

# Mac Security Superguide



**Macworld**

\$9.99

# Table of Contents

## Safeguard Your Data

### 6 Take Advantage of User Accounts

If you share your Mac with other people, user accounts are a must. Take advantage of this feature for maximum security.

### 15 Protect Your Passwords

Pick the strongest passwords, unlock the mystery that is the key-chain, and troubleshoot common password problems.

### 21 Encrypt Sensitive Files

Do you have sensitive information on your Mac that you wouldn't want ending up in the wrong hands? Lock it up by encrypting it.

### 26 Thwart Potential Thieves

Your beloved Mac is a coveted target for thieves. Keep it safe with these tools, including security cables, insurance, and alarms.

## Protect Your Privacy Online

### 30 Surf Safely

If you spend any time on the Internet,

you leave a trail. Ensure that nobody can see your browsing history or get their hands on your passwords or credit card information.

### 34 Secure Your Communications

E-mail, file transfers, and instant messages are all vulnerable to snoops while traveling to their destinations. Encode and protect them with these security measures.

### 43 Fight Spam and Phishing

The biggest threats to Mac users are spam and phishing scams. Recognize and avoid threats with the right combination of settings, software, and common sense.

## Inoculate Your Mac Against Viruses

### 54 Know the Dangers

Viruses, Trojan horses, and other malware are rare on Macs but not unheard of. Learn about the possible threats to your system.

### 57 Prevent Infection

Antivirus software and reliable download sources are the best way to keep your Mac malware-free. This section has our top program picks for every kind of Mac user.



## TABLE OF CONTENTS

### 61 Locate and Treat It

Worried that your system is already compromised? Track down and remove suspicious programs from your computer.

## Shield Your Network

### 64 Set Up a Firewall

Thwart would-be intruders by making your Mac invisible with a firewall. Familiarize yourself with your computer's ports and get instructions on setting up OS X and third-party firewalls.

### 73 Let Outsiders Access Your Mac

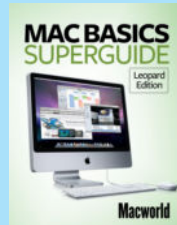
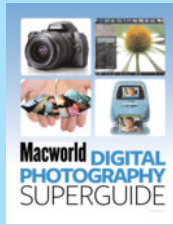
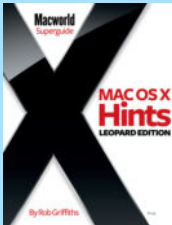
Sharing access to your computer is a snap in Leopard, but it also has its risks. Make sure your connections are secure by hand-picking who has access to what.

### 79 Secure Your Wireless Connections

It's true that your wireless connections can be intercepted. Guard your data by being smart about your Wi-Fi, coffee shop hotspot, and VPN connections.

Cover image by Joe Zeff

## ALSO FROM THE EDITORS OF *MACWORLD*...



Get more insider tips and troubleshooting advice from the Mac experts. Our Superguide series offers useful insights and step-by-step instructions for the latest Mac hardware and software.

Each of the books in the series is available in one of three different formats: as a downloadable PDF

for immediate access; on CD for easy, offline storage; or as a full-color bound book printed on high-quality paper.

Go to [macworld.com/superguide-offer](http://macworld.com/superguide-offer) to order any of the Superguide books or to download a free preview.

Enter the code  
**MWREADER6**  
to get a discount  
on your next order.

# Contributors

**Jason Cook** previously managed product development for HotBot.com and Webmonkey.com. He's currently working as a product marketing manager at Google.

**Glenn Fleishman** writes daily about Wi-Fi at the Wi-Fi Networking News site ([www.wifinetnews.com](http://www.wifinetnews.com)). He is the author of *Take Control of Sharing Files in Leopard* (TidBits Publishing, 2007; [www.takecontrolbooks.com](http://www.takecontrolbooks.com)).

Senior Editor **Dan Frakes** reviews iPod, iPhone, and audio gear for *Macworld* and runs the Mac Gems and Mobile Mac Weblogs on Macworld.com.

Senior Editor **Rob Griffiths** runs MacOSXHints.com, writes *Macworld's* monthly *Mac OS X Hints* column, and offers weekly Mac hints on *Macworld's* Mac OS X Hints blog.

