The rules need to know to enhance the security of iPhone, iPad and Android

Whether you use a device running iOS, or Android, there are common device security principles, preventing virus infection or account hacking.

The risk of being infected with viruses or malware is now not only a computer system, but also a telephone device within the scope of the attack. Whether you use iPhone, iPad, Android devices, or Windows Mobile, you can easily encounter dangers, from viruses, account hacking, information theft, etc. Therefore, you protect your smartphone first. The dangers are essential, with some basic principles that we should not ignore.

1. Root or jailbreak increase virus infection:

To be able to download and install many applications, programs from outside, or customize some settings on the computer, we usually root Android device or jailbreak iPhone / iPad.

However, when rooting or jailbreaking, it means that you have broken all available settings for the operating system, going into the operating system and also means "clearing the way" for hackers and malware to enter the device. . When the security barriers of iOS and Android have been broken, the risk of virus infection will increase. It's best not to root or jailbreak your device.

2. Installing the App from source contains many risks:

Nowadays, apps for Android and iOS are developed in many rich and diverse sources, not only on App Store or Google Play Store. There are even many applications that cannot be found at the two main stores, but can be installed from an external source.

However, downloading pirated apps from outside, not downloading from two official sources above also contains many risks, similar to when you install computer software from outside sources. Most users will install cracking applications through a number of websites, using a developer-only mechanism to test applications that bypass the App Store. Or choose to search for sources to download the APK file of the application or game.

Because of installation from an external source, there will not be any verification, checking from Apple or Google. And of course, all kinds of malicious software can be installed directly on a tablet or phone, when we install unofficial application files. There have been many cases of being attacked when installing the application in the above way, from which the account information was compromised, hacked the device to sneak on the microphone or camera.

So it's best to find apps on 3 main sources: App Store, Play Store and Windows Store. So what if you want to find applications on external sources?

Amazon App Store is a store that can be trusted for users, or access online stores by each manufacturer such as LG Store, Samsung Store, .

3. Don't ignore the screen lock feature, the system:

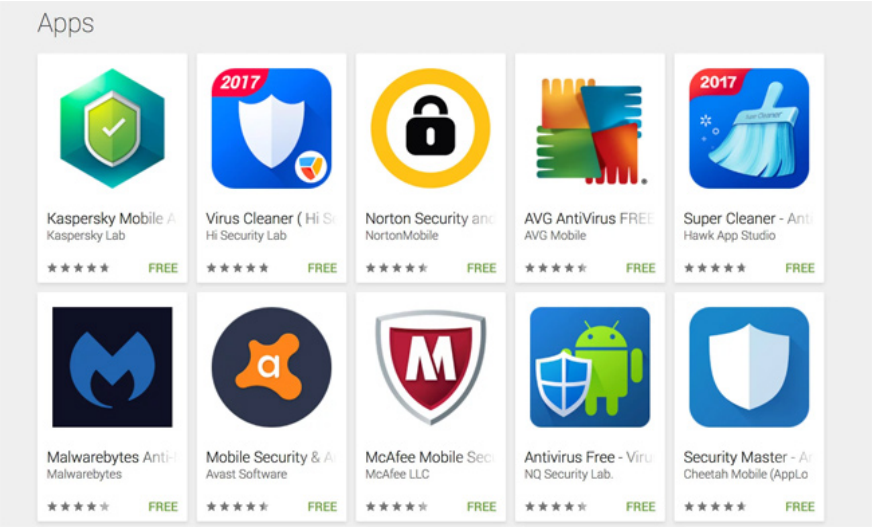
The security lock mode such as screen lock, PIN code creation, fingerprint lock or Galaxy S8 has security mechanism with iris, not only prevents unauthorized opening, but also prevents the card on the system. When you set up security methods, if any app wants to intervene it is necessary to enter the correct security code, such as entering the correct fingerprint set.

Or simply when you want to add an online account to the device also need to authenticate by PIN, fingerprint, . If any application wants to add an account to the machine to track information or data synchronization, then forced to overcome this security barrier.

4. Be wary of virus scanning app:

It is not difficult for you to find a virus scanning application on the app store, with ads for powerful antivirus protection. However, is it really necessary to install those apps, when iOS and Windows Mobile are never able to get infected?

