Anti-malware tools, safety protection for smartphones

Smartphones and tablets are now not only communication devices, but also a place for many important personal data. If you do not protect the device properly, these data will be stolen by bad guys.

Here are useful tools to install on your smartphone and tablet, to help detect whether or not the device is infected with any spyware and prevent potentially dangerous malware. enter the machine in the future.

Determine if there is an application that arbitrarily uses the camera and microphone on the smartphone

Many spy applications will silently use the camera and microphone on the smartphone to take pictures or eavesdrop from the smartphone without the user knowing.

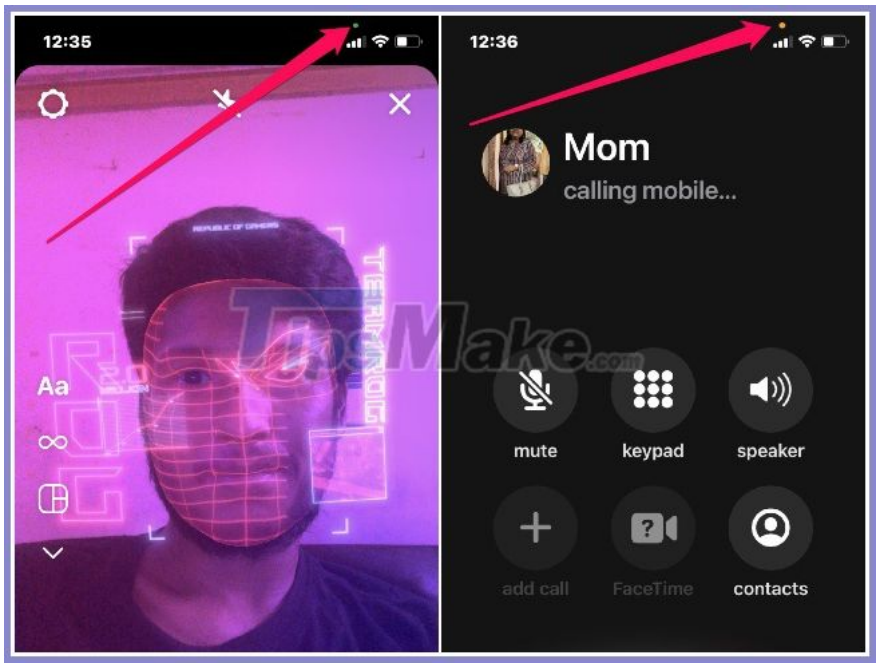
With iOS 14 for iPhone, Apple has equipped a very useful feature, that is, every time a user launches an application on the device and that application is secretly using the camera or microphone on the iPhone, iOS 14 immediately displays a small icon for notification. This makes it easy to identify which apps are using the camera and microphone to be cautious and find out if it is a spy application to remove from the device.

A blue dot appears on the iPhone's screen running iOS 14 to warn the app is using the camera

To use this feature, iPhone users can upgrade the device to the iOS 14 beta beta (now widely available to users) or wait until Apple releases the official iOS 14 and then upgrade. your device.

For Android users, you can take advantage of an app called Access Dots. This is a free application, in which every time you launch a certain application and the application is accessing the camera or microphone of the smartphone, on the device screen will appear two colored dots (blue indicates the application is in progress. use

the camera and the orange indicates the app is using the microphone).



Access Dots apps appear blue or orange dots on the Android smartphone screen to warn when an app is using the device's camera or microphone.

Based on this, you can know if a running application is silently accessing and using the camera / microphone or not, to remove this application if in doubt. For example, if you activate the photo / video capture app, Access Dots will display both orange and blue dots, which is normal since the camera app needs to use both the camera and the microphone to take the photo. and video recording.

However, if you activate a web browsing application or a certain game, but Access Dots appear colored dots on the screen, it means that this application or game is silently using the smartphone's camera and microphone. All you should do is remove the app or game from your smartphone for safety.

Currently, Access Dots only has version for Android, readers can download and install here (compatible with Android 7.0 and up).

The app helps to check if your smartphone is being tracked or not

The common way of working for spy applications is to silently steal data on users' smartphones, then send this data to an external server via an Internet connection. Based on how this works, users can determine whether on their device is being tracked or not thanks to the help of Data Counter Widget.

