# 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 – including harassment, making threats, stalking and patterns of controlling behaviour.

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.

It's a good idea to review your online safety regularly – especially if your situation changes. You may want to work through this checklist with the support of a trusted person or a domestic, family and sexual violence support worker.

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

## Put safety first

Tech-based abuse can make you feel isolated and trapped but you don't have to deal with it on your own. It's not your fault if you're being abused and there is help available.

Your safety, and the safety of any children in your life, is the highest priority. It may be best to talk with children about the safety measures you can take together. But it's important to think about any possible safety risks the checklist steps could have, especially if you share care of the children with the abusive person. 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**.

## Use safe devices

A safe device allows you to make calls, send messages and go online without the abusive person knowing. It can also be used to collect evidence safely, if you need to report abuse to the police or get legal help.

It might be your personal device (if your abuser can't access the device or any shared accounts on the phone), a trusted person's device, or a computer at your work or a public library.

- [ ] **If you're planning to use a phone, decide if you want to get a new device, borrow a device from a trusted friend or use your existing phone** – you can ask your local family violence worker about programs that provide access to new phones. If you plan to keep your phone or device, make sure you wipe information and restore the factory settings.
- [ ] **Do not reinstall this device from a backup** – as it will bring across shared Apple IDs, Google Accounts, apps and any spyware.
- [ ] **Set it up as a new device and ensure your account is not linked to the abuser**. If you have to sign up or sign in to use the phone or another device (such as a computer, tablet, smart watch or fitness tracker), set up a new Apple ID or Google Account and use a new email address and password or passphrase, so the abusive person does not find out about it.
- [ ] **You can block the calling display** – so it doesn't show your number if you need to contact your ex-partner (but be aware that this does not always work with text messages because some mobile carriers display phone numbers in text message) – see our 'how to' videos.
- [ ] **Create a new number** – only share your new number with people you trust. Use the new phone number to verify multi-factor authentication when you set up new online accounts.

## Protect access to your device

It's common for people in relationships to share access codes to devices and passwords and passphrases for online accounts, but 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.

- [ ] **Use face ID/recognition or a fingerprint scan** to access your phone and other devices including tablets, computers, smart watches and fitness trackers.
- [ ] **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. See our advice on setting strong passwords or passphrases.
- [ ] **Install anti-virus protection software on all your devices** to help identify and block spyware and malware. Spyware, monitoring and tracking apps can reveal every call you make, every email or message you send and your browser history. This low-tech software can also tell an abuser where you have been and what you've been doing on your device, and it may be used to access the camera to take photographs or videos and record conversations without you knowing. Some signs that spyware, monitoring or tracking could be installed include the battery of your device draining faster than usual, or the device operating slower than normal.
- [ ] **Install updates as soon as available, or set to update automatically,** as these usually contain security updates.

## Manage your online account security

- [ ] **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. It's best to review your children's shared accounts too, so you're aware what information is being shared with an abuser.

- [ ] **Use strong passwords or passphrases for your online accounts**. Make sure you don't use previously saved word and number combinations or ones the abusive person might guess, such as birthdates, children's or pet's names, favourite foods, colours, singers or band names. Consider using a password manager. See our advice on setting strong passwords or passphrases.

- [ ] **Set up and use multi-factor authentication** (also called two-factor authentication) where possible, to secure your new accounts – and make sure the validation code is sent to a new email or a safe device.

- [ ] **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. 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 of it on an external hard drive.

- [ ] **Do not link new accounts to any bank accounts the abusive person has access to or can see statements for**. Also be mindful if using PayID that your full name or other details such as your email address might be revealed to other people. Most banks will also show your full name before an online transfer is initiated on an authentication screen.

## Review your social media settings

- [ ] **Adjust the settings on all social media apps and set the privacy settings to the highest level** – consider making your social media accounts private to stop your personal information and photos being shared. Many social media services make your full name and profile image publicly available online, even if you have a private account, so you may want to use a profile picture that doesn't identify you.

- [ ] **Know if your personal information is being shared** – check the privacy policy to see which third-party apps or companies might be connected to your social media accounts and remove any you don't recognise or want.

