Tips to detect spyware stealing information on the phone

Currently, there are many spyware that install malicious codes to steal personal information of phone users. So how to detect these malicious software.

On the CH Play app store currently there are a lot of malicious applications installed to collect some information on the user's device, although it only takes away some information that the application is granted access to. but more or less annoying the user.

The most obvious sign when the phone is installed with spyware is that the battery often drops quickly; regularly receive / send data when there is an Internet connection; the device runs abnormally slower .

In fact, according to the sharing of technology experts of Mobile World, to detect whether the phone is being installed with spyware or not, users can use an application called Antivirus & Mobile Security. This is a tool to help remove hidden people from the user's device.

The main function of Antivirus & Mobile Security is to be able to scan and remove viruses, malware, spyware and trojan applications as well as detect dangerous easy-to-exploit vulnerabilities such as Heartbleed, FakeID, Privacy Disaster. and Shellshock.

In addition, this application also helps to backup private data including contacts, call logs and SMS messages as well as restore this data to other devices. Locate & sound lost phone alarms. Find lost or stolen device by ringing, alarming and flashing the device flash right in silent and dark mode.

So to detect whether the device has spyware or not, the user just needs to select Check It Now for the application to check automatically.

Also in the App Manager, Antivirus & Mobile Security will list out applications that are collecting personal data of users for advertising. If it finds it, it will display Passive grayware and the user can remove it immediately under Uninstall.

In case of detecting suspicious signs of spyware infection, users should also install and use an anti-virus application for Android platform to scan and check their device.

For added safety, users should back up all the data on their device, then perform a device restore to the original state (Restore factory settings) to bring the device back to the Like when it was released from the factory, this helps to wipe out applications (including malicious apps) that have entered the system.

Remove unnecessary applications: the more applications are installed on the device, the more security vulnerabilities created by applications are hidden so that hackers can exploit and infiltrate. Removing unnecessary, rarely used apps is a useful way to keep Android device safe.