Online safety checklist

Our online safety checklist can help if you're experiencing tech-based domestic, family and sexual violence.

Tech-based abuse can include things that happen online or that use digital technology, such as harassment, threats, stalking and patterns of controlling behaviour.

Tech-based abuse can make you feel isolated and trapped, but you don't have to deal with it on your own. The abuse is not your fault and there is help available.

It's best to work through this safety checklist with a domestic, family and sexual violence support worker. It's a good idea to review it regularly – especially if your situation changes.

Please note the technical instructions cover most devices and accounts, but you may have to search online for more specific steps for your model or operating system. It's best to do this on a **safe device**.

A safe device allows you to make calls, send messages and go online without the abusive person knowing. This might be your phone or another personal device (if the abuser can't access it), a trusted person's device, or a computer at your work or a public library.

Put safety first

This checklist includes steps you can take to improve your safety. What is safest for you will depend on your situation. For example, whether you're still in the relationship, whether you're living with the abusive person, or whether children are involved may raise specific safety issues. You should always consider what steps are right, relevant and safe for you to take.

Talk with any children in your care about safety measures you can take together. Keep in mind the possible safety risks that may come with taking these safety measures if you share care of the children with the abuser. For example, if you plan to change the settings on children's devices, think about whether the abusive person may become dangerous and, if necessary, take additional precautions to keep you and your children safe.

If you are in Australia and feeling unsafe right now, call the police on Triple Zero (000) or contact 1800RESPECT or another **specialist counselling or support service**.

eSafety has legal powers to help you deal with the most serious online abuse, including **adult cyber abuse** and **image-based abuse** (sometimes called 'revenge porn'). You can follow our steps for reporting online abuse if it's safe to do so. We also have more information about domestic, family and sexual violence and patterns of controlling behaviour known as **coercive control**.

If you're a woman, you may also be able to access assistance through the Government funded initiative Keeping Women Safe in their Homes.

In this checklist:

Communicate safely

It's important to be careful about how you communicate because your calls, messages and emails may be checked by the abusive person. Here are steps you might take:

- [ ] Change your main contact numbers and emails if you are concerned about unwanted contact from your abuser.
- [ ] If you are in a situation where your communications are being monitored, use a safe device that the abuser can't access, such as a new or borrowed phone. You can ask your local family violence worker about programs that provide access to new phones.
- [ ] Use encrypted messaging apps (such as Signal or WhatsApp) for sensitive communication. This prevents the contents of messages from being accessed by anyone other than the sender and recipient.
- [ ] Enable features such as disappearing messages. These are features available in most messaging apps which automatically delete messages after a set period, reducing the risk of messages being seen. You can usually find these in your Privacy settings.
- [ ] If anyone has access to your device, they can see your downloads, and check your search history and previous logins by looking at your browser. To avoid this, regularly delete downloads, and clear browsing histories and chat histories. On Chrome you can go to the three dots menu button at the top of your browser and then 'Clear browsing history'. On Safari you can do this by going to the 'Bookmarks Icon' (which looks like an open book) and going to the 'Clock' icon then selecting 'clear' to delete browsing history.
- [ ] Use incognito mode or private browsing when browsing the web. This means you can use the search engine without your browser saving any of the websites you visited. On Chrome, you can find this in your menu under 'Open new incognito tab' or on Safari you can find this by choosing 'Private' on the tab on the bottom right hand corner.
- [ ] Block your calling display if you don't want your abuser to see your number when you call. You can do this by changing the settings on your phone. But be aware this doesn't always work with text messages.

Check your devices are secure

It's common for people in relationships to share access codes to devices, as well as passwords and passphrases for online accounts. This can allow the abusive person to find out who you are contacting, where you are going and what you are doing – even after the relationship ends. It may also allow them to harm you – for example they could pretend to be you on social media or could transfer money out of your bank accounts. Here are steps you can take:

- [ ] Use face ID/recognition or a fingerprint scan to access your phone and other devices including tablets, computers, smart watches and fitness trackers. This is usually done by accessing your settings and going through the 'Security' and 'Privacy' options.
- [ ] Change passwords, passphrases or passcodes on your devices, and don't allow web browsers or apps to store them for future use. Avoid using passwords and passphrases you have used before or known details such as birthdates, children's or pet's names, or favourite places.
- [ ] Where possible, enable two factor authentication, or '2FA' (also called multi-factor authentication or 'MFA') to secure your new accounts – and make sure the validation code is sent to a new email or a safe device. You can set this up by accessing your settings and going through the 'Security' and 'Privacy' options.
- [ ] Update operating systems and apps regularly, and check for unfamiliar apps or changes to device settings. This can be done by accessing your settings and going to 'Software Update'.
- [ ] Turn off wi-fi for your phone and other devices.

