How to Figure Out Who Hacked Your Phone

by Natasha Stokes on June 16, 2020

Article Courtesy of: https://www.techlicious.com/tip/how-to-tell-who-hacked-your-phone/

Techlicious editors independently review products. To help support our mission, we may earn affiliate commissions from links contained on this page.

For most of us, our phones are the center of our daily lives, and as a result, they contain a treasure trove of personal information, from banking details to messaging and email accounts. This sensitive data can be pretty enticing to a range of the nefarious, from cybercriminals to someone you may even know.

Phone hacking can involve the unknowing download of spyware that relays information on your activity – such as logging keystrokes to scrape passwords; spy apps downloaded by someone with access to your device; or other malware that exploits your phone, for example by using its internet bandwidth in a botnet, as occurred with malware that infected nearly 20 million Android devices.

“The most common way that smartphones can be hacked is to infect the device with malware,” says Victor Chebyshev, a security researcher at Kaspersky Lab. This malware can arrive on the device buried inside apps downloaded by the user – and the likelihood of a malicious app rises when downloading away from the official app stores, which police their content.

While iPhones aren’t immune to hacking, Apple’s strict vetting policy means the incidence of bad apps targeting iPhones (at least non-jailbroken ones) is lower than for Android phones. “Android devices are more susceptible to these kinds of attacks because they have the option to install applications from third parties,” says Chebyshev.

9 steps to figuring out who hacked your phone

A sluggish phone or fast-draining battery are common symptoms of a compromised phone – but they can also indicate your device needs a spring clean to spruce up performance or improve its battery life. Another red flag is if your data usage has gone through the roof – this could indicate a dodgy app is sending data back to its mothership.

“Whether a user can determine who is responsible for a compromised phone depends on what kind of threat was on the device,” says Chebyshev.

According to Verizon’s 2020 Data Breach Investigation, 86% of cyberattacks are motivated by monetary gain – for example, through selling someone’s stolen credentials on the dark web, gaining access to financial accounts, or hacking sensitive data and holding the victim to ransom. In these cases, hackers usually rely on malware that remotely exploits vulnerabilities in apps or operating systems to steal information (or in the case of phishing malware, trick people into inputting their critical data).

However, somebody known to you who wants to monitor your movements – whether that’s a disgruntled ex or suspicious parent – and who has physical access to your device might also be able to install a spy app that acts like malicious software, tracking your location, photos, messages and calls.

To narrow down the field of suspects, you can try to determine exactly how your phone is being compromised.

1. Check your phone bill

Are you being charged for premium-rate texts you never sent – or texts you never signed up for? You’ve probably been infected by malware that forces your phone to send or receive texts that generate revenue for cybercriminals. This common form of mobile malware is believed to be the first type found targeting Android, back in 2010, and today plenty of it is still floating around.

If you’re receiving premium-rate text messages, try texting STOP to the number. If this doesn’t work, you’ll have to contact your cell carrier who should be able to block the number.

If your phone is sending the texts, you may be able to fix it by running a security app such as Bitdefender or McAfee to find and remove malware (on Android only; security apps for iOS don’t have this feature). Also, try deleting any third-party messaging apps and any other apps you installed just before the phone started sending the texts.

2. Go through your apps list

If there are any apps you don’t remember downloading, look them up online to see if any of them have been reviewed negatively for malware or other suspicious activity. In this case, the apps will have been compromised by a hacker who likely isn't targeting you personally but is distributing malware with the aim of scraping as much data as possible. The BankBot malware, for instance, is a trojan that has infected hundreds of Android apps to display a phishing screen to steal users' banking credentials.

"If it was a regular trojan [malware coded within another app] the user will not be able to attribute who was responsible for the attack," says Chebyshev. "If it was commercial spyware, it's sometimes possible to figure out the responsible person."

3. Look up your flashlight and battery-saver apps

Got a phone full of apps and can't remember for sure which you downloaded? Some categories of apps have attracted more than their fair share of malicious actors – several flashlight apps on Google Play were infected with malware that tried to scrape users' financial info, while one should be wary of battery-saver apps as they have often been used for malware, says Josh Galindo, director of training at phone repair service uBreakiFix.

