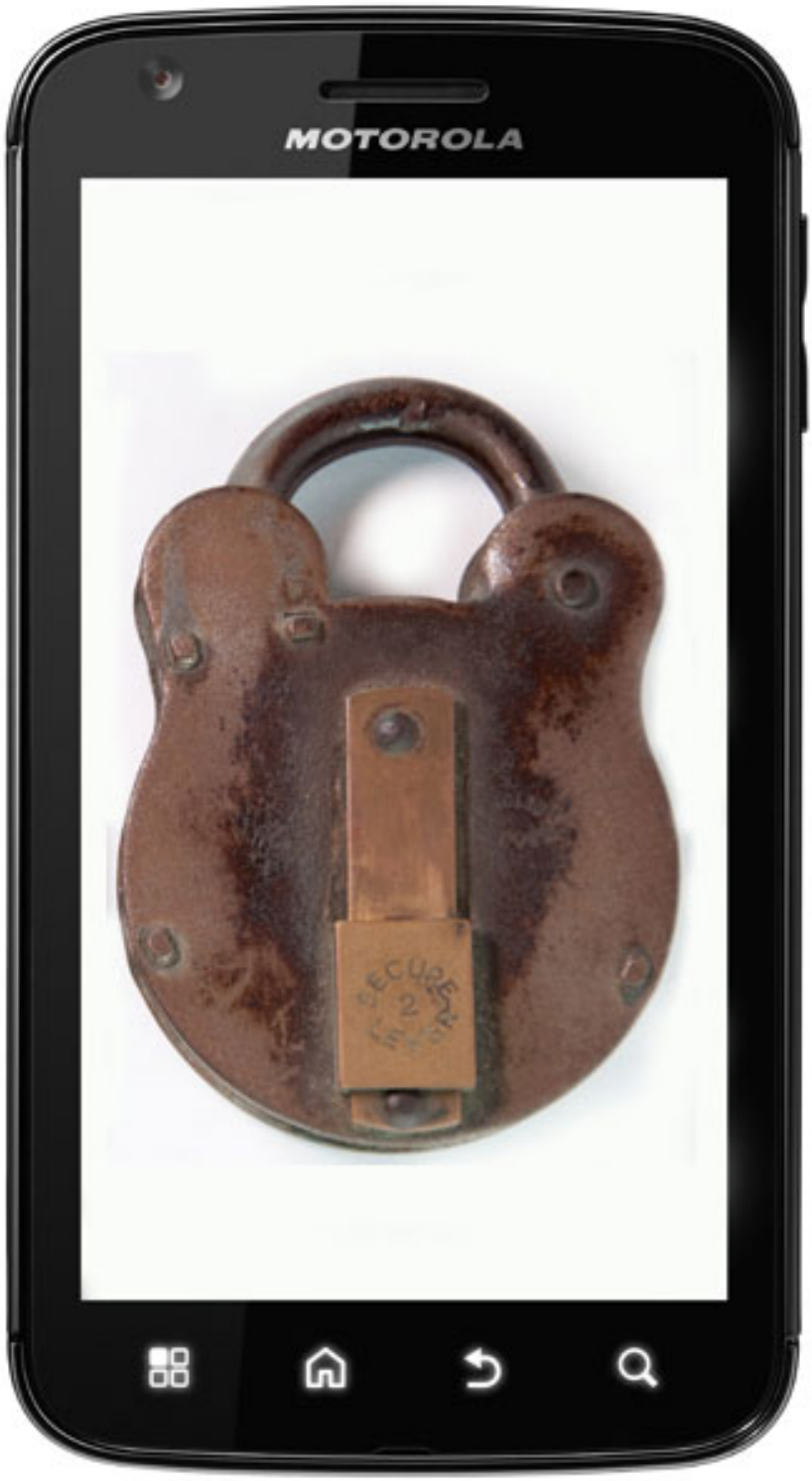
Android security: 6 tips to help protect Google Phone

Now it's time for us to keep more eyes on Google Android security. The 6 tips and tricks below will help you do this.