**Mathew Honan** has written for the *National Journal's Technology Daily*, Salon.com, and *Wired*. He is also the author of *Barack Obama Is Your New Bicycle* (Gotham Books, 2008; [barackobamaisyournewbicycle.com](http://barackobamaisyournewbicycle.com)).

**Joe Kissell** is the senior editor of TidBits ([www.tidbits.com](http://www.tidbits.com)) and the author of *Take Control of Easy Backups in Leopard* (TidBits Publishing, 2007; [www.takecontrolbooks.com](http://www.takecontrolbooks.com)).

Visit **Kirk McElhearn's** blog Kirkville ([www.mcelhearn.com](http://www.mcelhearn.com))

for more information about Macs, iPods, books, and music.

**Scott McNulty** is a senior contributor at Macuser.com and cohost of the cooking podcast Fork You. He also runs his personal Web site, blankbaby ([blankbaby.typepad.com](http://blankbaby.typepad.com)).

**Derek K. Miller** is a writer, an editor, a musician, and a podcaster who blogs at Penmachine.com.

**Rich Mogull** is a contributor to TidBits ([www.tidbits.com](http://www.tidbits.com)) and runs Securosis LLC ([securosis.com](http://securosis.com)), a security consulting practice.

**Chris Pepper** is a systems administrator and a TidBits ([www.tidbits.com](http://www.tidbits.com)) contributor.

## Macworld

### Macworld's Mac Security Superguide

Editor	Kelly Turner
President and CEO	Mike Kisseberth
VP, Editorial Director	Jason Snell
Managing Editor	Jennifer Werner
Associate Editor	Heather Kelly
Copy Editor	Peggy Nauts
Art Director	Rob Schultz
Designers	Lori Flynn, Carli Morgenstein
Production Director	Steve Spingola
Prepress Manager	Tamara Gargus

Macworld is a publication of Mac Publishing, L.L.C., and International Data Group, Inc. Macworld is an independent journal not affiliated with Apple, Inc. Copyright © 2008, Mac Publishing, L.L.C. All rights reserved. Macworld, the Macworld logo, the Macworld Lab, the mouse-ratings logo, MacCentral.com, PriceGrabber, and Mac Developer Journal are registered trademarks of International Data Group, Inc., and used under license by Mac Publishing, L.L.C. Apple, the Apple logo, Mac, and Macintosh are registered trademarks of Apple, Inc. Printed in the United States of America.

Have comments or suggestions? E-mail us at [ebook@macworld.com](mailto:ebook@macworld.com).



# Safeguard Your Data

Keep Sensitive Files Away from Prying Eyes

**Y**our Mac is a beautiful machine. But its sleek design and chic status also make it a target. Thieves are certainly interested in the computer itself, either for their own use or to sell. But even if your computer is right where it's supposed to be, other people can still get to your personal information. Anyone with a bit of curiosity and a few minutes could discover all kinds of useful things about you by examining your files—including your address, credit card numbers, and all your passwords, which can be as good as cash. Someone who's truly determined could use information they pilfer to steal your identity and wreak havoc on your finances.

While you may not be able to completely deter an experienced criminal who is determined to sneak off with your machine, you can at least make it as hard as possible to get any valuable data off of it by limiting access, choosing good passwords, and encrypting truly sensitive data. In most cases, OS X already includes all of the tools you need.



## TABLE OF CONTENTS

- 6** Take Advantage of User Accounts
- 15** Protect Your Passwords
- 21** Encrypt Sensitive Files
- 26** Thwart Potential Thieves

