

**EXHIBIT B
TO DECLARATION
OF JOHN WRIGHT**


- Featured:
- [HTC Sensation](#)
- [Windows Phone Forums](#)
- [Android](#)
- [BlackBerry](#)
- [iPhone / iPad](#)
- [HP Palm webOS](#)
- [Windows Phone](#)
- [Nokia](#)

androidcentral

[Join our Community](#)
[Login](#)

Search Android Central

- [Articles](#)
- [Reviews](#)
- [Forums](#)
- [Devices](#)
- [Apps](#)
- [Tips & Tricks](#)
- [Rooting](#)
- [Podcast](#)
- [Tip Us](#)
- [Contact](#)
- [About](#)
- [RSS](#)

-  **Android Central Store**
- **Cases**
- **Chargers**
- **Batteries**
- **& more**

FREE SHIPPING ON ALL ORDERS OVER \$50. Limited Time Only.

Rooting - is it for me? Some Q&A

Posted on Saturday, Jun 5, 2010 by [Jerry Hildenbrand](#)

Like 157



Ed. Note: The story originally was published on Feb. 14, 2010. We've updated it with new information and present it again for those of you new to Android.

Each day more and more Android handsets are being sold, and that means users are faced with a major decision: To root, or not to root. Some of us will do it simply because we can, others will decide not to do it as they enjoy the phone as-is, but the majority of us will be on the fence about the whole idea of rooting.

Hopefully some of those questions can get answered and you'll have a clearer picture of the process and some understanding to make the decision a bit easier. I'm sure this won't answer every question you'll have when considering whether or not to root your device, but hopefully this is a good start and a basis for further discussion.

What, exactly, is rooting?

Rooting your Android device involves adding in a small Linux application called “*su*”. It stands for SuperUser, and allows applications and commands to run with elevated permissions. Everything that runs code, whether it's an application or the user, has a permission level set by the operating system.

Why Linux? Well the heart of the Android operating system is the Linux kernel. You'll hear a lot of nerdy geek-speak about the Linux kernel, but all you really need to know is that it's what is interfacing Android to your hardware, and ultimately has complete control. When you stray outside the "normal" way of using Android and start entering commands directly, the kernel is who you're talking to.

The root user is *the* boss and can do anything (good or bad) on the device. From simple things like [clearing the cache from core applications](#), to more advanced things like wirelessly [tethering](#) a laptop or iPod touch through your phone, root can do it. The su program is a sort of gateway that lets applications or users act as root while doing tasks. If you're the curious type (I know some of you are ;)) here's a more in-depth review of root as used in a Linux system by the [Linux Information Project](#) .

OK, so why would I want to root my phone?

Good question! Maybe you don't. Everything in a Linux system is a file, or is treated as a file. Since Android runs on top of Linux, it acts the same way. Most of the files you will need to access or change are available to you without having elevated permissions. "**Most**" being the key term here.

When you want to do things that affect or change the core software of your device -- like [updating the version of Android on your phone](#), or adding a [nice piece of software from another device](#) -- you'll have to do it as root. Dream and Magic users have been running Eclair on their phones for a good while now, and it's because they have rooted their device. Rooting also gives you access to some handy software that you couldn't use otherwise. Things like a complete system backup or [ad blocking software](#) require you to root your device. Don't root your phone just for the sake of rooting your phone, but if you come across something you feel you could use or would like to have, then consider it. You'll find that the open source community is usually pretty helpful and encouraging new people to do new things is common. And when you get to the point where you can lend a hand to the new folks, [pay it forward](#).

So it's like jailbreaking?

Pretty darn close. [Jailbreaking an iPhone or iPod touch](#) opens up things like [using applications that aren't manufacturer-approved or changing the look and feel of the device](#). Android already allows this to a large extent. The changes behind the scenes are the same way. A lot of what you can do with a jail broken iPhone you can already do with your Android phone, but to really unlock everything you'll need to root it. The concept itself is identical. You're allowing things that usually wouldn't have root permission to have them.

Is it dangerous? Will it break my phone? Will it void my warranty?

It can be, It might, and Yes. By not allowing access to the superuser account, [the manufacturer and your carrier have basically protected you](#) from doing things that change the system and make it unusable. All it takes is one wrong keystroke to turn your shiny new Android phone into a plastic and metal brick with no connection. Most times this is recoverable, but not always. You have to decide how capable you feel you are, and how well written the instructions you've found seem to be. Nobody will blame you if you decide against the risk, especially your cell carrier. All major carriers and manufacturers plainly state that altering or using unapproved software voids your warranty, and

rooting falls into that category. While that seems a bit harsh, they need to be able to support the products they sell. For that to happen, they need to know exactly what's running and what it's doing.

