FACTSHEET FOR E-SAFETY

If you think you are being followed, stalked or controlled online, here's what you can do:

Use a safe device Search for help, do your banking and any safety planning or personal chats on a different device. Do not use your own device. Use a library computer or a friend's or family members' device that your partner will not check or have access to.

Ditch the device If you think the abuser is tracking your location through your device, leave the device at home as often as you can, particularly if you are going to an agency, friend or to the police for help. Trust your instincts on this.
If possible get a new phone. Even basic or older phones will let you make calls. Get a prepaid service or make sure the bill is in your name so it does not go to the abuser. Make sure they can't find it.

New accounts Create a new email account that does not feature your name, for example use whitelillies@email.com, but not YourRealName@email.com. Use this email to set up and for safety planning.
Use this new email for all safety planning such as setting up any new bank accounts or contacting Centrelink. If you need to use another email to verify your identity, use a trusted friend or family member's email and avoid any emails or phone numbers your abuser may have access to.

New passwords Create new passwords for all new accounts that will not be obvious to the abuser. Do not use birthdates, children's or pets' names, favourite foods, colours or singers. Using two words together with numbers or symbols (*&^) in the middle of the words can work well. If you are worried you may forget your new passwords leave a list of them at a safe place, like a trusted family member's home.

Be selective with future contacts On social media, only add 'friends' you can trust not to communicate with the abuser. Activate the privacy settings on your social media accounts.

Passcode all devices Add a new passcode to your phone or tablet and set Auto-Lock to one or two minutes. Add passwords to computers and laptops.

Sign off and log out Always log off or sign out of social media and email accounts rather than just closing the window, and make sure the privacy settings on social media are private.

Don't let him know where you are Turn off location settings and services on your phone and devices and do not post your location or photos on social media.

Technology can help Install anti-virus protection on all your devices as this can help block spyware. Find out more at Stay Smart Online.

Check your child's device Make sure all of this is done for your children's devices as well as yours, especially if the abuser has given a device to them as a gift.

Is spyware being used? Spyware can tell abusers every call you make, every email or message you send and every place you take your device. It can be hard to know if an abuser has installed spyware on your device. Some signs are:

- the battery of your device is dying faster than usual
- unknown programs are operating in the background of your desktop
- your speeds are slower
- your abuser knows a lot about what you are doing, where you are, who you are talking to online, through emails, texts and calls.

If you think spyware is on your device, use a safe device for all important correspondence. If possible get a new device, even if it is a very old or basic model.

Provide copies of court orders to every Government agency you use. This includes MyHealth, MyGov, Medicare, DSS, Child Support and Centrelink. Ask these agencies to provide written confirmation that your private details will not be accessible by the abuser, particularly if the abuser is your child's father and is able to access some information about the child.
Do the same with banks, schools, childcare, kindergartens and preschools, sporting clubs and any other place your child attends.

Change your electoral enrolment to 'silent elector' The Australian Electoral Commission (AEC) is able to put you on the electoral roll or update your details based on information from other government agencies. This means that your address is publicly available and can be easily accessible.
By becoming a silent elector only your name and division will appear on the roll. You can apply to be registered as a silent elector if you believe that having your address shown on the publicly available electoral roll could put your personal safety, or that of your family, at risk.
To do this you should go to the Australian Electoral Commission website and fill out the applicable form for your State. Information regarding any protection orders or any police reports may be helpful.

Pets If you are leaving an abusive relationship and taking any pets with you, consider if you are the registered owner. If you are, contact the registry and/or your local council to confirm or update any contact details and flag your situation.

Check all accounts Check credit card or direct debit payments that may give away your location. Accounts such as eToll and eTag and public transport travel cards may be linked to the abuser's credit or debit card. Contact these agencies to have your car and cards removed from the accounts so the abuser can't track your movements.

More technical information about installing anti-virus software and protecting your devices is available at smartsafe.org.au.