

Check for Updates
Make sure you have the latest information!



TidBITS Publishing Inc.

Take Control of

v1.0

Networking and Security in iOS 6

Glenn Fleishman

\$10

[Help](#) [Catalog](#) [Feedback](#) [Blog](#)

Click here to buy the full 127-page "Take Control of Networking & Security in iOS 6" for only \$10!

Table of Contents

Read Me First

Updates and More	4
Basics	5
What's New in This Edition	7

Introduction

Quick Start to iOS Networking and Security

In-Depth on Wi-Fi

Managing Wi-Fi Connections	11
Wi-Fi Troubleshooting	20
Tweaking Your Network for Faster Performance	22

Connect to a Secure Wi-Fi Network

Connect with WPA2	25
Outdated Methods	27

Work with Cellular

Two Kinds of Mobile Networks	32
Why Use Mobile Data on an iPad.....	37
Pick a Data Plan	39
Keep Usage Restrained.....	47
Choose to Use Cellular Data or Wi-Fi	51
Cross-Border Mobile Use	53
Alternatives to Cellular Data Plans	57

Make a Mobile Hotspot

Pay for Personal Hotspot.....	60
Turn On Personal Hotspot	61
Connect to Personal Hotspot	65

Set Up Bluetooth

Bluetooth Basics.....	79
Pairing Any Device.....	80

Apple Wireless Keyboard	82
Hands-Free Profile	84
Audio Devices	85
Airplane Mode	
What's Airplane Mode?	87
Turning Radios off Separately	89
Transfer Data Securely	
Exposure	90
Secure Solutions	96
Keep Data Safe	
Exposure	103
The Danger of Safari's AutoFill.....	106
Mitigation	106
When Your Device Goes Missing	
Safety Tips While Out and About.....	109
Find My iPhone (and Other Devices)	109
Remote Tracking Software	120
About This Book	
Ebook Extras.....	123
About the Author	124
About the Publisher.....	125
Copyright and Fine Print	
Featured Titles	

Read Me First

Welcome to *Take Control of Networking & Security in iOS 6*, version 1.0, published in November 2012 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and edited by Tonya Engst and Michael Cohen.

This ebook describes how to use your iPhone, iPod touch, or iPad with iOS 6 on a Wi-Fi or cellular/mobile network securely, making connections with ease while protecting your data. It also covers Bluetooth networking, tracking an iOS device, solving connection problems, and picking the right mobile broadband plan or other option for cellular connectivity.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted [classroom and Mac user group copies](#) are available.

Copyright © 2012, Glenn Fleishman. All rights reserved.

Updates and More

You can access extras related to this ebook on the Web (use the link in [Ebook Extras](#), near the end; it’s available only to purchasers). On the ebook’s Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and—usually—Mobipocket. (Learn about reading this ebook on handheld devices at <http://www.takecontrolbooks.com/device-advice>.)
- Read postings to the ebook’s blog. These may include new tips or information, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see [Ebook Extras](#).

Basics

In reading this book, you may get stuck if you don't understand a few rules of the road.

Software and Hardware

- **iOS:** iOS is the name of the operating system (OS) that handles all hardware and software operations on Apple's mobile devices.
- **Mobile devices:** I cover networking and security for all Apple devices that can run iOS 6. As of November 2012, that comprises:
 - iPhone 3GS, 4, 4S, and 5. The iPhone 5 ships with iOS 6 and cannot run any earlier version. Except for the discontinued 3GS, all these devices may be purchased new.
 - iPad 2, 3rd-generation iPad (early 2012), 4th-generation iPad (late 2012), and iPad mini. Except for the 3rd-generation model, all these devices remain for sale.

Apple updated its iPad line-up in October 2012 to include the iPad 2, 4th-generation iPad with Retina display, and iPad mini. The iPad 2's cellular version has up to 4G networking, while the 4th-generation iPad and iPad mini support LTE. The latter two devices also have the potential to transfer data over Wi-Fi faster.

