5

Simple Steps to Secure Your *Android*-Based Smartphones

x^2

Google's open-source *Android* platform is quickly catching up with Apple's *iOS* and RIM's *BlackBerry OS* and is gaining its own loyal followers. From a mere 6.8 million units sold in 2009, the worldwide *Android*-based smartphone sales reached a whopping 67 million at the end of 2010.

With the growing sales figure, it's clear that the "Age of the *Android OS*" is fast dawning. Everybody is looking for a smartphone that does not only come with basic communication and messaging features but also with more technologically advanced capabilities. Whether for business or recreational use, apps for *Android*-based smartphones have made this a reality.

_____

* The Android Robot that appears in this e-book was made available by Google under the terms of the Creative Commons Attribution License.

One of the most interesting features of the *Android OS* is that it offers developers the ability to build their own extremely rich and innovative apps. <u>More than 130,000 apps are available</u> in the *Android Market* to users in 48 countries. The majority of these apps may be downloaded free of charge, which unfortunately spells out possible danger for some who download and try out all kinds of apps. It is, after all, no longer uncommon for cybercriminals to Trojanize apps for their own gain.

The fact that *Android* apps are also available in third-party stores and in the developers' own sites poses even more risks, as this, too, hasn't escaped cybercriminals' attention.

With all the valuable data stored in your smartphone, you should strive to keep it safe from all threats. Here are a few tips on how to maximize your *Android*-based smartphone's security settings.
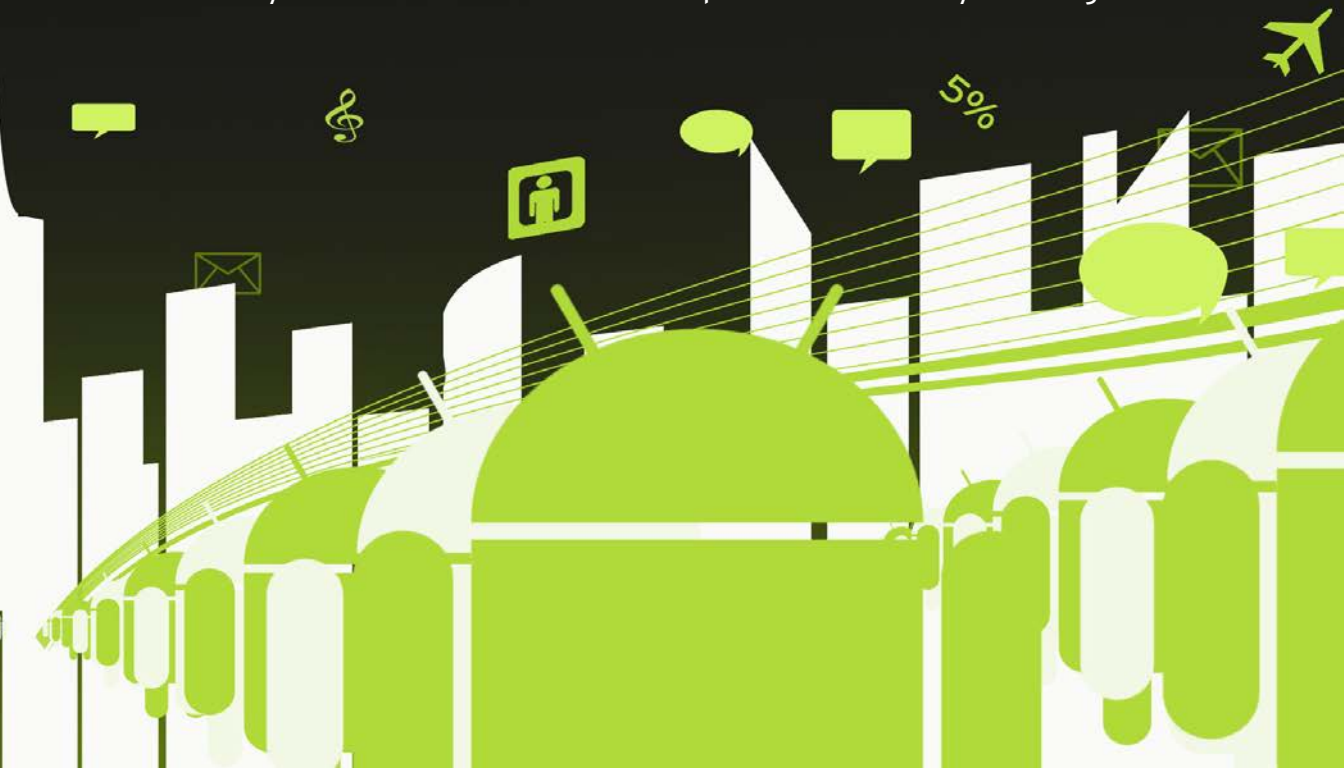
1 Use your *Android*-based smartphone's built-in security features.