Basically, Data Counter Widget is an application that allows to manage the amount of Internet used on smartphones (including WiFi and mobile networks). However, the Data Counter Widget also has the feature of knowing which applications frequently connect to the Internet and whether or not to send data from smartphones to outside.

Based on the information provided by Data Counter Widget, you will determine whether there is a spy application silently active on your smartphone and sending data out.

Currently the app is only version for Android, readers can download for free on the app store Google Play Store, or download directly **here** or **here** (compatible with Android 6.0 and above).

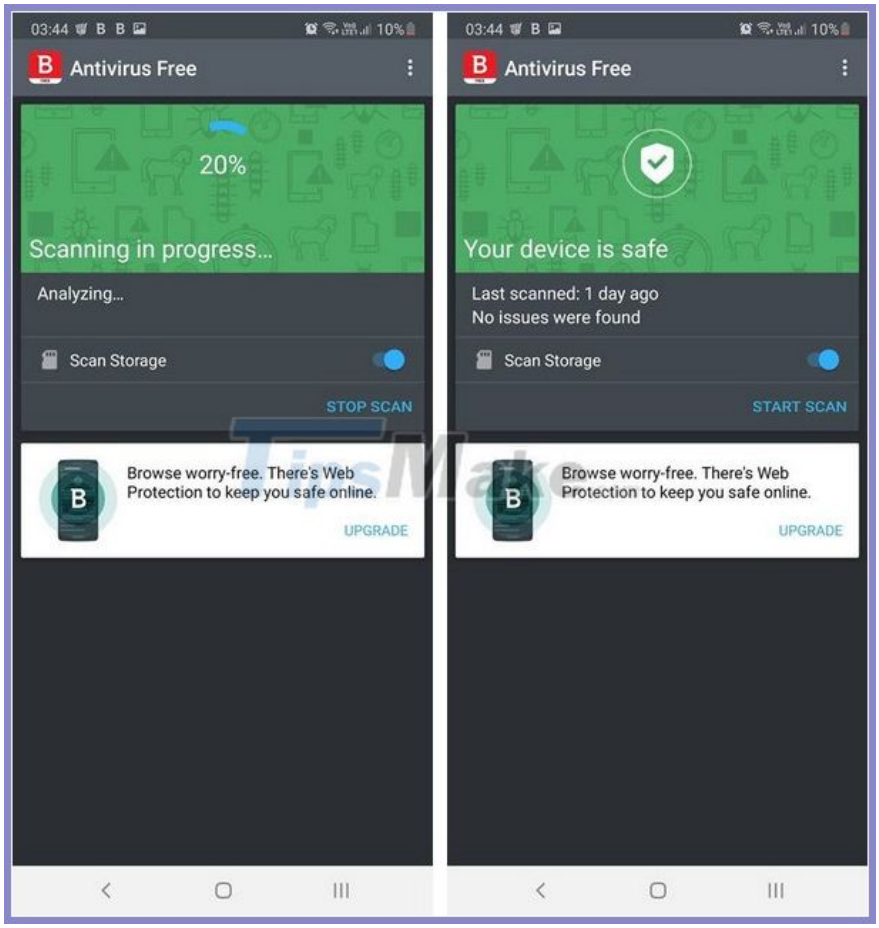
Apps that help your smartphone resist the intrusion of malicious code

Android is considered the number one target of hackers when it is estimated that up to 99% of new malware appears targeting this mobile platform. Malware types targeting the Android platform are often very diverse, but mainly they impersonate as 'clean' apps to trick users into installing, then silently collect personal information on the device to send out. outside.

For amateurs, it's hard to spot fake apps in the conventional sense. Therefore, to be on the safe side, you should use security apps to automatically scan and identify 'clean' apps before allowing them to work on the device.

There are quite a few anti-malware applications available for Android smartphones. Basically, smartphones don't really need anti-malware apps, what users need to do is always be careful and carefully check the apps before installing on their device.

In case you want to install a security application to increase safety for your smartphone, you can use Bitdefender Antivirus Free application. This is a compact and simple tool, so it does not affect the performance of the smartphone.



After installation, Bitdefender Antivirus Free will be in automatic protection mode, users do not need to do any setup steps. Every time you install a new application on your smartphone, Bitdefender Antivirus will automatically check if the installed application is 'clean' before allowing it to work.