- iPod touch 4th- and 5th-generation models, which were first released in 2010 and 2012, respectively. Only the 5th-generation iPod touch may be purchased new.

When I write, "iPhone," "iPad," or "iPod touch," I mean all such models that can run iOS 6, unless a difference has to be called out.

Excluded: *The excluded models are the iPhone (original), iPhone 3G (2008), original iPad (2010), and 1st- through 3rd-generation iPod touch (2007–2009).*

- **Radio types:** All iOS 6-capable devices have Bluetooth and Wi-Fi radios. *Bluetooth* is a short-range wireless technology for linking devices with accessories such as audio headsets, and keyboards—and even each other. *Wi-Fi* is a high-speed networking standard for moving data among devices on a local network.

The cellular iPad and all iPhones covered have two more radios: a *cellular modem*, which allows data communications on mobile networks, and a *GPS receiver* for calculating position based on satellite signals, just like with a standalone GPS navigator. Depending on the device, the cellular modem may be for either a GSM or a CDMA network or for both.

- **Desktop vs. mobile:** In this ebook, a *desktop device* is either a laptop or a traditional computer that would sit on a desk, typically running Mac OS X or Windows. A *mobile device* means a portable device such as an iPhone, iPad, iPod touch, Android phone, Kindle Fire, Nook Tablet, or Blackberry smartphone. *Mobile software* refers to software running on a mobile device, such as the mobile version of Apple's *desktop* Safari Web browser, which is technically called *Mobile Safari*, even though Apple calls it "Safari" on the iOS 6 Home screen.

Information Related to Mobile Networking Is Boxed

I use a special blue box to call out information particular to 3G, 4G, and LTE *mobile networking* hardware and service plans.

Cellular Networks

GSM and CDMA are the two most widely used cellular standards in the world. GSM is in far greater use, with major carriers across Europe, Asia, and the Americas relying on GSM, including AT&T and T-Mobile in the United States. CDMA is used by Verizon Wireless and Sprint Nextel in the United States and by a few other carriers in limited markets, often for just 2G service.

The number plus *G* for *generation* convention, as in "2G" in the previous paragraph, breaks out as follows:

- **1G:** 1G networks, the first mobile networks deployed, were analog only and very inefficient in their use of spectrum. All U.S. analog networks have been turned off in favor of digital ones.
- **2G:** 2G was the first digital-only standard, encompassing voice and slow data at dial-up modem speeds. It uses separate standards for voice and data.
- **2.5G:** 2.5G was developed as an interim or bridge between 2G and 3G networking when it became clear that 3G networks weren't

being built as quickly as originally planned at the start of this century. 2.5G allowed cellular networks to gain efficiency without the full expense of 3G. 2.5G service runs at a few hundred Kbps.

- **3G:** 3G networks were designed to use data for both voice and data, making it possible to mix the two for efficiency and use the same connection for calls and Internet access. 3G networks operate at the speed of slow DSL broadband connections: from a few hundred Kbps up to 2–4 Mbps at the fastest.
- **4G:** 4G pushes rates into low-end cable speeds: 3–7 Mbps downstream, typically, with lots of variation.
- **LTE:** A truly different network technology, Long Term Evolution (LTE) has a lower *latency* (round-trip time for data) and a higher bandwidth than 4G. Early versions can easily top 10 Mbps downstream, and future versions might be ten times faster a few years hence.

Navigating in iOS

- **Settings app:** I often tell you to adjust options in the Settings app. By default, this app appears on the first page of the Home screen. To open the Settings app, tap its icon.
- **Navigation:** To describe moving around in the iOS 6 interface, I sometimes use a shortcut. For example, if I wanted to tell you on an iPad to open the Settings app, tap the Wi-Fi option at the left, and then—in the right hand Wi-Fi pane—tap Other, I might instead tell you to “tap Settings > Wi-Fi > Other.”

What’s New in This Edition

This ebook significantly updates and brings together two separate Take Control ebooks that I wrote previously about networking and security in iOS 3 and iOS 4. One covered the iPad, and the other discussed the iPhone and iPod touch. Because of Apple’s release schedule, having separate ebooks made sense.

