How to Tell if Your Phone Has Been Hacked

by Natasha Stokes on May 28, 2020

Article courtesy of: https://www.techlicious.com/tip/how-to-tell-if-your-phone-has-been-hacked/

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

From email to banking, our smartphones are the main hub of our online lives. No wonder that smartphones rival computers as common targets for online hackers. And despite the efforts of Google and Apple, mobile malware continues to land in official app stores – and these malicious apps are getting sneakier. According to the McAfee 2020 Mobile Threat Report, over half of mobile malware apps "hide" on a device, without a homescreen icon, hijacking the device to serve unwanted ads, post bogus reviews, or steal information that can be sold or used to hold victims to ransom.

And while iPhones can be hacked, more malware targets Android devices. In its 2020 State of Malware Report, MalwareBytes reported a rise in aggressive adware and preinstalled malware on Android devices designed to steal data – or simply victims' attention.

Malware can also include spyware that monitors a device's content, programs that harness a device's internet bandwidth for use in a botnet to send spam, or phishing screens that steal a user's logins when entered into a compromised, legitimate app.

It is often downloaded from non-official sources, including phishing links sent via email or message, as well as malicious websites. (While security experts recommend always downloading from official app stores – like the Apple App Store or Google Play – some countries are unable to access certain apps from these sources, for example, secure messaging apps that would allow people to communicate secretly.)

Then there are the commercial spy apps that require physical access to download to a phone – often done by those well-known to the victim, such as a partner or parent – and which can monitor everything that occurs on the device.

Not sure if you may have been hacked? We spoke to Josh Galindo, director of training at uBreakiFix, about how to tell a smartphone might have been compromised. And, we explore the twelve ways your phone can be hacked and the steps you can take to protect yourself.

6 Signs your phone may have been hacked

1. Noticeable decrease in battery life

While a phone's battery life inevitably decreases over time, a smartphone that has been compromised by malware may start to display a significantly decreased lifespan. This is because the malware – or spy app – may be using up phone resources to scan the device and transmit the information back to a criminal server.

(That said, simple everyday use can equally deplete a phone's lifespan. Check if that's the case by running through these steps for improving your Android or iPhone battery life.)

2. Sluggish performance

Do you find your phone frequently freezing, or certain applications crashing? This could be down to malware that is overloading the phone's resources or clashing with other applications.

You may also experience continued running of applications despite efforts to close them, or even have the phone itself crash and/or restart repeatedly.

(As with reduced battery life, many factors could contribute to a slower phone – essentially, its everyday use, so first try deep cleaning your Android or iPhone.)

3. High data usage

Another sign of a compromised phone is an unusually high data bill at the end of the month, which can come from malware or spy apps running in the background, sending information back to its server.

4. Outgoing calls or texts you didn't send

If you're seeing lists of calls or texts to numbers you don't know, be wary – these could be premium-rate numbers that malware is forcing your phone to contact; the proceeds of which land in the cyber-criminal's wallet. In this case, check your phone bill for any costs you don't recognize.

5. Mystery pop-ups

While not all pop-ups mean your phone has been hacked, constant pop-up alerts could indicate that your phone has been infected with adware, a form of malware that forces devices to view certain pages that drive revenue through clicks. Even if a pop-up isn't the result of a compromised phone, many may be phishing links that attempt to get users to type in sensitive info – or download more malware.

6. Unusual activity on any accounts linked to the device

If a hacker has access to your phone, they also have access to its accounts – from social media to email to various lifestyle or productivity apps. This could reveal itself in activity on your accounts, such as resetting a password, sending emails, marking unread emails that you don't remember reading, or signing up for new accounts whose verification emails land in your inbox.

In this case, you could be at risk for identity fraud, where criminals open new accounts or lines of credit in your name, using information taken from your breached accounts. It's a good idea to change your passwords – without updating them on your phone – before running a security sweep on your phone itself.

What to do if your phone is hacked

If you've experienced any of these symptoms of a hacked smartphone, the best first step is to download a mobile security app.