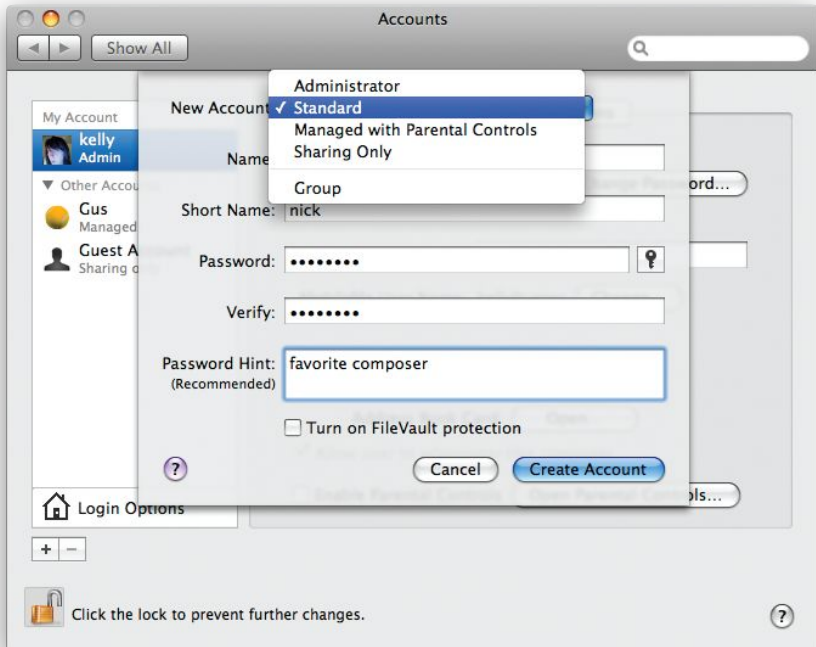
# Take Advantage of User Accounts

One of the easiest things you can do to keep out casual snoops and to protect the files on your computer is to require users to log in. OS X lets you set up separate user accounts for everyone who uses your Mac, giving you precise control over how much access each account has and who can access your Mac at all.

But to be effective, you have to make sure you've set up your user accounts in the most secure way. In many cases this means turning off default settings.

## Don't Share User Accounts

You wouldn't let your little brother use your diary to record his own thoughts, so why would you give



**Security Check** OS X gives you several choices when setting up new accounts so you can limit how much access each person has to your system.

## Privileged User

	Administrator	Standard	Managed	Guest
Can change all system preferences	yes	no	no	no
Can change system preferences that affect his or her account	yes	yes	no	yes
Can manage user accounts	yes	no	no	no
Can install software for all users	yes	no	no	no
Can install software for personal use	yes	yes	no	no
Can run all applications installed on the Mac	yes	yes	only those selected by the administrator	yes

him access to all of your files and settings on your Mac? If more than one person uses your computer, make sure each user has a separate account. Doing so keeps mail, documents, keychains, browser history, and other personal data safe from casual snooping.

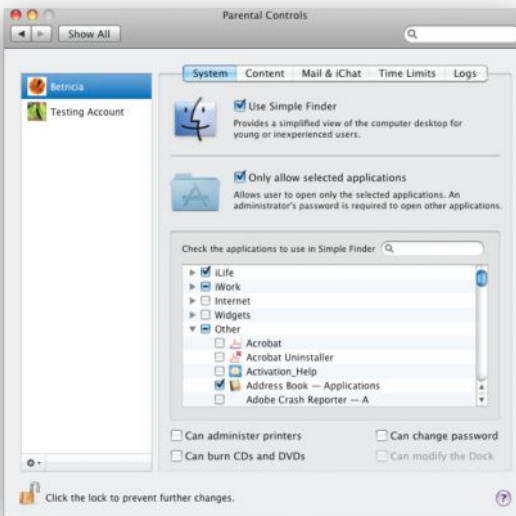
Each user account has its own Home folder (also called the user folder), which holds the user's personal files—documents, music, and photos, for example—and the preference files that record customizations to the Finder (such as the desktop background and screen saver) or to individual applications. But that's not all. Your user account also stores your e-mail address and password, the home page for your Web browser, your

iChat account name, and much more. And since other users can't view or open your files, your user account also protects your privacy.

Every Mac has at least one administrator account. This type of account gives you the freedom to install software in the root-level Applications folder, change preferences that affect the entire system, and create and delete other user accounts. However, it's not a good idea to give other users this much power over your system. That's why OS X 10.5 offers several additional types of accounts that place limits on these activities (see "Privileged User").

**STANDARD ACCOUNTS** A *standard* account lets the user work with the Mac freely, install

## SAFEGUARD YOUR DATA



**Limited Options** When you apply parental controls to a managed account, you can specify which programs the user can access, whom he or she can chat with, and more.

applications in his or her Home folder, and modify some benign System Preferences settings—the desktop pattern and alert sound, for example. (System preferences that can't be modified without an administrator's password contain a lock icon.) However, a standard user can't perform the system-level tasks that administrators can.

**MANAGED ACCOUNTS** You can restrict an account further by applying parental controls. These accounts are called *managed* accounts. You can choose exactly which applications managed users can run and which tasks they can perform in the Finder (see “Limited Options”). This is a

particularly good idea if you're concerned that young computer users may unknowingly open themselves (or your Mac) to dangers. For example, you can restrict what Web sites can be accessed, monitor e-mail associates, and more.