[Apps that run as root need a little further consideration](#). You need to have a level of trust in the person who wrote the app first and foremost. Does the developer have other software available? Do the user comments (for Market apps) have anything that raises a red flag? Do the requested permissions seem a little odd? These are all questions you need to think about before you allow something to run as root. For a further level of security, think about installing an application that warns you anytime something tries to run as root. SuperUser Whitelist ([Android Market link](#)) is a great little app that does exactly that. If you decide to go on and root, ask users with the same device as you for a link to a version of SuperUser Whitelist that works with your firmware. Once installed, anytime something wants to run as root, the app intercepts and asks if you would like to allow it. You're given the choice to accept, decline, or grant the app in question full privileges each time it runs.

One last thing to touch on here. Many custom ROMs include some sort of [SSH server](#). This can be a wonderful tool, or it can get you in hot water. This is what caused the whole ["Rick-Roll" episode with the latest iPhone jailbreak](#). The server sits and waits for an outside connection, and if that connection provides the right password full control of the device is turned over. In the case of the iPhone, users never bothered to change the default SSH password for root. A clever (or devious) group of users simply scanned for servers listening on the correct port, then attempted to sign in as root with the default password. Lesson learned, but this is easy to prevent. Ask other users of the ROM or firmware you're thinking of flashing if there is a server listening, and if so how to disable it or change the default password.

If I root, will I still receive operating system updates from my carrier?

Maybe. More than likely if you've just rooted your phone so you could have access to the full file system and haven't drastically changed things, the phone will still pass your carrier's checks and upgrade. If you've delved deeper and really customized your device, count on not being able to upgrade. Carrier updates were designed to work with the original software, so they need to be sure

that's what the phone is running. Again, this is for your own good. T-Mobile or Verizon can't offer technical support for things they haven't trained their technicians on, and if you flash a carrier approved update over custom software it's probably not going to work.

The good news is that failing the checks the carrier does during an update won't cause any damage to your phone. The update will just quit and you'll be back where you started. Then you can [decide if you would like to un-root and upgrade](#) or take another path. The worst case scenario is that the phone passes the carriers checks, updates, and then things get broken. That's pretty unlikely, but possible. If that would happen, you won't be alone. Everyone in your situation will scramble to their [favorite Android user forum](#) and hopefully a work around can be found.

Note - a carrier update may also break the ability to root the device and a new method will need to be found. Any discussion of upgrading and root needs this mentioned as well. Most folks who root and decide to install a custom ROM wait for the [ROM developer to provide an update](#) that includes any bug fixes or new capabilities of the carrier update.

Will I still get application updates?

Yes. While it's not being used, the program that allows permissions to be upgraded just sits and does nothing. Normal applications won't even be aware it's there, and applications that use it expect it to be there. Application updates, whether they are [from the Market](#) or [other third parties](#) will still install as normal.

If I decided to 'un-root' my phone, how do I do that?

It depends on the model of your phone. Some are [ridiculously easy to revert](#), some [not so much](#). This is the most important question you can ask before you dive in and root your phone. Usually the [website you found the method to root your phone](#) will also have a discussion about un-rooting and going back to stock firmware. Take the time to find and read this information so you're aware of just how difficult it's going to be to go back. Pay close attention and create backups when recommended while you're rooting your phone, as these may be needed to go back. I've not heard of any device that can't be restored to factory firmware provided the original was backed up properly as recommended during the rooting process. [The most important thing to always remember is to ask for help](#). If you do find yourself stuck without a backup or a working phone and need to roll back, ask for advice. Our forums are full of fine folks from all walks of life, and the majority are more than happy to help. There's a good chance you're not the first person in that situation and a solution has already been worked up!

As you can see it is something that needs a little thought before you dive right in. But if you decide you need root access, consider some of the information we've laid out here. The security and other risks are real, but are pretty easy to work with. There's no reason you can't safely root and use your phone, just do your homework first!

[Email this Story](#)

1
reddit

157

Share

42

247

Share

Android Security: Six Tips to Protect Your Google Phone

Al Sacco

March 8, 2011 [\(CIO\)](#)

Google's Android Market mobile software shop was hit last week with its first major malware attack; a popular application called "DroidDream" proved to be infected with malicious code that could steal users' personal information, and [Google was forced to use a built-in Android "kill-switch"](#) to do away with the problematic app--but not until after it had already infiltrated thousands of [Android smartphones](#).

