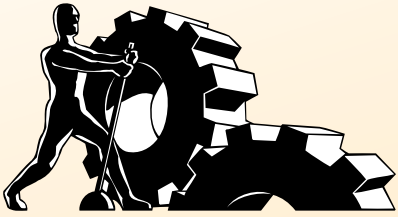


**Check for Updates**

Make sure you have the latest information!



**TidBITS Publishing Inc.**

**Take Control of Your**

**vi.7**

# Wi-Fi Security

**Adam Engst &  
Glenn Fleishman**

**\$10**

[Help](#)

[Catalog](#)

[Feedback](#)

[Blog](#)

[Order Print Copy](#)

Click here to buy the full 109-page "Take Control of Wi-Fi Security" for only \$10!

# Table of Contents

## **READ ME FIRST 4**

Updates and More.....	4
Basics .....	5
What's New in Version 1.7 .....	6
What Was New in Version 1.6.....	6

## **INTRODUCTION 7**

## **WI-FI SECURITY QUICK START 9**

## **DETERMINE YOUR SECURITY RISK 11**

Evaluate the Likelihood of Attack .....	12
Determine Your Liability .....	15
Calculate Lost Opportunity .....	24
What You Should Do .....	25

## **PREVENT ACCESS TO YOUR WIRELESS NETWORK 27**

Use Secure Settings.....	27
Ignore These Sops to Security .....	30
Watch out for WEP Encryption .....	32
Use Wi-Fi Protected Access (WPA or WPA2).....	35
Enable Guest Access .....	44

## **SECURE YOUR DATA IN TRANSIT 46**

Encrypt Email Passwords .....	47
Encrypt Specific Files and Messages .....	49
Encrypt Sessions and Data Sequences with SSL/TLSwith SSL/TLS	55
Encrypt Data Streams with SSH.....	60
Encrypt All Data with a VPN .....	66

## **PROTECT YOUR SYSTEMS 68**

Get Paranoid .....	68
Install Antivirus Software.....	71
Assign Private Addresses for Passive Protection .....	73
Enable an Active Firewall .....	75

## **SECURE SMALL OFFICE WI-FI 80**

Three Security Options .....	80
Use a Shared Key .....	81

Use WPA2 Enterprise Logins.....	82
Use a VPN .....	88

**GLOSSARY 93**

**APPENDIX A: PASSWORD ADVICE 101**

Generate Three Passwords.....	101
Learn to Create a Highly Secure Password.....	103

**ABOUT THIS BOOK 105**

Ebook Extras.....	105
About Glenn.....	105
About Adam.....	106
Authors' Acknowledgments .....	106
Shameless Plugs.....	106
About the Publisher.....	107
Production Credits .....	107

**COPYRIGHT AND FINE PRINT 108**

**FEATURED TITLES 109**

# Read Me First

Welcome to *Take Control of Your Wi-Fi Security*, version 1.7, published in November 2010 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and Adam C. Engst, and it was edited by Tonya Engst.

This book is devoted to helping you most effectively secure your home and office wireless network under Mac OS X and Windows using common networking hardware.

Copyright © 2010, Glenn Fleishman and TidBITS Publishing Inc. All rights reserved.

If you have an ebook version of this title, please note that if you want to share it with a friend, we ask that you do so as you would a physical book: “lend” it for a quick look, but ask your friend to buy a new copy to read it more carefully or to keep it for reference.

Discounted [classroom and Mac user group copies](#) are also available.

---

## UPDATES AND MORE

---

You can access extras related to this book on the Web (use the link in [Ebook Extras](#), near the end of the book; 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 purchase any subsequent edition at a discount.
- Download various formats, including PDF and—usually—EPUB and 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.
- Get a discount when you order a print copy of the ebook.

---

## BASICS

---

Here are a few “rules of the road” that will help you read this book:

- **Path syntax:** We occasionally use a *path* to show the location of a file or folder in your file system. For example, Mac OS X stores most utilities, such as Terminal, in the Utilities folder. The path to Terminal is: [/Applications/Utilities/Terminal](#).

The slash at the start of the path tells you to start from the root level of the disk. You will also encounter paths that begin with `~` (tilde), which is a shortcut for any user’s home directory. For example, if a person with the user name `joe` wants to install fonts that only he can access, he would install them in his [~/Library/Fonts](#) folder, which is just another way of writing [/Users/joe/Library/Fonts](#).

