We are licensed to scan and remove spyware from mobile devices. We can also assist you in backup your device and reset completely. Advise upon consultation for future awareness and best practices . Call us on 08 1888 1888 or mail us on service@calltech.co.za www.calltech.co.za

Mobile device Spyware

Cell phones usually store a great deal of personal data that trace back over the last couple of years.

You probably use your cell phone on a daily basis to: send text messages and emails; store voicemails; send pictures or videos to friends, your family or partner; browse the internet and social media - the list goes on and on.

What if someone had access to all of your personal data? That would be an absolute disaster.

But, why would someone spy on you? There could be multiple reasons for someone to spy on your phone.

Perhaps your phone contains important business data that a spy wants to know about, or a spouse wants to find out about a potential affair, or you're very wealthy and someone wants to hack into your checking account.

Maybe you have an important job or one with a lot of responsibility. For example, scientists, journalists, judges or other government workers could all be potential targets for the bad guys.

So, how do you know if someone is spying on your cell phone, and what can you do about it?

Unfortunately, even a strong login password on your phone is not going to protect you from harmful spies. And there are plenty of spying apps on the market that can monitor all of your cell phone activity without your knowledge.

In this guide, I'll provide you with 10 ways to tell if someone is spying on your cell phone and how you can stop them.

How to Tell Whether Someone is Spying on Your Cell Phone

There are a few signs that should ring the alarm bells and could point to the possibility of your cell phone being infected with spy software that is either tracking or monitoring your activities - or both.

The signs vary and some are hard to spot. However, if you're aware of the typical signs, it's not that difficult to determine whether there's spy software installed on your device.

Here are 10 ways to tell whether or not your phone is being monitored.

1

Abnormally High Data Usage

Is your monthly data usage unusually high? Then there's a decent chance someone has installed a spy app on your device.

Generally, lower-quality spy software tools use a significant amount of data to send the collected information from your cell phone.

On the other hand, the top-notch spy software on the market requires much less data to send the information collected from your phone. It's nearly impossible to see if a high-end spy app is installed on your device on your monthly data usage overview.

2

Cell Phone Shows Signs of Activity in Standby Mode

Aside from standard incoming calls, messages and other standard notifications that trigger activity on your cell phone, your cell phone screen should not be lighting up in standby mode.

Also, unexpected noises or sounds should ring the alarm bells that something is wrong.

3

Unexpected Reboot

Does your cell phone reboot without an obvious reason, or without you making it do so? In that case, it's not unlikely that someone has unauthorized, remote access to your cell phone.

And, if someone has remote access to reboot your device, it would surprise me if that were the only thing they could do or see.

4

Odd Sounds During Calls

In the past, phone lines were not always stable and without any weird background noises.

However, today's networks usually have a strong signal and stable connection. Therefore, it's not normal to hear odd clicking sounds or distant voices interrupting your conversations.

If you are hearing voices in the distance, and you are sure it's not someone close to the person you're talking to, there's definitely a possibility that your conversation is being tapped.

5

Unexpected Text Messages

Have you received any odd-looking text messages?

Typically, a message that contains a variety of weird symbols, random numeric sequences or other characters points to the possibility of a potential spy software tool on your cell phone.

Poorer-quality spying software uses this kind of "code language" to communicate with its remote feature. And, in this case, it's a sign that their software isn't working properly.

6

Deteriorating Battery Life

An obvious indication of spy software on your cell phone is if you experience a sudden drop in the performance of your cell phone's battery life.

Spy software on a phone monitors all of your activities and sends these recordings to a third-party device. In addition to the increase in data usage discussed earlier, if your cell phone is losing battery percentages at an unusually high rate, chances are it's because of spy software.

When spy software is making recordings with the camera or speaker, it will drain a significant chunk of your phone's battery - especially considering that your phone was supposed to be idle at the time.

If you're not sure whether it's just an old battery or actual spy software, simply test this by using a different set of batteries or trying your own battery in a different device. Then, measure the battery usage.

7

Increasing Battery Temperature in Idle Mode

This is one of the least obvious signs, because the battery temperature of a cell phone can be tied to a large number of different technical issues as well.

