How to detect malicious apps on Android

Installing applications outside of Google Play is often potentially risky, making users more likely to steal personal data and money. Therefore, the detection of malicious applications on Android phones will help you distinguish what will be a safe application, where the application contains malicious code, thereby minimizing the download of dangerous applications. Security and protection of Android devices become safer.

Android is one of the most popular operating systems in the world, but this does not mean it is the safest operating system in the world. Installing applications outside of Google Play is often potentially risky, making users more likely to steal personal data and money. Therefore, the detection of malicious applications on Android phones will help you distinguish what will be a safe application, where the application contains malicious code, thereby minimizing the download of dangerous applications. Security and protection of Android devices become safer.

1. 4 ways to uninstall apps for Android devices
2. 6 tips to enhance security for Android phones
3. 3 signs that your Android device is attacked by a virus

1. Use the malicious application detection feature

You may not know, this is an extremely useful feature that Google has integrated on each device through the Google Play application to help you prevent malicious applications on the phone and identify dangerous applications. dangerous. This new feature is called Play Protect, when you install an application of unknown origin, the system will immediately check. With malicious applications on Android, this feature will notify and prevent users from installing applications.

How to enable this feature is already in the content of the article Protect Android device by sending unspecified applications to Google that previously Network Administrator ever shared, you can review to know how to use it details.

2. Absolutely not install applications of unknown origin

Currently, there are many sources of application downloads, APK files for Android are not clear origin, so the device may face the risk of being attacked by malware. Fix this situation, you absolutely must not install applications from poor quality sources, unknown sources. In addition, limiting the use of third-party marketplaces is widespread because it is likely that the application has been infected with malicious code, causing your device to be affected during operation and operation.

