How to detect and remove eavesdropping software on smartphones

Phones with eavesdropping software will cause a lot of trouble and trouble for users, not to mention security issues. So how do I detect if my phone has eavesdropping software and how to remove the eavesdropping software from my phone?

What is phone eavesdropping software?

Phone eavesdropping or eavesdropping software is software that can be installed on mobile phones, allowing someone to monitor activities on the phone remotely.

Depending on the type of eavesdropping software installed, most of these software will monitor:

1. Call history, including phone number, date and call duration
2. Text messages, including phone numbers and SMS content
3. Phonebook
4. Browse the Internet, including history and bookmarks
5. Location of the phone
6. Photo taken on the phone
7. Email is downloaded to the phone

If your iPhone device is jailbroken or Android phone is rooted, this eavesdropping software can track more:

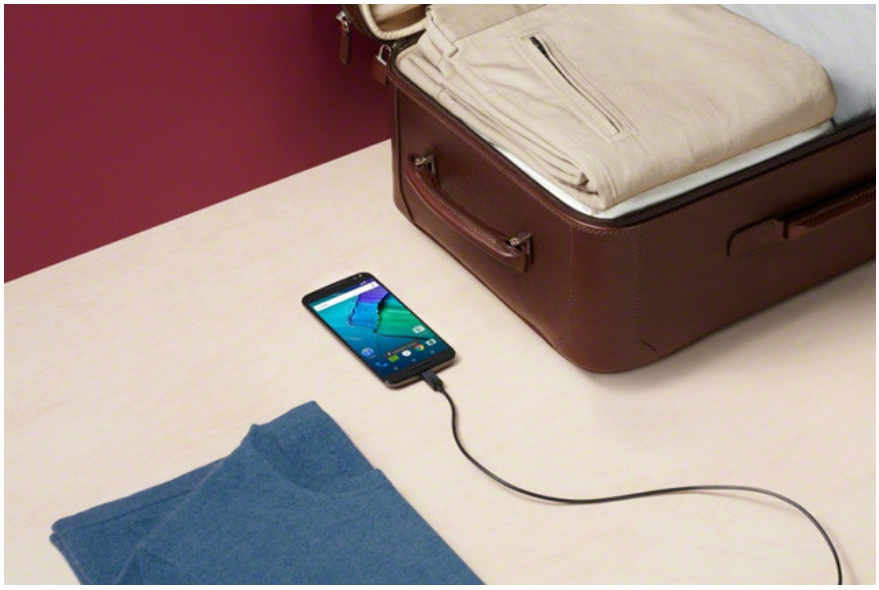
1. Certain messaging applications, such as WhatsApp, Viber, Skype
2. Phone conversation
3. Use your phone's microphone to record everything around

When eavesdropping software is installed, bad guys can track all the above activities via the online website.

Signs that the device may have bugged software installed

Battery dropped suddenly

Over time, you'll find that your phone's battery life is no longer the same as when you first purchased it, which is perfectly normal. But if you see a sudden battery drop, you need to consider.



Phone eavesdropping software can take up a lot of resources, they are active in the background, running GPS and performing other tasks. So when the battery suddenly drops rapidly without you using the phone, your device may have bugged software installed.

See also: 9 tips to extend battery life for Android phones you should apply today

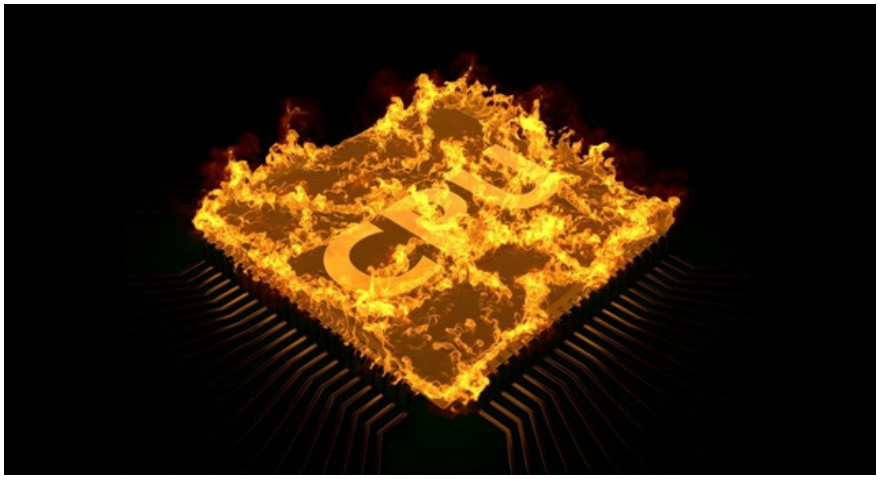
Check mobile data

Phone eavesdropping software often uses a lot of data to perform its behavior. Do you notice abnormal signs in using your data? If so, eavesdropping software is the reason for this abnormality.

The day is especially bad when you use a day-to-day data plan, even when using unlimited data packages is often slow after using a certain amount of data.

See also: Mobile data connection too slow? Try the following 7 network acceleration techniques

Phone temperature increased unexpectedly



Is your phone too hot? This is usually due to playing games or while charging, but if the phone is in standby mode or performing light tasks that are still too hot, this is an unusual phenomenon and may be caused by eavesdropping software. If the temperature rises abnormally on the phone, you need to consider it carefully.

