How To Tell If Your Phone Is Hacked

By Jack Gillespie

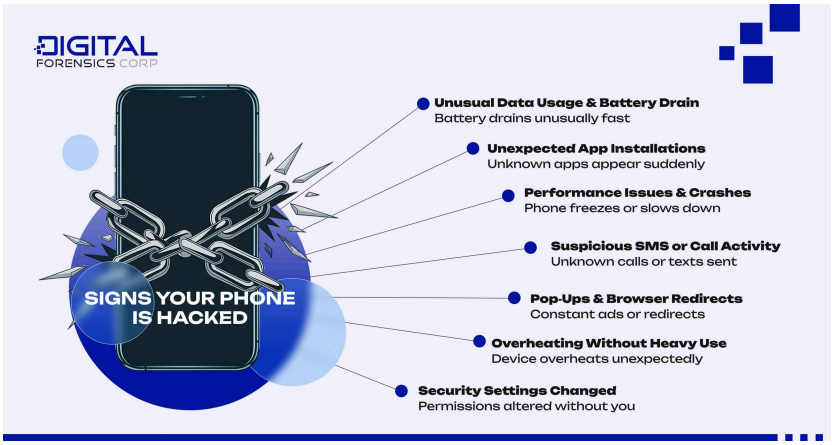
Published: 2025-04-10 · Archived: 2026-04-02 12:12:02 UTC

As of 2024, nearly every American owns a cellphone of some kind with 91% owning a smart phone[1]. Of these, roughly 78% use their device for mobile banking and over half use it as a digital wallet, storing all their financial data in one location.

On top of this, just under half of smart phone users protect their device and its multiple apps and services, including online banking, behind the same PIN[2]. That is if they use a PIN or password on their device at all, which over a quarter of Americans don't[1].

As a result, cybercriminals have focused their efforts toward compromising mobile devices. Unique mobile malware samples increased by 13% last year, and 83% of phishing sites now target mobile devices[3].

Because of this, it's never been more important to ensure that your mobile device, your activity on it, and the networks you connect to are secure. Many people worry about claims that someone can hack a bank account with just a phone number. In reality, these fears usually come from misunderstandings about how mobile security works and how cybercriminals actually gain access to accounts. Read on to learn about proactive safety practices, signs of intrusion, and steps to take if your mobile device has been hacked.



Understanding the Attack Vectors: How Phones Get Hacked

There are numerous ways that a cell phone can be infiltrated. Cybercriminals will exploit any vulnerability available to gain access to your devices and the data stored upon them. Knowing their strategies can help you avoid risky behaviors that may put your device's security at risk.

Malicious Apps and Software:

Roughly one in every four protected mobile devices experience malware exposure[3]. This is due in large part to the practice of sideloading, or downloading programs from unofficial app stores. Devices that have engaged in sideloading are 200% more likely to contain malware[3].

Specifically, Android devices have a vulnerability in their OS that allows malicious apps to send permission requests that overlay requests from legitimate apps. This means when an app like Instagram asks for permission to your photos or camera, a malicious program can sneak a request in as well[4].

Phishing and Social Engineering:

In addition to the rise in phishing sites targeting mobile devices, there was a 28% increase in vishing attacks and a 22% increase in smishing attacks in 2024[5]. Together, this has resulted in over half of all personal devices encountering a phishing attack each quarter[6].

These attacks utilize social engineering to pose as a trusted entity, such as a business the target uses. A recent example of this is the fake toll payment text scams that have been circulating in early 2025. These texts take targets to a fake payment website which harvests their log in and financial credentials.

Network Attacks (Man-in-the-Middle and Rogue Wi-Fi):

Your mobile security may be jeopardized by a hacked Wi-Fi router or unsecure public network. Over half of internet users use public Wi-Fi(1), and roughly 4 in 10 public Wi-Fi users have had their private information compromised, with some instances taking less than 10 minutes from the time of connection for malicious activity to be detected(3).

MITM attacks are often carried out by setting up an imposter Wi-Fi network in areas such as airports, cafes, libraries, and other public venues that typically offer free internet. Hackers may even compromise a legitimate public Wi-Fi network by manipulating rogue access points. Regardless, MITM attacks allow cybercriminals to intercept personal data including log in credentials, banking information, and other private communications conducted on your device.

Zero-Day Exploits and Operating System Vulnerabilities:

Zero-Day exploits are vulnerabilities that are manipulated by bad actors before the software distributor recognizes their existence and patches them. They are significant because the developer has “zero days” to secure the software since it is already being exploited.

Because of this, it’s important to install software updates as soon as they become available. However, 75% of smartphone users in the United States say they only update their operating system when it’s convenient with an additional 3% saying the never perform updates(7). It’s important not to fall into this demographic for the sake of your mobile security.

Physical Access and Device Tampering:

If a hacker can obtain physical access to your device, they may be able to install malicious programs like spyware and remote access trojans (RATs) directly to your device without the need for a backdoor.

Hackers may use rubber ducky devices, which are Human Interface Devices (HID) which appear like USB drives. However, these devices can be used to harvest user data and inject malicious software while going undetected as it appears as a HID device. Because of this, it’s important to never leave your phone or other devices unattended.