For Android, we like Avast, which not only scans for malware but offers a call blocker, firewall, VPN, and a feature to request a PIN every time certain apps are used – preventing malware from opening sensitive apps such as your online banking.

iPhones may be less prone to hacks, but they aren't totally immune. Lookout for iOS flags apps that are acting maliciously, potentially dangerous Wi-Fi networks, and if the iPhone has been jailbroken (which increases its risk for hacking). It's free, with $2.99/month for identity protection, including alerts of logins being exposed.

Who would hack your phone?

By now, government spying is such a common refrain that we may have become desensitized to the notion that the NSA taps our phone calls or the FBI can hack our computers whenever it wants. Yet there are other technological means – and motives – for hackers, criminals and even the people we know, such as a spouse or employer, to hack into our phones and invade our privacy. And unless you're a high-profile target – journalist, politician, political dissident, business executive, criminal – that warrants special interest, it's far more likely to be someone close to you than a government entity doing the spying.

12 ways your phone can be hacked

From targeted breaches and vendetta-fueled snooping to opportunistic land grabs for the data of the unsuspecting, here are twelve ways someone could be spying on your cell phone – and what you can do about it.

1. Spy apps

There is a glut of phone monitoring apps designed to covertly track someone's location and snoop on their communications. Many are advertised to suspicious partners or distrustful employers, but still more are marketed as a legitimate tool for safety-concerned parents to keep tabs on their kids. Such apps can be used to remotely view text messages, emails, internet history, and photos; log phone calls and GPS locations; some may even hijack the phone's mic to record conversations made in person. Basically, almost anything a hacker could possibly want to do with your phone, these apps would allow.

And this isn't just empty rhetoric. When we studied cell phone spying apps back in 2013, we found they could do everything they promised. Worse, they were easy for anyone to install, and the person who was being spied on would be none the wiser that there every move was being tracked.

"There aren't too many indicators of a hidden spy app – you might see more internet traffic on your bill, or your battery life may be shorter than usual because the app is reporting back to a third-party," says Chester Wisniewski, principal research scientist at security firm Sophos.

Likelihood

Spy apps are available on Google Play, as well as non-official stores for iOS and Android apps, making it pretty easy for anyone with access to your phone (and a motive) to download one.

How to protect yourself

- Since installing spy apps require physical access to your device, putting a passcode on your phone greatly reduces the chances of someone being able to access your phone in the first place. And since spy apps are often installed by someone close to you (think spouse or significant other), pick a code that won't be guessed by anyone else.
- Go through your apps list for ones you don't recognize.
- Don't jailbreak your iPhone. "If a device isn't jailbroken, all apps show up," says Wisniewski. "If it is jailbroken, spy apps are able to hide deep in the device, and whether security software can find it depends on the sophistication of the spy app [because security software scans for known malware]."
- For iPhones, ensuring you phone isn't jailbroken also prevents anyone from downloading a spy app to your phone, since such software – which tampers with system-level functions - doesn't make it onto the App Store.

- Download a mobile security app. For Android, we like McAfee or Bitdefender and for iOS, we recommend Lookout for iOS.

2. Phishing messages

Whether it's a text claiming to be from a coronavirus contact tracer, or a friend exhorting you to check out this photo of you last night, SMS texts containing deceptive links that aim to scrape sensitive information (otherwise known as phishing or "smishing") continue to make the rounds.

And with people often checking their email apps throughout the day, phishing emails are just as lucrative for attackers.

Periods such as tax season tend to attract a spike in phishing messages, preying on people's concern over their tax return, while this year's coronavirus-related government stimulus payment period has resulted in a bump in phishing emails purporting to be from the IRS.

Android phones may also fall prey to texts with links to download malicious apps (The same scam isn't prevalent for iPhones, which are commonly non-jailbroken and therefore can't download apps from anywhere except the App Store.). Android will warn you, though, when you try to download an unofficial app and ask your permission to install it – do not ignore this warning.

Such malicious apps may expose a user's phone data, or contain a phishing overlay designed to steal login information from targeted apps – for example, a user's bank or email app.

Likelihood

Quite likely. Though people have learned to be skeptical of emails asking them to "click to see this funny video!", security lab Kaspersky notes that they tend to be less wary on their phones.

