# How to Detect a Phone is Hacked

If you believe that your cell phone or landline is being tapped, you can look for some clues to support that suspicion. However, some of the signs below may be caused by other causes, so you need to check for multiple signs instead of relying on just one. After finding enough evidence, you can ask the authorities for help. Below are the signs you need to look for if you suspect your phone has a listening device installed.

## Initial doubts


**Pay attention when secrets leak out.** If confidential information that only a few trusted people know about is suddenly leaked, it's likely that the leak was caused by phone tapping, especially if you discussed the information at some point in time. there.

This is especially worth noting if you hold a position that makes you an important person to watch. For example, if you are a senior executive at a large company with many competitors, you may become a victim of the undercover information hunting industry.

On the other hand, the reason why you are being wiretapped can also be very simple, for example you are going through a complicated divorce process. Your spouse who is about to divorce you may eavesdrop on you if they want to dig up information that will benefit the divorce process.

If you want to test this, you can reveal a fake (seemingly important) piece of information to someone you trust not to tell anyone. If that information is leaked, it proves that someone is eavesdropping on you.


**Be alert if your home has recently been burglarized.** If your home was recently burglarized but nothing of value was lost, this alone indicates something is wrong. Sometimes the reason is that they break into your house to install a listening device on your phone.

## Signs of eavesdropping on phones in general


**Listen to the noise.** If you hear a lot of white noise or other background sounds while talking on the phone, it's likely that the noise is being interfered with by a listening device.

However, this is not the most obvious sign because echoes, white noise and clicking noises can also be caused by other random objects, or by a poor connection.

White noise, random sounds and sudden noises can be caused by the discharge of two electrical conductors when connected.

High-pitched humming is a more obvious sign.

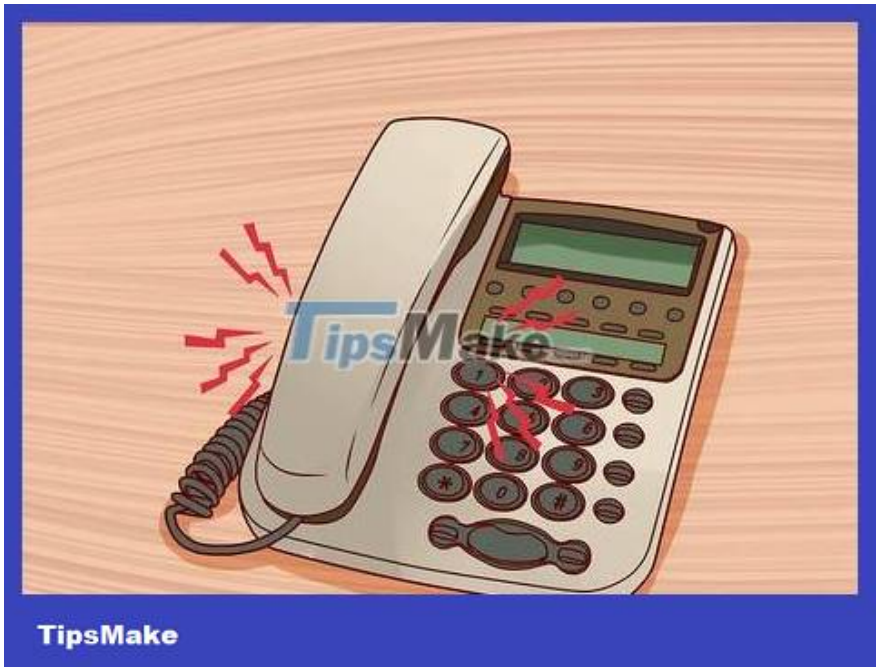
You can use a low-frequency sound sensor to check for sounds that are normally inaudible to the ear. If this sound occurs many times every minute, it is likely that your phone has been tapped.


**Use your phone next to other electronic devices.** If you suspect your phone is being tapped, walk past the radio or TV while listening for the next call. Even if you don't hear any interference on your phone, it's likely that interference occurred when you were standing next to another electronic device, causing white noise with that device.

You should also watch for signs of interference when you are not actively using your phone. A phone's active radio signals can interrupt data transmission even if there is no other software or hardware installed on the phone, but passive signals cannot.

