Intelligence and Investigations
GII-PII LLC
If the information is out there, we will find it.

Cell Phone Spyware Protection 10-Step Guide

Cell phone spyware is a very real and present danger. It is powerful, easy to install, and allows unlimited access to your private information.

Someone can access all your texts, passwords, photos, emails, and locations without your knowledge from anywhere in the world.

Cyber-spies can look through your cell phone camera, listen through your microphone, and upload all your data to an offsite server. You won't even notice until it's too late.

Spyware makes you vulnerable to the following cyber-attacks!

- Tracking Location
- Stealing Call Logs
- WhatsApp Spy
- Social Media
- View Contents
- Ambient Listening
- View Photos/Videos
- World Wide Web
- Read Texts/SM
- Record Calls
- Email Spy
- Read Notes

The smartphone has become one of the most important tools used daily for many of us. It tracks your movements, displays emails and text messages, and notifies you of every birthday and appointment. Every second, information floods your smartphone. Unless you switch them off, your apps work round-the-clock, obeying your every setting and preference.

Your phone collects private data all day long, and if criminals can break into it, they can steal all kinds of things, from banking details to compromising photos and videos. And they don't have to steal your phone to do it.

Spyware is kind of like a computer virus, except instead of messing up your hard drive, it enables strangers to spy on you. Skilled hackers can install spyware on your phone without you even realizing it.

Here are 10 steps you can follow to protect against spyware attacks on your cell phone.

#1 – Don't click on strange links

The easiest way to avoid downloading spyware is this: Don't click on strange links. If you receive an email from a suspicious stranger, don't open it. If you receive an email or text from someone you do know, but the message seems peculiar, contact your friend by phone or social media to see if the message was intended.

This might sound obvious, but sometimes our curiosity gets the better of us. When a link appears, some of us struggle to avoid clicking, just because we want to know where it leads. Other times, an authentic-looking email is actually a phishing scam in disguise. If you're the least bit doubtful, don't click.

#2 – Keep your phone locked

Though some phones are more susceptible to spyware than others, owners can dramatically reduce their chances of infection by locking them. A simple PIN number will deter most hackers. This is one of the easiest steps you can take to safeguard your device.

Also, avoid lending your phone to strangers. Yes, some people honestly forget their chargers at home and urgently need to call their spouses, but a clever con artist needs your unlocked phone for only a minute to cause a lot of damage. In this case, being a Good Samaritan is risky business.

#3 – Avoid unsecure free Wi-Fi in public

Unsecured free wi-fi, which is common in public places such as airports and cafes. If you log onto an unsecured network, the bad guys can see everything you do while connected. Pay attention to warning messages your device may give you, especially if it indicates that the server identity cannot be verified. Protect yourself by avoiding such unsecured connections.

#4 – Keep your phone operating system up-to-date

Operating system (OS) flaws, which creates exploits that could let attackers infect a mobile device. Smartphone manufacturers frequently release OS updates to protect users, which is why you should install updates as soon as they are available (and before hackers try to infect out-of-date devices).

#5 – Avoid misleading or untrusted mobile apps

Malicious apps, which hide in seemingly legitimate applications, especially when they are downloaded from websites or messages instead of an app store. Here it's important to look at the warning messages when installing applications, especially if they seek permission to access your email or other personal information. Bottom line: It's best to stick to trusted sources for mobile apps and avoid any third-party apps.

#6 – Don’t Root or Jailbreak your mobile device

To jailbreak your phone is a hack that seems to promise free apps, extra features, and better performance. Also called rooting (which is the same thing), it instead removes essential security features from your device, leaving you vulnerable to stalkers, hackers, and thefts.

It is important that each installed app can only read its own data and cannot access the data of other apps. Otherwise, they could obtain encryption keys, passwords, or your personal information. You would need to trust all your apps with all the data in your phone—an unnecessary and dangerous undertaking.