How to protect yourself

- Keep in mind how you usually verify your identity with various accounts – for example, your bank will never ask you to input your full password or PIN.
- Check the IRS's phishing section to familiarize yourself with how the tax agency communicates with people, and verify any communications you receive
- Avoid clicking links from numbers you don't know, or in curiously vague messages from friends, especially if you can't see the full URL.
- If you do click on the link and try to download an unofficial app, your Android phone should notify you before installing it. If you ignored the warning or the app somehow otherwise bypassed Android security, delete the app and/or run a mobile security scan.

3. Unauthorized access to iCloud or Google account

Hacked iCloud and Google accounts offer access to an astounding amount of information backed up from your smartphone – photos, phonebooks, current location, messages, call logs and in the case of the iCloud Keychain, saved passwords to email accounts, browsers and other apps. And there are spyware sellers out there who specifically market their products against these vulnerabilities.

Online criminals may not find much value in the photos of regular folk – unlike nude pictures of celebrities that are quickly leaked – but they know the owners of the photos do, says Wisniewski, which can lead to accounts and their content being held digitally hostage unless victims pay a ransom.

Additionally, a cracked Google account means a cracked Gmail, the primary email for many users.

Having access to a primary email can lead to domino-effect hacking of all the accounts that email is linked to – from your Facebook account to your mobile carrier account, paving the way for a depth of identity theft that would seriously compromise your credit.

Likelihood

“This is a big risk. All an attacker needs is an email address; not access to the phone, nor the phone number,” Wisniewski says. If you happen to use your name in your email address, your primary email address to sign up for iCloud/Google, and a weak password that incorporates personally identifiable information, it wouldn’t be difficult for a hacker who can easily glean such information from social networks or search engines.

How to protect yourself

- Create a strong password for these key accounts (and as always, your email).
- Enable login notifications so you are aware of sign-ins from new computers or locations.
- Enable two-factor authentication so that even if someone discovers your password, they can’t access your account without access to your phone.
- To prevent someone resetting your password, lie when setting up password security questions. You would be amazed how many security questions rely on information that is easily available on the Internet or is widely known by your family and friends.

4. Bluetooth hacking

Any wireless connection may be vulnerable to cyber-snoops – and earlier this year, security researchers found a vulnerability in Android 9 and older devices that would allow hackers to secretly connect over Bluetooth, then scrape data on the device. (In Android 10 devices, the attack would have crashed Bluetooth, making connection impossible.)

While the vulnerability has since been patched in security updates out soon after, attackers may be able to hack your Bluetooth connection through other vulnerabilities – or by tricking you into pairing with their device by giving it another name (like 'AirPods' or another universal name). And once connected, your personal information would be at risk.

Likelihood

"Rather low, unless it is a targeted attack," says Dmitry Galov, security researcher at Kaspersky."Even then, a lot of factors have to come together to make it possible."

How to protect yourself

- Only turn your Bluetooth on when you are actually using it
- Don't pair a device in public to avoid falling prey to malicious pairing requests.
- Always download security updates to patch vulnerabilities as soon as they're discovered

5. SIM swapping

Another reason to be stringent about what you post online: cybercriminals can call up cellular carriers to pose as legitimate customers who have been locked out of their accounts. By providing stolen personal information, they're able to get the phone number ported to their own device and use it to ultimately take over a person's online accounts. In a spat of Instagram handle thefts, for example, hackers used known login names to request password changes and intercept multi-factor authentication texts sent to the stolen phone number. The purpose? To hold victims for ransom or, in the case of high-value names, sell on underground marketplaces. Some people have also had cryptocurrency accounts hijacked and drained.

On top of that, researchers found that there were representatives at all five major carriers who authenticated users giving the wrong information (such as billing address or zip code), by instead asking for the last three digits of the last two dialed numbers. Researchers were able to provide these details by first sending a text instructing users to call a certain number, which played a voicemail telling them to call a second number.

Likelihood

"Currently, SIM swapping is especially popular in Africa and Latin America," says Galov. "But we know about modern cases from different countries worldwide."

How to protect yourself

- Don't use guessable numbers for your carrier PIN – like your birthday or family birthdays, all of which could be found on social media.

- Choose an authenticator app such as Authy or Google Authenticator instead of SMS for 2FA. “This measure will protect you in most cases,” says Galov.
- Use strong passwords and multi-factor authentication for all your online accounts to minimize the risk of a hack that can reveal personal information used to hijack your SIM.

