# How to protect yourself from unethical or illegal espionage

There are a number of tools that will help you find hidden applications and spyware on computers, smartphones or other devices. This is how to protect yourself from being followed.

A quick search on Google with the keyword "spy software" or "spyware" yielded more than 150 million results. There is a great concern about utilities and spyware. Regardless of motive or justification, espionage is an illegal act. This is considered a privacy invasion in most countries of the world.

You don't have to suffer if someone is watching you. There are a number of tools that will help you find hidden applications and spyware on computers, smartphones or other devices. This is how to protect yourself from being followed.

## How to protect yourself against spyware?



## 1. Phone spy application on smart phones

Smartphones are one of the most important personal gadgets of the digital age. For many people, smartphones are the largest repository of personal information. You access email and text messages, take photos, store bank information and more on your smartphone. Therefore, smartphones are the main target for spying and data theft applications.

Once installed on a smartphone, a mobile spy application will use your data connection to send a remote log to your followers secretly. Things that can be logged include:

1. Calls

2. Message and email
3. Photos and videos
4. Data from Facebook, Twitter and other social networking applications
5. Location tracking data

Spy apps can invade every area of ??your smartphone. The amount of data collected depends on the spy application. For example, some spy apps on a smartphone can send data back to a remote server for analysis, while others can activate the smartphone microphone to listen live. Phone call or location tracking in real time via GPS.

A spy application on a smartphone will not have a clear user interface. In most cases, the spyware application can hide its application icon, whether on iOS or Android. Moreover, the key to success is that spies can access their logs and applications remotely without having to contact their smartphones anymore.

## How to avoid spyware apps on Android and iOS

Take the following measures to avoid spyware applications on Android and iOS:

1. Always keep the phone under your control.

2. Use a strong password to lock the device. Do not use easy lock options such as basic PIN or pattern combination (unlock pattern). Add a biometric course if possible.

3. Consider your surroundings while unlocking and using the device.

4. Monitoring equipment if strange behavior is detected. Strange behaviors include random on screen, unexpected activity, increased network usage, unusual network connections, etc.

5. Bandwidth monitoring with data monitoring application. Check for unknown applications that use data. The application is that it can be a spyware that sends data.

## How to find hidden spy apps on Android


Android devices are particularly susceptible to spyware, for a few reasons.

First, a series of devices that Android can run on means that vulnerabilities are easy to find. Android also runs on old hardware, which is vulnerable to vulnerabilities. The range and long-standing appearance of hardware made Android a major target for spyware.

Second, it's easier to root an Android device than jailbreaking an iOS device (read more about jailbreaking below). Root Android device provides access to the entire device. A spy can root an Android device, then hide the spyware in it.

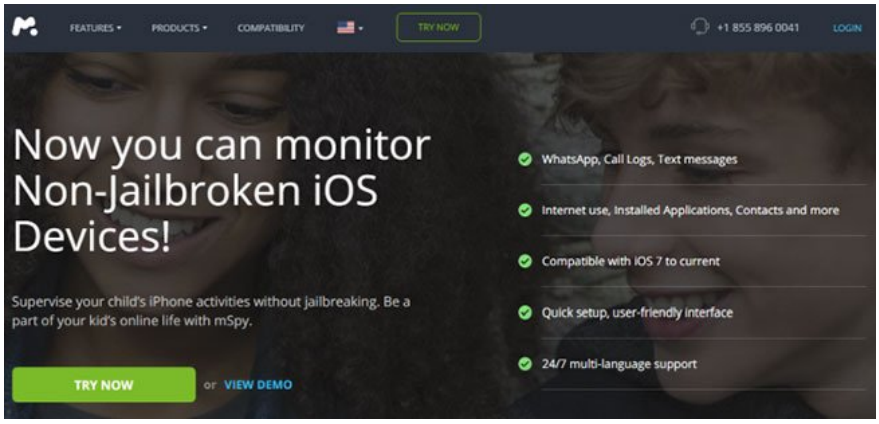
Android users have two options for monitoring and removing spyware.

First, scan the device with Malwarebytes Security. Malwarebytes is a well-known antivirus and malware tool. Download and scan your Android device with this tool, then delete any malicious apps it finds.

1. Download Malwarebytes Security for Android (Free).

If the spyware problem persists, the only option is to perform a full factory reset. A full factory reset will delete all apps on the device.

## How to find hidden spy apps on iOS




IOS spyware is different than on Android. The iOS operating system is more secure, providing better integrated security features. The central part of that security is the App Store. If an app is not available on the app store, you must jailbreak your iPhone or iPad to install it on the device.

The easiest way to check your jailbroken iOS device is to look for the Cydia app. The Cydia application installs and allows for extensive customization, as well as non-native iOS options. If you find the Cydia app, you can reset your device's factory settings to remove jailbreaks and any installed spyware that is exploiting the vulnerability.

Recently, a new generation of iOS spyware applications no longer requires jailbreak. These applications require physical access to the phone for setup, but can monitor and monitor in real time. A spy can extend the functionality of these non-jailbreak spy apps with access to the victim's iCloud login information.

Unfortunately, finding one of the latest iOS spyware applications is extremely difficult. Users should keep track of data usage, texting, incoming and outgoing calls, as well as battery charge statistics. A spyware application will negatively impact the battery as it continuously writes data. The software will also impact the device's data

usage when it sends and receives information.

## 2. Spy apps on the desktop

Remote access applications, keyloggers and malware are the weapons of choice to spy on the desktop. The VNC application allows people to view all activity on your computer as it happens. Similarly, Remote Access Trojan (RAT) is a much more dangerous type of malware that can give hackers access to your system.

Finally, a keylogger records every keystroke you make on your system and can provide bank passwords, social networks, as well as many other applications to hackers without ever warning you.

