Tech abuse might include when someone does any of the following without your consent:

- ✗ reads your text messages
- ✗ abuses or threatens you via messages or phone calls
- ✗ sends you lots of messages or repeatedly calls you
- ✗ checks your emails, internet browser history or social media accounts
- ✗ changes your passwords
- ✗ shares, or threatens to share, intimate images or videos of you.

Tech abuse might also include when someone tracks you. For example, they might:

- ✗ download or enable apps or software on your devices so that they can track your location
- ✗ follow you to your location and threaten to share it with other people
- ✗ check your GPS device to see where you've been
- ✗ give your child a device which has spyware or surveillance software installed.

What are some warning signs of tech abuse?



Someone might show up where you or your children are, when you're not expecting them to.



Someone might know your passwords. For example, the password for your email or bank account.



Someone might make changes to your device. For example, they might:

- change the settings
- add software or apps.



Someone might talk about information that they shouldn't know. For example, they seem to know:

- where you've been
- who you've contacted online.



You might notice strange things about your device. For example:

- new apps on your device
- that some apps on your device open automatically.



You might also notice that your device:

- turns on and off
- has different settings
- is using a lot of data
- runs out of battery quickly.



You might not be able to log into your accounts, even though you don't remember changing the password.



How can you be safer online?

There are steps you can follow to protect yourself online. You should:

- ✓ use different passwords and passcodes on all your devices and accounts
- ✓ change your passwords often – including your Apple ID or Android password, which someone can use to find your location
- ✓ set up security questions or 2-factor authentication for your online accounts.

You should also:

- ✓ download and run security software and anti-virus apps
- ✓ set your computer to automatically install updates to keep security software up to date
- ✓ check the apps on your device and know what each of them does
- ✓ uninstall any apps on your phone that you don't know.

You should protect your location.

For example, you should:

- ✓ turn off GPS or location settings on all your devices
- ✓ set your Bluetooth to 'non-discoverable'.

If you and your partner separate, you might want to consider:

- ✓ blocking or deleting their contact
- ✓ creating new social media or email accounts and only sharing this information with people you trust.

You should also:

- ✓ make your social media profiles private
- ✓ delete your web history after using the internet.

You can find more information about deleting your internet history on the [Queensland Government website](#).

Your safety is the most important thing. You should be careful if you do any of these things.

Can you just delete tech abuse?

It's a good idea to keep a record of tech abuse. The police might be able to use this information as evidence for a domestic violence protection order (DVO) or criminal charges.

The police might ask you to give them your device so they can download evidence. If you can't keep your device, make sure you save the evidence somewhere safe. For example, you could give the evidence to a family member or friend who you trust. They can keep the evidence on their device or at their house.

You might not be able to safely take screenshots of the abuse. For example, because your partner or ex-partner will get a notification if you do. You should ask a friend or family member you trust to take photos or videos of your phone or computer.

Can you apply for a DVO if you're experiencing tech abuse?

A DVO can help protect you if you are experiencing tech abuse from your partner or ex-partner. It can also help protect your children.

A DVO will always include a condition that your partner or ex-partner is *'not to commit acts of domestic violence and to be of good behaviour.'*

You can ask for specific conditions for online abuse. For example, you can ask that your partner or ex-partner not be allowed to contact or try to contact you in any way.

In court they would say:

'The respondent is prohibited from contacting or attempting to contact or asking someone else to contact the aggrieved by any means whatsoever including telephone, text or internet.'

You can also ask that they not be allowed to post pictures or comments about you online. **In court they would say:**

'The respondent is prohibited from using the internet (including social networking sites) to communicate with, publish pictures of or make adverse comments concerning the aggrieved.'

You can apply for a DVO:

- by yourself
- with a solicitor – a lawyer who can give you advice about the law and represent you in court.

The police can also sometimes apply for a DVO for you.

What to do if someone is stalking you online

Stalking is a criminal offence whether it is online or offline.

If someone is stalking you, report it to police.

You should try to give the police records of:

- emails
- text messages
- phone calls
- social media posts.

You can find more information about tech abuse on the [Tech Safety website](#) and on the [Office of the eSafety Commissioner website](#).

This factsheet includes general information only and is not a substitute for legal advice.