Worried your smartphone might get hacked? Here's how to prevent

JINAT JAHAN KHAN

For hackers, a smartphone is like a digital passport holding a wealth of confidential information about any individual. Most people now rely more on smartphones to access their social media accounts, bank accounts, business emails, and to store sensitive personal and official data. Ultimately, it is like a hacker's paradise for all the wrong reasons.

While there is no foolproof way to identify and protect against smartphone hacking, here are some easy-to-follow steps to check primarily if your smartphone has been breached and some ways to protect it from such an attack.

4 telltale signs that your smartphone may have been hacked

Excessive usage of battery

If you suddenly observe a significant drop in your phone's battery life or if the battery is draining more quickly with your unchanged phone behaviour, then hacking may be the reason behind it. Sometimes malware can leave traces of hacking on your device. So go to 'Settings', tap on 'Battery', click on 'Battery Usage'/ 'Phone Battery Usage' option, and have a look at the list of apps. If you find any unknown app or something usual, that's a sign of concern.

Unusual and high data usage

In case your phone use habits remain the same but your data usage is skyrocketing without any valid reason, it's time to investigate. You need to check your 'Data Usage' from your mobile settings and poke around a bit. If any random app that is not much used by you but still uses 5GB data or more than it in a month, then something is wrong with that app.

Unrecognised apps and unusual pop-ups

Another telltale sign of smartphone hacking is if you find unrecognised apps installed on your device. Navigate to Settings and check the App list to see if there's something unusual. But be cautious that you know about your phone's pre-installed apps by its manufacturers and do not try to get rid of your smartphone's vital components.

Moreover, popping up random ads and inappropriate content frequently while browsing Google, Facebook or other well-known websites is an indication that your smartphone has some malware.

Unknown social media activities, phone calls, and messages

Unrecognised phone calls and messages initiated from your phone imply that someone else has access to your device. If you get email notifications of unknown login locations or sign-ups for any of your social media accounts or have unusual social media activities, be prepared to reset your accounts and phone.

How to prevent your smartphone from being hacked

Avoid auto logins

No doubt that using auto logins is a big time-saver. But it also increases the risk of getting hacked. An intruder just needs to open your browser and boom! They will get access to all of your online accounts and bank accounts. So login manually every time you need to use an online account. You can use a password manager app if needed. And avoid using the same password for every account.

Don't jailbreak or root your smartphone

Jailbreaking your iPhone or rooting your Android phone can compromise the security posture of your device and void the warranty. Installing unofficial apps from random sites makes your device vulnerable and more exposed to attackers. They can easily insert malware and steal your confidential data. Always download apps from trusted app stores such as Google Play Store and Apple App Store.

Avoid using public charging ports and unsecured WiFi

When you have a dying smartphone battery in an unfavourable situation, you may not think much before using any random and public charging ports. But it can increase the chance of juice jacking where a perpetrator can steal your data and track your keystrokes through the USB cable attached to your phone. Similarly, using unsecured public WiFi should be avoided as it can give access to your personal information to hackers.

Carry your own power bank to avoid using public charging ports. And if you have no way other than using such charging ports, try to use a wall outlet. In public places, use cellular data. But in case you need to hop on unsecured WiFi, enable your VPN. If you observe overheating or diminishing battery life later, it may indicate that your phone has been breached.

Clean browsing history, cookies, and cache regularly

A simple way to protect personal data from hackers is to delete or clear web history, cookies, and cache after every session. It is better to do it monthly or bimonthly. New layers of protection against threats are often added by developers. So make sure that you update your browser on a regular basis. Furthermore, never use the 'Remember my password' feature of your browser under any circumstances. Install a reliable password manager app instead.

Strengthen your security settings Always use phone locks. It will take a substantial amount of time for hackers to break such barriers and meanwhile you can block your most important accounts. If possible, add a Face or Fingerprint lock for better protection. In addition, to add an extra layer of security to your Google account, you can turn on two-factor authentication (2FA).

ILLUSTRATION: ZARIF FAIAZ