Due to Take Control’s crowded publication calendar, those ebooks skipped iOS 5 completely. Now, in a single ebook, I cover networking and security for all Apple devices that can run iOS 6.

Introduction

Networking should be simple, and security should be automatic. And money should grow on trees. Despite how intuitive it is to pick up and use an iOS device, requiring little thought as to how it connects to a cellular or Wi-Fi network, it becomes quite complex as soon as you drill down to any details. This is especially true when connectivity fails, and you try to troubleshoot the problem.

Security is an even denser area. Apple makes the default choices in iOS reasonably secure, but to ensure real protection for your data—whether your device is stolen or while your bits are traveling through the æther—you need to know how it all works.

As someone who has spent a decade writing about wireless networking, I can confirm that it can simply work. When it doesn't, that's when you need to roll up your sleeves. This ebook is full of advice about what to do when your network connection fails or can't be made in the first place.

I discuss the ins and outs of choosing a cellular data plan, living within the constraints of such offerings, and reducing data usage or offloading it to Wi-Fi. I also cover Bluetooth networking.

While iOS has plenty of security features, to use them properly you may need to supplement the limited settings that Apple offers with third-party apps. This is especially true when it comes to keeping your data safe from others' prying eyes, whether your data is stored on your iOS device or sent over a network, and when you need to recover a lost or stolen device.

No iOS device is an island. This book will help you learn how to connect easily and securely to the “main”—the rest of your network and the Internet.

Quick Start to iOS Networking and Security

This ebook explains how to use your iOS 6 device safely on a network, including how to connect and how to customize a connection, and how to secure data that's on the device or that's passing over a network. You can read the ebook in order or skip to topics of particular interest.

Make a connection:

- Hook up with Wi-Fi without worries by reading [In-Depth on Wi-Fi](#).
- Discover the ins and outs of cellular data plans from AT&T, Verizon Wireless, and Sprint, and get advice about other carriers, in [Work with Cellular](#).
- Connect your device to a Bluetooth accessory, see [Set Up Bluetooth](#).
- Turn on the mobile hotspot and use its connection with another iOS device, Mac OS X, or Windows. Read [Make a Mobile Hotspot](#).

Ensure you're secure:

- Set up a secure Wi-Fi connection. Read [Connect to a Secure Wi-Fi Network](#).
- Prevent others from sniffing your passwords and data over wireless networks. See [Transfer Data Securely](#).
- Don't let your data fall into the wrong hands. See [Keep Data Safe](#).
- Learn how to set up the "Find My iPhone" service, and find out what to do [When Your Device Goes Missing](#).

Go under the hood, gain more control, and solve problems:

- Read [Managing Wi-Fi Connections](#) to learn the ins and outs of joining and forgetting hotspot networks, configuring your device to connect in complex scenarios, and work through problems with [Wi-Fi Troubleshooting](#).
- Find tips for setting up a residential Wi-Fi network to work well with iOS devices in [Tweaking Your Network for Faster Performance](#).

- Avoid unexpected data service plan fees. See [Keep Usage Restrained](#) and [Choose to Use Cellular Data or Wi-Fi](#).
- Keep cellular data costs under control outside your home country. Read [Cross-Border Mobile Use](#).
- Learn how to turn off the wireless radios in your device in [Airplane Mode](#).

In-Depth on Wi-Fi

Wi-Fi works quite simply in iOS, but there's a lot of hidden detail. In this chapter, you'll learn how to interpret the Wi-Fi settings view, handle automatic hotspot connections, manipulate custom network settings, and troubleshoot common problems.

At the end of the chapter, in [Tweaking Your Network for Faster Performance](#), you'll find specs that will help you configure a home or small office Wi-Fi network for the particular flavor of Wi-Fi built into any of your devices.