The most effective way to keep your smartphone safe is to properly configure its location and security settings. To do this, go to the *Location & security* option under *Settings*.

It also wouldn't hurt to use the pattern, PIN (numeric), or password lock features of your smartphone. Though typing in your password to reactivate it from its idle state may seem time-consuming, this helps you keep your data safe when you physically lose your phone.

If this isn't enough, however, you may opt to user the fingerprint lock option. This is probably the best option, as it ensures that you're the only one who can access the data stored in your smartphone.

Keep in mind that using any of the security options above is always better than throwing caution to the wind. Passwords are, after all, created for a reason—to deter cybercriminals from accessing your data.

2 Disable the Wi-Fi auto-connect option.

Apart from properly configuring your *Android*-based smartphone's location and security settings, it may also be useful to disable the automatic wireless connection option despite the convenience leaving it on offers.

There are several reasons to doubt the security or lack thereof of using free wireless Internet access. Connecting to an open network may be easy, free, and convenient but doing so comes with risks. Automatically accessing open wireless networks essentially means opening the door for just about anyone. The data stored in your smartphone freely flows to the wireless router or access point and vice versa. As such, anyone on the same network can see even what you may not want him or her to.

The same threats that PC users face can plague *Android*-based smartphone users. This applies to the risks that come with automatically joining wireless networks, especially insufficiently secured ones. Turning the automatic wireless connection option off is thus another means to keep mobile threats at bay.
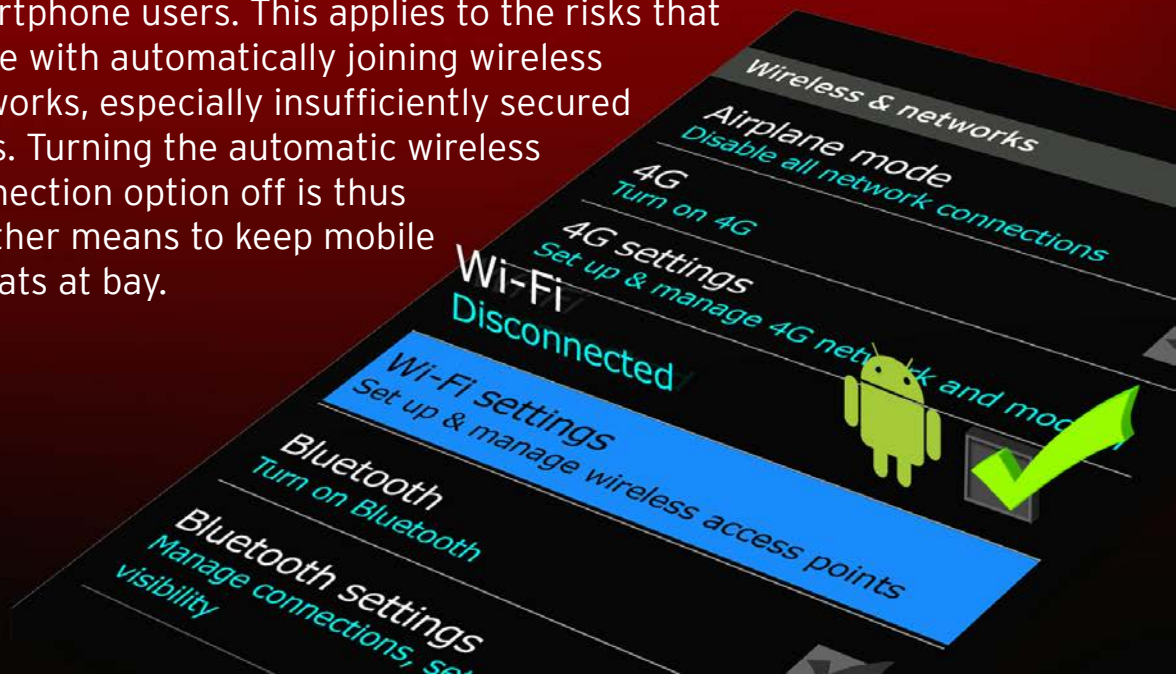
3 Consider blocking apps from stores other than the *Android Market*.