- [ ] **Review your friend and follower lists** and restrict who can view them if the option is available. Consider removing anyone you don't know well or restrict their access to what you post.

- [ ] **Be wary of accepting new friends or followers** – some abusers may use imposter accounts, or pretend to be someone else, to track or find out more information about you and what you are doing.

- [ ] **Restrict who can see your 'online' or 'active' status** – some abusers may use this to find out when to try to contact or control you.

- [ ] **Limit what you post and share** – avoid including personal details about where you are or what you're doing.

- [ ] **Restrict who can see your location** – or adjust your settings to only show a rough location. Depending on your situation, avoid 'checking in' online and consider disabling location services while not using the app or turn them off completely. Check that any photos or videos you post don't reveal your location by mistake – sometimes the background can show clues about where you are, like street signs.

- [ ] **Turn off geo-tagging or metadata when posting or sharing photos and videos** – not all social media services remove metadata attached to an image (such as location and device information), so check before sharing or posting, because this could reveal your location.

- [ ] **Be wary when using tags or commenting on posts** – tagging social media photos and posts could reveal your location, while tagging companies, comments made on public posts and hashtags can generally be seen by the public, even if you have a private account.

- [ ] **Consider privately asking friends not to share content about you or your children or tag you in photos or videos**, to protect your privacy and location. This is especially important if they are online followers or friends with the abusive person.

- [ ] **Turn off read receipts** – these are notifications that allow people to know when you have read a message and indicate when you are (or have been) online.

- [ ] **Block intimate images or videos from being uploaded to specific platforms** – you need a copy of the image or video, but you don't need to send it to the platform – you can use an online tool to create a digital 'fingerprint' (or 'hash') and submit it through the free online tool StopNCII.org. This will stop your image or video being shared with StopNCII partners, such as Facebook, Instagram, TikTok, Bumble, OnlyFans and Reddit.

## Keep your online history private

- [ ] **Use 'private' or 'incognito' mode to browse the internet and regularly clear your browsing history.** This will help to hide the websites and information you have visited (if malware is not being used to track it in some other way).

- [ ] **Remember to not save your passwords or passphrases in your browser** (and make sure to remove any that are already saved) as they may allow an abuser to access your online accounts through a shared device, a child's device, or if they were able to access your device while it was unlocked.

- [ ] **Always sign off and log out when you have finished using online accounts** like social media, email accounts and online bank accounts. Don't just close the window, because the abusive person might be able to reopen it. Also make sure you log out of any accounts or services that are connected to each other, such as both Facebook and Facebook Messenger.

- [ ] **Check to see what comes up when you search your name and contact details online** – you can also check reverse phone lookup websites to see if a search of your phone number reveals any other details about you. You may be able to submit a request to search engines such as Google or Bing, asking to remove or hide URLs with your information, or remove images or videos from search results.

# Protect your location information

Your location can be tracked or recorded in many different 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 location information.

If you think the abusive person could be tracking your location through your devices or accounts, read the following information about the signs and advice for limiting tracking. Follow the steps for yourself and any children in your care, if they are safe for your situation.

If you're still worried you're being tracked, consider leaving your devices at home when you go out, if it's safe to do so – especially if you're going to a support agency, lawyer, friend or to the police for help.

## Signs that someone may be tracking you

- 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 or car that does not belong to you.
- Your phone notifies you that an unknown tracking device is travelling with you.

# How to limit the ways your location can be tracked

- [ ] **Prevent or limit location tracking on devices** – make sure the default mode on any location, map, navigation or GPS feature is set to 'switched off' and only switch it on when you need to and it's safe. You may also be able to control your device privacy settings to hide your location. If these devices are controlled by online accounts, update the passwords or passphrases, enable multi-factor authentication and ensure they are not linked or synced with the abuser.

- [ ] **Clear stored location data** connected to map, navigation or GPS devices, and delete your search and trip history. Do not set your actual home address as 'home' unless it's safe to do so.

- [ ] **Customise apps that use location services** – customise location settings including on social media, messaging apps, travel and restaurant guides, online dating apps and games. Adjust the settings to only use location services when the app is in use, avoid checking in on social media, and consider setting your location to private or hiding it completely. See more about reviewing your social media settings.

