Signs of a Compromised Smartphone

Sudden Loss of Battery Life

A sharp increase in battery usage could indicate a compromise. Some malware commonly seen on Android devices, for example, will launch a service in the background to quietly consume data like GPS location without users' knowledge.

"Quickly, your phone goes from lasting the entire day to nearly running out of power by lunchtime," says Stephen Banda, senior manager of security solutions at Lookout. "With no other reason for this, it's likely that malware exists on the phone and is running processes that consume battery power."

You can check for this by opening battery settings on your iOS or Android device and reviewing how much power different apps consume. Checking the percentages can help determine any offending applications so they can be deleted.

Excessive App Permissions

Mobile apps can't consume certain types of data unless the user gives permission. Security pros urge smartphone owners to check the permission settings for each app they use and be sure the permissions granted are appropriate on a case-by-case basis. A gaming app, for example, shouldn't be able to read text messages or process outgoing calls, explains Nikola Cucakovic, senior security consultant at Synopsys.

"It's common practice for apps to not run unless full permissions are granted," she says. "For this reason, many users -- particularly those without a security background or focus -- often choose convenience and access over the potential threat posed by a given app."

Security experts strongly recommend only downloading apps from official and trusted app stores. This doesn't completely eliminate the chance of installing a malicious program; however, official stores do serious vetting to reduce the chances of malicious apps being published.

"I would advocate never installing an app from other than an accepted app market," says CrowdStrike's Meyers, noting Google and Apple do a lot of work to protect their stores from harmful apps.

Your Account Is Sending Messages, But You Aren't

Lookout's Banda points to this as a "classic sign" an attacker has snatched your credentials and gained access to your contacts, which they use to message friends and family in an attempt to spread their campaigns.

"Immediately change the password to your email account and also to other accounts where you might use that same password," he says. "Additionally, ensure that you have applied the latest security patches to your operating system and your email app."

Suspicious Texts and Unknown Websites

If you didn't order a FedEx package, you shouldn't be getting text messages saying a shipment has arrived, says Brian Foster, SVP at MobileIron. Smishing, or a text-based phishing attack, is a popular technique to convince people to open malicious links.

When victims click one of these links, it's tougher to see on a smartphone whether they're on a legitimate website. "It's hard for you to tell, am I really on Fedex.com, or on a FedEx property, or am I somewhere else?"' Foster says. If you're not expecting a message from someone and you receive a link, it's better to not click it.

Spike in Data Usage

Malicious code may communicate with external websites to download payloads or exfiltrate data, Lookout's Banda says. While adware may also contribute to higher data usage, that type of threat is usually more visible because it can cause the browser to erratically load a website, he explains.

This issue can be resolved by reviewing the phone's data usage metrics for excessive use by individual apps or system processes. Most wireless carriers also provide detailed reports of data usage trends, which can help narrow down any source of a sudden increase in data use.

"Depending on what you discover, it may make sense to restore your device to a previous device backup," Banda adds.

Key Passwords No Longer Work

If your password is no longer working and you're certain it's correct, it could mean someone has captured and changed your credentials. This could be done using a keylogger, says Banda, who notes one can be installed on a device through a phishing attack.

"Once the attacker has access to your account, they can change the password and gain full access to sensitive information within the account," he says. Banda advises resetting passwords for all critical accounts; as an additional measure, you could restore the device to a clean backup in case malware is at play.

Not All Attackers Leave a Trace

“While some mobile attacks may be obvious, others leave no clues at all,” says Boris Cipot, senior security engineer at Synopsys.

"It's important for users to understand that not all malicious acts leave red flags and that they don't always take place on your mobile device," he says. “One scenario in which an attack may be hard to identify could involve a compromised connection to a trusted gateway in which a reconnection is triggered and leads the user to a malicious gateway. A trusted VPN can protect against this kind of attack,” he notes.

Additional Steps You Can Take

In addition to a VPN, Cipot advises avoiding password reuse. If an attacker prompts a target to enter account data on a malicious web page -- for example, registering with a username and password to access Wi-Fi -- a VPN may be of little help.

"Never reuse passwords so as to limit any potential attacker from successfully accessing other services you may utilize," he says. "Password managers are advisable to maintain strong, unique passwords."

Cipot also suggests considering anti-malware software for smartphones to check whether installed apps contain any known malware or require unusual permissions, which should be flagged, he adds.

Other protective steps include keeping all applications up-to-date, adopting complex passwords and password managers, using multifactor authentication where possible, and only keeping applications you use. On occasion, check the list of devices allowed to use your primary apps using the Web version, and remove devices you no longer use.