TipsMake.com - **Due to growing concerns about malware on Android, we will share with you 6 tips and tricks - along with some free software - to help you protect your smartphone Your Google Phone, as well as ensuring personal data is always safe.**

Google's Android Market application market has been attacked with the first malware attack, a popular application called "DroidDream" has been found to be able to infect malicious code to steal user's personal information. and Google was forced to use a "kill-switch" built-in tool for Android to remove this troubling application. However, this is only done when the application has infiltrated thousands of phones running the Android operating system.

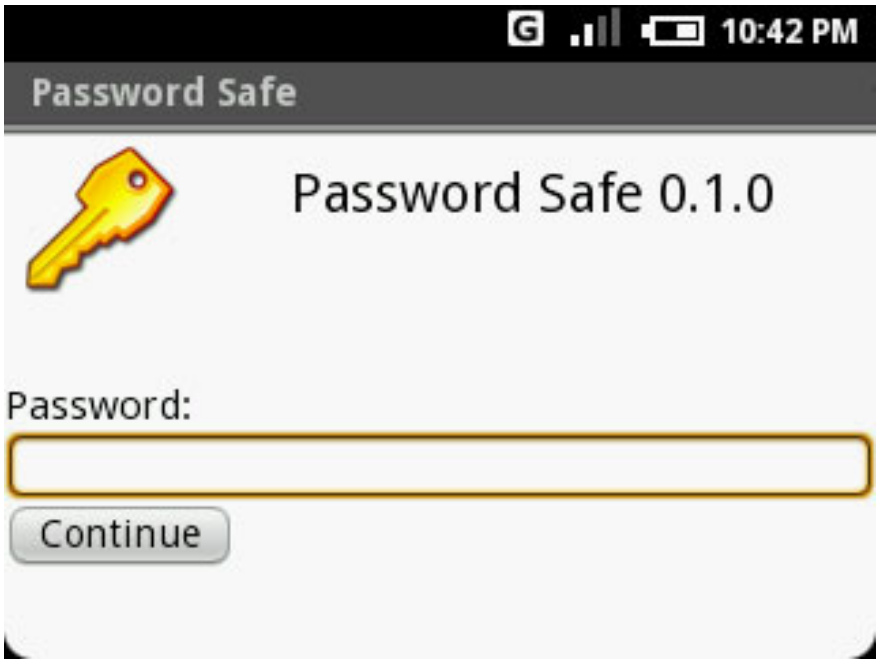


According to ComScore, the Google Android operating system was not very popular in the past. However, Android currently holds 31% of the smartphone market share in the US. This has helped this operating system become the most popular smartphone operating system in the United States.

Besides, Android has never been a favorite target for hackers and eye-peeping eyes to take advantage of the popularity of this platform to profit. In other words, it's time for us to keep more eyes on security for Google Android. The 6 tips and tricks below will help you do this.

1) Phone protection with password - Immediately!

The simplest but most effective protection method you can apply to protect your Android device is to lock it with a password. Listening is simple, but strong passwords - even weak passwords - can protect you and your phone from a lot of attacks. If a malicious code does not have the password to unlock the screen, your data and all other information on the device is safe.



Depending on the Android phone model you are using, you will have a lot of password options, but they are all accessible in the same way. Open the **Settings** menu on Android and scroll down to the **Location & Security Settings** or similar section. First, open **Screen Unlock Security** and then you will see a series of password options to choose from, based on your device.