**THE GUEST ACCOUNT** Leopard also introduced a new user account called the *Guest* account. By enabling this account, you can let someone use your Mac temporarily without giving him or her access to your own account or going through the hassle

of setting up a fresh account. A Guest account doesn't require a password and doesn't have administrator access (you can further limit what the Guest account can do by applying parental controls). Once the guest user logs out, all data and settings in that account's Home folder are deleted—the account is wiped clean for the next guest user.

**SETTING UP A NEW ACCOUNT** To add an account on your Mac, open the Accounts pane in System Preferences. If the lock icon at the bottom of the pane is locked, click on it. When the Authenticate dialog box appears, enter your administrator password.

## The Key to Your Mac

You have a key to your house—why not to your Mac? That's the idea behind GT Security's \$130 SecuriKey Professional ([www.securikey.com](http://www.securikey.com)). It combines a software password with a USB key—or *token*—that hangs on your key ring.

When you start up your Mac after installing the SecuriKey software, you must enter your password *and* insert the key. Without the key, no one can access your files, even with the correct password. SecuriKey also offers you the option of creating an encrypted partition on your hard drive.

Using AES-128 encryption, SecuriKey places a partition on your hard drive that is effectively impossible to break. If you're frequently working on sensitive documents or you have important personal documents on your hard drive, you'll really appreciate this feature.

Then click on the plus-sign (+) button right above the lock to create a new account. In the sheet that drops down, enter a user name, a short name (which doesn't have to match the user name), and a password (you'll have to verify the password by entering it again). If the user is worried about forgetting the password, you can enter a password hint as well—OS X will display this hint if the user enters

It's simple to set up an encrypted partition, and during the setup process you can choose to have your Mac mount the partition upon login.

GT Security provides two duplicate key fobs for your use with a key code unique to your installation. The first is to carry around with you, while the backup should be stored in a safe place in case you lose the first one. Make sure you keep that second key safe, because it can take some time and expense to get a replacement key. More important, you need to register the product when you initially install it, because GT Security won't provide a new key unless you do. Without the key, you can't access your system, and any data on the encrypted drive can't be recovered.

an incorrect password three times in a row. Finally, from the New Account pull-down menu, select which type of account the new user should have. When you've finished, click on the Create Account button at the bottom of the sheet.

In the main account screen, make sure the Allow User To Administer This Computer option is deselected—this part is crucial. If you'd like to further limit the



**TIP**

## Erase Your Drive

There may come a time when you have to bid a fond farewell to an old computer. Whether you want to sell it, donate it, or simply recycle it, you should take steps to protect yourself from giving away sensitive data along with your old hardware.

First, if you use programs that are registered with your Mac, make sure you deauthorize them. This includes apps such as iTunes and the programs in Adobe Creative Suite. In iTunes, go to Store: Deauthorize Computer. For Adobe apps, go to Help: Transfer Activation to install the software on your new machine.

Using Disk Utility, you can remove both your personal data and installed software in one pass. Before you begin, make sure you've transferred vital data to another location. Once you've saved those files, start up from the system disc—insert it in the drive, and restart your Mac while holding down the C key. Select a language, click on the arrow button, and choose Utilities: Disk Utility in the screen that appears. (These instructions are based on the latest installation discs, but the general procedure should work for whatever version you have.)

When the Disk Utility window opens, select the hard drive in the pane on the left; then click on the Erase tab. Select Mac OS X Extended (Journaled) from the pull-down menu; then click on the Security Options button and make sure Zero Out Data is selected. This will overwrite your drive with zeros. (Newer versions of Disk Utility also include 7-Pass Erase and 35-Pass Erase options—overkill for those of us who don't keep state secrets on our machines.) When the process finishes, close Disk Utility and follow the installer prompts to reinstall OS X.



account, select the Enable Parental Controls option and then click on the Open Parental Controls button to define what programs and activities the user is allowed access to.

Once your accounts are set up, be sure to use them. Whenever you finish working on your computer, choose Log Out *user name* from

the Apple menu. The computer will then display the login screen, where the next user can enter a user name and password to log in.

