- Use this list to protect yourself against spyware & covert surveillance
- · Make sure you keep this list somewhere safe
- If you are unsure how to do any of the below steps, Google it on a safe device or get the help of a trusted friend, family member or social worker

What is spyware? Spyware is malware that can be installed on devices such as computers, tablets & smart phones to secretly monitor a person's private information. Spyware may access keystroke logging (all typed information), photos/videos, social media accounts, Apps, contacts, notes, browsing history, call logs, text messages, email, location, activate your camera, microphone or record calls. It may be used to delete things off your device, block certain websites or numbers & may be remotely deleted.

OII	your acvice, bloc	ok certain websites of	numbers & may be ref	notely deleted.	
1	General precautions	Don't leave your devices where they can be easily	PIN / password protect devices, change passwords	Log out of & close devices/apps/ accounts after use	Don't open suss email attachments or .exe files
	•	accessed by others	••••• △		
	Update device software	Always use private browsing	Set up new email on safe device	Don't use personal details in usernames, emails or passwords	Set up 2-step verification on accounts where possible
	C		\sim	RUPERT	8
•	history. Downlo	ng can be used on all co pads will still be saved	& need to be manually	es. It won't save passwo deleted if you are cond any identifying features	erned.
	Change				
2	device settings	Turn off location settings	Turn off cellular data	Turn off Wi-Fi	Turn off Bluetooth
	(C)			\tilde{m}	*
•	You may need	to change the setting	on your children or fan	ff these settings increas nily member's devices. to change these settings	•
	Look for				
3	suss	USBs or hard drives in computers or keyboards	Look for anything unsual around your house, car, wallet, bags, keyring etc	Check new or unfamiliar objects/ things you were given	Cover cameras on devices with tape
		H		T	

- Cameras, microphones & tracking devices can be hidden in everyday objects like clocks, chargers, bags, toys, jewellery or rear view mirrors. Some GPS trackers are small tiles or magnets.
- Keystroke logging can be done through external devices that may look like a USB or hard drive.
- Mechanics or Police can sometimes sweep a car if you think a GPS tracker has been installed.

Review your Apps & accounts



Delete any Apps, accounts & software you don't need or recognise



Limit what you & others share about you online



Upgrade privacy & security settings in Apps & accounts you keep





Check "mail forwarding" & "SMS forwarding" is not set up on your email or device





Some Apps allow you to upgrade security settings for two-step verification, notifications of logins on unknown devices & to show recent login times & locations. Facebook allows you to download your data.

Make your devices safer

5



Do a factory reset



Install anti-spyware Apps & software on all devices



Consider getting a new device



Update the settings on your new/safer device



- A factory reset is usually effective, but isn't a 100% guarantee to remove Spyware. Google how to back up contacts, photos & messages if you're unsure. Be careful what you restore when using a backup - don't restore all Apps.
- Changing a SIM card on a device won't remove spyware. Getting a SIM & a new number is still a good protective measure to keep you safe. To keep your number private, hide caller ID in your phone settings.
- Did someone give you the device? Some devices can be purchased with spyware in-built so it can't be removed. Consider getting a new phone.
- Escaping domestic violence? Call 1800-WESNET to see if you're eligible for a free safe phone.
- Do some research on anti-spyware & anti-virus software. Talk with an IT specialist or look for reviews on reputable websites.

WARNING SIGNS YOUR DEVICE MAY BE INFECTED WITH SPYWARE

Device battery draining faster than usual



Device constantly checking for location



Device switching itself on & off



Unexplained spikes in data usage



Changes to your device, e.g., Apps, emails, SMS





Unexplained activity on your social media or email

Unable to call certain numbers. access websites



Warning signs for iPhones & iPads

- Some spyware requires an iPhone or iPad to be "jailbroken" to operate.
- If jailbroken, an App called "Cydia" may be installed on your device. It can be hidden so it's not visible on the device.
- Search for "Cydia" in Spotlight. If you find Cydia, your phone has been jailbroken without your knowledge.
- Spyware may be in installed inside Cydia with a name like "IphoneInternalService" (MSpy).

Precautions to increase safety on an iPhone or iPad

- Update your iOS this may remove jailbreaks & increase security.
- Turn off iCloud backup. iCloud may be used to spy remotely where the phone is not jailbroken.
- A factory reset is the most effective way to remove a jailbreak on an Apple device.
- Consider taking your device to an Apple Genius bar to be checked.





SuperUser

icon

Warning signs for Android devices

- Some spyware attaches to your Android's security settings as a Phone Administrator. Look around these settings (go to Settings > Security > Device Administrators) & your Apps for anything strange.
- Some spyware requires "rooting" on an Android device for full access to your installed Apps. Sometimes an App called "SuperUser" is used for rooting. Search your device for "SuperUser" or "SU." Free "root checker" Apps can let you know if your phone is rooted. Often your device's operating system will not be able to update when it is rooted.
- Some spyware can be uninstalled through security settings. E.g., Mspy may be uninstalled in Phone Settings > Security > Device Administrators > Update Service > Deactivate > Get back to Settings > Apps > Update Service > Uninstall.
- A factory reset will not unroot an Android device. Google how to do this or get assistance from your Service Provider.

Learn more about online safety at www.esafety.gov.au

For free legal advice about technology-facilitated stalking or abuse, refer clients to Legal Aid NSW's Domestic Violence Unit on (02) 9219 6300