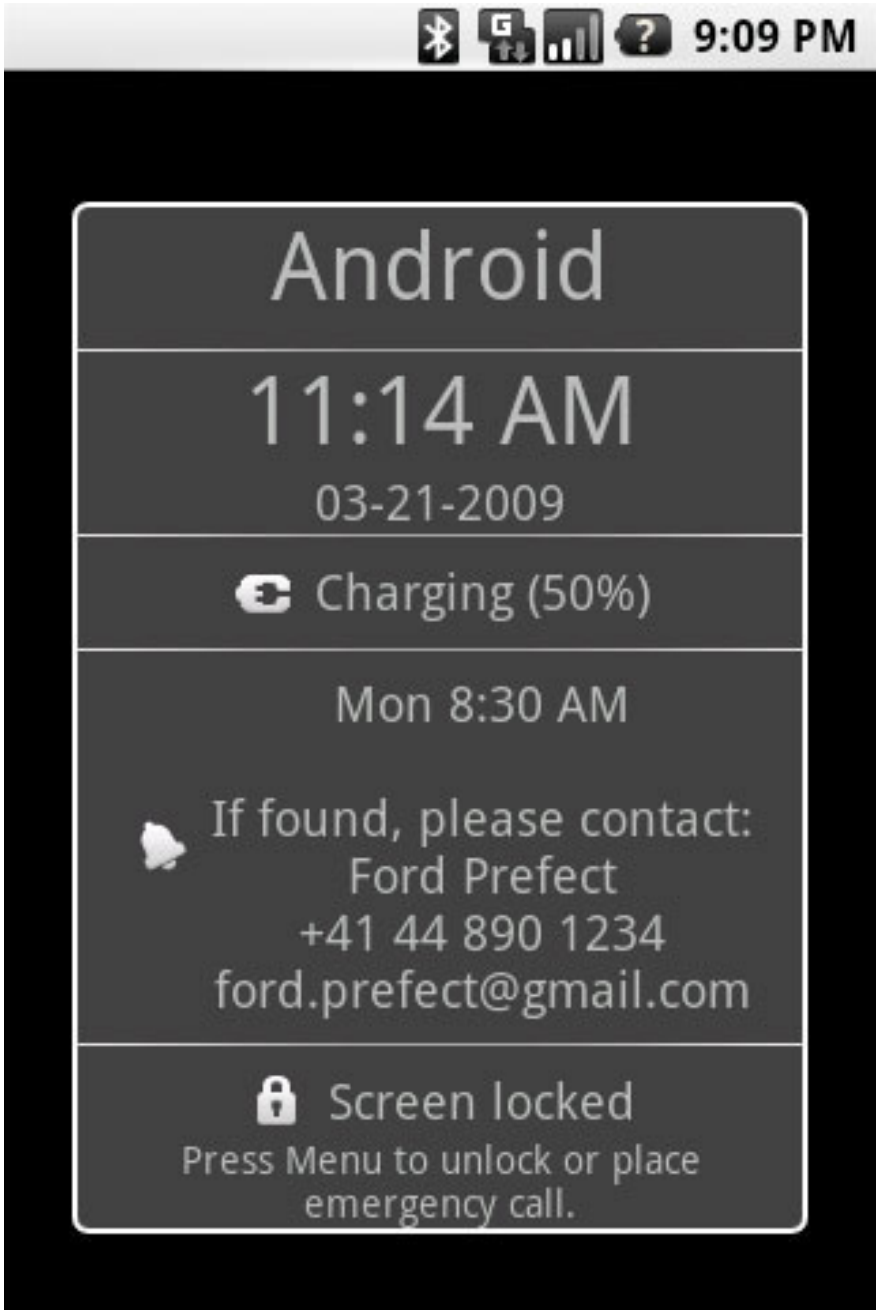
For example, the Motorola Atrix 4G device offers password options like a pattern lock - Pattern Lock - helps you put a 'model image' to unlock your device; a Pattern Lock, using numbers to protect the device; a Password Lock, so you can use both characters and numbers; and finally the biometric Fingerprints Lock, use the Atrix's fingerprint reader to confirm.
Although Fingerprint Lock is the most secure option, there are still many people concerned about storing biometric information on Google's servers, so there are other options like Password Lock. In order of security, Fingerprint Lock is the safest, followed by Password Lock, PIN Lock and finally the Pattern Lock. However, using one of these protected password options of Android is still much better than not using a choice at all.

(**Note:** If you choose to select Pattern Lock, you should regularly clean the screen because if you 'paint' too many times it will leave a trace on the screen and the hacker can pay attention and try to access your device. you by the way).

After setting the password for the Android device, you should set the Screen Timeout option to the lowest level so that your device will display and lock itself in a shorter time after you touch it. To do this, open the Android **Settings** menu, scroll down and select **Display** . On the next screen, find the **Screen Timeout** option and set a value - one minute or less should be set to get the highest security.

2) Customizing the home screen is locked with Owner Info

Imagine that you unfortunately forgot your smartphone in a bar. Someone who is kind to find the phone and wants to return it to the real owner . however, it is locked and the home screen only displays a pretty Vista screen but it does not help.