- **Menus:** When we describe choosing a command from a menu in the menu bar, we use an abbreviated description. For example, the abbreviated description for the menu command that creates a new 802.1X connection in Internet Connect is “File > New 802.1X Connection.”
- **Wi-Fi, AirPort, and wireless networking:** *Wi-Fi* is an industry term that encompasses four short-range, unlicensed, radio technologies: 802.11n, 802.11g, 802.11b, and 802.11a. Apple calls 802.11b “AirPort” and 802.11g and 802.11n “AirPort Extreme.” Regardless of the term, it’s all wireless networking. For many more definitions and a further explanation of how the standards work, read [Take Control of Your 802.11n AirPort Network](#) (focused on newer 802.11n gear from Apple). For more details, see the [Glossary](#).
- **Adapters and gateways:** A standard wireless network has two distinct components: a wireless network adapter (or wireless card) and a wireless gateway (or wireless router). The *wireless network adapter* is attached to or inserted into a computer and connects to a *wireless gateway*, which in turn manages the entire wireless network and shares your Internet connection.

---

## WHAT'S NEW IN VERSION 1.7

---

This update includes the following changes:

- The ebook still covers Mac OS X 10.5 Leopard, but minor changes for 10.6 Snow Leopard are now incorporated. It also still refers to older versions of Windows, but some bits of information about Windows now include Windows 7.
- The ebook is updated to be aware that iPhone OS is now iOS and that the iPad has joined Apple's line of mobile devices.
- [Determine Your Liability](#) was updated to discuss the latest state of affairs, with numerous small changes.
- In [Use Wi-Fi Protected Access \(WPA or WPA2\)](#), we've added clarifying details and updated the discussion generally, plus we've made several revisions to move our emphasis to the newer WPA2 security standard.
- The topic "Share via Devicescape" is now called [Share via Easy WiFi](#), and it now describes the latest details on this Web service that helps you manage and share access to your Wi-Fi hotspot or network.
- Overall, we've added a few snippets about recent security flaws in Wi-Fi and related protocols, and we've moved the discussions forward to reflect a late-2010 point of view.

---

## WHAT WAS NEW IN VERSION 1.6

---

We created this new version to update the ebook in a variety of areas:

- The ebook is now fully updated for Mac OS X 10.5 Leopard.
- You'll find an updated discussion of Wi-Fi Protected Setup (WPS), a simpler way of securing Wi-Fi networks. See [Use Wi-Fi Protected Access \(WPA or WPA2\)](#).
- The ebook covers how to [Use Apple's guest networking](#).
- [Secured Web sites](#) now discusses Enhanced Validation Web sites, something you may be interested in knowing about next time you do online banking.

# Introduction

*Just because you're paranoid doesn't mean they're not out to get you.*

*–Internet security saying*

Networking wasn't supposed to be like this. When computer networks were invented, no one anticipated hundreds of millions of naïve users. Nor did they expect crackers, viruses, worms, spam, or spyware. But that's where we've ended up. Most people are clueless about security, and few people devote any time to making their systems secure.

The biggest security risk comes from the fact that computers are all networked these days: to each other and to the Internet. Want a totally secure computer? Make sure it isn't connected to the Internet, or to any other computer, and put it in a locked room with an armed guard checking identification on those who enter. Not very useful, eh?

Wireless networking, because it makes connecting computers so simple, makes proper security even more critical. Before wireless networking, you could rely on a locked door to restrict access to your Ethernet jacks, and thus to your network. But now, transmissions over wireless networks—because they go through locked doors, along with walls, ceilings, floors, and other obstructions—are easily intercepted by consumer-level equipment just like the gear you use to connect your computers and access point.

So anyone in range of your wireless network can connect to it, and, unless you've taken appropriate precautions, wreak all sorts of havoc. And, unfortunately, understanding the reality of wireless security is nowhere near as simple as setting up a wireless network to start.

Our goal in *Take Control of Your Wi-Fi Security* is to bring clarity to the topic; to help you decide how worried you should be about security problems; and to help you to lock down your network, protect your data in transit, and secure your systems against attack.