Managing Wi-Fi Connections

iOS centralizes Wi-Fi management in the compact space of the Wi-Fi settings view (**Figure 1**). To reach it, open the Settings app and tap Wi-Fi.



Figure 1: The Wi-Fi view has a list of available networks.

Connect to a Secure Wi-Fi Network

Most home networks are now secured, and nearly all businesses networks employ some way of keeping outsiders out. Connecting to these secured networks is often as easy as entering a password, but not always, and this chapter helps you handle any difficult security situations that you might encounter.

Also, if you're setting up Wi-Fi security for a network, this chapter discusses what sort of security to set up and how users with iOS devices will connect to it.

Wi-Fi security divides into three main types:

- **Simple:** Since 2003, the best option for a home or small office network is Wi-Fi Protected Access 2 (WPA2). Consult [WPA2 Personal](#).
- **Corporate/academic:** Many companies and colleges rely on WPA2 Enterprise, a stronger method of security that's fully supported in iOS. Read [WPA2 Enterprise](#).
- **Outdated, unreliable:** Some older ways to "secure" networks are still in place. See [Wired Equivalent Privacy \(WEP\)](#) and [Mac Address Filtering](#) to learn more.

Of course, I'd prefer that you always made a secure connection, but you may not have control over how a network is protected.

Note: Cellular networks have their own security methods, which are partly based on the Subscriber Identity Module (SIM) for GSM networks and on a unique set of identifiers for CDMA networks.

Hotspots not hot on security! Public hotspots, whether free or fee, typically have no security; if they do, it's a shared password that provides no protection from other people on the network. When you connect, I recommend using only secured services or a virtual private network (VPN) connection. Read [Transfer Data Securely](#) for details.

Work with Cellular

Cellular networks provide ubiquitous access to an iOS device that sports a built-in mobile broadband radio. That includes any iPhone or cellular model of the iPad, but excludes all iPod touch models and the Wi-Fi-only iPads.

The iPhone features voice calling and Internet access, while an iPad works only with data—although you can use Skype or other apps to make voice calls over the data side of the network.

When you're picking out a new iPhone or cellular iPad, you should consider what type of cellular network you want to connect it to—and what kind of data plan to purchase. Or, if you already have one of these devices, perhaps you're curious about the cellular network that it can communicate with. You might also need background information to understand how an iOS device communicates.

In this chapter, I talk about all these topics, plus at the end, I discuss [Alternatives to Cellular Data Plans](#) to help you extend cell service to any iOS device even if it doesn't have a cellular radio.

Note: Americans tend to say *cellular* to refer to mobile networks run by companies to provide seamless coverage for a fee. In the UK and some other countries (and in translation), that term is *mobile*. When I refer to *cellular data* in this chapter, it's interchangeable with *mobile data*. I also use the term *mobile broadband*, which is used in both America and other English-speaking lands.

Two Kinds of Mobile Networks

Around the globe, two kinds of cellular communications standards dominate mobile networks: GSM and CDMA. Until the iPad 2 and iPhone 4, which were released in separate versions for Verizon Wireless in early 2011, all iPhones and cellular iPads worked only on GSM cell networks. GSM is the dominant standard worldwide, with billions of voice and data subscribers. Verizon uses the competing CDMA flavor of cellular networking, which has far fewer users internationally.

Make a Mobile Hotspot

The iPhone has a built-in cellular modem that lets the phone access high-speed mobile data and voice networks. So why can't we use that same built-in modem with our laptops (or other devices) when we're traveling instead of having to buy a separate cellular modem or router and pay a separate monthly service fee?

The good news is that you can with the Personal Hotspot feature. This feature was added in iOS 3, and activated in the United States with iOS 4. While the name implies a Wi-Fi hotspot connection, which is one component of it, you may also use Bluetooth or USB with desktop computers and other devices to extend access. All three methods may even be used simultaneously.

Personal Hotspot turns an iPhone, 3rd- or 4th-generation iPad, or iPad mini with an active mobile broadband subscription into a cellular modem.

Hotspot or Tethering?