Check your online accounts are secure

Abusers may be able to gain access to any account you own (even if they didn't ever share it with you) then use it to track, harass and intimidate you. So, it's important to make sure all your online accounts are as secure as possible.

Avoid using your device or email for account password recovery if the abuser can access it. Make sure the device or email is secure first.

Here are steps you can take:

- [ ] Secure your online accounts and cloud storage by changing your password and log in methods. Many apps and services store your data online (also called 'the cloud') which means they can be accessed from different devices if you log in with your account. This includes emails (such as Gmail or Outlook), messaging apps (such as WhatsApp or iMessage) and photo and document storage (such as Google Drive, iCloud or OneDrive).

- [ ] Create new accounts, if possible, or unlink shared accounts. It's a good idea to create a new email account, and use this to set up and access any other new online accounts on your safe device – such as Apple IDs (and linked 'Find My' options), Google Accounts (and linked 'Find My Device' options), bank accounts, government service accounts like MyGov, social media accounts and streaming service accounts like Netflix and Stan.

- [ ] Review any accounts your children share with the abuser so you know what information they can see. Do not link or sync any of your new accounts to existing ones the abusive person may be able to access, such as 'Family' or shared accounts. This includes messaging apps, calendar apps, shared drives, photo and video albums, streaming services and subscription apps like Spotify and Netflix. If you're worried you may lose access to the content, especially shared drives and photo albums, you may need to make a separate backup on an external hard drive.

Be aware that if you leave or remove someone from an Apple Family Sharing account the abuser may receive a notification about it.

- [ ] Do not link new accounts to any bank accounts the abusive person has access to or can see statements for. Be aware when using PayID that your full name or other details such as your email address might be revealed to other people. Most banks will also reveal your full name when someone else puts your account details into an online transaction.

- [ ] Some abusers get into the other person's email account and set up mail forwarding to their own account (email providers such as Gmail, Outlook and Yahoo offer this function). This means copies of all emails are sent to the abuser without the account owner's knowledge. You can check this by going to your settings and looking for an option such as 'Forwarding', then turning off or deleting any unknown email addresses you see.

Adjust your social media settings

Abusers may also be able to gain access to your social media accounts and use them to track, harass, intimidate or impersonate you, so it's important to make sure they are secure. Here are steps you can take:

- [ ] Check to see what comes up when you search your name on a social media platform, so you can see what information is visible and change anything you don't want to be public.
- [ ] Set the 'Privacy' settings to the highest level – most platforms offer a privacy check-up to help you do this. You will need to adjust the 'Privacy' settings in both apps and web versions of your account, as they have different features, and some settings are device-specific.
  - ◯ Restrict who can see your 'online' or 'active' status.
  - ◯ Turn off geo-tagging by going to 'Disable location services' in your 'Privacy' settings, so others can't see the location where your photos or videos were taken or your posts were made.
- [ ] Review your friend and follower lists to make sure they don't include any connections of the abuser who might give them details of your activity. Be wary of accepting new friends or followers. 'Mute' your abuser if they are trying to contact you on the platform.

> **Blocking or reporting an abuser on social media might provoke them, so muting is often a better option as they are less likely to know you've done it.**

- [ ] Limit what you post and share and be wary when using tags or commenting on posts. Ask children in your care not to post photos that might reveal their movements or location.
- [ ] Consider privately asking friends not to share content about you or your children or tag you in photos or videos.
- [ ] Always sign off and log out when you have finished using online accounts.

Make sure your home is secure

If your home network and 'smart' devices are not secure, they may allow someone to monitor or control your environment. Securing your wi-fi, router and any internet connected devices reduces the risk of unauthorised access. Here are the steps you can take:

- [ ] Update the security of your wi-fi and router by changing the default username and password or passphrase. This can be changed by going to the 'Settings' for the wi-fi or router (this can be accessed through the provider's website – the default name and password is usually printed on a sticker on the back or bottom of the physical router).

- [ ] Check who can access your 'smart home' technologies that are connected to the internet. Change the passwords or passphrases and the access permissions in the settings if needed. This includes:
  - ◯ doorbells
  - ◯ smart locks
  - ◯ virtual assistants
  - ◯ smart lights
  - ◯ vacuum robots
  - ◯ pet and baby monitors
  - ◯ other devices that can be controlled from outside the home, such as air conditioners and fridges.

Collect evidence

If you suspect you are the victim of tech-based abuse it's important to collect as much evidence as you can, in case you decide to seek help from the police or eSafety. Here are steps you can take:

- [ ] Take screenshots of abusive messages, or emails, including the timestamp.

- [ ] Store the evidence in secure encrypted cloud services or hard drives hidden from the person abusing you.

- [ ] Keep a diary of incidents including dates, times and any witnesses.