A spy can install a remote spy application more easily than a smartphone. Some operating systems are easier to work with. Like Android on smartphones, installing spyware on Windows computers will be easier, due to the known vulnerabilities and the common nature of this operating system. However, users of macOS and Linux are not necessarily safe.


### How to avoid spy apps on the desktop

The variety of spy apps on desktop and laptop means there are a few strategies to consider. Consider the following measures to prevent your computer from being tracked:

1. Set strong unique password for all accounts, including login to desktop.

2. Set a very short screen lock time and always lock the desktop when you leave the room.

3. Never allow anyone to use your desktop with admin rights. With admin rights, a spy can install any application that violates privacy he wants. Only the real admin should have permission to install the application.

4. Install a powerful suite of anti-virus and malware software. This combination will prevent remote access to the computer and install malware.

5. Check the list of programs regularly to detect unexpected changes. Most spyware, malware or keyloggers will not appear in the program list, but it should still be monitored regularly.

This is not a complete list. If someone really wants to monitor your desktop, he will find a way to install spyware without your knowledge. In most cases, spyware comes from someone who has direct access to the desktop and is manually installed.

### How to find and delete spy applications on the desktop

If your desktop has spyware installed, you may notice a few changes. The problems are similar to malware because in fact, they are the same. Your computer has:

1. Is it slow or runs like a turtle?
2. Starting to meet the embassy randomly (while it was normal before)?
3. Displaying many pop-ups or other adware?
4. Force you to redirect to random websites?
5. Experience unwanted browser settings?
6. Show random error message?

If you encounter these situations, you may have encountered a problem with spyware. Finding and removing spyware is not easy, but you can do it.

Windows and macOS users should download and install Malwarebytes Premium, then scan their system. Boot the system into Safe Mode, then run the scan. Spyware and malware can be hidden during normal startup. Safe Mode, meanwhile, is a minimalist boot process, with fewer processes and services so spyware can't hide later.

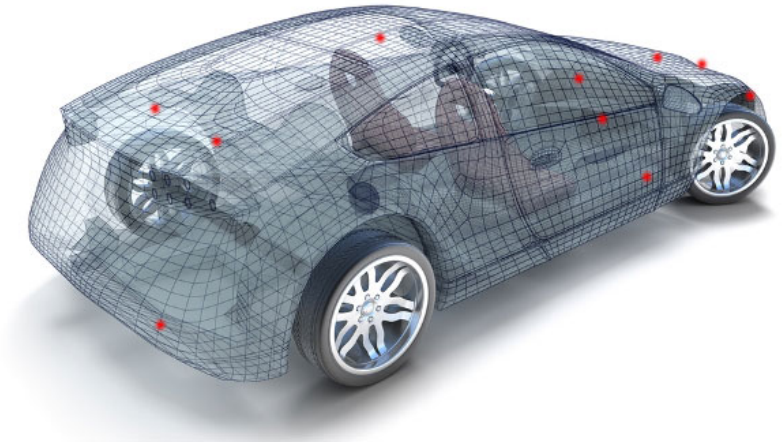
The process of booting into Safe Mode will be different for Windows and macOS. Windows users can learn how to boot in Safe Mode on Windows 10.

## 3. GPS tracking device

If your followers can't access your smartphone or desktop, he can try to track your movements instead. GPS tracking device is relatively cheap. They also easily 'hide' on a large object, such as a car.

There are some signs that someone is following your vehicle. If you suspect someone is getting your location information using a GPS tracking device, here are some key places to check:

1. Inside dampers
2. Under the protective shield
3. Under the steering wheel radiator
4. Distance between hood and window
5. Under the dashboard before
6. Inside the speaker located in the car door
7. The top of the hood
8. Inside the rear speaker section
9. Inside the third rear brake light
10. Inside plastic impulse rear
11. In the storage box



A GPS tracking device can be very small. If you want to see it in your car, you have to search extremely carefully.

You can also check the On-Board Diagnostics (OBD) port on the vehicle for suspicious hardware. You may also cause interference with GPS signals. However, jamming devices are illegal tools for many reasons.

If you can't find anything, try using a radio frequency detector to isolate any suspicious transmissions.

## 4. Camera and micro spy

Like GPS trackers, spy cameras and microphones are constantly downsized. A high-end spy camera and microphone combination can hide behind most household items. The camera may also have additional functions, such as night vision, motion tracking, face recognition, live streaming, and more.

A spy can hide hidden cameras and microphones in many places thanks to its small size. If you suspect there are cameras and microphones in your office, home or elsewhere, check these locations:

1. Lights
2. Smoke alarm
3. The shelves
4. Speak
5. Under the table
6. Flower vase
7. Lampshade
8. Clock
9. Wall paintings
10. Anywhere else can hide a miniature camera.

You should also look for small holes in the wall where a pinhole camera can be used. Another option is to turn off all the lights at night and scan the surroundings to find the bright LED.

1. How to detect hidden cameras, hidden cameras in the room is simple

If you can't find the camera or microphone but suspect someone is spying on you, try and locate the camera with your smartphone. A range of smartphone applications can scan to detect radio frequency or electromagnetic field

transmission. The application is available for both iOS and Android devices. Wireless cameras transmit at frequencies from 900MHz to 5.8GHz.

You can also check in-house WiFi network. Perhaps you will find a suspicious spy camera that uses the Internet to play back images and audio back to the spy.

## What to do if someone is spying on you?

Discovering someone illegally following you is a horrible feeling. But you need to consider what should be done next. In most cases, calling the police is the best option once you have proof. Without evidence, it is difficult for the police to accept any complaints.

Spyware is not the only problem that smartphone users face. Android users should also protect their device from stalkerware, an equally dangerous type of application that violates privacy.