However, if you haven't experienced such an increase in battery temperatures before and you didn't use your phone, but it's still relatively warm anyway, it could be caused by spying software that's sending data to another device.

8

Increased Shut down Duration

Similar to a PC, which always closes all active processes after you decide to shut it down, a cell phone follows the exact same routine.

Your cell phone will close all of its active processes before it shuts down completely. Therefore, it will take quite a bit longer for a phone to shut down if it also has to cancel all the data-transmitting activities of spy software.

This is particularly true if you've been actively using your phone.

For example, maybe you just finished a number of calls or text messages and then tried to turn off your device, and it took an unusually long time. It could be caused by the software that's still actively running in the background, recording the newly-generated data.

9

Difficulty Shutting Down Your Device

Are you experiencing difficulties while trying to shut down your device? It could be a sign that your cell phone has been compromised. Typically, spy software keeps running in the background and might prevent you from shutting down your device completely.

If your cell phone's backlight does not seem to switch off to a completely black screen, it's likely that a spy app is causing this.

10

Your Cell Phone is Growing Increasingly Slower

The newest cell phones are equipped with powerful hardware and software. Your phone should be able to run many different apps at the same time.

If you feel like your cell phone suddenly shows signs of a significant drop in speed, it's potentially being remotely controlled and monitored.

How to Find and Remove Spy Software on Your Cell Phone

As mentioned before, there are plenty of spying applications available on the market. A few examples are:

1. Spyera
2. TheOneSpy
3. FlexiSPY
4. mSpy
5. Highster Mobile

All the applications listed above can monitor and record text messages and phone calls.

With these apps, a spy can take control of your phone's microphone and listen to everything that happens in your surroundings.

Furthermore, the more advanced applications can even steal your passwords, use your camera to physically spy on you, or even lock your phone completely so you can't use it anymore.

So, how can you find whether this software is installed on your device, and how can you remove it?

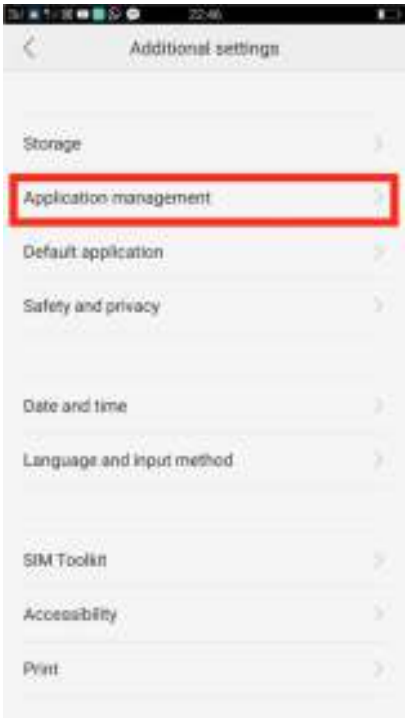
1

Solution for Android Users

If you are the owner of an Android device, you can check whether there is spy software installed on your phone by looking at your phone's files.

1. Go to Settings.
2. Find "Additional settings."

3. Click on “Application management.”



In that folder, you will find a list of file names. Once you’re in the folder, search for terms like spy, monitor, stealth, track or trojan.

In the screenshot below, you’ll see an example of common file names for spy software found on an Android device.

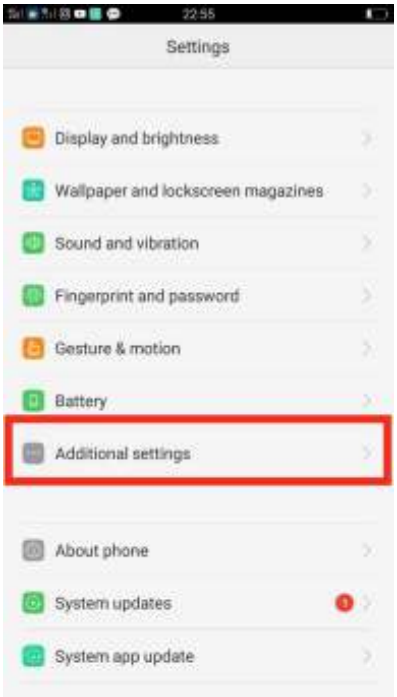
4. If found, delete any suspicious applications.