Additionally, rooting makes it easier for others to manipulate the software on your device, for example, by accessing its operating system when you plug it into somebody else’s USB port.

Your personal information would be entirely exposed, leaving you without privacy or any control of your data.

#7 – Turn off your Bluetooth

Do the words: bluebugging, bluejacking, or bluesnarfing sound familiar to you?

These words refer to a circumstance where an individual (hacker) can get access to your devices via your Bluetooth connection. Once they are within 25 – 30 feet of your device, a bluejacker can access your data and private information in seconds. So please, unless you absolutely need to use your device’s Bluetooth, turn it off. Just be aware these methods are not using commercial spy apps – they are forms of hacking and are illegal.

#8 – Remember to log out

While it may seem extremely convenient to have your device always logged into eBay, Amazon, PayPal, your personal bank account, or any other online shopping service; this is an extremely dangerous practice. Your phone should never be left logged into any website that is directly connected to your finances.

If your device gets stolen, not only are you losing your phone, you are also giving someone unhampered access to your funds. To avoid this, simply uncheck any checkboxes that ask to remember your password, username or login information.

This advice is also applicable to your web browser as well. You should try not to give your browser permission to record/save your login information to sensitive websites. Periodically clearing your browser’s history is also recommended as well.

#9 – Use an antivirus/security software

Your smartphone is literally a small handheld computer. As a result, it is susceptible to a lot of the same types of virus/malware attacks and risks. Even the most “tech savvy” individuals will consistently update their computer’s antivirus security, while their smartphone gets zero antivirus protection.

Virtually all smartphones (over 90% of them) come shipped with **no antivirus software at all** (not even a trial version). Additionally, very few smartphone owners even think about the malware risks that their devices incur, and they don’t go through the trouble of getting security software such as an antivirus.

Now, a common question is – **will antivirus programs find spy software**? It leads to a lot of debate – but the simple answer is that you can’t rely on them to find spy programs. Antivirus and security apps can only find what they are programmed to find, and the spy companies are not their top priority. They also stay a step ahead by changing and hiding file names. Still having the extra protection is worth it.

#10 – Disabling location tracking

Location technology is helpful when looking for the nearest gas station, but it can also enable others to retrieve information about your whereabouts, legally or illegally. One method of location tracking involves the use of wireless signals to triangulate your position between cell towers. Another method uses the GPS radio on your phone to pinpoint your location. A third method uses the Wi-Fi hot spot to which you're connected to approximate your current position. If you suspect you're being tracked using your cell phone, disabling any of these features can help prevent tracking.

Turn off the cellular and Wi-Fi radios on your phone. The easiest way to accomplish this task is to turn on the "**Airplane Mode**" feature. This shuts down both your cell radios as well as the Wi-Fi radio installed inside your phone so that neither of them can connect to their respective networks.

Disable your GPS radio. Some phones have this as a stand-alone setting, while others bundle it into menus like Privacy or Location Settings. Turning off location-based features on your phone can prevent your GPS from being activated, which in turn keeps it from providing your phone's location.

#11 – (BONUS) Factory reset your phone

If you have been able to locate the spyware software present, but do not have any kind of access to it, then you can simply take your phone to your nearest service center to have the technicians take a look at, and factory reset your phone; of course, you need not worry about your phone's safety as they will safely and efficiently backup all personal data present on your phone that needs to be backed up. Factory resetting your phone thus ensures the safe deletion of the spyware software.

Tip: if your phone has been rooted, be aware that attempting to factory reset your phone yourself could result in “Bricking” your phone. If this happens, your phone is as good as dead and will no longer work. Use caution.

Are you a victim of cell phone spyware?

The GII-PII Remote Extraction Machine will scan, identify, and remove dangerous spyware from your cell phone to keep you safe. The process is quick, inexpensive, and your phone never leaves your possession. Let us protect your private and confidential information from digital criminals.

For a GII-PII Professional Spyware Safe Scan,

Contact 812-291-6034 or visit GII-PII.COM