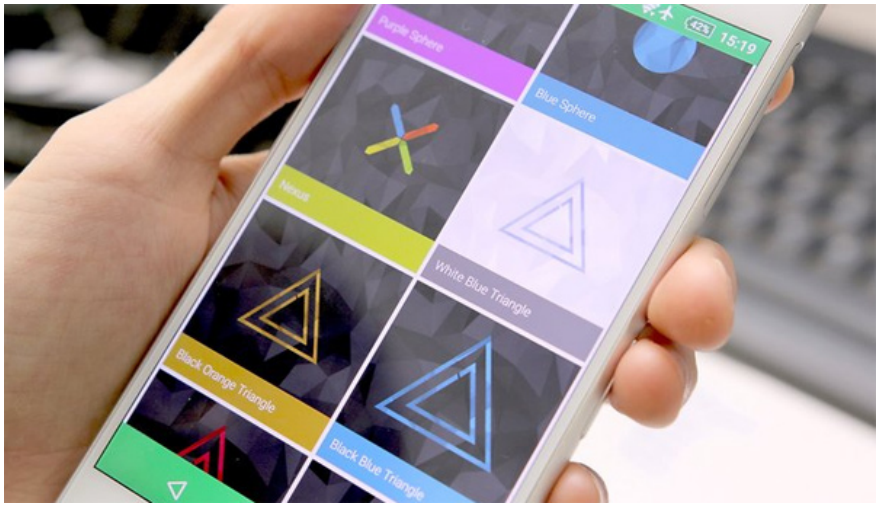
With the Android operating system, most applications labeled with antivirus are actually only capable of cleaning up memory. In addition, there are many cases of malware pretending to be anti-virus applications to attack users' devices.



5. Check apps for freeing RAM, optimizing battery, increasing performance, app wallpaper:

Similar to antivirus applications, these apps are also often hacked by hackers, especially on Android. There are many cases where the wallpaper app is installed with malware that controls the device remotely, or the optimized app of adware disguised battery to collect user information, etc.

With the continuous development of the smart mobile industry today, the device has the ability to turn off unused applications to increase storage capacity and reduce system resources. Or you can manually clean the system manually, like turning off the app running in the background, clearing the application cache, .

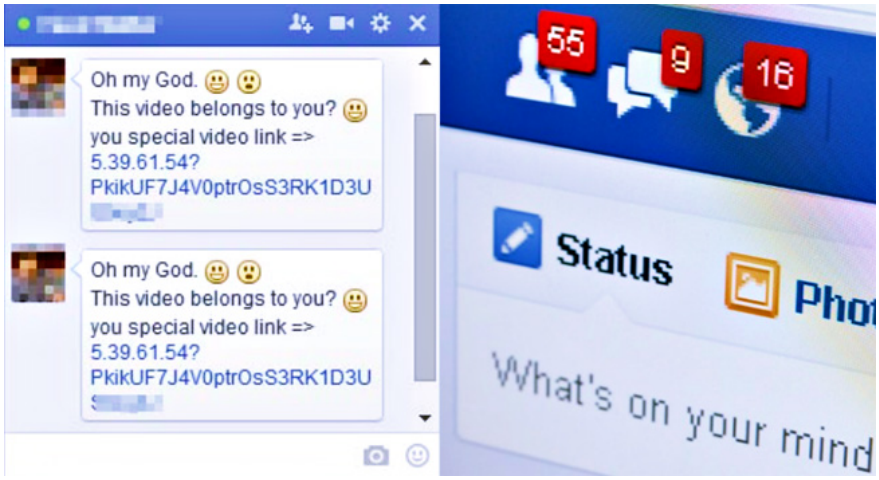


If you need to use it, first check through the app reviews, or search on Google to see what others say about the application.

6. Avoid clicking strange links, on Messenger, messages:

The infection of malicious malware via links is an uncommon phenomenon, occurring on computers on smartphones. There are many cases where your friends' Facebook accounts are hacked, send you a malicious link and if you are not alert, we will become the next victim.

Before opening any link, please confirm it clearly with the sender, if you know the person. If with strangers, absolutely do not click on that link. Now the number of hackers taking advantage of SMS / MMS and Messenger is on the rise, because these two services have a large number of users.



Whether you use Android, iOS or Windows Mobile, being infected with malware is inevitable. Therefore, protect your 'mobile phone' against dangerous risks. Only with the above basic rules, users can also partially prevent the security risks of using the phone.

Hope this article is useful to you!

You finished reading the article "**The rules need to know to enhance the security of iPhone, iPad and Android**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and

tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.