6. Hacked phone camera

As video calling becomes increasingly prevalent for work and family connection, it’s highlighted the importance of securing computer webcams from hackers – but that front-facing phone cam could also be at risk. A since-fixed glitch in the Android onboard Camera app, for example, would have allowed attackers to record video, steal photos and geolocation data of images, while malicious apps with access to your camera app (see below) might also allow cybercriminals to hijack your camera.

Likelihood

Less prevalent than computer webcam hacks.

How to protect yourself

- Always download security updates for all apps and your device.

7. Apps that over-request permissions

While many apps over-request permissions for the purpose of data harvesting, some may be more malicious – particularly if downloaded from non-official stores – requesting intrusive access to anything from your location data to your camera roll.

According to Kaspersky research, many malicious apps in 2020 take advantage of access to Accessibility Service, a mode intended to facilitate the use of smartphones for people with disabilities. “With permission to use this, a malicious application has almost limitless possibilities for interacting with the system interface and apps,” says Galov. Some stalkerware apps, for instance, take advantage of this permission.

Free VPN apps are also likely culprits for over-requesting permissions. In 2019, researchers found that two-thirds of the top 150 most-downloaded free VPN apps on Android made requests for sensitive data such as users’ locations.

Likelihood

Over-requesting permissions happens commonly, Galov says.

How to protect yourself

- Read app permissions and avoid downloading apps that request more access than they should need to operate.

- Even if an app’s permissions seem to line up with its function, check reviews online.
- For Android, download an antivirus app such as McAfee or Bitdefender that will scan apps before download, as well as flag suspicious activity on apps you do have.

8. Snooping via open Wi-Fi networks

The next time you happen upon a password-free Wi-Fi network in public, it’s best not to get online. Eavesdroppers on an unsecured Wi-Fi network can view all its unencrypted traffic. And nefarious public hotspots can redirect you to lookalike banking or email sites designed to capture your username and password. Nor is it necessarily a shifty manager of the establishment you’re frequenting. For example, someone physically across the road from a coffee shop could set up a login-free Wi-Fi network named after the café, in hopes of catching useful login details for sale or identity theft.

Likelihood

Any tech-savvy person could potentially download the necessary software to intercept and analyze Wi-Fi traffic.

How to protect yourself

- Only use public Wi-Fi networks that are secured with a password and have WPA2/3 enabled (you’ll see this on the login screen requesting password), where traffic is encrypted by default during transmission.
- Download a VPN app to encrypt your smartphone traffic. NordVPN (Android/iOS from $3.49/month) is a great all-round choice that offers multi-device protection, for your tablet and laptop for example.
- If you must connect to a public network and don’t have a VPN app, avoid entering in login details for banking sites or email. If you can’t avoid it, ensure the URL in your browser address bar is the correct one. And never enter private information unless you have a secure connection to the other site (look for “https” in the URL and a green lock icon in the address bar).
- Turning on two-factor authentication for online accounts will also help protect your privacy on public Wi-Fi.

9. Apps with weak encryption

Even apps that aren’t malicious can leave your mobile device vulnerable. According to InfoSec Institute, apps that use weak encryption algorithms can leak your data to someone looking for it. Or, those with improperly implemented strong algorithms can create other back doors for hackers to exploit, allowing access to all the personal data on your phone.

Likelihood

“A potential risk, but a less likely threat than others such as unsecured Wi-Fi or phishing,” says Galov.

How to protect yourself

- Check app reviews online before downloading – not only on app stores (which are often subject to spam reviews), but on Google search, for sketchy behavior that other users may have reported.
- If possible, only download apps from reputable developers – for example, who turn up on Google with positive reviews and feedback results, or on user reviews sites like Trustpilot. According to Kaspersky, “the onus is on developers and organizations to enforce encryption standards before apps are deployed.”

10. SS7 global phone network vulnerability

A communication protocol for mobile networks across the world, Signaling System No 7 (SS7), has a vulnerability that lets hackers spy on text messages, phone calls and locations, armed only with someone’s mobile phone number.

The security issues have been well-known for years, and hackers have been exploiting this hole to intercept two-factor authentication (2FA) codes sent via SMS from banks, with cybercriminals in Germany draining victims’ bank accounts. The UK’s Metro Bank fell prey to a similar attack.