The [Google](#) Android platform has never been more popular; in fact, Android now holds a commanding 31% of the U.S. smartphone market share, making it the most popular smartphone OS in the country, [according to ComScore](#).

Slideshow: [8 Essential Android Security Apps](#)

Android has also never before represented such a significant target for hackers and other baddies looking to profit off of the platform's popularity. In other words, now is the time to get smart about Google Android [security](#). The following six tips and tricks will help do just that.

1) Protect Your Android with a Password--Now!

The single most effective security measure you can take to protect your Android device is to lock it with a password. It sounds simple, but a strong password--or even a weak one--will protect you and your smartphone from the vast majority of threats; if a malicious party can't get past your password screen, your data and everything else on-device is generally secure.

Depending on the model of your Android smartphone, you'll have a variety of password options, but they're all accessed in mainly the same way. Open up your Android Settings menu and scroll down to the section called Location & Security Settings or something similar. First, enable Screen Unlock Security and you'll then be presented with a number of password options, depending on your device.

For example, my Motorola Atrix 4G provides password options for a Pattern Lock, for which you can set a specific "swipe pattern" to unlock your device; a PIN Lock that uses numbers to secure your handheld; a Password Lock, for which you can employ both letters and numbers; and finally, a biometric-based Fingerprints Lock that employs the Atrix's fingerprint reader for authentication.

Though the Fingerprint Lock is the most secure option...I'm a bit wary of storing my biometric information on Google's servers, so I opt for the Password Lock. In order of "secureness," the Fingerprint Lock is most secure, followed by the Password Lock, PIN Lock and finally, the Pattern Lock. But using any one of these Android password security options is better than not using one at all.

(Note: If you choose to employ the Pattern Lock option, it's a good idea to frequently wipe your touch screen clean, since repeated entry of your pattern lock can leave a "trail" that can be spotted by hackers and used to gain access to your device.)

After you set your Android password, you should set your Screen Timeout options to a relatively low option, so your device display shuts off and locks itself shortly after you last touch it. To do so, open up the Android Settings menu, scroll down and select Display. On the following screen, locate the Screen Timeout option and pick a value--I suggest one minute or less for maximum security.

2) Customize Locked Home Screen with Owner Info

Imagine you accidentally leave your smartphone at a bar. A good Samaritan locates the device and wants to get it back to its rightful owner...but it's locked and the home screen shows only a beautiful, albeit useless, ocean vista.

This scenario plays out all the time, and if more smartphone owners only added owner information to their devices' home screens, many more lost devices would likely be returned. Unfortunately, Android doesn't have any built-in option that lets you post owner information on your device's locked home screen, like other mobile platforms, including Research In Motion's (RIM) BlackBerry OS. But a couple of third-party applications will do the trick.

My favorite option for adding owner information to your Android home screen: the [Phone Found - Owner Info app](#), which is available for free via the Android Market. To customize the Owner Info app, simply launch the software, hit the Edit menu options and enter in your contact information. You can then open up the app's Settings and choose which information you want to display on your device's locked home screen.

3) Do NOT Root Your Android Device

To "root" your Google Android device means to remove a number of manufacturer- and wireless-carrier-imposed restrictions put on your smartphone to make it easier for said parties to install and deliver the applications and services they want you to employ, among other things.

Rooting also opens up system-level access to your device's core resources, which is not a good thing, at least from a security perspective, since doing so also removes a number of safeguards installed to help protect your device from malware and other potentially dangerous code.

Unless you're a developer or someone who is very familiar with Android and you're simply willing to take your chances, you should NOT root your Android device. Ever. Not rooting might mean limited access to some cool, custom applications and services, and you won't be able to download apps from many unofficial third-party app stores. However, avoiding a root does vastly increase security, because in large part applications can't gain system-level access without a root.

Bottom line: Don't root your Android device. But if do, beware that in rooting your smartphone, you're significantly reducing your device's existing security safeguards.

4) Stick to the Official Android Market for Apps

It's a good idea to be very selective about where you download your Android mobile

applications. In fact, I suggest only downloading applications from Google's Android Market, even though the whole DroidDream situation proves the official Android Market is not 100% free of malware and other harmful apps. (Following the DroidDream debacle, Google did, however, [vow to bolster Android Marketplace security](#).)

