

Is your phone **hacked** ?

Smartphones have become a part and parcel of our lives. From emails to banking all our activities have gone online. Even after a lot of efforts by Google and Apple, mobile malware is present in the official app stores. Malware includes many different types of threats like viruses, spyware, worms, Trojans, etc. Malware is often downloaded from non-official sources, like phishing links sent via emails or messages or from malicious websites. The hacker can remotely access the data on the hacked phone and can also get access to the sensitive information. It becomes very important to recognize that the smartphone has been hacked.



How to know if your phone is hacked ?

When a Smartphone is hacked it exhibits various noticeable changes in behaviors. If looked carefully it can be easily noticed that the smartphone is hacked. Given below are various changes you should look for.

Battery draining very quickly or getting hot- Your phone's battery is draining very quickly or is not lasting long as it should do. This is due to increased activity on your phone. When a phone is hacked various processes run in the background, which cannot be easily detected by the user. People receiving messages from your phone which you never sent- If your phone is affected by malware, it often tries to use your messaging or email services to spread itself. It usually sends messages with a link to infect other devices. It uses your name to send messages, so if someone complains that they are receiving messages from you which you never sent then this may be a sign to look for.

A new app is installed or antivirus is uninstalled- If you notice that a new app is installed in your mobile phone which you never installed then this may be spyware installed by the hacker. If your antivirus got uninstalled automatically, then this may be malware which may sometimes uninstall your antivirus.

Strange Behaviour - Your phone is not working the way it should. Apps don't work properly. Your phone switches on and off unexpectedly or it crashes when you try to open anything.

Increased data consumption - You are using your phone as usual but your data consumption has increased. Hackers use the phone as a proxy to send information or mine bitcoins which requires data. This is a good sign to look for.

Pop-ups - If you notice a lot of pop-ups on your screen, then your phone may have been infected with adware which is also a form of malware that forces the devices to view certain pages.

Google Play Protect has been disabled - This is only for Android users. Google Play Protect is an inbuilt virus and malware scanner. Whenever an app is installed on an android phone it scans for virus or malware. A hacker may need to turn this off to gain access to the phone.

Mysterious Bank Transactions - Once a hacker gains access to your mobile device, he can skim your bank account information and do transactions from your card. There may be various reasons for mysterious bank transactions but one of them is malware on your smartphone or PC.

What to do if your phone is hacked ?

Remove some apps - Uninstall apps which were installed automatically or which you installed using an unofficial source. Also, check online to see if that app is a threat.

Run anti-malware software - There are various software online to check for malware on your device. Make sure that the software which you use is safe and reliable.

Change all your passwords - It is possible that if your phone is hacked, your accounts are also hacked. Change all passwords to restrict the hacker from entering your accounts.

Stay updated on various new threats- Various cybersecurity websites often write about new widespread threats. Stay updated on those threats and remove any such threat from your phone.

Reset your device - This is a great way to remove malware and malicious apps from your device. Just restore the phone to factory settings to remove the hacker from the phone.

Update your device- Various device updates often include security bug fixes. This may help to remove malware from your device. Update your device as soon as you get a notification to update.

It may not be always possible to remove the malware from your phone on your own. Consult a professional to remove malware from the device. Try removing the malware as soon as possible to minimize the damage. Adopt good cybersecurity practices to prevent the hacker from entering into the device.