Before we get started, we want to mention a few important caveats:

- We're writing this book for individual users with wireless networks at home and for people who run small to medium-sized office networks (from 2 to 50 people), not for veteran network administrators who manage large institutional networks.
- Security, whether you're talking about protecting your car, your home, or your wireless network, is hard, mostly because it's a battle with another human being. Locking your door with a simple knob lock stops amateur thieves, but keeping more experienced thieves out requires a strong deadbolt. And if you live where burglary is likely, or if you have especially valuable property, you have to think about if multiple locks, alarm systems, or bars on the windows are also necessary. Unfortunately, the kind of people who break into networks are usually much smarter than garden-variety thieves, and as a result, the security measures you must take are commensurately more complicated. So, our apologies up front, but some sections of this book are inherently quite technical.
- Because every network uses different hardware, software, and configurations, we can't give exact, foolproof, step-by-step instructions for every task we explain. That said, by the time you finish reading this book, you should have the background necessary to configure the networking hardware and software you do have (or are willing to purchase) to the level of security you want to achieve.

We've been using and writing about networking for more than 40 years combined, and we've both set up and maintained numerous wired and wireless networks over that time. And over those years of networking computers together, we've experienced the seedier side of the industry: attacks on our networks via the Internet, password thefts, wireless snoopers, and more. We've shared our experience in many articles and public presentations, and now we look forward to sharing it with you.

**Tip:** For more about wireless networking, check out these other ebooks written by Glenn: [Take Control of Your 802.11n AirPort Network](#), [Take Control of iPad Networking & Security](#), and [Take Control of iPhone and iPod touch Networking & Security, iOS 4 Edition](#).

# Wi-Fi Security Quick Start

You can read this title in the order shown here, or you can click a link to jump to a topic immediately. That said, if you're new to the topic of security, we encourage you to read [Determine Your Security Risk](#) first to get a sense of how concerned you should be about security.

## **Determine how worried you should be about security:**

- Learn about the three Ls of security: likelihood of attack, liability in the event of loss, and lost opportunity. See [Determine Your Security Risk](#).
- Figure out where you stand on the continuum of people who should be concerned about security. See [What You Should Do](#).

## **Lock down your wireless network:**

- Take care of three basic security measures with the configuration of your Wi-Fi router. Read [Use Secure Settings](#).
- Discover which widely used security mechanisms won't prevent determined attackers. See [Ignore These Sops to Security](#) and [Watch out for WEP Encryption](#).
- Turn on wireless security that is guaranteed to keep intruders out. Find directions in [Use Wi-Fi Protected Access \(WPA or WPA2\)](#) and [Simplify with Wi-Fi Protected Setup](#). Also, be sure to read [Appendix A: Password Advice](#).
- Consider setting up special access features for guests; see [Use Apple's guest networking](#) and [Share via Devicescape](#).
- If you need to protect more than just a home computer or two, be sure to read [Secure Small Office Wi-Fi](#) for additional details.

## **Protect your data in transit:**

- Keep miscreants from discovering your passwords and reading your communications. Consult [Encrypt Email Passwords](#) and [Encrypt Specific Files and Messages](#).

- Armor your Internet sessions inside protected tunnels to keep snoopers from listening to your traffic. Read [Encrypt Sessions and Data Sequences with SSL/TLS](#), [Encrypt Data Streams with SSH](#), and [Encrypt All Data with a VPN](#).

**Secure your computers:**

- [Protect Your Systems](#) from viruses, spyware, and crackers.

# Determine Your Security Risk

Security is something we tolerate, not embrace. Your comfort level with security may vary enormously depending on your background and location. Growing up in rural New York State in the early 1980s, Adam left his car keys in his elderly Dodge Colt when it was parked at home. No one lived within a mile; cars driving by were infrequent, easily seen, and usually announced by the family dog; and a rusty Dodge Colt wasn't worth much.

Living in a populous suburb of Seattle a decade later, Adam not only didn't leave his keys in his shiny, red Honda Civic when it was parked in the driveway, he also locked the doors. Adam's behavior changed—more paranoid or more realistic, take your pick—because of a different evaluation of the three Ls of security: likelihood, liability, and lost opportunity. You can get a better idea of where you stand in terms of likelihood, liability, and lost opportunity by answering these questions:

- **Likelihood:** How likely is it that someone will break into your wireless network or *sniff* (monitor) the traffic going across your wireless connection? (See [Evaluate the Likelihood of Attack](#), next page, for more info.)
- **Liability:** What is the potential liability if someone breaks in to your network, either to monitor your traffic or to use your connection for other purposes, including illegal ones? (Read [Determine Your Liability](#), ahead, for details.)
- **Lost opportunity:** How much money and effort are you willing to expend on the security of your wireless network? (See [Calculate Lost Opportunity](#), further ahead, for details.)