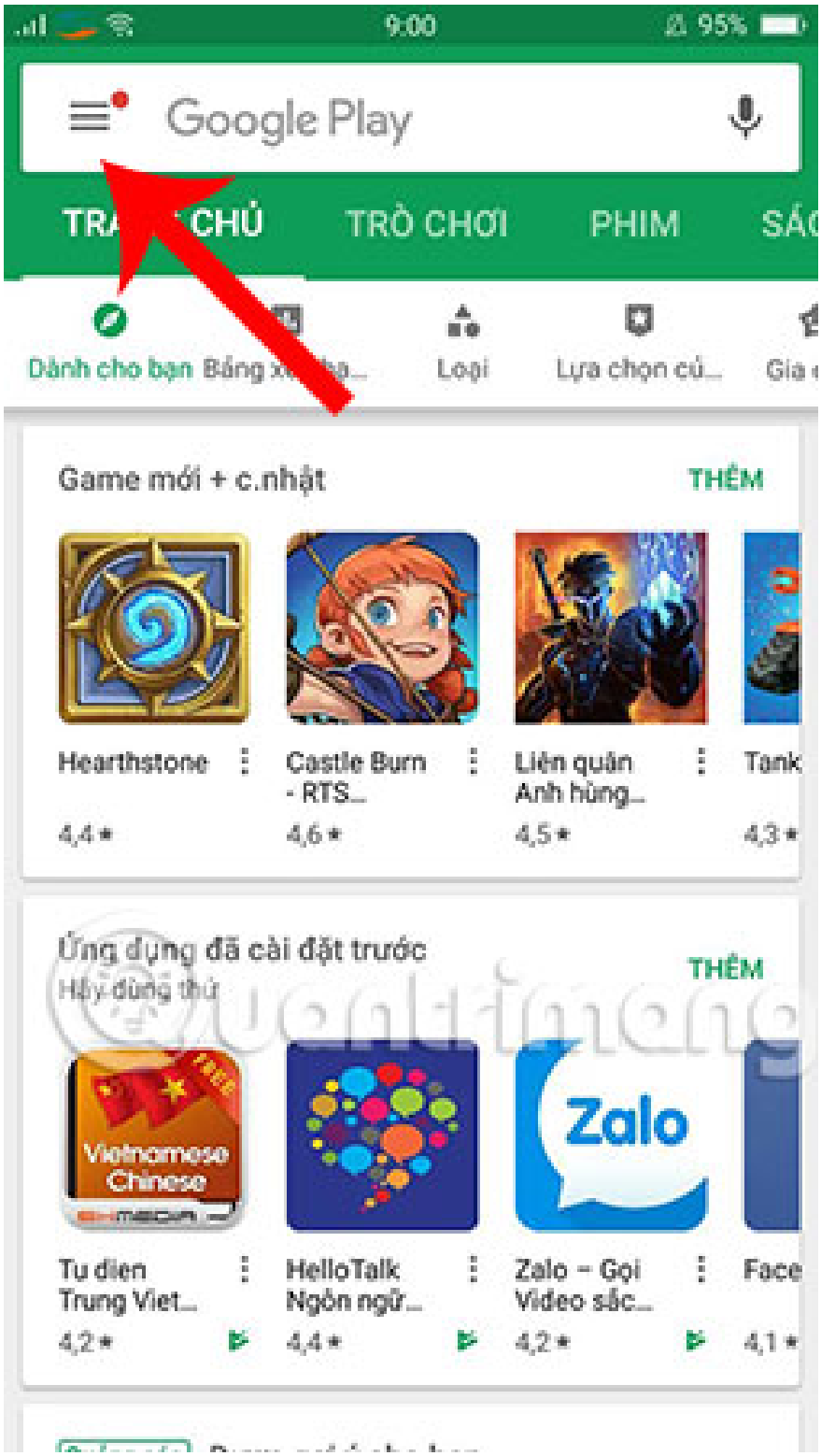
3. Scan harmful apps on Android

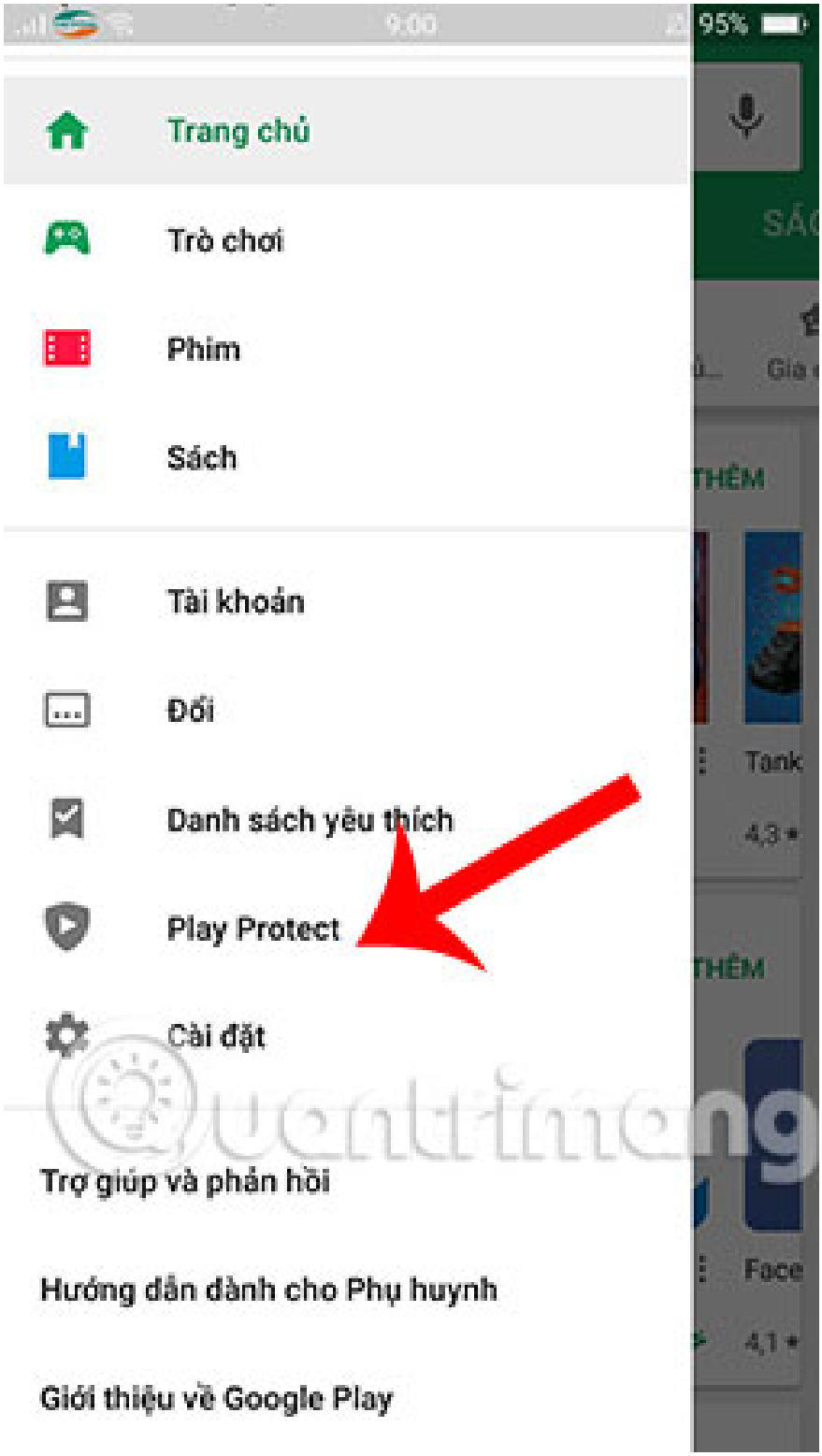
Similar to the previously used malicious application detection feature, the Play Protect feature that has been integrated on current Android devices can help users to detect malicious applications. Android by checking and

scanning harmful apps on Android.

