Domestic Violence Prevention Centre

Resource One

Establishing Technology Safe Behaviours

- Establish a password on ALL your devices or change them if you already have them – phone/laptop, social media accounts etc. Use passwords that are new, long, unique, and unpredictable.
- Do the big clean: This means checking ALL your privacy settings on your devices and apps including social media. Most devices and apps now have locations associated; however, you can make your social media private only and DO NOT accept invitations to share with anyone you don't know. If you want to confirm that are who you think they are, follow up with a phone call as fake accounts are a common strategy. Ensure you are not on shared accounts for calendars and photos etc. Ensure you have location settings off and turn off blue tooth. Disconnect the GPS with your maps where you have a linked account.
- Clean up your apps by deleting those apps you don't need and keep only what is essential. Ensure you have privacy settings on, that you have not shared the app, and that you have updated the details with your safe phone number and email.
- Engage in smart operating by watching what you post, by not sharing location details, or advising when you will be away. Always think things through before you post.
- Do NOT open attachments or click on links from unknown users or download files you don't know where they have originated.
- If you find an app on your device you don't recognise, remove it.
- Ensure your webcams can not be activated without you knowing by putting on a webcam protector to cover the camera when you don't want it on.
- If you are ever in doubt, turn off your phone or put in airplane mode as this stops your phone from connecting to the network and stops an app from transmitting your location. Please note that aluminium foil has NO effect.
- Third parties that you have bank accounts and credit cards with need to confirm with you that they aren't shared so they won't reveal your location or patterns. Make sure you update your details with government suppliers and update your privacy settings with doctors, chemists, work and school.
- For extra security, use MultiFactor Authentication or MFA as this enables an added layer of security by sending you a text message with a number as well as your password. This is best established when you have a stable phone number to rely on.
- If you are concerned about spyware on your device, be sure that you can reset your phone to factory settings and this will remove all your settings including your photos, text messages, contacts, and any saved passwords, and so you can be sure there is no spyware on your phone when you restore to factory settings. You can then re-establish your phone. Make sure you have made a backup away from your device of ANYTHING you want to keep as there is no going back after a factory reset.
- If you are concerned about tracking devices check what is in your bag and car by taking a good look. If it is an apple tracker, you can search using your apple phone or by downloading the Tracker Detect app from an android. This will scan your area and detect any apple tracker device that is travelling with you. You can then activate a sound so you can find it.
- A new you: consider establishing a new email, a new computer, a new phone and/or phone number and new social media accounts. You could establish new accounts, or you could reformat your current devices, whatever feels right for you.

Gold Coast or Beenleigh region:
Free counselling, support, information and referral for women and their children who have or are experiencing domestic and family violence. Phone: (07) 5532 9000 (9am–4.30pm, Monday to Friday) · **info@domesticviolence.com.au**