4 Compelling Security Reasons Not To Jailbreak Your iPhone or iPad

iOS is one of the most secure, safest mobile operating systems out there, but this security also comes with a lot of restrictions; the App Store is very tightly policed, and it's impossible to install third-party apps without jailbreaking. But jailbreaking can put you at risk, so it's important to weigh the benefits and potential drawbacks. Here are a few potential security risks that you should keep in mind.

What Is Jailbreaking?

In a nutshell, jailbreaking removes the security restrictions on your iPhone or iPad. This means apps are given a lot more access to the core functions of the phone, like contact lists and the ability to send emails or make calls. On a stock iOS device, a user has to give permission to an app to get access these functions; on a jailbroken one, that's not the case.

By removing the restrictions that are placed on your device by the manufacturer (much like rooting an Android phone), you gain access to third-party apps, additional functionality from some of the apps you already have, and a number of system tweaks. This can make your phone or tablet more useful, but it can also create some security problems (not to mention some potential legal ones as well). And it'll invalidate your Apple warranty and any AppleCare package that you've purchased.

Third-Party Apps Can Be Dangerous

There's a reason that Apple keeps a very tight leash on App Store apps: because a malicious app can wreak a lot of havoc on your device. It's always possible that you'll get a bad app, but if you start downloading apps that haven't been OK'd by Apple for the App Store, the chances of getting malware goes up.

For example, a recent piece of malware called AdThief was discovered in some extensions from Cydia, one of the most popular non-Apple app stores. AdThief committed ad fraud, which amounts to stealing ad revenue from app developers that use ads to make money from their apps. The malware only affects jailbroken devices, but it's infected up to 75,000 phones so far.

Credit: http://www.makeuseof.com/tag/4-compelling-security-reasons-jailbreak-iphone-ipad/

The App Store Isn't As Secure As You Think

Whether you got an app from the App Store or from a third party, that app has full access to all of the parts of your phone, and this should be some cause for alarm. Obviously you're more likely to be safe with an app from the App Store, but even well-intentioned or reputable apps can be compromised by hackers or by mistake.

For example, a research team from Georgia Tech showed last year that Jekyll, a malicious app, could sneak past the App Store inspection by using self-assembling pieces of code that activate only after the app has been approved. And while it took a team of researchers to create an app like this, there's no reason to believe that someone else wouldn't be able to do it, too. It's possible that code like this could more easily be constructed to target jailbroken iPhones or iPads, even if Apple learned a lesson from Jekyll.

Everyone Knows the Default Root Password

One of the worst-kept secrets about iOS is its root password, "alpine." It's long been known that this is the password, and Apple shows no intention of changing it anytime soon. Having the root password gives a user access to the core functions of the device, and this can be disastrous if an ill-meaning person gets access to yours. Fortunately, this password can be changed from a shell app, but it's an easy thing to forget to do.

Many people forget to change the root password after jailbreaking their device and downloading an SSH app. This is absolutely crucial for your security, so if you decide to jailbreak your phone, don't forget to do this! The process was explained in our article on how to configure an FTP server on your iPad.

Security Patches Won't Download

After you've jailbroken your iPhone or iPad, you won't be able to update iOS without reverting back to the un-jailbroken default mode. While this isn't a big deal, most people who have jailbroken their iOS devices will wait until a new jailbreak is available for the update before they download and install it so that they don't have to go back to the stock iOS implementation for an extended period of time.

What this means is that you may find yourself vulnerable to security holes in iOS until a new jailbreak is released, putting you in danger. Of course, if there's a really significant known security flaw, you could always just download iOS and wait a couple weeks for a new jailbreak, but if there's a flaw that you don't know about, you could be putting yourself at risk every time there's an update.

You also might find yourself unable to access other apps; there have been reports of video streaming, communication, and banking apps that deny access to jailbroken devices.

Is Jailbreaking a Good Idea?

Everyone has to weigh the risks and benefits of jailbreaking for themselves. There are plenty of great things you can do with a jailbroken iPhone or iPad, like using theActivator gesture-recognition tweak, customizing your icons with Transparency, and create a custom lock screen with LockMS. In fact, we have an entire list of our favourite Cydia tweaks.

Credit: http://www.makeuseof.com/tag/4-compelling-security-reasons-jailbreak-iphone-ipad/