In the rest of this chapter, we help you answer those questions. We don't want to turn you into a tic-ridden paranoid. Instead, we want to present a fair discussion of the risks and potential outcomes when you rely on wireless networks.

# Prevent Access to Your Wireless Network

Wireless networks weren't originally designed to be very secure. The only encryption available initially, Wired Equivalent Privacy (WEP), was supposed to work as well as those locks you find on old bathroom doors that can be picked with a paperclip. The designers assumed most people wouldn't have the interest in getting in. When Wi-Fi became popular, so did cracking techniques and tools, busting WEP's never-strong encryption. Further, most people buying Wi-Fi after the first wave weren't early adopter geek tech-heads. So security options, when available, weren't turned on.

As cracks and flaws evolved, so did replacement technologies: Wi-Fi Protected Access (WPA and WPA2), WEP's replacements. You can now reliably secure home and small business networks without much fuss. Even small businesses now can achieve corporate-level security without much cost or complexity.

In this chapter we first look at three easy things you can do immediately to enhance your network's security. We then look at common mistakes and techniques that don't provide any real security, and we run through how to secure your network with assurance.

We also offer a few suggestions on enabling safe access for visitors.

---

## USE SECURE SETTINGS

---

The first task in preventing access to your network is changing three default settings that—when left as they come from the factory—make cracking significantly easier. Connect to your wireless gateway with its management software and then:

- Change the admin password to one that's not obvious but that you'll remember.
- Verify that remote administration from outside the network is off.
- Change the network name.

# Secure Your Data in Transit

In the previous chapter, we explained how to prevent people from accessing your wireless network. However, you may still find yourself in circumstances in which you want protection but restricting access to the network won't help:

- You're sharing your local wireless network without encryption or using a shared network on which encryption can't be enabled.
- You're using a public wireless network in a location such as a coffee shop, hotel, airport, or community networking hotspot with a laptop, smartphone, iPad, or other mobile device.
- Your employer won't let you use any network except its wired network without encrypting communications to and from your computer.

You have an alternative: you can encrypt the data before it leaves your machine, and have it decrypted only when it arrives at its destination. By creating end-to-end links using strong encryption standards, you can keep your data completely safe from prying network sniffers. Even if people can join your network and reach the Internet—hijacking your link—they still can't see your data. Encrypting your data in transit is a lot more difficult than setting up a closed WPA2-protected network, but it provides more security.

We look at five popular categories and methods of securing data in transit, ranging from simple password protection up to full network encryption of all data, summarized in **Table 2**, coming up.

**Tip:** An added bonus of encrypting data from end to end is that the data you send and receive becomes completely unreadable by others not just on your wireless network, but also on every Internet link between your computer and the destination machine. That's why large organizations generally require their employees to use encryption technology for all communications.

# Protect Your Systems

One part of security is protecting your data in transit; the other part is protecting your systems—your computers, any Internet servers you run, your wireless gateway, and so on—from online intruders. Because wireless networks potentially expose your systems to attackers who would never have the same kind of access on a wired network—unless they broke into your house or business—you need to exercise greater care when protecting your computers on wireless networks.

You can secure your computers against snooping or attack in two ways: an active firewall or network address translation. You can use them separately or, for additional security, combined. And of course, it's essential to run current antivirus software if you use Windows. But first, why worry?

---

## GET PARANOID

---

You might think that you don't need to protect your computers, but, unfortunately, organized and disorganized crime has become rampant on the Internet, and these criminals need machines to do their bidding. There are seemingly hundreds of thousands amoral people or their agents out there constantly and automatically scanning large blocks of Internet addresses for weaknesses.

For the last few years, it's been only a matter of minutes after a computer first receives a *publicly routable IP address*—one that can be reached from anywhere on the Internet—before the first attack is launched against it.

These attacks focus on known bugs in software that allow a remote program or person to infiltrate your computer and take control of some of your software or the entire operating system. Once the attacker has established that level of control, he typically turns your computer into what's called a *zombie*.

