Mobile Spyware:
Identification, Removal, and Prevention

What is mobile spyware

Mobile spyware is software that can be installed onto a mobile phone that will allow someone else to remotely monitor activities on the phone. (Note: mobile spyware is slightly different from computer spyware. Read our *Computer Spyware and Safety* handout for more on computer spyware.)

Depending on the type of spyware installed, in most cases, the 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

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

How do I identify if mobile spyware has been installed?

It is difficult to identify whether spyware has been installed, since most spyware products operate in "stealth" mode, so it cannot be detected on the phone. The best way to identify whether spyware has been installed is for a forensic examination of the phone to be completed, often by police.

If it is not possible to get the police to do a forensic examination, some clues that spyware might have been installed include the following.

Physical access to the phone

All of the commercially-available spyware products requires someone to download the software and run the installation. This can be the abusive person or someone who is installing the product on behalf of the abusive person. It is generally difficult for the user to accidently install the software since this is an active process. The installation process generally requires 15-20 minutes to install.

Abusive person's knowledge

Another clue that perhaps spyware might be installed is if the abusive person knows more than they should and that knowledge encompasses the activities listed above that spyware monitors. Because spyware monitors a wide range of activity, the assumption is that abusive person will know all of that information. If the abusive person knows less information than spyware provides or more information than spyware provides, they might be gaining that knowledge from another source.

Strange activity on the phone

In some cases, because spyware is running on the phone, you may notice increased battery usage or data usage. If the phone has been jailbroken or rooted, the phone is less secure, which could result in faulty type behaviour on the phone, such as the phone shutting down or consistent dropped calls.

How do I remove mobile spyware?

If you suspect that spyware is on the phone, and your goal is remove the spyware, you can reset the phone to factory setting. This should remove the spyware from the phone, since for it to be reinstalled, the installation process needs to re-occur. The best option is to get a new phone.

For further security, it is best that backups or SD cards from the previous version of the phone not be installed on to the new phone.

How do I preserve evidence of mobile spyware?

It is illegal to install spyware on devices for the purpose of spying or stalking another person. If you choose to remove the spyware, it will also remove the evidence. If your goal is to preserve the phone for evidence, it is important to work with local police, who may have a specific process on analysing mobile phones for evidence purposes. Until you speak to the police, it is best to put the phone in airplane mode and keep the phone's battery charged.

Think about your safety

If you suspect that spyware has been installed, be aware that certain activities on the phone are being monitored, and you may not want the abusive person to know that you suspect spyware is on the phone. Talking about the spyware in text message, phone calls, in email, or near the phone might alert the abuser that you know. Also keep in mind that spyware monitors 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.

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

There are many other products that is similar to spyware, such as parental monitoring programs. Unlike spyware, most parental monitoring programs are visible on the phone, meaning that you can see that some type of monitoring service is running on the phone. Go through your phone to see if an app was installed without your knowledge. There are some parental monitoring programs that are hidden and can't be seen by scrolling through the phone's apps. In this case, resetting the phone to factory setting should also remove the parental monitoring program.

Also think about whether the abusive person may have access to your accounts, such as the iCloud or Google account, email, the telco account (and your phone bills), or other social media app that might be tracking your location. Having access to those accounts could also give the abusive person similar knowledge to spyware.

How do I prevent spyware from being installed?

- Since installing spyware requires physical access to the phone, the most important thing is to put a passcode on your phone to prevent someone from being able to get into your phone.
- On Android phones, disable "allow installation from unknown sources" under Settings / Security.
- On Android phones, select "verify apps," which scans apps for malware. Depending on the type of phone you have, this is under Settings/Security or Google Settings/Security.
- On iPhones, make sure that it is running the latest operating system.
- As a general security practice, go through apps on your phone and delete apps that you no longer use. Although spyware is hidden and won't show up as an app, removing apps that you don't use is generally a good habit.