In addition, users can also use BitDefender Antivirus Free to scan the entire device to check for the presence of malicious code available on the previous system.

Due to the use of cloud computing technology, with the database all stored on Bitdefender's server, this application works very gently and does not affect the performance or battery life on the device.

However, due to the use of cloud computing technology, users need to have an Internet connection every time using BitDefender Antivirus Free's scanning function (only when scanning, but normally, no Internet connection is required. can still be protected by the application).

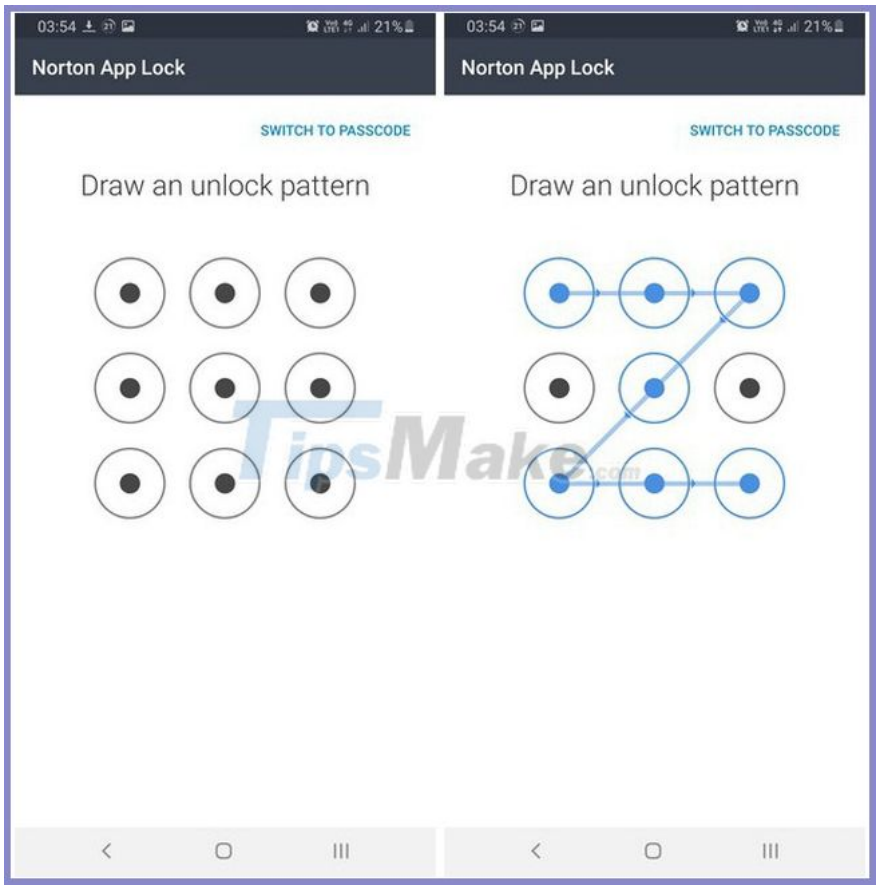
Currently the application only has version for Android, readers can download and install from the Google Play app store, or download directly here or here (compatible with Android 4.1 and up).

Tool to help protect important applications and data on smartphones

In addition to tools that help protect the attack and intrusion of malicious code from outside, users should also install a tool to actively protect privacy right on your smartphone.

Many people often lend their phones to their friends to play games or surf the web, but they are afraid that they will read their private messages on it, or do not want them to see the pictures taken on smartphones .

Also, you are concerned about whether your smartphone is stolen and bad guys can unlock the smartphone and view the contents inside.



An application called Norton App Lock will help you to solve this problem. This is a free application of Norton security firm, allowing users to set a password to protect access to applications installed on smartphones, such as messaging applications, email, photo albums .; from there, you are not allowed to activate these applications by outsiders to protect your privacy.

One advantage of Norton App Lock is that the protection can be turned on / off easily, so you can activate the protection when needed, for example, when lending your phone to a friend or child.

Currently the application only has a version for Android, readers can find and download from the Google Play application store, or download the application directly here or here (compatible with Android 4.2 and above).

The above are useful tools that should be installed on your smartphone so as not to get malicious code or spyware from entering the device, to avoid the case of important and sensitive data on the smartphone being stolen by bad guys.

You finished reading the article "**Anti-malware tools, safety protection for smartphones**" 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.