Every once and a while, I'll download an Android app from a source other than the Android Market, but I'm always aware of the potential danger, and I always use some type of antivirus scanner after the download to help ensure security--more on Android antivirus coming up in the next section.

As a rule of thumb, it's a wise idea to get your Android software directly from Google's Android Market.

5) Google Android Antivirus

A good mobile antivirus app scans new Android software downloads for obvious signs of tomfoolery, such as strange permissions- or download-requests. And a number of free and commercial, or paid, Android antivirus apps are currently available in the Android Market.

I can't personally vouch for the effectiveness of them all, but in general, running one of the more popular antivirus apps is better than not running any antivirus at all. The app I've used most is [Lookout Mobile Security](#). Lookout is available as a free download, with a basic antivirus scanner, Find-My-Phone features to help locate lost or stolen devices and backup/restore options. You can also upgrade Lookout for more in-depth security features, but the free version should provide basic protection for average users.

Another free antivirus option is the aptly named [Antivirus Free](#) app.

Even if you choose not to constantly run an Android antivirus application, it's a good idea to download one and scan your device occasionally for potentially harmful apps.

6) Android Wireless Connectivity and Security

In general, it's a wise idea to disable any and all unused wireless-connection options on your Android smartphone. In other words, you should turn off your Wi-Fi when you leave home and won't be in range of another Wi-Fi network for the day. When you're done using that Bluetooth headset in the car, turn off Bluetooth. Doing so will not only conserve battery life, it'll reduce the risk of malicious parties detecting, or even connecting to, your device without your knowledge.

In addition, you should also disable your Wi-Fi auto connect option--if your device has such an option--to ensure you don't automatically connect to a public Wi-Fi hotspot, through which a Bad Guy could access your device data. Turn off Wi-Fi auto connect by opening up your Android Settings menu, then choosing Wireless & Networks and next, Wi-Fi Settings. If your device has a Wi-Fi auto connect option, you should see it listed here. Uncheck the auto connect box to turn off this functionality.

On the Wireless & Networks settings page, you'll also see a Bluetooth Settings option. Open up your Bluetooth Settings and turn Bluetooth on if it's not already. Then click the Device Name option and change your Android's name to something unique and specific to you. This will reduce confusion in the future, should you attempt to connect your smartphone to another device via Bluetooth.

If your Android device supports mobile hotspot features, you'll want to secure your personal network. First, again open up your Wireless & Networks settings and then scroll down to and select Mobile Hotspot. Next, turn on your Wi-Fi hotspot feature and click the Wi-Fi Hotspot Settings settings menu.

Once the hotspot features are activated, your Wi-Fi Hotspot Settings page should show an option to Configure Wi-Fi Hotspot. Open up this menu, assign a new, unique name to your network, choose WPA2 PSK security from the dropdown menu and then assign a password to your network. Save your changes, and your Wi-Fi hotspot is now secure.

It's a good practice to turn off you Wi-Fi hotspot when not in use, so unauthorized parties cannot employ your network, eating up you monthly data allotment and/or accessing your device information.

[AI Sacco](#) covers Mobile and Wireless for CIO.com. Follow AI on [Twitter @ASacco](#). Follow everything from CIO.com on Twitter [@CIOonline](#) and on [Facebook](#). Email AI at asacco@cio.com

Malware in Android Market highlights Google's vulnerability

By [Peter Bright](#) | Last updated about a month ago

Google has removed 21 applications from the Android Market after it was discovered that the apps secretly installed malware. The applications themselves included pirated and renamed versions of legitimate Android software that had been modified to include the malware and then offered for free on the Market. Together, the 21 programs received more than 50,000 downloads over the course of about four days.

The malicious applications sent personal details, including the phone's unique IMEI number, to a US-based server. Worse, it exploited security flaws to root the phone, and installed a backdoor application that allows further software to be installed to the handsets. Though Google has now purged the applications from the Market, the rooting and backdoor mean that the anyone who has run one of the malicious programs should reset their phone to stock conditions to clean it up. The flaw used to root the operating system was fixed in Android 2.2.2 and 2.3, so users of those versions should be able to get away with simply removing the applications. The programs were all (re)published by an entity named Myournet; it too has now been removed from the Market.

A full list of the 21 programs can be found at [Android Police](#), who originally reported the issue, after the republished applications were spotted by redditor [lompolo](#). lompolo investigated the applications after noticing that one of them did not have the publisher he expected; he posted his findings to reddit after noticing that one of the applications appeared to contain exploit code.