Extending a cellular modem connection via USB used to be called *tethering* because the phone was physically tethered to a laptop with a USB cable. It was also typically a one-to-one connection: one phone extended one laptop. Later, this terminology was extended to Bluetooth connections.

More recently, tethering has gone out of use as a generic term, and Apple has opted to call its sharing feature Personal Hotspot, whether you use Wi-Fi, Bluetooth, or USB.

In this chapter, I talk about a *mobile hotspot* or *Personal Hotspot* to refer to all the features, but use the term *tethering* when the discussion is specifically about Bluetooth or USB.

Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, earpieces, headsets, and keyboards to an iOS device for listening to music and entering text.

Read this chapter to learn how to set up and manage Bluetooth devices.

Tethering: *Bluetooth can provide Internet service to an iOS device from another piece of hardware, such as an iPhone with Personal Hotspot on, a laptop, or a cellular router with Bluetooth as a an option. See the previous chapter, [Make a Mobile Hotspot](#), for details.*

Bluetooth Basics

The Bluetooth SIG, a trade group, certifies devices as Bluetooth compliant for particular *profiles*, which include things like text entry, stereo audio, file transfer, and modem access. Apple's iOS devices work with any device that meets the Bluetooth spec for several profiles, including audio, peer-to-peer transfer, and external keyboards.

Note: Apple documents iOS device compatibility in a support note at <http://support.apple.com/kb/HT3647>.

When you connect with Bluetooth, the process is known as *pairing*. Some devices can be paired with several hosts (like computers or mobile devices); others can pair with only one host at a time, and must be re-paired to switch. Bluetooth devices are *discoverable* when they are set to allow a pairing connection.

Bluetooth is handled from the Bluetooth view (Settings > Bluetooth). This view lets you turn Bluetooth on and off and displays a list (under Devices) of Bluetooth peripherals. The list shows any devices that have been previously attached to the device and the current status of such devices. The list also displays any discoverable devices within range.

Note: Bluetooth options used to be a level down in Settings > General > Bluetooth. It's now a top-level item in iOS 6.

Airplane Mode

Before you're flying so high with some guy in the sky, you need to disable radio communications on your mobile device. The Airplane Mode switch makes this simple.

Contrary to urban myth, cellular phones don't cause planes to crash. That's good, because research has shown that mobile phones are left on (and even used) during practically every flight.

The reason that worldwide flight authorities, including the FAA in the United States, demand that passengers turn off most kinds of electronics that produce or receive radio signals during a flight, as well as all electronic devices while flying below 10,000 feet, is because of a slight potential for risk that hasn't entirely been teased out from the reality of risk.

All electronic devices produce some emissions, and it's thought from years and years of testing that certain *avionics*—aircraft electronics—may be susceptible to some radio signals that are otherwise benign. Under 10,000 feet, a particular reading being knocked for a loop could be extremely dangerous. Hence the desire to reduce such risks.

What's Airplane Mode?

The Airplane Mode in iOS, available to all iOS devices, is a simple way to set your device to a legally required quiet mode during flight. In the Settings app, tap the switch next to Airplane Mode. It shows On reversed out of orange when the mode is active, and you see an airplane ✈ icon in the top status bar at the left.

Saves battery life, too: *If you don't need to use any of the radios for network access, peripherals, or location, Airplane Mode is an effective way to extend battery life, too.*

Transfer Data Securely

Any networked mobile device, whether an iPad, laptop, Nintendo game player, or what have you, can be in constant communication with a network, which means that you could unintentionally reveal a lot about yourself—including passwords and private data—as your data flows between a central hub and the device. With an iOS device, that hub is either a Wi-Fi router or, for a mobile broadband model, it could instead be a cellular base station on nearby a tower.

On open public networks, such as the Wi-Fi found in restaurants, cafés, and airports worldwide, anyone in your vicinity can use free, simple *sniffing* software to capture all the data passing by, extract passwords and personal information, and use it to wreak havoc, commit identity theft, and order goods and services for themselves. While it may sound paranoid, there's no built-in protection for some of your data, and you thus have to assume from the perspective of risk that someone is always trying steal your data.