Software on a zombie can be remotely directed to cause attacks on targets that are blackmailed to get the activity to stop. But more

# Secure Small Office Wi-Fi

Small businesses used to be unable to afford the equipment, software, or know-how needed to put in place the information technology (IT) infrastructure of a big organization. That's changed. A lot of technology that was available only in server hardware or software that cost thousands or even tens of thousands of dollars has now been scaled down and made affordable. This change lets offices of as few as five people increase the security of their in-house Wi-Fi networks and the security of their mobile users using wireless networks in cafés, hotels, and at home, all without breaking the bank. In some cases, a small office of even one or two people can take advantage of these tools.

While many small offices use Wi-Fi, it's clear that many more small offices have avoided Wi-Fi or used it in limited fashions because of security concerns: You may have no dedicated IT personnel or pay consultants by the hour for assistance, and thus have been leery of installing a wireless network that could expose confidential business or customer information. In this chapter, we offer some simple and cost-effective suggestions that won't send you scuttling to the classifieds to hire an expensive staffer. Instead, you might be able to set up a secure, small-office wireless network by yourself, or at least spend only a few hours with a consultant.

---

## THREE SECURITY OPTIONS

---

In this chapter, we look at three ways that you can secure your local Wi-Fi network against snoopers and unauthorized access:

- **Use a Shared Key:** With a shared key, security is achieved through a single encryption key that is shared among all users on the network. (We recommend a WPA2 key, because WEP is too weak.)
- **Use WPA2 Enterprise Logins:** In this case, an authentication system that provides each user with a unique user name and password and then assigns a unique network encryption key to each user each time they log in.

# Glossary

**802.11:** A set of wireless networking standards developed by the IEEE engineering standards body that include lettered protocols (802.11a, 802.11b, 802.11g, and 802.11n) that define the speed and spectrum used on a network, security (802.11i), and other parameters.

**802.11i:** A security standard from the IEEE intended to replace WEP. 802.11i encompasses two unique encryption algorithms: TKIP and AES-CCMP. 802.11i isn't the same as Wi-Fi Protected Access (WPA); rather, WPA and its successor, WPA2, were derived from different stages of the 802.11i task group's work. The 802.11i standard was rolled into 802.11-2007.

**802.11-2007:** This standard is a "roll-up" of previous 802.11 standards that have been cleaned up and put into one spec. The 802.11i security standard is now referred to as part of the 802.11-2007 roll-up.

**802.1X:** An authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides credentials, like a user name and password, that are verified by a separate server. In 802.1X, there are three roles: the supplicant (client), authenticator (switch or access point), and authentication server. WPA2 Enterprise is a version of 802.1X that works over Wi-Fi and provides only WPA2 encryption keys to clients.

**access point:** The hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point. Access points are often abbreviated to AP in industry literature, and you may also see them referred to as "wireless routers," "wireless gateways," and "base stations."

**AES-CCMP:** This extremely strong encryption standard that's part of WPA2 and 802.11-2007 is comprised of two elements. First, there's *AES*, which stands for Advanced Encryption System. Second, there's *CCMP*, which is a complex abbreviation standing for Counter-mode CBC-MAC Protocol; *CBC-MAC* stands for Cipher Block Chaining-

# Appendix A: Password Advice

We talk blithely about passwords throughout this book, and more generally, passwords are all around us. But are you picking good passwords? A bad password can be cracked easily, often just by guesswork. So here's some advice.

We can also recommend our colleague Joe Kissell's book on this subject: *Take Control of Passwords in Mac OS X*. Although it is focused on the Mac, it has broad advice applicable to everyone.

---

## GENERATE THREE PASSWORDS

---

Because it's nearly impossible to remember different passwords for every possible service, we recommend using three different passwords. If you restrict yourself to three passwords and always use the same email address or user name, the likelihood of forgetting your access information for any given site or program is low:

- **Low-security:** Create a standard low-security password that's simple and easily remembered. Since it's low-security, make sure to use it *only* for Web sites that don't store personal information about you (such as your address, birth date, or credit card number). In essence, this password protects only your online identity; if someone were to guess it, they could pretend to be you in a discussion forum or the like. Don't use this password for email accounts!
- **Medium-security:** For Web sites and accounts where some personal data is at risk, create a medium-security password. It will be harder to type, since it should include upper- and lowercase letters, numbers, and punctuation.
- **High-security:** Everyone should have a highly secure password that is long, hard to type, and impossible to guess. Use it for accounts, like your bank and PayPal, where money is involved, and for programs that store other passwords. Using a longer password

# 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](mailto: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 a subsequent edition at a discount.
- Download various formats, including PDF and—usually—EPUB and 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.
- Get a discount when you order a print copy of the ebook.