Some recording or eavesdropping devices use frequencies close to the radio band, so if your radio hisses when set to mono and tuned to the farthest position on the band, you may Maybe one of those devices is in use.

Similarly, eavesdropping devices can interfere with television broadcast frequencies on UHF channels. Use a TV with an antenna to check if there is an interfering device in the room.




**Listen to the phone when not in use.** Your phone will not make any sound when you are not using it. If you hear beeping, clicking, or other sounds from your phone when it's not in use, there may be eavesdropping software or hardware installed on the phone.

Specifically, you need to listen to the white noise emitted according to amplitude.

If this happens, it can be concluded that the microphone and speaker are working even when you are not using the phone, the reason being that an electrical circuit is connected to the phone. Any conversation you have within 6 meters of your phone can be overheard.

For landline phones, if you hear dialing sounds when you are not using the phone, this is a sign of eavesdropping. Confirm the presence of this noise using an external audio amplifier.

## Signs of eavesdropping on mobile phones


**Pay attention to the temperature of the battery.** If your cell phone battery is unusually hot when not in use and you don't know why, there may be eavesdropping software running in the background, causing the phone battery to continuously drain.

Of course, a hot battery can also simply be caused by being used too much. This is especially true if your phone is more than a year old, because cell phone batteries degrade over time.


**Note the number of times you have to charge your phone.** If your phone's battery life suddenly drops for no reason, forcing you to charge it twice as many times as usual, it could be because eavesdropping software is constantly running in the background and consuming all the power.

You also need to consider how much you use your phone. If you've been using your phone a lot lately, the need to charge it more may simply be due to the phone being more active. This is only true if you barely touch your phone or don't use it more than usual.

You can monitor the life of your mobile phone's battery with apps like BatteryLife LX or Battery LED.

Note that cell phone batteries will lose their ability to hold power after a period of use. If this change happens after you've had your phone for a year or more, it's simply because the battery is old.


**Try turning off the phone.** If the power off process is delayed or cannot be completed, this strange situation indicates that someone is controlling your phone through a device wired into the circuit board.

Pay close attention to see if your phone stays off longer than usual, or if the backlight stays on after you've turned it off.

Although this could be a sign that the phone is being wiretapped, it could also be a problem with the phone's hardware or software and is completely unrelated to eavesdropping.


**Watch for random activities.** If your phone automatically lights up the screen, turns off the power, starts up, or installs applications without your intervention, it is possible that someone has jailbroken the phone and controlled it with a device connected to the circuit board. .

On the other hand, this situation can occur if there is accidental interference during data transmission.


**Pay attention to unusual messages.** If you recently received an SMS message containing any string of letters or numbers sent from an anonymous sender, those messages are a very clear sign that your phone is being controlled.

Some programs use SMS messages to send commands to the controlled phone. If these programs are poorly installed, messages may appear.


**Pay close attention to your phone bill.** If data costs are skyrocketing and you know you haven't done anything to cause them, it's possible that someone is using your data through a tracking device or app.

Many tracking programs send call history to servers using your cellular data. Older programs use a lot of mobile data so they are easy to detect, but new programs are better at hiding because they use less data.

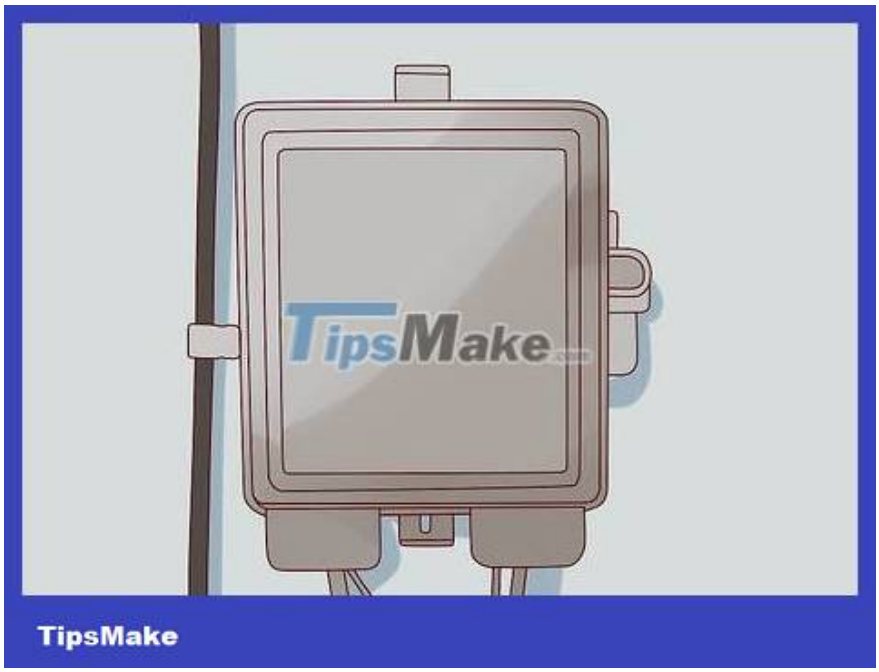
## Signs of eavesdropping on desk phones


