BC Society of Transition Houses

Mobile Spyware

The content of this information sheet does not constitute legal advice. The information contained below is current as of September 2019 and discusses what can be done in BC if you believe that mobile spyware has been placed on your phone or device.

Safe phone/device

If you suspect that your phone or device is being monitored, use a phone/device you believe is safe when searching for information or calling for support. This could be a computer at a public library, an anti-violence organization or a trusted family member or friend's phone or computer.

If you suspect someone is monitoring you using technology, the perpetrator may also be making you feel unsafe in other ways. If you would like to explore support options available, you can contact VictimLink BC at 1-800-563-0808 from a safe phone or device. If you are receiving support from an anti-violence worker, it may be helpful to discuss the monitoring and technology-facilitated violence with them and incorporate a response into your safety plan.

Safety Planning

Before taking action, please consider how the perpetrator may react if you stop or limit their ability to monitor. When discussing a safety plan, you may wish to discuss with an anti-violence worker the possible reactions if you remove access to the perpetrator and build specific safety measures into your safety plan. For information about strategies for enhancing safety plans for technology-facilitated violence see BCSTH's technology safety planning guide.

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

For spyware to be placed on your phone, someone would need to have physical access to the phone or know your iCloud password.

If someone had physical access to your phone, and they knew your password, it is conceivable that spyware was placed on your phone. This information sheet will help you identify whether that is likely, and what steps can be taken to help identify and potentially remedy the spyware monitoring.

What is spyware and what can it do?

"Mobile spyware" refers to an app or program that is deliberately placed on someone's mobile device to monitor that person. Mobile spyware is a category of stalkerware. Stalkerware is defined as "all spyware that is explicitly sold or licensed to facilitate intimate partner violence, abuse, or harassment,

inclusive of deleteriously intruding into the abused partner's private life by way of physical or digital actions[1]."

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 content
- Keystrokes that have been typed
- Contacts
- Internet browsing, including history and bookmarks
- Location of the phone
- Photos taken on the phone
- Emails downloaded onto the phone

If the phone has been jailbroken (iPhone)[2] or rooted (Android)[3], 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 can be difficult to identify whether spyware is installed, since most spyware products operate in "stealth" or hidden mode, so the products cannot be detected on the phone.

Once the software is installed, the perpetrator can monitor all the above activity via an online website or an App.

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

There are other ways that a person can track or monitor the activities of another person using different technology such as:

- Monitoring information on Facebook

---

[1] 2019 Citizen Lab, "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry," by Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert.

[2] Jailbreaking means bypassing the restrictions Apple puts on the operating system and taking full control over an Apple device. Rosencrance, Linda (2017). 10 Pros and Cons of Jailbreaking Your iPhone or iPad. Retrieved https://www.tomsguide.com/us/pictures-story/537-jailbreaking-iphone-pros-cons.html

[3] Rooting is the process that allows you to attain root access to the Android operating system code. Bullguard. (n.d.) "The risks of rooting your Android phone." Retrieved https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/android-rooting-risks.aspx

- Logging into the iCloud or Google account associated with the phone which accesses sensitive information including location
- Using phone functions such as "Find My Phone" to locate the owner of the phone. These built in capabilities advertised as helpful tools can also provide location tracking in the context of criminal harassment (stalking) for example.

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 unless the perpetrator has access to your iCloud password.

If you have an older iPhone model, **or have not been updating your iOS on a regular basis**, the risk of spyware being on your iPhone without your knowledge is possible if: (a) someone had physical access to your device; (b) that person was aware of your device password, as well as your Apple ID login and password; and (c) your iOS is not able to be updated to the latest version.

If another person does have access to your physical device, your device password, as well as Apple ID login details, and you think spyware is on your device, please contact your local anti-violence organization to develop a safety plan.

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.)

Compared to an iPhone, the Android operating system is more vulnerable to spyware being placed on someone's device without their knowledge. It is also easy for a user to conceal traces of spyware on Android devices. If you think another person does have access to your physical device, your device password, and you believe spyware is on your device, please contact your local anti-violence organization from a safe device for further information on spyware and safety planning.

I think that spyware is being used on my phone or devices right now. **What can I do to protect myself?**

If you do not have the opportunity to contact an anti-violence organization, but have reasons to believe that spyware is monitoring you, here are some temporary, emergency steps you can take to protect yourself.

- Consider using another phone or safe device for private communications or other activities such as searching for support services. Continue to use the suspected monitored phone for "public" activities until it is safe to check the device for spyware. This combination can be helpful if you do not want the perpetrator to know that you suspect spyware is on the phone.

As a precaution, have private conversations on another device or in person out of earshot of the suspected device, as some spyware is able to record the sound in the area surrounding a phone/device.

- Also, keep in mind that spyware can monitor location, so be careful about where you go with your phone. For example, if you take the phone to the police, the perpetrator may then know that the phone is at the police station. Think through any potential risks and how to plan for safety.

- Spyware will only communicate information while the phone is turned on and is connected to the internet. Turning off the phone or turning on 'Airplane mode' will allow temporary relief from GPS tracking or any danger of the camera capturing pictures, audio, or video.

  However, turning on 'Airplane mode' or turning off the phone is only a temporary measure to prevent the spyware from tracking your phone. Once 'Airplane mode' is disconnected and the phone is turned back on, the spyware will access the activities (for example, a photo taken) and location that occurred while it was in Airplane mode and/or disconnected. Consideration should be given as to when you can safely turn your device back on.

- 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. Seeking further information from your anti-violence organization is advisable. An anti-violence organization will be able to assist you with: 1) how to preserve evidence if necessary; 2) how the perpetrator might react if you remove their ability to monitor you; and 3) developing a safety plan.

- Consider using a reputable anti-virus or anti-malware program to detect and remove spyware. ***Some*** spyware programs can be detected and removed using these programs.

- 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 require a more forensic examination that is not readily available to individuals who work in computer or smartphone stores and may require consultation with an anti-violence organization.

- As a last resort, purchasing a brand-new phone should remove the threat of spyware. However, if purchasing a new Android device, avoid using the full back up from the old device when setting up the new one and change your Google login passwords on a safe device. If you have

an IPhone, changing your ICloud password should be sufficient unless there are additional ways (desktop computer and key logger) in which the perpetrator is monitoring you.
    - 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.

- For more information, see the BC Society of Transition Houses (BCSTH) Technology Safety and Privacy Toolkit https://bcsth.ca/technology-safety-project-resources/

Adapted from and in cooperation with the Technology Safety Project at The Women’s Services Network (WESNET), Australia. Special thanks to Christopher Parsons, Citizen Lab, Munk School of Global Affairs & Public Policy; Dr. Diarmaid Harkin, Deakin University; Dr. Adam Molnar, Deakin University and Ms. Erica Vowles, Deakin University.