Recognizing the Signs: Indicators of a Compromised Phone

There are a multitude of signs that may indicate that your mobile device’s security has been compromised. If you’ve noticed the following behaviors, it may be a sign that a hacker has infiltrated your phone:

- **Unusual Data Usage and Battery Drain:** Malicious programs often run in the background of your device, leading your battery to drain quicker than normal. While battery life slowly worsens as phone batteries decay over time, rapid changes are abnormal. Check your battery usage data to see if any unrecognized programs are draining your battery.
- **Unexpected App Installations and Changes:** While many devices come with preinstalled apps, these programs come from the manufacturer. Unauthorized third-party programs can be an indication of a hack and can contain spyware and other malicious programs. Check your installed apps and review their permissions within your device's settings.
- **Performance Issues and System Instability:** If your phone is regularly freezing, running slowly, crashing, or generally suffering from poor performance, this may be a sign that your device has been hacked or infected. Restart your device and make sure it's OS is up to date to troubleshoot any performance issues.
- **Suspicious SMS/Call Activity:** Unauthorized calls and texts are common in mobile device malware attacks as the perpetrator attempts to spread the infection to other devices. You can check call and text logs on the device and retrieve deleted logs by contacting your carrier or accessing your account online.
- **Pop-up Ads and Browser Redirections:** Adware remained the most prevalent threat to mobile devices last year, accounting for 35% of all mobile malware detections[(8)]. These programs display unwanted ads, harvest your browsing history, redirect traffic, and can install other malicious programs such as spyware.
- **Hardware Overheating:** Much like the software, your physical device can experience performance issues due to unauthorized programs running in the background. This can lead to components overheating and even melting in extreme cases. If you receive alerts that your device is overheating irregularly, it may be a sign that you've been hacked.
- **Changes in Security Settings:** Malicious programs, such as spyware, may disable security features like screen locks or find my device settings. Additionally, they may grant permission to features like camera and microphone access. You can check your security settings and permissions in your device's privacy settings.

Taking Action: Steps to Mitigate and Recover

Once you've recognized that your phone has been hacked, you need to act quickly. Securing your mobile device, online accounts, and the rest of your connected network as quickly as possible will help minimize the damage and contain the potential reach of the hacker. While your first instinct might be to simply ignore the scammer, doing so without first securing your digital footprint can leave your sensitive data exposed to ongoing threats.

Isolating the Device

Disconnect your hacked device from your networks to prevent the spread of malicious programs to your other devices. You should also disconnect other devices in case the router has been hacked. This can be done by opening device settings and searching for Wi-Fi, connections, network, internet, or cellular and disconnecting from the network.

Running Antivirus and Anti-Malware Scans

Research and select a reputable mobile anti-malware security provider, such as Bitdefender and Norton. Once you've installed one of these apps, run a scan to determine if your device has any malicious programs running and remove them. These programs should be downloaded and ran prior to a hacking threat to secure your mobile device.

Factory Reset and Data Recovery

In extreme cases, your only option may be to perform a factory reset. However, this will wipe all of the data on the device, including any evidence that you may need to pursue the perpetrator. Because of this, it's important to perform regular data backups prior to any threat of your device being hacked.

Changing Passwords and Securing Accounts

If your device has been infected with spyware, you will want to update the passwords of any accounts you've accessed on it. Furthermore, you should maintain the strength of your passwords by performing routine updates and enabling two-factor authentication when the option is available.

Reporting the Incident to Authorities and Service Providers

You should document the incident, including any unauthorized programs, phishing messages, performance issues, or signs that you've been hacked and then blackmailed, and file a report. You should begin by reporting the situation to your carrier, financial institutions, and local law enforcement.

If further action is needed, you should continue by reporting the instance to your national agencies, such as the FBI and FTC. It is important that you report instances of phone hacking to secure yourself and help protect all mobile device users from future hacks.

When to Call the Professionals: Digital Forensics Corp.

If the steps outlined above have failed to resolve your issue, you may wish to consider consulting digital forensics professionals who have experience investigating cases of cell phone hacking. These organizations have years of experience and access to tools that you wouldn't have alone.

The Importance of Expert Analysis:

Receiving assistance from experienced cell phone forensics experts can help you uncover critical evidence and discover the root cause of a phone hacking that you wouldn't be able to do on your own.

You may be able to detect that a malicious third-party program is running on your device or notice a decrease in your phone's performance, but this is only part of the solution. There are experts that can help you secure your device, including the team at DFC.

Digital Forensics Services for Mobile Devices:

Here at DFC, we have years of cell phone forensics experience, and we've developed proven techniques in that time. Through cell phone mapping, we can determine the type of device being used, the geolocation of the device, and which cell tower a device has connected to.

Furthermore, our certified engineers are well-versed in recovering and analyzing cell phone data. We can perform device imaging on damaged devices, regardless of whether the problem is software or hardware related.

If you believe your mobile device has been hacked, now is the time to act. Call Digital Forensics Corp. today and see how we can help you hang up on the hacker.

Sources:

1. Demographics of Mobile Device Ownership and Adoption in the United States
2. New research shows that security is failing to keep pace with smartphone utilisation by consumers – Nuke From Orbit
3. 2024 Global Mobile Threat Report
4. Android Malware Abuses App Permissions to Hijack Phones | PCMag
5. apwg_trends_report_q3_2024.pdf
6. Over 50% of personal devices were exposed to a mobile phishing attack | Security Magazine
7. Many smartphone owners don't take steps to secure device
8. The mobile threat landscape in 2024 | Securelist