---

## ABOUT GLENN

---



Glenn Fleishman has written for hire since 1994, starting with *Aldus Magazine*. He contributes regularly to *Macworld*, *Ars Technica*, the *Economist*, *BoingBoing*, and the *Seattle Times*. He's also a senior editor at *TidBITS*.

Glenn spends much of his time writing about wireless networking. He has written several Take Control books, including *Take Control of Your 802.11n AirPort Network*. He edits Wi-Fi Networking News (<http://wifinetnews.com/>). He lives in Seattle with his wife and two sons. His older son's first word was not "Wi-Fi"; it was "book."

---

## ABOUT ADAM

---



Adam C. Engst is the publisher of *TidBITS*, one of the oldest and most respected Internet-based newsletters. He has written numerous technical books, including the best-selling *Internet Starter Kit* series, and many magazine articles (thanks to Contributing Editor positions at *MacUser*, *MacWEEK*, and now *Macworld*).

Adam's innovations include the creation of the first advertising program to support an Internet publication (in 1992), the first flat-rate accounts for graphical Internet access (in 1993, with Northwest Nexus for *Internet Starter Kit for Macintosh*), and the Take Control ebook series. In addition, he has collaborated on several Internet educational videos and has appeared on a variety of internationally broadcast television and radio programs.

Adam's indefatigable support of the Macintosh community and commitment to helping individuals has resulted in numerous awards and recognition at the highest levels. In the annual MDJ Power 25 survey of industry insiders from 2000 through 2007, he ranked in the top five most influential people in the Macintosh industry, and he was named one of *MacDirectory's* top ten visionaries. And how many industry figures can boast of being turned into an action figure?

---

## AUTHORS' ACKNOWLEDGMENTS

---

Thanks to Tonya for all she does, both in editing this title and in keeping Take Control running.

A tip of the mouse to Chris Pepper, Larry Rosenstein, and Joe Kissell for their excellent comments during our collaborative editing phase.

---

## SHAMELESS PLUGS

---

If you liked this title, you'll undoubtedly like our other works:

- ***TidBITS***: For award-winning Apple commentary and editorial from both Adam and Glenn, be sure to read *TidBITS* (<http://www.tidbits.com/>).

- **Wi-Fi Networking News:** Glenn writes about Wi-Fi and other wireless networking daily or nearly so at this blog that dates back to early 2001. He has tracked developments like the rollout of hot-spots worldwide, new 802.11n hardware, the municipal wireless movement, and security problems and their solutions. Visit <http://wifinetnews.com/>.

---

## ABOUT THE PUBLISHER

---

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

Adam and Tonya are known in the Mac 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

Editor in Chief: Tonya Engst

Publisher: Adam Engst

# Copyright and Fine Print

*Take Control of Your Wi-Fi Security*

ISBN: 978-0-975950-39-5

Copyright © 2010, Glenn Fleishman and TidBITS Publishing Inc.

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.

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 trademarks or 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 Back to My Mac* (Glenn Fleishman). Make the most of all your Internet-connected Macs via Back to My Mac, with this helpful guide. \$10

*Take Control of Screen Sharing in Snow Leopard* (Glenn Fleishman). Figure out which type of screen sharing to use when and how to get the most out of screen sharing. \$10

*Take Control of the Mac Command Line with Terminal* (Joe Kissell). Release your inner geek and learn to harness the power of the Unix underpinnings to Mac OS X! \$10

*Take Control of Users & Accounts in Snow Leopard* (Kirk McElhearn): Find straightforward explanations of how to create, manage, and work with—and among—user accounts. \$10

*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. \$15

*Take Control of Apple Mail in Snow Leopard* (Joe Kissell): Joe gets you going and helps you get the most out of Mail. He also gives detailed directions for how to sign and encrypt messages in Mail. \$15

*Take Control of Sharing Files in Snow Leopard* (Glenn Fleishman): Find friendly advice and steps for sharing files from your Mac, and get further ideas for using an Internet-hosted service. \$10

*Take Control of Passwords in Mac OS X* (Joe Kissell): Create and manage strong passwords that keep your data safe without taxing your memory! \$10

*Take Control of iPhone and iPod touch Networking & Security* (Glenn Fleishman): Learn fascinating and practical geek-level details about iOS networking and security. Covers Wi-Fi and 3G networks. \$15