Fortunately, it's easy to avoid having data grabbed with a small amount of preparation and configuration. Here's what you need to know to stay protected while using local networks and the Internet.

Exposure

To figure out how to respond to the risk of data being captured as you transfer it, let's first consider what precisely is at risk and not at risk.

Note: Cellular data is encrypted by default, and cell networks have far less risk associated with their use. See [Cellular Data Networks](#) for more details, later in this chapter.

What's at Risk?

When your iOS device is connected via Wi-Fi, the risk is both to data passing over the air to the Wi-Fi router, and data passing between the Wi-Fi router and a broadband modem over Ethernet. Malicious software that's found its way onto a computer that's connected via Ethernet to a Wi-Fi router could sample all data coming and going between Wi-Fi-connected devices and the Internet. In the paragraphs

Keep Data Safe

Someone using a completely unprotected iOS device can access any precious information stored on it, as well as any accounts related to apps or Web sites. You can secure that data, whether you leave your device on a living room table or your office cubicle and walk away for an hour, or if your device is stolen.

Let's begin by looking at what might be at risk. We'll then discuss [The Danger of Safari's AutoFill](#) and look specifically at [Mitigation](#) measures that you can take.

Exposure

Let's start with your exposure. iOS keeps relatively little data accessible; rather, what's at risk is access to resources.

What's at Risk?

A person who uses your device without permission can't, for instance, recover your email account password, but could use your email account to read your email and send email purporting to be from you, or view any document that you have in a word-processing program, or view your photos.

Here are some examples:

- Read your email and send new messages.
- Access content in any app that doesn't have password protection, such as Calendar or Contacts, and make changes, copy items, or view what you've been up to.
- See your entire Safari browsing history.
- Access, and potentially change or delete, files on any server to which you've linked and for which you've stored a password in apps for remote file access, such as Air Sharing HD and GoodReader. This includes FTP, SFTP, WebDAV, and other file-sharing apps.
- In an app that provides access to a password-protected account, view the content (but not the password) associated with the

When Your Device Goes Missing

Your mobile device is a desirable item for thieves. It's compact, it has a high retained value, and there's a huge market for used models.

Without freaking you out about theft, I want to tell you how you can protect your data when your device has disappeared, make it impossible for a thief to use your device, and find your device if it's stolen or lost.

Safety Tips While Out and About

Let me start with a few practical tips, applicable to any mobile device:

- **Don't pull out your device outdoors or in large open public spaces indoors if you can be approached from behind:** I don't suggest always keeping your back to the wall, but if you're in a crowded railway station and whip out the unit, it would be easy work for someone to run by and snatch it.
- **Don't set it down and turn away:** Leaving it on a table at a café while you turn away to talk to someone could provide a thief with a good opportunity to relieve you of your device.
- **Lock your device when you're not using it:** If you use the passcode lock described in [Set a Passcode](#) and hit the Sleep/Wake button when you're not using the device, it's more likely that a thief would be prevented from accessing your data.

Find My iPhone (and Other Devices)

Find My iPhone, introduced by Apple in 2009, has a name that belies its utility: it works with every kind of iOS device and, starting in Mac OS X 10.7 Lion, with Macintoshes, too (as Find My Mac in the iCloud preference pane). You can find the last reported position of any iPod

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments at tc-comments@tidbits.com.

Ebook Extras

You can [access extras related to this ebook](#) on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and—usually—Mobipocket. (Learn about reading this ebook on handheld devices at <http://www.takecontrolbooks.com/device-advice>.)
- Read postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try the directions above and find that the device you're reading on is incompatible with the Take Control Web site, contact us at tc-comments@tidbits.com.

About the Author



Glenn Fleishman was trained as a typesetter, received a degree in art, and works as a journalist and programmer. His writing appears regularly in the *Economist*; the *Seattle Times*, where he been a Mac columnist since 2000; and *TidBITS*, for which he programs, writes, and helps with strategy and planning.