See also: Hot iPhone, causes and remedies

Listen to strange sounds when making calls

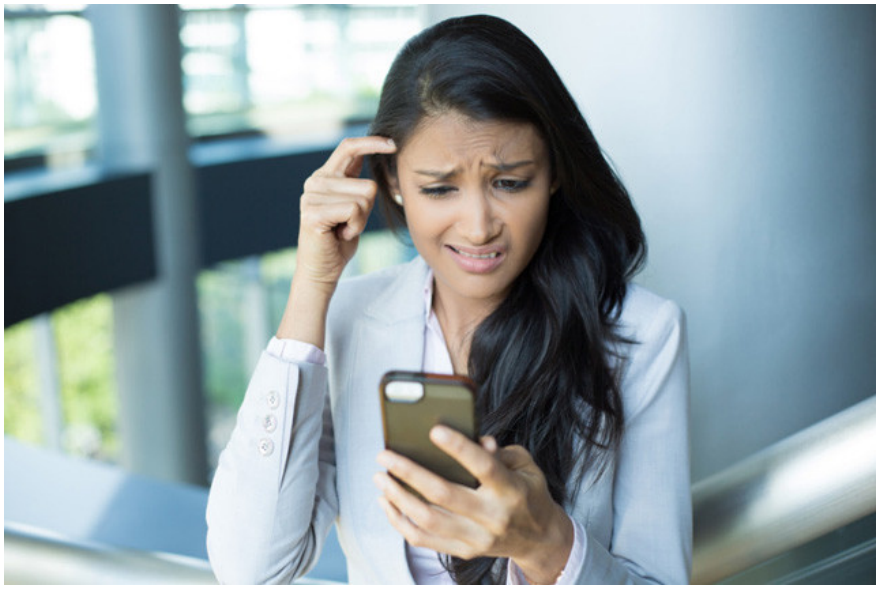
Sometimes your phone is being monitored, which may cause strange sounds while calling, such as white noise, beeps or echoes. Of course, there are times when we encounter a bad call signal, a signal loss, but if you encounter this problem often, you may be being followed.

The phone turns on and off randomly

Other common signs show that your device has bugged software installed and that the device is started and turned off randomly. Of course on some old phones this may be normal, but you should still carefully consider the other signs if this strange behavior takes place.

See also: Causes the phone to be powered off continuously and how to fix it

Receive strange messages



You get strange text messages with a series of letters and numbers, just like code? This may be a sign that your phone has been hacked. Attackers often use them to communicate with the device and send it a command. If you need your address, they can request it by sending you a message with a predefined code.

How does eavesdropping software enter the phone?

Did you notice some strange applications appearing on the phone? This may be because malware or spyware can download and install applications on the phone without approval.

Measures to handle phone eavesdropping software

Is your phone rooted and jailbroken?

Google Play Store implements policies to help users be safe, but it seems that users do not know how to protect themselves. You can easily install the application outside the store if the phone is rooted and in danger of being compromised.

Apple's iPhone security is one of the most stringent products. You can only install applications and software from Apple Store, so if you install programs other than Apple Store, you need to jailbreak. Usually when the iPhone is penetrated, you won't find it. Software like Cydia, Icy, Installer, Installous and SBSettings are some of the tools used for cracking. If you find one of these applications in your iPhone, it is very likely that your phone has been exploited. Look for it in the main screen.

Rooting Android or jailbreaking iPhone gives you some specific benefits because you can dig into the system and modify the code. However, this makes the phone more vulnerable to penetration and it is difficult to resist eavesdropping software. So do not root or jailbreak your phone to ensure your own safety.

See more:

1. Is root Android phone still a must-do?
2. Should or should not jailbreak iPhone?

Try to find eavesdropping software manually

The first step to take is to suspect that there is an eavesdropping software on your phone that you can find suspicious files or applications manually by going to **Settings> Apps** and finding anything you find suspicious.

These eavesdropping software often don't use its real name and logo, it often disguises itself as something like the Notepad application. You should visit it and see if anything is out of the ordinary and if you don't remember installing the application, delete it.

Set up the phone to the initial default mode

It's hard to find and handle eavesdropping software, the only way to make sure all is gone is to set up the phone for the initial installation. But remember to back up your important data wisely because when you do this it will delete everything.

See more:

1. Instructions for restoring original Android phone settings on versions
2. How to restore original settings Reset iPhone

Use antivirus application

Many people use phones that "don't believe" in antivirus applications because it is rare for phones to be infected with malware if you are always in the "protective arms" of Google and Apple. But the truth is that these antivirus applications are capable of helping to combat eavesdropping software, software and other malicious applications. You can refer to the article Top best antivirus application for Android phones and Top 5 antivirus software for iPhone.

Protect your phone from eavesdropping software

Your phone is a very personal device, so don't let anyone have access and rummage like a doorless house. Keep your phone safe and protect it against eavesdropping software like this. You can do this by protecting the lock screen with a password, Pin code, fingerprint, etc. and when installing the application, check it carefully.

See more:

1. 14 most effective anti-spyware software
2. 4 ways to avoid tracking technology
3. How to detect your PC and email is being monitored?

You finished reading the article "**How to detect and remove eavesdropping software on smartphones**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.