MOBILE SPYWARE

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of August 2022.

Safe phone/device

When searching for information or calling for support we recommend using a phone/device you do not suspect is monitored. This could be a public library, support worker or a trusted family member or friend's phone or computer.

National Sexual Assault, Domestic and Family Violence Counselling and Information – 1800 RESPECT

If you suspect someone is monitoring you using technology, the abusive person may also be making you feel unsafe in other ways. If you would like to explore support options available, you can contact 1800RESPECT by phone (1800 737 732) or online chat (24 hours) from a safe phone or device. If you have a support worker, it may be helpful to discuss the monitoring and technology abuse with them and incorporating into your support and safety plan.

Safety Planning

Before acting, please consider how the person may react if you remove their ability to monitor you. You may wish to discuss this with a support worker and incorporate removing access into your safety plan.

I am concerned that spyware is on my phone. Is this possible?

For spyware to have been placed on your phone, it is most likely that someone would have needed physical access to the device. There have been instances of remote introduction of spyware onto a device (in the context of domestic violence), but the chances are much greater in circumstances where the abuser has had physical access to the device. It should also be noted that those who own an Android device have a greater risk of having their device remotely infected than those who own an iPhone. Therefore, it is possible but unlikely that spyware has been introduced remotely (particularly if the user did not click suspicious links or visit compromised websites).

If someone did have physical access to your phone, and they knew your passcode, it is *possible* that spyware may have been placed on your phone. This article, however, will help you identify whether that is *likely,* and what steps can be taken to help identify and potentially remedy possible threats.

What is spyware and what can it do?

This document considers "mobile spyware" to refer to an app or program that is deliberately placed on someone's mobile device for the purpose of monitoring that person.

Depending on the type of spyware installed, in most cases, mobile spyware will monitor:

- Call history, including phone number, date, and length of call
- Text messages, including phone number and SMS content
- Contacts
- Internet browsing, including history and bookmarks
- Location of the phone
- Photos taken on the phone

- Email downloaded onto the phone

If the phone has been jailbroken (iPhone) or rooted (Android), spyware software can monitor more, including:

- Certain messaging apps, such as WhatsApp, Viber, Skype
- Phone conversations
- Using the phone's microphone to record the phone's surrounding

It is difficult to easily identify whether spyware has been installed. Closer inspection of the phone from a trusted analyst with the suitable expertise to subject the phone to data-traffic analysis or digital forensics could provide more confidence on whether the device has been compromised. Finding such an expert can be an issue.

Once the software is installed, the abusive person can monitor all the above activity via an online website.

If it's not spyware, what else could it be?

There are several methods by which a person can track or monitor the activities of another person using technology other than Spyware. Monitoring information on Facebook, for example. Similarly, if a person can login to the iCloud or Google account associated with the phone, information from the phone can be accessed that may include location information. Many phones have functions such as "Find My Phone" that can be used to locate the owner of the phone. Within the context of this document, we do not consider these to be "spyware". It is recognised, however, that these can be a problem from the perspective of tracking and stalking. For information on how to address those issues, please see information available in the WESNET Women's Technology Safety and Privacy Toolkit. [www.techsafety.org.au/resources]

I own an iPhone. What are the risks of spyware on iPhones?

If you have an iPhone 6 or higher and have been regularly updating the iOS (operating system), the likelihood of spyware being on your phone without your knowledge is UNLIKELY. But again, please keep in mind that apps other than spyware may be revealing signs of your location or activities.

If you have an older iPhone model or have not been updating your iOS on a regular basis, the likelihood of spyware being on your phone without your knowledge is still largely unlikely. In this circumstance, the risk of spyware being on your iPhone without your knowledge is more likely if (a) someone had physical access to your device, (b) that person was aware of your device passcode, as well as your Apple ID login and password.