Step 1:

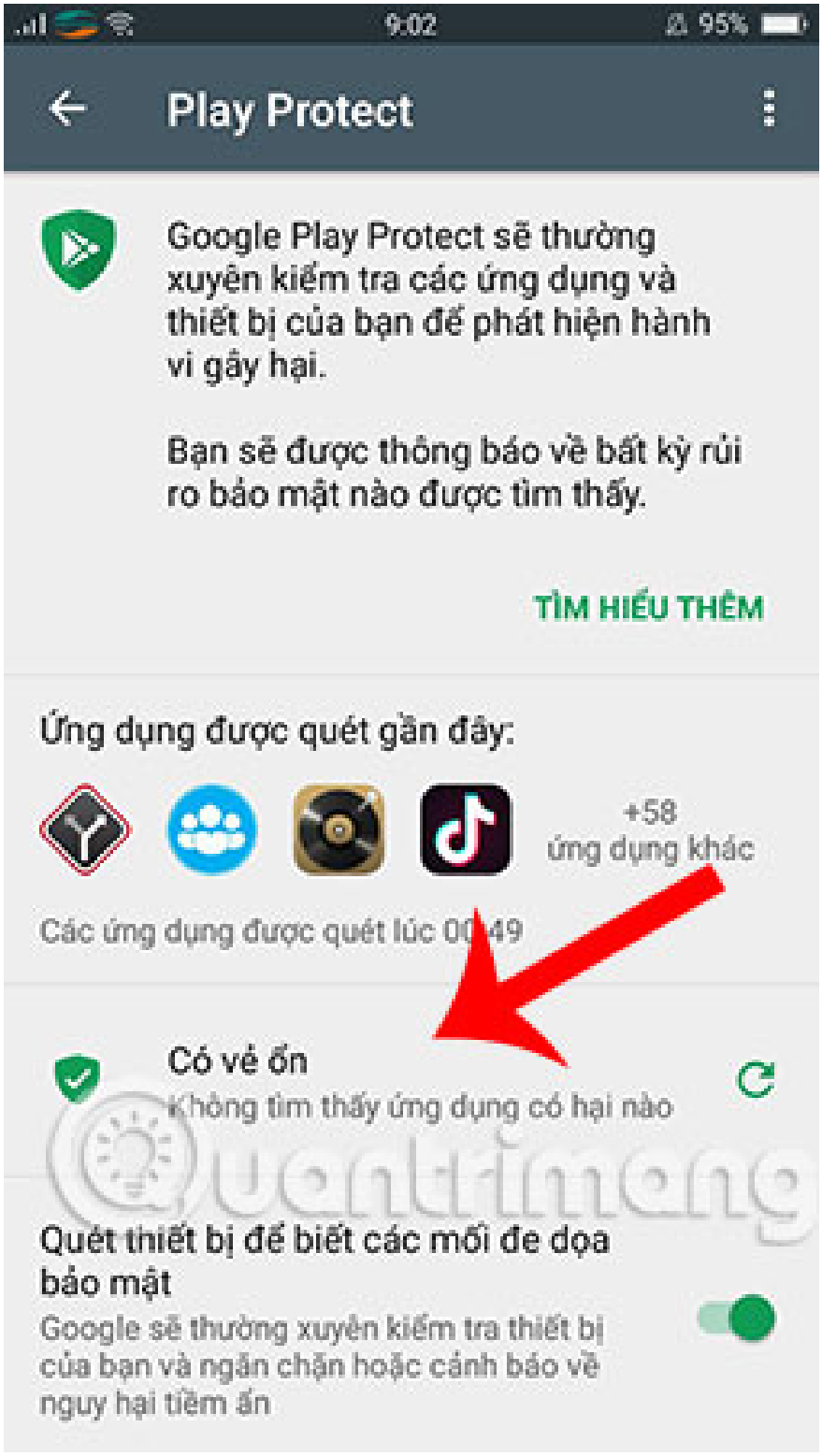
Open the Google Play app on your phone, click on **the 3 dashes icon** in the upper left corner like the picture and select **Play Protect** .





Step 2:

Next, select **Scan device for security threats** . The system will check all applications that you have downloaded and installed on Android. When results show up with **Look Good** , this means that the applications you download on Android are quality applications, you can rest assured and continue using them.



