BC Society of Transition Houses

Mobile Spyware: Identification, Removal and Prevention

WHAT IS MOBILE SPYWARE?

Mobile spyware is software or an app that can be installed onto a smartphone that will allow someone else to remotely monitor activities on the phone. (Note: mobile spyware is slightly different from computer spyware. Read our 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[1] (iPhone) or rooted[2] (Android), spyware software can monitor more, including:

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

Once the software or app is installed, the perpetrator 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 or if she does not want to involve the police, some clues that spyware might have been installed include the following.

[1] Jailbreaking a mobile device context, is the use of an exploit to remove manufacturer or carrier restrictions from a device such as an iPhone or iPad. (https://whatis.techtarget.com/definition/jailbreaking)

[2] Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.

- ***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 perpetrator or someone who is installing the product on behalf of the perpetrator. 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.

- ***Perpetrator's knowledge***
  Another clue that perhaps spyware might be installed is if the perpetrator 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 perpetrator will know all of that information.

- ***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 to 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. This is not guaranteed and phones do have the capacity to keep data that has been "reset "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 analyzing smartphones 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 perpetrator 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 perpetrator 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 perpetrator 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 are 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 perpetrator may have access to your accounts, such as the iCloud or Google account, email, 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.

Adapted from and in cooperation with the WESNET Safety Net Australia project at the Women's Services Network, Australia