Mobile Spyware Concern Tips Guide

Compiled by the Clinic to End Tech Abuse

Last Updated: August 17, 2020

This guide presents tips that may be useful for you if you are concerned about mobile spyware.

What is spyware?

“Spyware” or “stalkerware” means an app that was designed to let someone else get information about you without your knowledge.

For example, spyware could let someone else see your location, your photos, or what you type on your phone.

How can I check for signs of spyware?

- ❏ Check the logos of all of the **apps installed** on your device.

  Are there any apps you do not recognize?

  If so, you may want to delete those apps.

  However, **please be aware that if someone is using an app to monitor you and you delete that app, the other person could realize right away that you have done this.**

  If you are worried that deleting an app could make your situation more dangerous, we strongly recommend talking to a domestic violence organization or other appropriate organization first.

- ❏ Check for **“dual-use” apps**

  There is a category of apps we call **dual-use apps** that can have legitimate uses, but that someone else could also potentially use to monitor you.

  Examples of these types of apps are Google Maps and Find My (iPhone). These apps are not spyware, but they could let someone else track you or get information about you.

We recommend that you go to the Settings menu on your phone and check the permissions those apps have. (For example, can the app get access to your location? Your camera?)

You can also check the app's settings to see if the app is set to share your location or other information with someone else.

Also, we recommend checking for apps that could allow remote access (access to your phone from another device), such as Team Viewer.

If you are worried about a "dual-use" app, you can try uninstalling it or turning it off. You can also change the app's settings.

❏ Consider if your phone could be **jailbroken** or **rooted**

"Jailbreaking" or "rooting" a phone is a type of phone hack in which someone changes the phone's basic security protections and permissions.

If a phone is jailbroken or rooted, this can make it easier for someone to install spyware or other harmful software on it.

If the person you are worried about has had physical access to your phone, they may have been able to get it jailbroken or rooted. On the other hand, if you have a new phone and the person you are worried about has never had physical access to it, the risk that the phone is jailbroken or rooted will be far lower.

Unfortunately, there is no easy way to find out if a phone has been jailbroken or rooted.

If you know your phone is jailbroken or rooted, or you're worried that it might be, we recommend getting a new phone if possible.

❏ Are you on a **family phone plan** with the person you are concerned about?

If you are on a family phone plan with someone you're concerned about, the phone plan could give that person access to information about your calls, texts, and location.

Some family phone plans also let adults on the account install tracking apps on phones that are on the plan. These apps are sometimes called "parental" apps and are usually intended to let adults monitor children. However, adults can also misuse them to track other adults.

You may want to check to see whether one of your phones or tablets, or a child's phone or tablet, has a tracking app from a phone company installed on it.

Some states have laws designed to help abuse survivors leave family phone plans. You may want to ask a lawyer or domestic violence organization in your area for more information about this.

What else can you do to protect yourself against spyware?

- ❏ Check for **software updates**

  Apple, Google, and Microsoft regularly release updates to the basic software that makes your phone, tablet, or computer run. This software is called the "operating system." For Apple devices, it will usually be iOS, iPadOS, or macOS. For Samsung, Google, LG, Motorola, Nokia, and Xiaomi devices, it will usually be Android. For other devices, it will usually be Windows.

  These system updates often include important security protections. We recommend that you install updates whenever they are available.

  Some apps will also ask you if you'd like to update them. If you think an app is legitimate, we recommend that you use the most up-to-date version.

- ❏ Install an **antivirus app** on your devices

  Antivirus apps are able to scan your phone or computer and notify you if they find spyware, malware, or adware installed. They can also alert you if a website you are visiting may be dangerous.

  There are several different antivirus apps available in the Apple App Store and Google Play Store, such as AVG Antivirus, Avast Antivirus, Kaspersky Mobile Antivirus, ESET Mobile Security & Antivirus, McAfee Mobile Security, and Malwarebytes Security.

  Using an antivirus app can help make your device safer. We recommend using an antivirus app if you can.

  However, be aware that antivirus apps will not necessarily flag a "dual-use" app as dangerous (see above). Spyware can also still be a risk even if you are using an antivirus app.

- ❏ Check the security of your **accounts**

  The person you are worried about could be getting information about you from one of your online accounts, instead of from spyware.

For example, if someone else guesses the password to your iCloud or Google (Gmail) account, this could give them access to your location, photos, calendar, emails, notes, or iMessages, depending on the type of account and the settings you're using.

We have guides to checking the security of your accounts and adding extra protections on our website: https://www.ceta.tech.cornell.edu/resources.

❏ Consider the **phone reset** option

Resetting the phone means changing the system and its settings back to their default state (the settings the phone had when it was first used).

This is sometimes called a "factory reset," since it's supposed to change the phone back to the way it was when it first left the factory.

Before doing a phone reset, we recommend backing up any information you want to save. You can back up your information by copying the information stored on your phone to another device such as a laptop.

Or, you could back up your information using an app like iCloud or Google Drive that can move your data to the cloud. This process may take a few hours depending on the amount of data you want to save (pictures, videos, chats etc.).

However, if the person you are worried about has access to your iCloud or Google account, they could see any information you back up there. This is also true for any other backup app.

It is important to highlight that, on a jailbroken or rooted phone, the phone reset option may not wipe out all spyware.

- If you have an **iPhone**:

  Go to Settings > General > Reset. Tap Erase All Content and Settings.

  https://support.apple.com/guide/iphone/erase-all-content-and-settings-iph7a2a9399b/ios

- If you have a phone running **Android**:

  Reset via Android settings:
  https://support.google.com/android/answer/6088915?hl=en

  Reset via power and volume buttons (Samsung example):

https://www.samsung.com/nz/support/mobile-devices/how-do-i-perform-a-hard-factory-reset/

❑ Consider switching to a **safer device**

If you are still concerned about mobile spyware, another option is to switch to a safer device. By “safer device,” we mean a different device that the person of concern has never been able to touch.

Please note that if the problem is not spyware, but rather that someone else is getting into one of your online accounts, then using a different device probably will not fix the issue. We recommend checking the privacy and security settings of all your accounts, changing your passwords, and turning on two-factor authentication (extra security).

You can find guides to making your account more secure and turning on two-factor authentication by going to our website: https://www.ceta.tech.cornell.edu/resources.