

How to Know If Your Phone Has Been Hacked



Smartphones have revolutionized our personal and business lives. We socialize on phones, take endless photos, use them to close deals, find restaurants, organize our schedules, and deposit checks. But all that power and flexibility brings inherent risks. Protect yourself by recognizing the signs that indicate your phone has been hacked.

Know the Hacker Playbook

Individuals can gain access to your phone and its data in a variety of ways. Understanding their methods will help you keep bad actors out. For instance, hackers may access your phone by:

- Direct access – With direct access to your phone, a hacker can install spying apps that may prove virtually undetectable. These apps can log your keystrokes, hijack your camera and microphone, and provide the hacker with remote access to your device.
- Access through iCloud – When iPhone users back up data to their iCloud account, hackers do not need to touch the phone at all. They simply need to access the iCloud account and begin spying from there.
- Through a malicious link or app – An email, text or website may contain a deceptive link that installs malware on the device when clicked. Likewise, hackers often embed malware in apps that then infect the device. Be wary of apps that over-request permissions, giving them access to critical data.



- Spyware – Parents use monitoring software designed to protect their children from predators and online dangers. Many of these apps allow for remote installation via an over-the-air link using just a phone number. Unfortunately, criminals also use these convenient monitoring apps to track location, communications, and internet history.
- Public Wi-Fi – Unsecured Wi-Fi networks give eavesdroppers free reign to view unencrypted traffic. Hackers may also use a public hotspot to redirect unsuspecting users to spoofed bank or email sites to steal credentials.
- Bluetooth – In a targeted attack, a hacker will connect to your device over Bluetooth and harvest information.
- SIM swapping – With a relatively minimal amount of personal information, a thief can call your cellular provider, posing as you, and have your number transferred to their device. Then, with access to authentication codes texted to your phone, they can take over your accounts.

Look for Signs of Trouble

A hacked phone will often provide some signs of compromise. Keep an eye out for unusual activity, such as odd popups that may include flashing ads or pornographic images. Higher than expected data usage, a quickly draining battery or slow processing times may also indicate an intrusion.

Additionally, take the precaution of periodically checking for unfamiliar calls or texts made from your number. This could indicate that a thief has hijacked your number. Likewise, unfamiliar apps on your phone suggest malware.



First Steps to Take After Your Phone Has Been Hacked

If you suspect that someone has hacked your phone, immediately change your passcode, as well as passwords on your online accounts. Next, take an inventory of all the apps on your phone, deleting any suspicious apps. Keep in mind that malicious apps may have names that make them look like a calculator or something equally innocuous.

Run anti-malware software. In fact, make a note to run it regularly from now on. Tell your friends and family to ignore suspicious messages that appear to come from your number. And keep an eye out for fraudulent credit card purchases or unusual activity in your bank account. You will need to take extra caution to protect against [identity theft](#).

As a last resort, you can also run a factory reset on your phone. However, be aware that this will wipe out any data stored on your phone, including photos, messages, and notes.

Mobile Device Security Protects Your Business

In an increasingly mobile business world, smartphones represent possible access points into critical business networks. Businesses should practice [mobile security best practices](#). Begin by implementing mobile device management and educating employees about phone hacking.

The cybersecurity professionals at eMazzanti will help you build mobile security into a [comprehensive security strategy](#). Call today for a free cybersecurity assessment.