If you have these types of apps, check online for any negative reviews. You can also try deleting them to see if this affects your phone performance. "If you install an app and the device performance decreases, that's an indicator," says Galindo. "If you uninstall the app and your device begins working properly again, this means that the app is likely contaminated with malware and you should avoid downloading it in the future."

4. Double-check your favorite popular games

Downloaded a new super-popular game recently? Ensure it operates like it's meant to – and validate that by looking up reviews online – otherwise it may be a scam version, potentially ridden with cryptojacking malware.

Cryptojacking trojans mine cryptocurrency unbeknownst to users, and their prevalence has risen on smartphones that when infected in thousands, can deliver attackers a high overall processing power. The idea is that, if a cryptojacker hacks other devices, they can get paid for mining without having to use their own resources (or pay the electricity bill).

On mobile, cryptojacking malware tends to hide inside innocent-looking apps such as fake versions of popular games. If your phone slows down, heats up and its battery is dying long before the end of the day – and you've tried to improve your battery life– it could be a sign that a malicious app like a cryptojacking trojan is hogging all the juice.

They're mostly prevalent on Android – and if you've downloaded from non-official app marketplaces, the risk is higher.

5. Scroll through your call list

Done all of the above and still convinced that someone somewhere has your personal data, siphoned from your smartphone? Apps aren't the only way a phone can be infected by malware. Have you picked up any random calls lately? "Callers offering a free cruise or claiming that you won a sweepstakes are likely scam efforts to hack your information or record your voice," says Galindo.

6. Did you click that link?

If you recently clicked on a link on a text message or an unexpected pop-up, you may have inadvertently fallen prey to phishing. Phishing often preys on panic or high emotion – as in the coronavirus-related scam texts claiming that receivers had been exposed to someone with COVID-19 symptoms, and exhorting them to click for more information.

It's often impossible to divine who is behind such scams, although you can report any phishing texts to your cell carrier and block these numbers.

7. Consider the last time you used public WiFi

According to Kaspersky Lab, one in four hotspots are unsecured, and even the ones that are password-protected could potentially be set up by someone with malicious intent. On top of that, the protocol (WPA2 or WPA3) that encrypts traffic between devices and routers can itself be vulnerable – as in the serious WPA2 flaw uncovered by researchers in 2017 that would have allowed certain traffic to be intercepted.

If your phone isn't protected by a VPN and you logged into an unsecured public WiFi hotspot, it's possible someone could have been spying on the connection – and scraped your sensitive information if you logged into your email or bought something online.

8. Is your iCloud safe?

iPhone user? A cracked iCloud login can allow someone to not only access your photos, but also make use of semi-legal spy software to remotely monitor your device's calls, messages, contacts and location.

Luckily, enabling two-factor authentication for your Apple ID drastically reduces this risk, because if someone tries to sign into your account from a new device, you'll receive an approval request and sign-in code on your iPhone (or other iOS/Mac devices linked to your Apple ID).

(To enable two-factor authentication, for iOS 10.3 and newer: Settings > [your name] > Password & Security. For iOS 10.2 or older: Settings > iCloud > Apple ID > Password & Security.)

However, a weak or reused password without two-factor authentication can put your account – and phone – at risk.

Here’s how it works: Many people use the same email address in their Apple ID as the login for dozens of online accounts. If this email address is revealed in a data breach, then hackers – who may purchase or find these login details at data dump websites – have access to your Apple ID.

Couple that with a weak password and your iCloud account can be breached by attackers who use cracking software to guess hundreds of hacked or common passwords in order to breach accounts.

Unfortunately, the same goes for an email and password combo that can be guessed or found out by someone you know who’d want to spy on you – especially if they can access your iPhone to use the two-factor code.

9. Run a security scan

Since most malware is designed to evade detection, you may not discover much on your own. Spyware apps – or stalkerware – is one category of particularly insidious apps designed purely to monitor a victim’s activity (rather than for any financial gain).