**Check the surrounding space.** If you suspect there is an eavesdropping device on the phone line, you should check the surrounding space. If something is misplaced, like a sofa or desk, don't automatically assume you're

hallucinating. This could be a sign that someone has snuck into your home.

The eavesdropper may have moved furniture while trying to access power or phone lines, so this is an important factor to keep in mind.

Specifically, look at the wall panels. You should pay close attention to the walls around the phone. If they appear to be moved, someone may have tampered with them.




**Look outside the phone box.** Maybe you don't know what the inside of a phone box looks like, but if you know a little, take a look. If the phone box appears to have been tampered with or its contents have been tampered with, someone may have approached it to install a listening device.

If you see any hastily installed hardware, even if you don't know what it is, you should have it checked by a technician.

Look closely at the 'limited contact' side of the box. This side of the box can only be opened with a hex key, and if it appears to be tampered with, there must be a problem.

There is only one box for each landline number and there are two cables connected to the box. Any additional cables or boxes may be a sign of eavesdropping.


**Count the number of utility trucks passing by your house.** If you suddenly see a lot of utility trucks running around your house, this could be a sign that they are not ordinary utility trucks. That's the car of the people who are eavesdropping on your calls and they are maintaining the wiretapping line.

This is especially notable if no one gets off or gets on the bus.

In general, the person eavesdropping on a landline line through a recording device will be 150-200 meters away from your home. The vehicles will be equipped with tinted windows.


**Be wary of mysterious repairmen.** If someone comes to your house claiming to be a repairman or a phone carrier employee, but you didn't ask for them to come, it could be a trap. Verify the person's identity by calling the phone company or company they claim to be from.

When calling the company, you should use the phone number in your contacts. Don't use a phone number given to you by that person.

Even if you have verified it, you still need to carefully observe this worker's actions while they are at your home.

## Confirm your suspicions


**Use eavesdropping detection devices.** Eavesdropping detection devices can be installed on your phone. As the name suggests, it can detect external signals and eavesdropping device signals, letting you know whether your suspicions are correct or not, and whether someone else is eavesdropping on your calls.

The usefulness of this device remains questionable, but for the device to detect eavesdropping it must detect electrical or signal changes on the phone line under test. Look for a device that can measure impedance and capacitance, along with the ability to detect changes in high-frequency signals.


**Install apps.** For smartphones, you can install a wiretapping detection application to detect eavesdropping signals and unauthorized access to phone data.

The effectiveness of this type of application is still up for debate, so they probably cannot produce convincing evidence. Some applications of this type can only detect recording devices installed by another application.

The app that claims to be able to detect recording devices is Reveal: Anti SMS Spy.


**Ask your carrier for support.** If you have good reason to believe that your phone is being tapped, you can ask the network operator to check with specialized equipment.

Standard analysis performed by the telephone company can detect all instances of illegal eavesdropping, eavesdropping devices, low-frequency devices, and phone line splicing.

Note that if you have asked the phone company to check for wiretapping and recording, but they deny the request or claim to have found nothing after a cursory review, it is likely that they are acting on a request. government demand.


**Go to the police station.** If there is clear evidence that the phone was tapped, you can ask the police to check. Furthermore, you can ask them to catch whoever is eavesdropping on you.

Most police stations have the necessary equipment to check for recording devices or eavesdropping devices on phones, but if you don't have reasonable evidence they won't use it.

You finished reading the article "**How to Detect a Phone is Hacked**" 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.