However, many spy apps do not use the actual name of the software tool, but instead use a fake name to hide it.

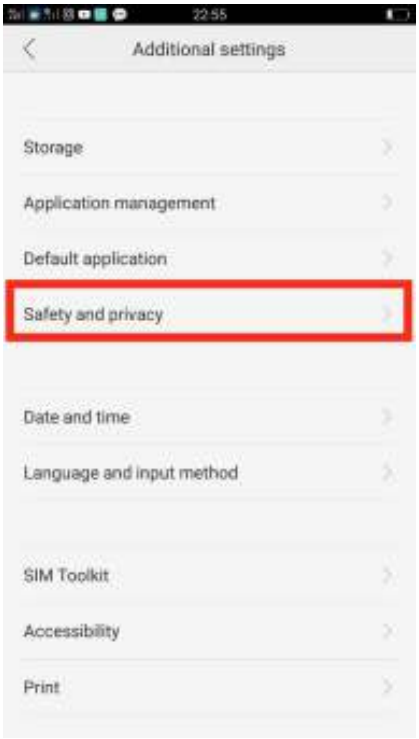
In that case, if you're suspicious, I recommend visiting your wireless provider's nearest store or go to an electronics store, like Best Buy - their tech team, called the "Geek Squad," can help you out in order to delete any file that belongs to spy software.

In addition, you can block unverified apps (apps that are not officially verified by the Google Play Store) by adjusting your security settings.

1. Go to Settings.
2. Find "Additional settings."

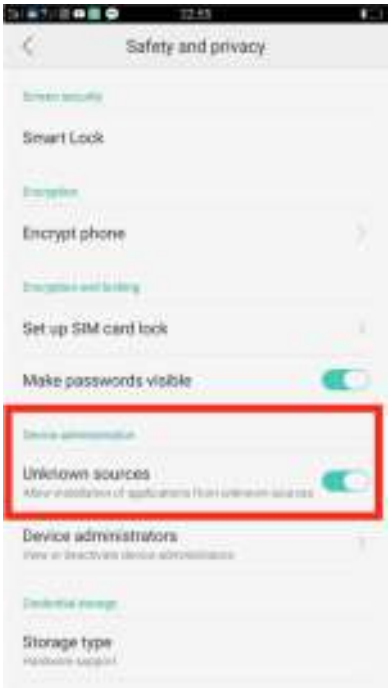


3. Find “Safety and privacy.”



4. Uncheck “Unknown sources” box.

This is a restriction that blocks the installation of applications outside of the Google Play Store.



This might not work against the best spy apps, but software of poorer quality will most likely be blocked. In case there might still be a spy app in your phone that you can’t detect or delete, I recommend that you jump down to the “Factory Reset” section for further instructions.

Registration no: 2017/128616/07 | 1397 Starkey Avenue, Waverley, Pretoria, 0186
MD: Michelle Henrico +27(0)84 208 1278 mhenrico@calltech.co.za | Service Desk: +27(0)8 1888 1888 service@calltech.co.za

Solution for iOS Users

In most cases, if a spy wants to monitor your iOS device, they have to jailbreak it. Jailbreaking an iOS device allows you to bypass Apple's security and the modification restrictions Apple puts on the device in order to take full control.

For example, mSpy is a legal application that's available in the App Store and works on a non-jailbroken iPhone. This app is marketed towards parents who want to monitor their kids.

However, a suspicious partner or employer could also install mSpy on your iOS device if they have access to it. All they need is the password of your iCloud account.

In case you're worried that mSpy is installed on your iOS device, simply change the password of your iCloud to stop all of mSpy's monitoring activities. To create a strong password.

In addition, there have been reports of vulnerabilities that were discovered in iOS security. In the past, it was possible to enter an iOS device by connecting to the same network to gain access by using malicious software tools.

Although these vulnerabilities have been fixed by now, there are always new threats at the end of the tunnel.

Checking the file folders of your iOS device isn't as easy as with Android devices. However, there is quite a simple solution to counter any suspicion.

Just update your device with the latest available updates via iTunes. This will remove a potential jailbreak and any third-party software.