Similar malware, dubbed "DreamDroid" has been found in even more applications, with applications from publishers named Kingmall2010 and we20090202 also removed. In total, more than 50 programs have been pulled.

This attack is notable in that it combines a wide range of smartphone issues all into one neatly packaged exploit: we have the lack of governance of the Android Market, the piracy and re-publication that is distressingly common on mobile platforms, the security flaws that allow rooting, and Android's inconsistent updating which leaves machines at risk of security flaws.

Google's Android Market is a free-for-all: unlike Apple's App Store and Microsoft's Marketplace, which both have strict eligibility requirements and mandate that programs are restricted only to a limited set of APIs, in the Android Market essentially anything goes. Google can remove applications that are found to be actively harmful, as it has done here, but this action tends to be reactive, not proactive. The [Android Market Developer Agreement](#) does prohibit this kind of application in section 4.4, but Google obviously took no steps to ensure that applications abided by this rule prior to publication.

Apple's strictly regulated store is criticised by many for its inconsistent rule enforcement and the apparently arbitrary decisions made by the those inspecting its applications. This regulation is by no means flawless—the [Handy Light](#) flashlight application contained a backdoor to allow iPhones to be tethered, showing that it can indeed be tricked—but it should nonetheless impede similar attacks on that platform. Microsoft's gatekeeping of the Windows Phone 7 Marketplace should similarly serve to stand in the way of such malicious applications. Incidents like this serve to vindicate the approach Microsoft and Apple have both taken to their application stores, and repeat performances could make users increasingly wary of the Android Market.

[Application piracy](#) is again an issue found on Apple's platform as well as Google's. Neither company earns much praise for their responses to piracy allegations: though both maintain that they will remove applications that infringe on the intellectual property of others, in practice their responses are slow and inconsistent. One of the developers whose game had been ripped off informed Google of this more than a week before the program was eventually removed—due to its malware—without receiving any response from Google.

Perhaps it is fortunate that that software *was* pirated, however, as it was this piracy that led to lompolo's closer inspection. Had it not piqued his curiosity, it may have lingered on the Market for weeks or months, quietly infecting users all the while.

The desirability of rooting handsets is also a continued problem. Rooting, to enable custom software and operating system builds to be installed to a device, is a widespread (albeit minority) activity among both iPhone and Android users. It creates an unusual alignment of interests—an exploit that can be used to root a phone is sought by both "good guys" (who just want to install custom firmware) and "bad guys" (who want to install nefarious malware). While the root flaw in this case was already patched, that patch is not widely distributed. This is due to Google's enormous dependence on handset OEMs and mobile networks to package and distribute firmware updates. Even security-conscious users who would like to upgrade to a fixed version can find themselves unable to do so for many months—if ever—due to unavailability of a suitable patch for their particular phone.

Apple, with its vertically integrated approach, has a much more robust response to such issues, as it can publish updates for all users of supported models, regardless of their network, simultaneously. If Microsoft can get the unfortunate teething difficulties in the Windows Phone 7 update process resolved, it too should have a considerable ability to deploy updates.

Android is now a major smartphone platform, estimated to be outselling the iPhone. For many, its openness and flexibility is a virtue, but it comes at a cost: it leaves the platform unusually susceptible to attack. And those attacks will come: just as popularity has made Windows an attractive target, so too will the black hats be drawn to Android. This will place Google in an increasingly uncomfortable position; locking down the platform may be appealing to most users, but it would infuriate and alienate the early adopters and trend-setters who championed the operating system in its early days. However, leaving it a free-for-all could make Android the Windows 98 of smartphone systems: virus-ridden and unsafe.

CNET.com

[CNET Home](#)

[Shop Motorola ATRIX 4G from AT&T](#)

- [log in](#)
- [join CNET](#)

- [Home](#)
- [Reviews](#)
- [News](#)
- [Downloads](#)
- [Video](#)

- [Home](#)
- [Reviews](#)
- [News](#)
- [Downloads](#)
- [Video](#)

[Android Atlas](#)

December 21, 2010 2:36 PM PST

Google encourages rooting of phones

by Scott Webster

36

Recommend

10

Google used its Android Developers blog yesterday to [deny a correlation](#) between rooting a handset and perceived poor security measures on the operating system.

In the blog, Android engineer Nick Kralevich pointed to comments on an Engadget post that



© 2010 CBS Interactive

characterized the [Nexus S](#) security as "crap." Samsung Nexus S
Not suprisingly, Krlevich disagreed.

