






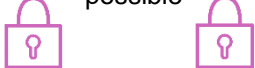
tipSHEET

SPYWARE CHECKLIST

- 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.

1 General precautions

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Don't leave your devices where they can be easily accessed by others	PIN / password protect devices, change passwords	Log out of & close devices/apps/ accounts after use	Don't open suss email attachments or .exe files
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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
				

- See the **Password Checklist**.
- Private browsing can be used on all devices including phones. It won't save passwords or your browsing history. Downloads will still be saved & need to be manually deleted if you are concerned.
- Set up a new email address on a safe computer. Don't use any identifying features in this email address (e.g., your name, year of birth).

2 Change device settings

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Turn off location settings	Turn off cellular data	Turn off Wi-Fi	Turn off Bluetooth
				

- Spyware needs access to the internet to operate. Turning off these settings increases immediate safety.
- You may need to change the setting on your children or family member's devices.
- Visit www.smartsafe.org.au for instructional videos on how to change these settings on your device.

3 Look for suss objects

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	USBs or hard drives in computers or keyboards	Look for anything unusual around your house, car, wallet, bags, keyring etc	Check new or unfamiliar objects/ things you were given	Cover cameras on devices with tape
			  	 

- 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.

