What is Spyware and Stalkerware?
Spyware or stalkerware refers to tools - apps, software programs, and devices - that let another person (such as an abuser) secretly monitor and record information about your phone activity. The term ‘stalkerware’ is a more recent term that draws attention to the invasive, intrusive, and dangerous misuse of these tools.

Phone spyware can be especially intrusive and dangerous for survivors, because it can monitor many things you do on your smartphone, including photos and videos you take, websites you visit, text messages you send and receive, your call history, and your location. Spyware installed on rooted (for Android) or jailbroken (for iPhone) devices can allow someone to turn on the webcam or microphone, take screenshots, see activity on third-party apps (such as Snapchat or WhatsApp), and intercept, forward, or record phone calls. (A rooted or jailbroken phone removes the protections that the operating system and phone manufacturer put on the phone. It is possible to find out if your phone has been unlocked without your knowledge, which could offer a hint that spyware may have been installed.)

Almost all phone spyware requires that the person have physical access to the device to install. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove. To access your phone activity, the person monitoring the device signs in to a website or accompanying app on a different device.

How Do I Find Out if Spyware is On My Devices?
Detecting spyware on your phone may be difficult. Some signs could include your battery draining rapidly, your device turns off and on, or spikes in your data usage. However, the most common sign that your activity is being monitored will be because of the abuser’s suspicious behavior. For example, they may know too
much about your phone activities without another explanation. Trust your instincts and look for patterns. If the abusive person knows too much about your phone activity or knows things that you’ve only done on your phone, it’s possible that spyware may be on your device. A trained professional may have to check the device to know for sure.

Responding to Spyware
Safety first. Before acting to find or remove the spyware, it is important to consider safety and the possibility of collecting evidence. Many abusers use spyware as a way to monitor and control survivors. Some abusers may escalate their harassing and abusive behavior if they suspect that the survivor is cutting off their access. Before removing the spyware, think through your safety as you consider ways to protect yourself, and talk with an advocate about safety planning. If you need an advocate, please reach out to the National Domestic Violence Hotline.

Gathering evidence. Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence needed for a criminal investigation or civil legal action. Their forensic tools may be the only way to determine for sure if spyware is on the device. Read more about Spyware Evidence.

Removing spyware. In most cases, a factory reset can remove the spyware. Be cautious of reinstalling apps or files from a backup or the App or Play Store as that might inadvertently re-download the spyware app. Manually add the apps or software that you want back onto the phone. You may also want to take the step of creating an entirely new iCloud or Google account for your device, and using that account to download apps. If you choose to do a reset, it’s critical that the phone not be connected to the backup to reinstall apps, contacts, photos, etc. When that happens, it’s incredibly likely that the spyware would reinstall too.

Use devices that aren’t being monitored. If you suspect that spyware is on your device, remember that most of your activity, including conversations, could be
revealed to the abuser. If you can, use a safer computer or phone – one the person has not had physical or remote access to, such as a computer at a public library, community center, or a friend’s phone – when you look for help or information.

**Update accounts.** Since spyware would have given the person access to your login information, consider resetting your passwords on a different device and no longer accessing certain accounts from the phone you are worried about as a way to keep them out of the account. Also consider changing passwords to sensitive accounts such as online banks, social media accounts, etc. Read more about [Password Safety](#).

**Preventing Spyware**

**Consider access.** Be cautious if someone wants to update or fix something on your phone and trust your instincts if you don’t trust their intention. If someone did have access, consider if it coincided with increased monitoring or stalking. Beware of gifts of a new smartphone or tablet from an abuser to you or your children.

**Lock your phone.** Because most spyware requires physical access to the phone to install, place a passcode lock on your phone (and don’t share it) to minimize the risk of someone installing spyware. Many devices allow you to choose between a number, pattern, thumbprint, or other security features. Read more [Phone Security Tips](#).

**Use anti-virus and anti-spyware protection.** Download anti-virus and anti-spyware apps to your phone; these apps can help either prevent spyware from being installed or scan your phone for malware or spyware apps.

**Use security features on your phone.** Most Android phones have a setting that allows installation from unknown sources. Turning this off will minimize the chances of apps outside of the Google Play store from being installed on the phone. Another feature on Android phones is to turn on Google Play Protect,
which will scan for apps with malware and viruses, which can protect the phone from most spyware. In addition, always install the latest operating system updates for your phone, which often include security patches.

**Do not root (for Android phones) or jailbreak (for iPhones) your phone.** Many of the more invasive spyware features don’t work unless the phone is rooted or jailbroken. On iPhones, most spyware cannot be installed unless it is jailbroken. A rooted or jailbroken phone will be more vulnerable to viruses and malware and make it easier for spyware to be installed.

**Not Spyware?**
There are many other methods someone can use to access information on your phone without installing spyware. If the abusive person has physical access to the phone, they may not need to install spyware, which is mostly for remote access.

Many of the apps and accounts on phones can be accessible from another device if the abusive person knows the username or email and password. Phones can also be monitored through the iCloud account for iPhones and Google account for Android phones. Increase the security of those accounts by ensuring that no one else knows the username and password.

Sometimes, an abusive person knows too much because of friends and family members. Look for patterns in what the person knows and where that information might have come from to help you to narrow down the possibilities. An advocate can help you figure out what may be happening and plan next steps.

© 2019 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.