Such a thing happens often, and if the smartphone owner adds more owner information to the phone's home screen, more and more lost devices are likely to return to the owner. However, Android does not have any built-in options that allow you to post information to the device's locked home screen, like other mobile platforms, such as RIM's BlackBerry operating system. However, there are some 3rd party applications that can help you do this.

Our favorite option whenever you want to add owner information to the home screen of your Android device: Phone Found application - Owner Info, is provided for free on the Android Market market. To be able to customize the Owner Info app, simply run the software, click on the Edit menu and fill in your contact information. You can then open the Settings section of the application and select the information you want to display on the device's home screen.

3) Do not root Android device

Rooting your Android device means removing many of the restrictions created by the manufacturer and the operator on the device so other third parties can install and provide the applications and services they want you to deploy. , along with many other things.

Rooting the phone also opens up the system access levels to the device's core sources, which is not a good thing, at least in terms of security. The reason is because doing so also means that you have removed the installed protection to protect your device from malware and other malicious codes.

Unless you are a programmer or someone familiar with Android and you simply want to take the challenge, you should not root your Android device. However, no root means restricting to some good applications and services, and you cannot download the application from many unofficial third-party applications. However, avoiding root will enhance security, because a large part of applications cannot access the system level without root.

Tips : Do not root your Android device. However, if you root the device, remember that when you root the device, you are significantly reducing the device's existing security.

---

4) Loyal to the official Android Market market application

Choosing a place to download applications for Android devices is a very good idea. In fact, we recommend that banjchir download applications from Android Market of Google, even if the DroidDream case proves that the main Android Market market is not 100% clean with malware and other malicious applications.

Usually, I often download Android apps from one source rather than the Android Market, however, I am still wary of threats, and I always use some virus scanning applications after downloading to ensure safety.

As a matter of fact, getting Android software directly from Google Market is always a smart idea.

5) Google Android Antivirus

A good anti-virus application for smartphones will scan for new Android software downloads to avoid misconduct, such as strange commands or strange download requests. And there are many antivirus applications for Android, free, commercial or paid currently available in the Android Market.

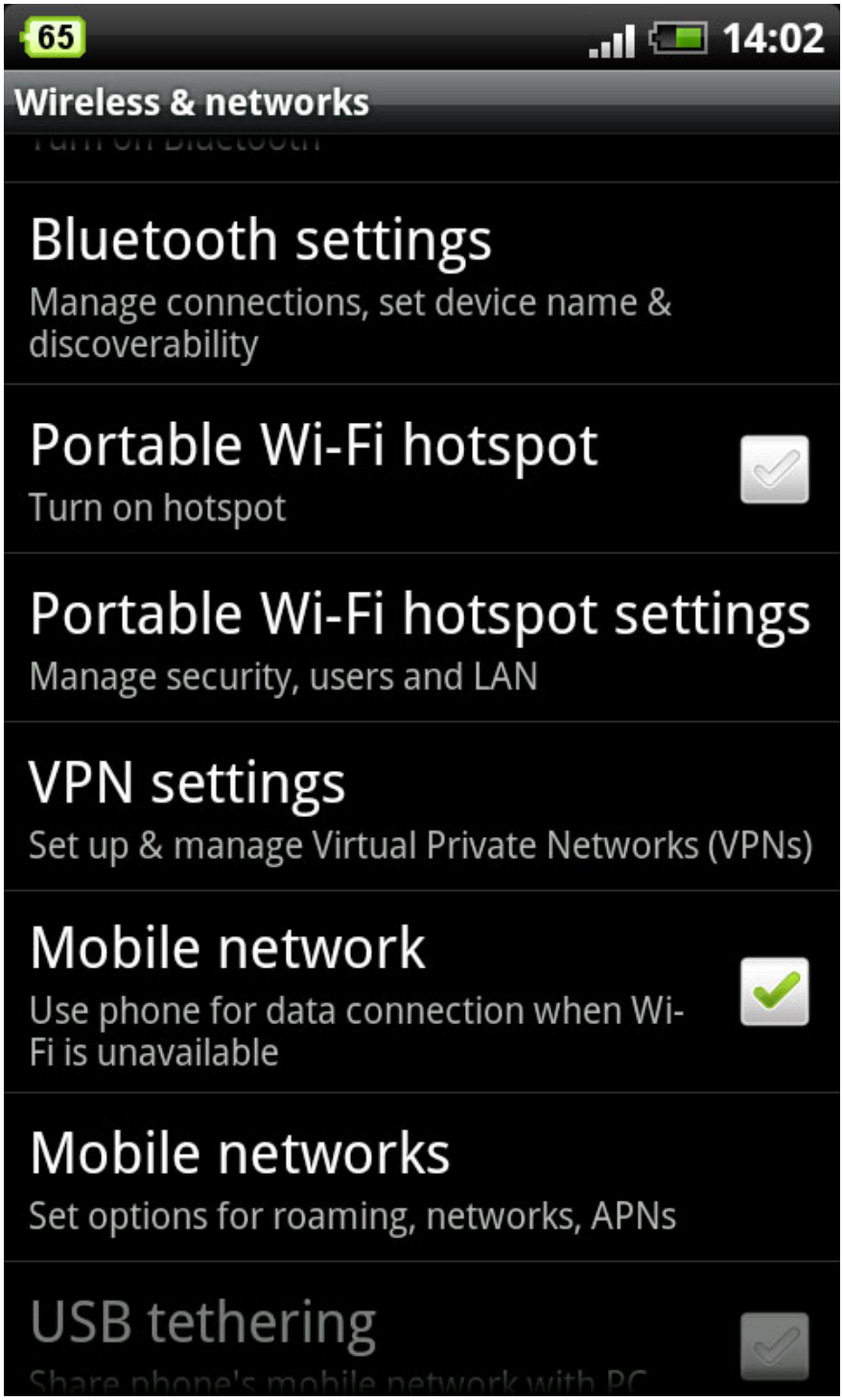
We cannot guarantee that all these software are effective, but generally, using one or more popular antivirus applications is better than not using any software. Our favorite application is Lookout Mobile Security. Lockout is a free application, with basic virus scanning, Find-My-Phone feature helps you find lost and stolen devices along with backup / restore options. Besides, you can also upgrade Lockout to get more protection features, but the free version also provides basic protection for ordinary users.