- [ ] **If you have children, adjust the location settings on their devices and apps too**, if it's safe to do so.

- [ ] **Adjust Bluetooth settings** – only turn on Bluetooth when you are pairing a device or sharing a file and make sure no-one else can access your paired devices. If possible, use a PIN or code when pairing wearables (like fitness trackers) with your device. Remove any devices from the list if you don't recognise them, or if you no longer use them or have them in your possession.

- [ ] **Limit Apple 'Airdrop', Android 'Nearby Share' and Bluetooth file sharing between devices**. If you are sharing content, like files and photos, only turn on the service when you need it and only accept invitations to share from people you know.

- [ ] **Review Apple ID 'Find My' and Google Account 'Find My Device' options**. If you haven't already, consider setting up a new Apple ID or Google Account, especially if these accounts were shared or linked with the abusive person. At the very least, change the passwords or passphrases for these accounts if it's safe to do so.

- [ ] **Review linked or shared accounts for fitness tracking devices** – restore the device to factory settings, set it up as a new device and, if possible, use a new account to log in. At the very least, change the password or passphrase for any accounts linked to fitness apps. Only share your fitness data, which may reveal your exercise routine, with trusted friends and family.

- [ ] **Check your online accounts like bank accounts and store cards that reveal your location when purchases are made** – use cash or limit the use of bank cards or store cards to protect your location from being tracked. If possible, set up new accounts and ensure the statements are not shared with your abuser.

- [ ] **Avoid travel cards and bank cards that register when you tap on and off public transport** – these can reveal your location or actions, especially when seeking help. Consider using single trip tickets. Make sure any new cards are password protected and not linked to your abuser's accounts.

- [ ] **Change toll accounts, such as eToll and eTag, which log trips made in your vehicle** – contact these agencies to create your own accounts and have your vehicle removed from these records. Make sure they're not linked to your abuser's credit or debit card.

- [ ] **Check ride share and food delivery apps that log your journey or delivery location** – make sure you only use these services if your accounts are not shared or linked with your abuser. Consider setting up new accounts or setting the address to a nearby address where you can be dropped off or pick up a delivery. Turn off location-services once you have finished using the app. Do not sign-in to these apps using your social media accounts.

- [ ] **Change log in details for Government service accounts like MyGov and Medicare that record trips to medical appointments and counselling services** – if you haven't already, apply for new cards and online accounts in your name.

- [ ] **If you have to update your pet's microchip details after moving, check if you can just provide a phone number without an address**. Ask the registry or your local council to confirm it will keep your personal information private, so it's not shared. Support services are also available for people whose animals are being threatened or have been hurt or abused within domestic and family violence, such as Lucy's project.

- [ ] **Change your electoral enrolment to 'silent elector' if you move**. Your name and address is publicly available on the Australian electoral roll, but you can ask to be listed as a 'silent elector' if your personal or family's safety is at risk. Visit the Australian Electoral Commission website to submit an application.

- [ ] **Apply to Australia Post for a free 12-month mail redirection if you move** – this is available for special circumstances.

- [ ] **Cover your cameras with removable non-transparent tape or a sticker when you are not using them, to stop your abuser using them to track you** – this includes the front and back cameras on your phone or other devices or any computers or linked webcams. You can also buy specific cases to cover your camera on a phone or device.

## Take control of your home security

- [ ] **Check who can access your smart home technologies, such as speakers and virtual assistants** – these can control things like televisions, lights, heating, air-conditioning, curtains or blinds in your home. Update the passwords and passphrases for all online accounts that control these smart technologies.

- [ ] **Make sure you have access and are in control of home security systems including alarms, digital locks or surveillance systems**. Also make sure they are working properly and have not been disabled – this is especially important if the abusive person set up the system. If you're no longer living with the abuser and it is safe to do so, update all passwords, passphrases and access codes and any online accounts they are linked to, and change them regularly. Make sure that only you, the police or ambulance services can access or override your security system.

## More tips

For more information on updating your device, social media, apps and online account settings see The eSafety Guide and our 'how to' videos.