Security apps, particularly for Android, can help determine if your phone contains such a malicious app, as well as help fend off future cyber attacks by, for example, preventing you from visiting malicious webpages.

Android: Commercial spyware is unfortunately all too easy to find online. Such spy apps have system-level access to extremely detailed information about your device activity such as the messages you write, photos you take and GPS location – and what’s more, these apps are hidden from view.

They also need to be downloaded physically to your device, which means if they’re on your device it was done by someone with access to your device (and your PIN). Chances are, you can figure who in your life would want to monitor your phone.

To find out if you have such apps on your Android phone, download a security app such as Bitdefender or McAfee, which will flag any malicious programs. You can also head to Settings > Security > Device administration and check if “Unknown sources” for app installations is enabled (and you didn’t do it) – this allows apps from non-official app stores, on which there’s likely to be far more stalkerware.

iPhone: Spy apps on a non-jailbroken iPhone are far less prevalent since such software – which tampers with system-level functions - doesn’t make it onto the App Store. (However, they do exist and work via someone knowing your iCloud login and password.)

If your iPhone is jailbroken, that opens it up to potentially malicious apps that haven’t been vetted by the App Store, including spy apps downloaded without your knowledge.

Security apps such as Lookout and Sophos will alert you if your iPhone has been jailbroken – so if you're alerted of this but haven't done it yourself, that can be a red flag.

However, whether security software – for Android or iOS – can find spy apps will depend on how sophisticated or new the spy app is since security software scans for malware that's already known. (That's why it's crucial to download updates to security software as soon as available since updates will incorporate new instances of discovered malware.)

3 steps to take if your phone has been hacked

1. Delete any apps or messages that may be malicious

If deleting them fixes any performance issues, great. Even if not, it's a good idea to clear your device of apps that may have been flagged from that security scan.

You can also try shutting down apps one by one, as soon as your phone starts to slow down or heat up. If shutting down a particular app seems to return things to normal, that app may be malicious – or at the very least, not play too well with your device.

2. Do a factory reset

If after deleting the suspicious app(s) your phone is still behaving strangely, this nuclear option is a quick way of clearing your device of malicious – or sluggish – software left behind.

Android: Settings > System > (Advanced) > Reset options > Erase all data

iPhone: Settings > General > Reset > Erase All Content and Settings

3. Check if your information is out there

Unfortunately, many hacks and malware present few to no symptoms and often the only time people are aware of a breach is when their digital services are hacked, or, worse, they're the victims of identity fraud, where hackers have used their stolen information to open accounts or lines of credit.

There are a few tools you can use to check if any of your information has already been compromised. Have I Been Pwned? is a website run by security developer and Microsoft Regional Director Troy Hunt that checks if email addresses have been exposed in breaches of popular apps and services.

Security apps including Bitdefender (Android) and Lookout (iOS) can also alert you if apps and services you use have been breached, putting your personal information at risk.

Depending on the scale of the data that has been exposed, you may want to set up a fraud alert at the major credit agencies, which will require any potential creditors to request additional verification of your identity.

Keeping your smartphone safe

If you find that your logins – particularly passwords – are floating around online, the first thing to do is to change your passwords. The best way to do that is to use a password manager which can automatically generate and save complex, unique passwords for each of your accounts. Check out our top-rated picks here. We like the Dashlane password manager, whose Premium version (from $4.99/month) also scans the Dark Web for instances of your emails or logins being posted for sale.

And to reduce the risk of future phone hacks, always observe general cybersecurity hygiene:

- Think twice before clicking links in SMSes, other messages and emails
- Review app permissions to minimize the risk of a malicious app download.
- Enable two-factor authentication for every online account possible – and especially primary emails and logins like your Apple ID.
- Download security updates for your phone when available to patch vulnerabilities that could otherwise be exploited.
- Protect your device with a PIN or biometric authentication.

Updated on 6/16/2020 with new tips and recommendations