This method could also be used to hack other online accounts, from email to social media, wrecking financial and personal havoc.

According to security researcher Karsten Nohl, law enforcement and intelligence agencies use the exploit to intercept cell phone data, and hence don’t necessarily have great incentive to seeing that it gets patched.

Likelihood

The likelihood is growing, as the minimal resources needed to exploit this vulnerability have made it available to cybercriminals with a much smaller profile who are seeking to steal 2FA codes for online accounts – rather than tap the phones of political leaders, CEO or other people whose communications could hold high worth in underground marketplaces.

How to protect yourself

- Choose email or (safer yet) an authentication app as your 2FA method, instead of SMS.
- Use an end-to-end encrypted message service that works over the internet (thus bypassing the SS7 protocol), says Wisniewski. WhatsApp (free, iOS/Android), Signal (free, iOS/Android) and Wickr Me

(free, iOS/Android) all encrypt messages and calls, preventing anyone from intercepting or interfering with your communications.

- Be aware that if you are in a potentially targeted group your phone conversations could be monitored and act accordingly.

11. Malicious charging stations

While travel and tourism may not be on the horizon anytime soon, last year the Los Angeles County District Attorney's Office released a security alert about the risk of hijacked public USB power charging stations in locations such as airports and hotels.

Malicious charging stations – including malware-loaded computers – take advantage of the fact that standard USB cables transfer data as well as charge battery. Older Android phones may even automatically mount the hard drive upon connection to any computer, exposing its data to an unscrupulous owner.

Security researchers have also shown it's possible to hijack the video-out feature so that when plugged into a malicious charge hub, a hacker can monitor every keystroke, including passwords and sensitive data.

Likelihood

Low. There are no widely-known instances of hijacked charging points, while newer Android phones ask for permission to load their hard drive when plugged into a new computer; iPhones request a PIN. However, new vulnerabilities may be discovered.

How to protect yourself

- Don't plug into unknown devices; bring a wall charger. You might want to invest in a charge-only USB cable like PortaPow ($9.99 for two-pack on Amazon)
- If a public computer is your only option to revive a dead battery, select the "Charge only" option (Android phones) if you get a pop-up when you plug in, or deny access from the other computer (iPhone).

12. Fake cellular towers, like FBI's Stingray

The FBI, IRS, ICE, DEA, U.S. National Guard, Army and Navy are among the government bodies known to use cellular surveillance devices (the eponymous StingRays) that mimic bona fide network towers.

StingRays, and similar pretender wireless carrier towers, force nearby cell phones to drop their existing carrier connection to connect to the StingRay instead, allowing the device's operators to monitor calls and texts made by these phones, their movements, and the numbers of who they text and call.

As StingRays have a radius of about 1km, an attempt to monitor a suspect's phone in a crowded city center could amount to tens of thousands of phones being tapped.

Until late 2015, warrants weren't required for StingRay-enabled cellphone tracking. The American Civil Liberties Union has identified over 75 federal agencies in over 27 states that own StingRays, but notes that this number is likely a drastic underestimate. Though some states outlaw the use of eavesdropping tech unless in criminal investigations, many agencies don't obtain warrants for their use.

Likelihood

While the average citizen isn't the target of a StingRay operation, it's impossible to know what is done with extraneous data captured from non-targets, thanks to tight-lipped federal agencies.

How to protect yourself

- Use encrypted messaging and voice call apps, particularly if you enter a situation that could be of government interest, such as a protest. Signal (free, iOS/Android) and Wickr Me (free, iOS/Android) both encrypt messages and calls, preventing anyone from intercepting or interfering with your communications. Most encryption in use today isn't breakable, says Wisniewski, and a single phone call would take 10-15 years to decrypt.

"The challenging thing is, what the police have legal power to do, hackers can do the same," Wisniewski says. "We're no longer in the realm of technology that costs millions and which only the military have access to. Individuals with intent to interfere with communications have the ability to do so."

From security insiders to less tech-savvy folk, many are already moving away from traditional, unencrypted communications – and perhaps in several years, it will be unthinkable that we ever allowed our private conversations and information to fly through the ether unprotected.

Updated on 5/28/2020 with new ways your phone can be hacked and what you can do to protect yourself.