Extra tip: you can also manually back up and restore your iPhone using iTunes.

Registration no: 2017/128616/07 | 1397 Starkey Avenue, Waverley, Pretoria, 0186

MD: Michelle Henrico +27(0)84 208 1278 mhenrico@calltech.co.za | Service Desk: +27(0)8 1888 1888 service@calltech.co.za

Well, at this point there isn't a solution required for Windows Phone users. The reason for that is because there aren't any spy software tools available for cell phones with the Windows operating system - for now.

Still, if you have a Windows Phone, you can rest easy knowing you're safe from the bad guys!

4

Last Resort: Factory Reset

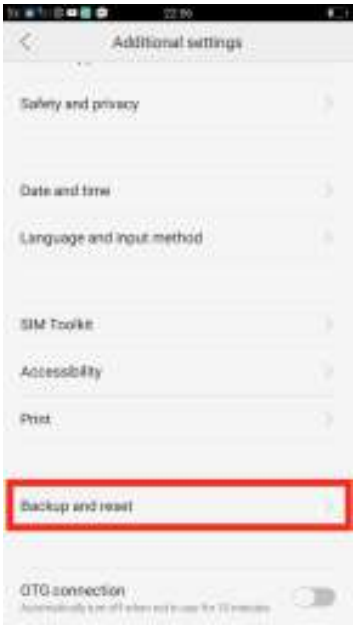
A factory reset is a last-resort option for both Android and iOS cell phones. Resetting your cell phone to its factory settings will delete all third-party apps - thus, any potential spy software will be removed as well.

If you choose to do this, I recommend creating a backup of your contacts, photos and other important files you don't want to lose.

Factory Reset for Android Users

1. Go to Settings.
2. Find "Additional settings."

3. Find “Backup and reset.”



4. Find “Factory data reset.”

5. Click on “Erase all app data and apps that can be uninstalled.”

After resetting your cell phone to its factory settings, you can download and install an app called AppNotifier that will notify you whenever a new application is installed on your phone.

That way, if someone is trying to install something on your phone that they shouldn’t, you’ll receive a head-ups about it.

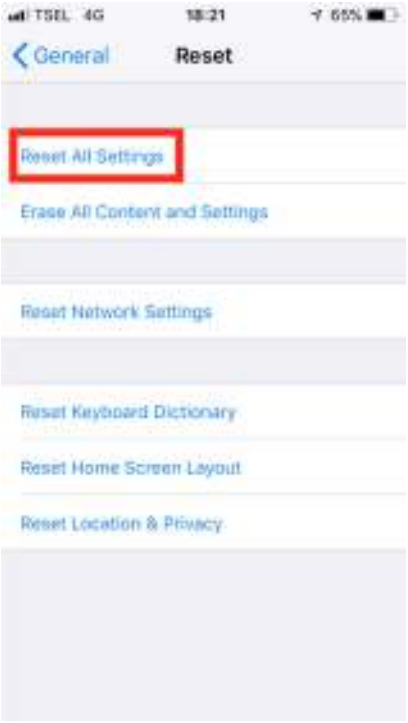
Factory Reset for iPhone Users

1. Go to Settings.
2. Find “General.”

3. Find “Reset.


TSEL 4G
18:21
65%
Settings
General
Keyboard
Language & Region
Dictionary
iTunes Wi-Fi Sync
VPN
Not Connected
Regulatory
Reset
Shut Down

4. Click on “Reset All Settings.”



Another possibility to reset your iPhone back to the factory settings is via iTunes.

1. Connect your iPhone to your computer.
2. Open iTunes.
3. Click on “Restore iPhone.”

Did You Find Out That Someone Is Spying on You?

Generally, many people that fall victim to spy software were not even aware of the fact that it was happening.

Once you discover that someone has been spying on you, it might cause a shock of disbelief. Whether it was with personal or business intent, the impact can be hard to cope with upon discovery.

If your cell phone is showing any of the signs listed above that suggest that someone might be spying on you, I highly recommend that you follow the provided solutions for your Android or iOS device.

Perhaps it's not a spy software tool causing any of these signs, but it's always better to be safe than sorry!