The <u>first *Android* Trojan</u> came in the guise of *Windows Media Player*. Shortly after, a new *Android* Trojan was found in certain <u>third-party app stores</u> based in China. Though we can't guarantee the security of apps available for download in the *Android Market*, it's safe to assume that as the official app store, it can be trusted more than others.

In line with this, we urge you to use the option that prohibits the installation of apps that did not come from the *Android Market*. This will serve as an additional layer of protection for your smartphone.
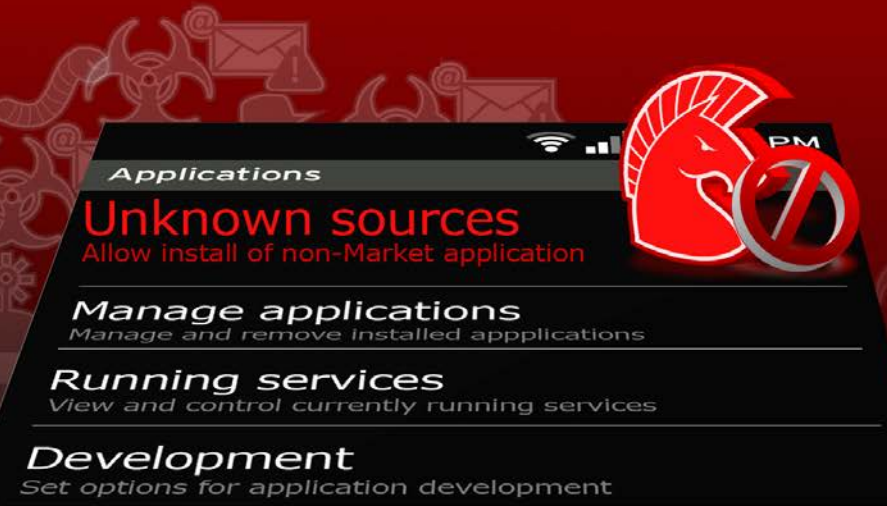
4 Understand the permissions you are allowing before accepting them.

After analyzing malicious *Android* apps, we realized that these usually ask that you allow them access to a long list of information stored in your smartphone. One such app is the recently discovered Trojanized version of the *Android Market Security Tool*. This sought permission to send text messages to premium-rate numbers, to see where you currently are, to view your saved text messages, and to change your system settings. Giving your permission allows it to act as a backdoor program. It gathers and sends device information to a remote URL. It also performs other functions without your authorization like modifying your call logs, monitoring and/or intercepting your text messages, and downloading videos.

Be careful when accepting requests for personal and/or device information or for other actions that aren't necessary for a certain app to work. Consider how an app intends to function. If it is, for instance, not a phone book application, it doesn't need access to your list of contacts.

5 Consider investing in an effective mobile security app.

Sometimes, being careful about downloading and installing apps just isn't enough. Because cybercriminals will never tire of coming up with ingenious ways to trick you into giving out personal information, using an effective security solution is still your best bet.

To stay protected anytime, anywhere, you can rely on solutions like *Trend Micro™ Mobile Security for Android™*. This protects the digital files you store in and secures the banking transactions you conduct on your *Android*-based smartphone. It identifies and stops malware before these can even reach your phone, giving you peace of mind. It is a full-featured security solution that leverages the Trend Micro Email and Web Reputation Technologies to effectively defend your phone against the latest mobile threats.

To know more about the latest threats targeting *Android*-based mobile devices, including smartphones, read our published materials in:

▦   📶 .ıll 🔋 9:00 PM

TrendLabs Malware Blog	TrendWatch
• <u>Trojanized Security Tool Serves as Backdoor App</u> • <u>Trojanized App Roots *Android* Devices</u> • <u>From RSA 2011: Mobile Security in Today's Threat Landscape</u> • <u>The "Consumerization" of Mobile IT: Risks and Rewards</u> • <u>*Android* Malware Spreads via Third-Party App Stores</u> • <u>Malicious *Android* App Spies on User's Location</u> • <u>First Android Trojan in the Wild</u>	• **Security Spotlight:** <u>Mobile Landscape: Security Risks and Opportunities</u> • **Security Spotlight:** <u>Mobile Phones Emerge as Security Threat Targets</u> • **Web Threat Spotlight:** <u>Backdoor App Comes in the Guise of the *Android Market Security Tool*</u>

Threat Encyclopedia

• **Web Attack Entry:** <u>Fake Apps Affect *Android OS* Users</u>