If you are in the circumstance whereby another person does have access to your physical device, your device passcode, as well as Apple ID login details, and you have reason to believe spyware is on your device, please contact WESNET from a safe device for further information on spyware. [email techsafety@wesnet.org.au]

I own an Android. What are the risks of spyware on phones that use the Android operating system?

(This includes phones by Samsung, Sony Xperia, Google Pixel, Huawei, LG, HTC, Nokia, etc)

The Android operating system is more vulnerable to spyware being placed on someone's device without their knowledge compared to iPhone. Unfortunately, it is also easy for a non-expert user to conceal traces of spyware on Android devices. If you are in the circumstance whereby another person does have access to your physical device, your device passcode, and you have reason to believe spyware is on your device, please contact WESNET from a safe device for further information on spyware.

Can I take my phone to the shop where it was purchased or to a local 'tech expert' to check for spyware?

There are certain forms of spyware that could be easily identified by an in-store, consumer retail outlet 'tech expert'. But there are also forms of spyware that would require a more forensic examination that is not readily available to individuals who work in computer or smartphone stores.

Depending on your situation, if the stalking/surveillance through spyware is just one part of the abuse you are experiencing you may wish to seek support from a family violence service to put a safety plan in place, or you may want to contact 1800RESPECT for advice.

I have strong reasons to believe that spyware is being used against me right now. What can I do right now to protect myself?

If you do not have the time or opportunity to seek support regarding spyware but have reasons to believe that spyware is tracking you, there are some provisional, emergency steps you can take to protect yourself.

- Consider using another phone or device for communication or other activities (such as searching for support services) that you would like to keep private. Continuing to use the phone in this way can be helpful if you do not want the abusive person to know that you suspect spyware is on the phone.
  (Note: As a precaution, we recommend having conversations (on another device or in-person) that you would like to keep private, out of earshot of the device as some spyware may be able to record the surroundings of the phone).
- Also keep in mind that spyware can monitor location, so you may want to be careful about where you go with the phone. If you take the phone to the police, the abuser may know that the phone is at the police station, for example, so think through of any safety issues that you might need.
- Spyware will only communicate information whilst the phone is turned on and is connected to the internet. Therefore, turning off the phone will allow temporary relief from GPS tracking or any danger of the camera capturing pictures, audio, or video.
  - (Note: Turning on 'Aeroplane Mode' or 'Flight Mode' is also likely to temporarily prevent the spyware from tracking your phone. However, there are rare circumstances under which this mode can be faked, and the phone may still be tracking your data despite being in 'Aeroplane Mode' of 'Flight Mode'. We recommend turning off Wi-Fi and Bluetooth before selecting this option.).
- If it is safe to do so, performing a factory reset on your device, ensuring the operating system is up to date and changing your Apple ID/iCloud or Google login passwords might rid the device of the spyware. This will work for many types of spyware but not all. (Hence why seeking further information from WESNET is advisable). A family violence support service will be able to assist you with considering if you would like to preserve evidence, how the abusive person might react if you remove their ability to monitor you, and help you develop a safety plan.
- As a measure of last resort, purchasing a brand-new phone should remove the threat of spyware. (However, if purchasing a new Android device, avoid automatically reinstalling apps from your app library and see additional settings below). Your new device should be free of spyware, but it is strongly advisable to change your iCloud/Apple ID or Google login passwords.
  - (Note: On Android phones, check the security settings and disable "allow installation from unknown sources" and select "verify apps" to assist in preventing spyware from being installed).

Grateful Acknowledgement

This information has been compiled by three researchers, Dr Diarmaid Harkin, Dr Adam Molnar and Ms Erica Vowles, who spent several months testing spyware apps on Android and Apple phones, in order to

determine what level of surveillance such apps enable, and the threat posed to phone users. This information is up to date as of August 2022. This document was developed in conjunction with representatives from WESNET and funded by ACCAN. *The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.*

Read this article for more information on Android phone privacy and security.
Read this article for more information on iPhone privacy and security.
Read this article for more information on Smartphones and location strategies
Read this handout for Computer Spyware and Safety