Glenn is the executive editor of Marco Arment's *The Magazine*, a senior contributor to *Macworld* magazine, and host of the podcast *The New Disruptors*. He also regularly pens pieces for *BoingBoing*. He lives in Seattle with his wife and two sons.

In October 2012, he appeared on the *Jeopardy* quiz show and managed to win—twice! Alex Trebek seems like a very nice fellow, but you never get to really know him.

Author's Acknowledgments

I dedicate this book to my wife, Lynn, and sons, Ben and Rex. They keep me sane and happy, and keep me from spending my entire day thinking about and using digital devices. A big thank you also to the tireless Tonya Engst.

Shameless Plug

If you ever have to monkey with Apple's Wi-Fi networking gear, look at my title *Take Control of Your 802.11n AirPort Network*. Twelve years of hard-won experience with Apple's equipment and Wi-Fi networking is distilled into this volume.

About the Publisher

Publishers Adam and Tonya Engst have been creating Apple-related content since they started the online newsletter *TidBITS*, in 1990. In *TidBITS*, you can find the latest Apple news, plus read reviews, opinions, and more (<http://tidbits.com/>).

Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.



Production credits:

- Take Control logo: Jeff Tolbert
- Cover design: Jon Hersh
- Production Assistants: Michael E. Cohen, Oliver Habicht
- Editing Assistant: Michael E. Cohen
- Editor in Chief: Tonya Engst
- Publisher: Adam Engst



Copyright and Fine Print

Take Control of Networking & Security in iOS 6

ISBN: 978-1-61542-412-2

Copyright © 2012, Glenn Fleishman. All rights reserved.

TidBITS Publishing Inc.

50 Hickory Road

Ithaca, NY 14850 USA

<http://www.takecontrolbooks.com/>

Take Control electronic books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control ebooks also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

This electronic book doesn't use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

You have our permission to make a single print copy of this ebook for personal use. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Although the author and TidBITS Publishing Inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this ebook is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are the trademarks or that are the registered trademarks of Apple Inc.; to view a complete list of the trademarks and of the registered trademarks of Apple Inc., you can visit <http://www.apple.com/legal/trademark/appletmlist.html>.

Featured Titles

Click any book title below or [visit our Web catalog](#) to add more ebooks to your Take Control collection!

[Take Control of Apple Mail in Mountain Lion](#) (Joe Kissell) Learn the basics and go under the hood with Apple's Mail application in OS X 10.8.

[Take Control of BBEdit](#) (Glenn Fleishman): Learn how to take full advantage of BBEdit's text-processing power!

[Take Control of CrashPlan Backups](#) (Joe Kissell): Join backup expert Joe Kissell as he shares real-world advice about protecting your data with CrashPlan's onsite, offsite, and cloud backups.

[Take Control of Getting Started with DEVONthink 2](#) (Joe Kissell): Store, organize, and locate your PDFs, paper documents, email messages, and scribbled notes with DEVONthink 2.

[Take Control of iCloud](#) (Joe Kissell): Understand the many features, get set up properly, and enjoy iCloud!

[Take Control of Mail on the iPad, iPhone, and iPod touch](#) (Joe Kissell): Develop your mobile email strategy and learn how to use email effectively on your handheld Apple devices.

[Take Control of Messages in Mountain Lion](#) (Glenn Fleishman): Communicate with confidence in Messages! Learn how to chat with text, audio, or video, and how to share screens.

[Take Control of the Mac Command Line with Terminal](#) (Joe Kissell): Explore the basics of the Unix command line that underlies Mac OS X, and get comfortable and confident when working in Terminal.

[Take Control of Speeding Up Your Mac](#) (Joe Kissell): Put the zip back into your Mac with advice based on Joe's extensive research and experimentation in the area of Mac performance.

[Take Control of Your 802.11n AirPort Network](#) (Glenn Fleishman): Make your AirPort network fly—get help with buying the best gear, set up, security, and more.