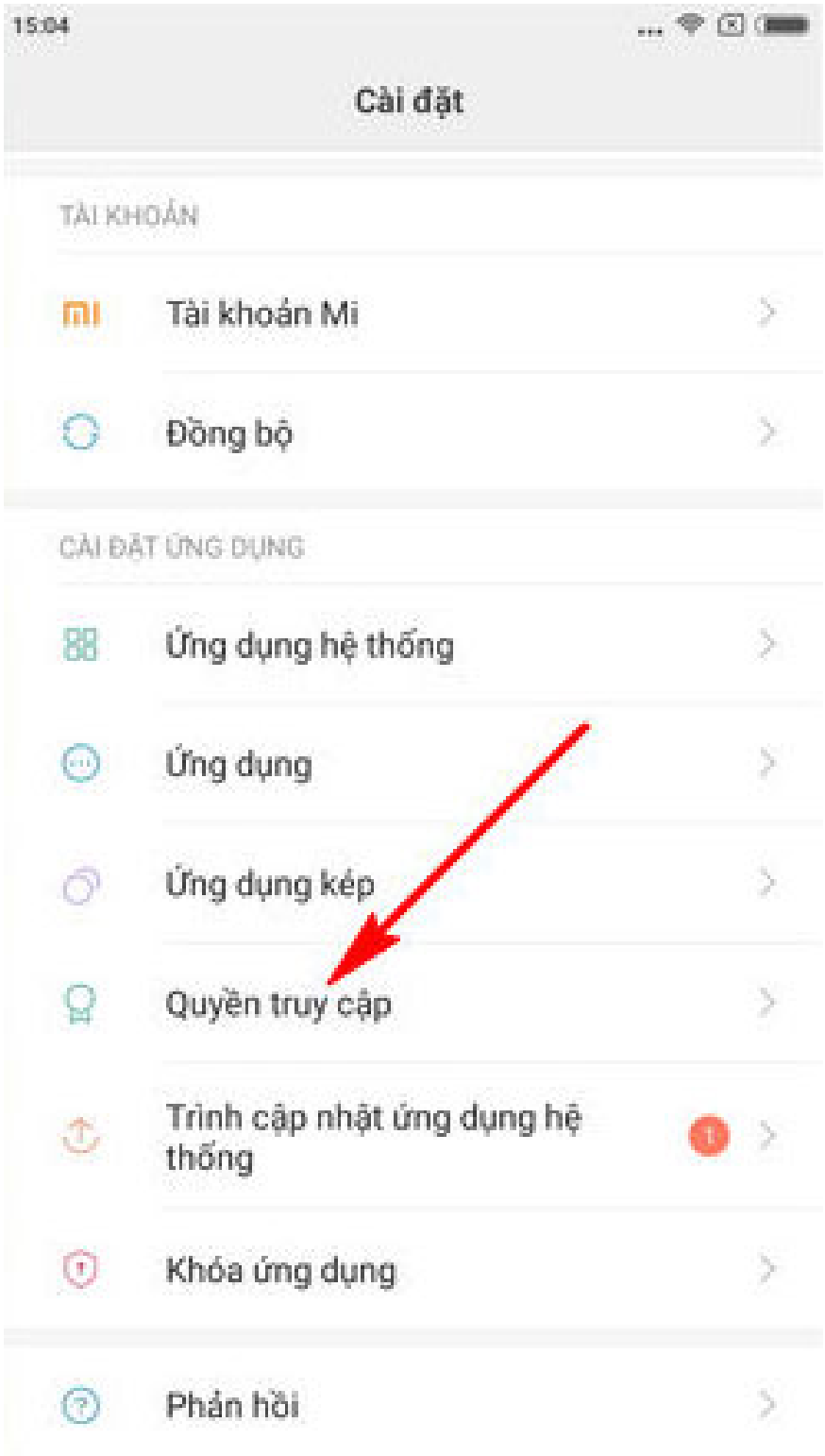
4. Restrict application permissions to access the device

Some applications, even if they are downloaded from Google Play itself, do not stop collecting user information by requesting device access. For example, with photo editing applications on Android will not need to access the calling program, so if you grant access to the device too much without noticing it is very easy to be collected by malicious applications. and use of personal data. You can track access rights of applications that we have granted

the following way:

Step 1:

Access the **Settings** app, search and click the Access Permissions section. For other Android devices, you can select from the application management screen on **the 3 dots icon** in the upper right corner of the screen and select the **Application permissions** .



Step 2:

At this point, the access rights on the phone that the application is using as well as the request will display, you check the access rights and find the connection permissions of applications that feel inappropriate. .

5. Always update the Android version

Similar to iOS devices, Android updates will help patch security holes and update features to enhance the user experience. You can refer to how to update Android operating system has been very detailed instructions by us to ensure the process of using your device.

Above is how to detect malicious applications on Android phones, please apply these ways immediately to protect Android phones better!

I wish you all success!

See more:

1. How to fix Pending pending download of apps on Google Play
2. How to remove malicious software (malware) on Android applications?
3. Top best antivirus application for Android phones