"Legitimately gaining root access to your device is a far cry from most rooting exploits," he wrote. "Traditional rooting attacks are typically performed by exploiting an unpatched security hole on the device. Android has a strong security strategy, backed by a solid implementation."

Though such assumptions spread like wildfire every time a security company or development team talks about Android's [exploits and vulnerabilities](#), Google argues that rooting a phone should be the beginning of an experience. "It should be no surprise that modifying the operating system can give you root access to your phone," Krlevich wrote.

Common reasons for rooting a phone include letting users decide which apps should be loaded or operating the handset on a different carrier's network. Most often, it's simply done to install custom operating systems such as [Cyanogenmod](#).

Krlevich also discussed two types of rooting. Root access, which gives users root level access to the device, opens the door to custom boot images and ROMs. Though hackers and modders are quick to take advantage of access whenever a new phone enters the market, they don't have to bypass much security to do so.

The second, and scarier, type of rooting is accomplished by exploiting the OS, but Android's nature makes it a fairly difficult task. As all apps and games are [sandboxed](#) from each other, exploiting one app should not affect the next. Also, all applications are required to declare the permissions they use.

Though hackers love to find weak spots in mobile Web browsers and sneak onto phones through the back door, the Android team moves quickly to patch documented holes and releases fixes as needed. And thanks to the open-source community, anyone and everyone is welcome to contribute to platform.

If Google does see a problem to rooting, it appears to be the wireless carriers. According to the blog, until carriers and manufacturers make it easier for users to unlock devices, "there will be a natural tension between the rooting and security communities."

"It's possible to design unlocking techniques that protect the integrity of the mobile network, the rights of content providers, and the rights of application developers, while at the same time giving users choice," Kralech wrote. "Users should demand no less." Unfortunately, there doesn't seem to be much wiggle room in the current system.



[Scott Webster](#)

Like

10

[Full Profile](#) [E-mail Scott Webster](#)

Scott Webster has spent the better part of his adult life playing with cell phones and gadgets. When not looking for the latest Android news and rumors, he relaxes with his wife and son. Scott also is the senior editor for [AndroidGuys](#). Scott is a member of the CNET Blog Network, and is not an employee of CNET. [E-mail Scott](#).

- [Reviews](#)
- [All Reviews](#)
- [Camcorders](#)
- [Car Tech](#)
- [Cell Phones](#)
- [Digital Cameras](#)
- [GPS](#)
- [Laptops](#)
- [TVs](#)

- [News](#)
- [All News](#)
- [Business Tech](#)
- [Crave](#)
- [Cutting Edge](#)
- [Green Tech](#)
- [Security](#)
- [Wireless](#)

- [Downloads](#)
- [Add Your Software](#)
- [All Downloads](#)
- [Mac](#)
- [Mobile](#)
- [Software Deals](#)
- [Webware](#)
- [Windows](#)

- [Video](#)
- [All Videos](#)
- [Apple Byte](#)
- [Buzz Report](#)
- [CNET Top 5](#)
- [Loaded](#)
- [Prizefight](#)

- [More](#)
- [About CBS Interactive](#)
- [About CNET](#)
- [CNET Deals](#)
- [CNET Forums](#)
- [CNET Mobile](#)
- [CNET Site Map](#)
- [CNET Widgets](#)
- [Corrections](#)
- [Help Center](#)
- [Newsletters](#)
- [Permissions](#)
- [RSS](#)


- [Join us on](#)
- [Facebook](#)
- [Twitter](#)
- [YouTube](#)

POPULAR TOPICS:

- [Apple iPhone](#),
- [Apple iPod](#),
- [LCD TV](#),
- [Apple iPad](#),
- [Smartphones](#),
- [Windows 7](#),
- [CES 2011](#),
- [Google Android](#),
- [HTC phones](#),
- [Android phones](#)

- [Top Brands:](#)
- [AT&T Products](#)
 - [Cell Phones](#)
- [Intel Products](#)
- [Samsung](#)
 - [Televisions](#)

- [Mobile Phones](#)
- [Blu-Ray & Home Theater](#)
- [Notebooks](#)
- [Monitors & Printers](#)
- [Cameras & Camcorders](#)
- [Acer Products](#)
 - [Notebooks](#)

- [© 2011 CBS Interactive. All rights reserved.](#)
- [Privacy Policy](#)
- [Ad Choice](#)
- [Terms of Use](#)
- [Mobile User Agreement](#)
- Visit other CBS Interactive sites: 