Another free antivirus application is an application called Antivirus Free.

Even if you do not want to regularly run an antivirus application for Android, you should still download an application and scan your device periodically to find malicious applications.

6) Wireless connection and security for Android devices

A very smart idea is to remove any or all of the wireless connection options you don't use on your Android device. In other words, you should turn off Wi-Fi every time you leave your home and not use another wireless network during the day. When you have finished using your Bluetooth headset, turn off Bluetooth. By doing so, you can not only maintain battery life, but it also helps you minimize the risk of detecting malicious parties, or even connecting to your device without your knowledge.



In addition, you should also disable the automatic Wi-Fi connection option - if your device has such an option - make sure your device doesn't automatically connect to public Wi-Fi spots. plus. Because through these points, some bad guys can access the data on your device. Turn off the Wi-Fi auto-connect feature by opening the Android **Settings** menu, selecting **Wireless & Networks> Wi-Fi Settings** . If your device has an automatic wireless connection option, you should see if it is listed here. Uncheck the auto-connect dialog to disable this function.

On the Wireless & Networks settings panel, you'll also notice a selection of **Bluetooth Settings** . Open this option and turn on Bluetooth if it is not turned on. Then, click on **Device Name** and change your device name, a

unique and familiar name for you. This will keep you from having trouble later when you want to connect your device to another device via Bluetooth.

If your device supports the hotspot feature, you should also protect your personal network. First, access the **Wireless & Networks** settings again and scroll down to select **Mobile Hotspot** . Next, turn on the **Wi-Fi hotspot feature** and click on the **Wi-Fi Hotspot Settings settings menu** .

Once enabled, the **Wi-Fi Hotspot Settings page** will display an option for you to **Configure Wi-Fi Hotspot** - **Wi-Fi Hotspot** configuration. Open this menu, assign a unique, new name to your network, choose **WPA2 PSK** protection from the Dropdown menu, and assign a password to your network. Save your changes and your Wi-Fi hotspot is safe.

A good habit is to turn off your Wi-Fi hotspot every time you don't use it, so that illegal objects can't take advantage of your network, increasing monthly usage and accessing information. Information available on the device.