- [ ] Hide apps you don't want the abusive person to see, if you have used them to save evidence. For example, you can move them to a folder that's different to where they would usually be found or give the folder a name that's not obvious.

Make sure no one is tracking you

Your location can be tracked or recorded in many ways. For example, by using location services or GPS tracking on your device or apps, through online accounts or shared accounts that show your location (such as when you check in on social media), or by using spyware or surveillance systems. If you have children in your care, you may also be tracked through their devices, apps and any services that share their location information. Here are steps you can take:

- [ ] Check your Bluetooth pairings and limit Apple 'Airdrop', Android 'Nearby Share' and Bluetooth file sharing between devices.
  - ◯ Usually on Android devices this can be done by going to 'Settings' then 'Connected Devices' or 'Connection Preferences', then 'Bluetooth'. Remove any unknown device that is paired.
  - ◯ On Apple devices go to 'Settings' then 'Bluetooth' then look at the list of 'My Devices' and tap (i) icon next to the device, then select Forget This Device.
- [ ] Check for any GPS tracking devices in your vehicles or personal belongings such as handbags. Check for unknown Tiles, Airtags or other small objects that are unfamiliar. It may be best to keep them as evidence, but make sure you store (or discard) them in a safe place away from your home or any other sensitive location.
- [ ] Check for unknown connections to your car's internal GPS tracking system by going to settings and removing any unknown Bluetooth connections.
- [ ] Electric vehicles can be set up to be controlled remotely. Check with your vehicle supplier, leasing provider or car app support helpline that the abuser has not connected their device to it. You can also check by going to app settings of your Connected App (for Tesla, Hyundai Bluelink, or BMW ConnectedDrive), driver profile settings or digital key sharing to see if any additional users have been granted access.
- [ ] Check and adjust location sharing or GPS tracking apps and services such as Find My iPhone, Google Find My Device, Samsung Find My Mobile. While this is a useful feature to help you locate a phone when lost, it can also be used by anyone with access to the related iCloud account to track the location of a device. This function can usually be turned off by going into your privacy settings and looking for 'Find My Device' or similar and toggling to 'Off' (or 'Settings' then 'iCloud' and 'Turn off Find my Phone').
- [ ] If you have children, adjust the location settings on their devices and apps.

  Make sure children are in a safe situation before changing their location settings. Please consult a domestic, family and sexual violence support worker if you are unsure.
- [ ] Turn off location tracking on apps that use it such as fitness trackers, online dating services and travel apps.
- [ ] Turn off location sharing for ride share and food delivery apps that track or log your journey or delivery location.
- [ ] Check who can access the microphone and camera on your devices. You can find this by going into your settings under 'Privacy'. In most cases you can select 'Permission Manager' then 'Camera or Microphone'. This will show a list of apps that have access to the camera and microphone. Turn off access for any app or devices you don't recognise.
- [ ] Cover your cameras with removable non-transparent tape or a sticker when you are not using them, to stop your abuser using them to watch you.
- [ ] Change login details for travel cards (such as Opal, MyWay, Myki, go card, Smartrider) if the abuser has access to any of the accounts.
- [ ] Change your electoral enrolment to 'Silent elector' if you move, so your address is not publicly available.

- [ ] Change login details for toll accounts, such as eToll and eTag, which show where trips are made in your vehicle.
- [ ] Change login details for government service accounts like MyGov and Medicare, because the claims can show where you go for medical appointments and counselling.
- [ ] If you move out, apply to Australia Post for a free 12-month mail redirection. This helps stop an abuser from opening mail that might contain details of your new location and accounts.
- [ ] If you have to update your pet's microchip details after moving, check if you can just provide a phone number without an address.
- [ ] Check for spyware on your devices such as phones and laptops. It's sometimes installed via an app or through email. An antivirus app can detect and remove existing spyware and malicious applications. Turning the device off and disconnecting from the internet or going on flight mode will stop the spyware's ability to track your location.
- [ ] Here are some signs that spyware may have been installed:
  - ◯ The battery of your device is dying faster than usual or needs to be recharged more often.
  - ◯ Your phone, tablet or computer is slower than normal or takes a long time to open programs or apps.
  - ◯ Unknown programs are operating in the background of your computer or there are unknown apps on your device.
  - ◯ You find a phone or tracking device in your home, car or personal items such as handbag.
  - ◯ Your phone notifies you that an unknown tracking device is travelling with you.

Terms and Conditions

The TFA Support Service (the Service), and the information provided through it, are provided 'as is' (and as a guide only) and are not a substitute for professional advice (whether medical, clinical, legal, technical, or otherwise). You should not rely on the Service to make any decision and you are encouraged to seek professional advice if appropriate. For more information about how the Service can be used, and its limitations, please read the full **Terms and Conditions**.