[News](#) | [Reviews](#) | [How-To's](#) | [Downloads](#) | [Shop & Compare](#) | [Apps](#) | [Business Center](#)

Magazine
Subscribe & Get a
Bonus CD
Customer Service

Sign in with

 or [Create a New Account.](#)[PCWorld](#) » [Blogs](#) » [Today @ PCWorld](#)[Facebook](#) 17 [Twitter](#) 53 [Share](#) 73 [5 Comments](#) [+43 Recommends](#) [Email](#) [Print](#)

TODAY @ PCWORLD

The Motorola Droid Gets Rooted

By [Ian Paul, PCWorld](#) Dec 9, 2009 5:36 AM

Add the [Motorola Droid](#) to the expanding list of hacked devices that give more adventurous users greater control over how they can use their smartphones. Late Tuesday [Wired's Gadget Lab](#) reported that instructions had been posted to an [Android forum](#) that supposedly show you how to gain administrator access to your Droid device.



A hacked Droid would allow you to modify the operating system any way you want, and add functions to the device that may have been previously restricted. The problem is that, for the moment anyway, an online community providing customized Droid hacks doesn't exist yet. But that is likely to change in the not-too-distant future.

Warning: Hacks can be hazardous to your Droid's health

Before you read on, keep in mind that rooting your Droid could brick your handset making it essentially useless. Also, tinkering with the inner workings of the software will almost certainly void the device's manufacturer warranty. So think carefully before you decide to try hacking your device.

Android phones are rooted, not jailbroken

In Android lingo a hacked phone is said to be rooted as opposed to being unlocked or jailbroken. With a rooted Android phone you can change the handset's visual theme, customize the operating system and [add multi-touch gestures](#). You could also use applications or functions that may be forbidden or restricted by your carrier [such as tethering](#).

How it's done, and why you should hold off

The [instructions found on AllDroid](#) for hacking your device look pretty straightforward: download a .zip file, rename it, and stash it on your handset's SD card. After that you restart your phone while holding down several keys, and then install the exploit using an onscreen menu. I have not verified this exploit myself, so I can't vouch for it.

According to the post, after the Droid has been hacked you can gain root access to the phone. But as I mentioned earlier, unless you already know how to modify to the Android OS, rooting your Droid won't do much for you at the moment. That's because software designed to take advantage of hacked Droids doesn't exist yet.

Hacking communities already exist for many Android HTC phones, and other devices running the Android 1.6 operating system (Droid runs Android 2.0). So in all likelihood you won't have to wait that long for Droid-related modifications.

But while you're waiting, you can check out what's already available for some rooted Android devices at the [Android Spin database](#), the [Cyanogen mod](#), and this dedicated [Android hacking and modding site](#).

Just remember: any tinkering you do with your Android device is at your own risk. So ask yourself if the benefits are really worth it, before trying to modify your handset.

Connect with Ian on Twitter ([@ianpaul](#)).

See more like this:[android,hackers,motorola](#)

Would you recommend this story? YES | 43 NO | 7

Sponsored Links

Free Remote PC Access

Remote Access From Any Web Browser. Fast, Easy & Secure - 30 Days Free
www.GoToMyPC.com

Virus and Trojan Remover

Download Free Trojan & Virus Scan. Recommend & Used by the Experts.
www.pctools.com

Computer Repair

FREE Estimates. PC & Mac Repair. Serving LA & Orange County. Let Us Help
ThinkComputersOnline.com

SHOCKING:\$9 Car Insurance

Auto Insurers are SCARED you will learn this secret.

www.LifestyleJournal.com

Comments



Leave a comment

Submit Comment

Once you click submit you will be asked to sign in or register an account if you are not already a member.

04mePCee says:

Wed Dec 09 06:19:36 PST 2009

PCWorld said

Post your comments for <http://www.pcworld.com/article/id,184077/article.html> here

I am always in awe of hackers for iPhone and now the Droid; the obsession to download software that runs the risk of turning your smart phone into a brick.

Is there a restore option for Droid ?

REPLY

Jodokai says:

Wed Dec 09 07:58:55 PST 2009

04mePCee said

PCWorld said

Post your comments for <http://www.pcworld.com/article/id,184077/article.html> here

I am always in awe of hackers for iPhone and now the Droid; the obsession to download software that runs the risk of turning your smart phone into a brick.

Is there a restore option for Droid ?

I'm not sure if there is a restore, but if you have root, I'm pretty sure you could do a back up of your OS.

As far as the "in awe" you have to weigh the benefits to the risk. Out of all the Jailbroken iPhones out there, how many have actually been unrecoverably bricked? I'd bet very few. If you search T-

mobile's forums you'll see their stance on Rooting is that it doesn't automatically void your warranty, they just won't fix it if rooting it caused the problem.

Look at tethering, some companies charge \$60 a month for this service. If you get away with it for 8 months you've just paid for your \$500 phone.

The Android OS has the limitation that it will only use installed memory to store programs. I think the most out right now is 256mb. A lot of games a lot of memory space, so this is a huge limitation that can be overcome with rooting.

I'm not saying everyone should run right out and root it, but I do understand why people do it. It's all about risk vs. reward.

[REPLY](#)

Nuke61 says:

Wed Dec 09 10:48:32 PST 2009

You can tether the Droid right now, without having to gain root. There could be other reasons why you want to get root access, but tethering shouldn't be among those reasons. I've tethered at roughly 1/2 of my cable modem speed using a USB cable connection to my laptop. When I used Bluetooth it was roughly 1/2 the speed of the USB connection.

[REPLY](#)

boden says:

Wed Dec 09 13:56:09 PST 2009

I wonder about the ethics of articles like this. The people who understand root access already know this can be done and how to do it right. The newbies will get just enough information to wreck their device. OR implant a lovely Trojan on their system.

Then we have to listen to them complain...

Boo Hoo I put software from some guy in Russia on my phone and now my phone company says i owe them X thousands of \$ because X number of phones are now using my data.. boo hoo.

[REPLY](#)

Jodokai says:

Wed Dec 09 17:25:02 PST 2009

boden said

I wonder about the ethics of articles like this. The people who understand root access already know this can be done and how to do it right. The newbies will get just enough information to wreck their device. OR implant a lovely Trojan on their system.

Then we have to listen to them complain...

Boo Hoo I put software from some guy in Russia on my phone and now my phone company says i owe them X thousands of \$ because X number of phones are now using my data.. boo hoo.

Root has nothing to do with your chances of getting a virus. You can load a virus now without rooting your phone, that's the downside to Open source and not having strict control like Apple does. In my opinion the upsides FAR outweigh the down, but that doesn't mean the down isn't there.

As I said in my first post, there are many more reasons than just tethering. A non-rooted Droid has 256mb to use for stored applications, a rooted Droid gets essentially unlimited storage for apps (limited only by the size of your microSD cards).

Add to that, T-Mobile at least, has said that rooting isn't an automatic deal breaker with the warranty (I can't find official word from Verizon or Sprint) and why not root it?

[REPLY](#)

Editors' Picks



[HTC Sensation 4G Hands-On: Beautiful, Dual-Core Beast](#)



[How to Tell if Your Android Phone Is Getting the Gingerbread OS Update](#)



[Many Unlimited Tech Services Appear to Have Limits](#)



[CyanogenMod 7 Goes Final, Now Does Gingerbread](#)

[Home](#)


Products

- [Android App Reviews](#)
- [Desktop PCs](#)
- [Laptops](#)
- [Storage](#)
- [iPhone App Reviews](#)
- [E-Readers](#)
- [Macs & iPods](#)
- [Tablets](#)
- [Business Center](#)
- [Gadgets](#)
- [Monitors](#)
- [Tech Industry](#)
- [Cameras](#)
- [Gaming](#)
- [Printers](#)
- [Tech Events](#)
- [Camcorders](#)
- [HDTV](#)
- [Software](#)
- [Upgrading](#)
- [Cell Phones & PDAs](#)
- [Home Theater](#)
- [Spyware & Security](#)
- [Windows 7](#)
- [Consumer Advice](#)


Network Sites

- [PCWorld Business Center](#)
- [Search for Jobs](#)
- [Macworld](#)
- [MacUser](#)
- [Mac OS X Hints](#)
- [iPhone Central](#)

About PCWorld

- [About Us](#)
-  [Ad Choices](#)
- [Advertise](#)
- [PCWorld Content Works](#)
- [Terms of Service Agreement](#)
- [Privacy Policy](#)
- [Site Map](#)

Resources

- [Newsletters](#)
- [FAQ](#)
- [Contact Us](#)
-  [RSS Feeds](#)
- [Magazine Customer Service](#)
- [Community Standards](#)

Visit other IDG sites: **Select One**

© 1998-2011, PCWorld Communications, Inc.