### Use Admin Accounts for Administration Only

When you initially set up your Mac, OS X creates a single user account

## SAFEGUARD YOUR DATA



**Downgrade Your Status** When you use a non-administrator account, it's harder for someone to walk up and take over your entire Mac. When setting up a new account, be sure the option to administer the computer **A** is not selected.

for you. That account includes administrative rights, which give you the authority to install, change, or delete anything on the computer.

But using an administrator account as your normal, day-to-day login account can be risky. First, you make it easier to mistakenly change or delete something crucial to your computer's operation. Second, you open a potential security hole: if you step away from your computer for a moment without logging out, anyone who walks up to your Mac would have complete access to your data and settings. (Also, in the unlikely event that your Mac does become infected by a malicious program, it may be able to use your expanded privileges to do greater harm.)

The safest course is to set up a second user account without administrative privileges, and use that as your main day-to-day account.

To set up a new nonadministrator account, follow the instructions given earlier for setting up a new account and select Standard from the New Account pull-down menu. Then click on Create Account. In the next screen, make sure that the Allow User To Administer This Com-

puter option *is not* selected (see "Downgrade Your Status").

If you want to transfer any data (such as preferences files or e-mail messages) from your current account to the new one, drag the items from their current location in your Home folder to the corresponding location in the new account's Home folder. Now, choose Log Out *user name* from the Apple menu and log back in as the new, nonadministrative user.

From now on, use your standard account except when you have a specific reason not to. You'll have to enter your administrator user name and password from time to time—for example, when installing software—but you'll have a safety net. And you can always log in to

## SAFEGUARD YOUR DATA

the administrator account if you need more control.

### Disable Automatic Login

By default, OS X logs you in when you turn on your computer. This is convenient, but it also leaves your Mac and its files vulnerable to anyone who pushes the power button. Forcing your Mac to ask for a password on such occasions can increase your security.

Open the Security preference pane in System Preferences and click on the General tab. If necessary, click on the lock icon at the bottom of the window and authenticate with your administrator

password. Then turn on the Disable Automatic Login option (see “Not So Fast”). This will ensure that all user accounts have the Automatically Log In feature disabled.

Now when you turn on your Mac, you’ll see a list of all users. Select the one you’d like to log in as and enter the appropriate password.

### Lock Down Other Potential Access Points

With automatic login disabled, your Mac will be protected when you log out or turn it off, but what about when you just step away? When you go to lunch, anyone can come



**Not So Fast** Choose the Disable Automatic Login option to make sure only authorized people can access your Mac.

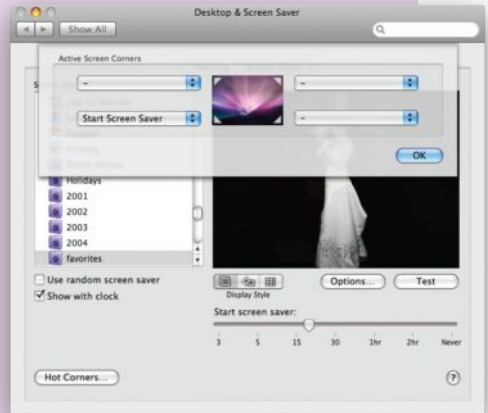
**TIP**

## Instant Lockdown

If you work with any kind of sensitive material—from trade secrets to love letters—you’ve probably wished for a way to block access to your Mac the minute you stand up. In fact, there are a couple of quick ways to do this while leaving all of your programs running.

**Hot Corners** A relatively quick method of locking your Mac is to activate the screen saver using a *hot corner* and then set your Mac to require a password to disable the screen saver (you’ll find this setting in the General tab of your Security preferences). To do this, open the Desktop & Screen Saver system preferences pane, select the Screen Saver tab, and click on the Hot Corners button. Decide which corner of your screen you’d like to use, then click on the corresponding pop-up menu and select Start Screen Saver. Now when it’s time to walk away, just fling your cursor into that corner of the screen, and you’ll trigger the screen saver.

**Switch to the Login Screen** Another method of locking your system is to show the login window, without actually logging out. You can do this by enabling fast user switching in the Accounts system preferences pane. Click on the Login Options button (you’ll probably have to enter your administrator password to do this), and then select the Enable Fast User Switching option. Once you have fast user switching enabled, you’ll see either an icon or a name in your menu bar, depending on what option you chose on the Login Options screen. Click on your name or icon in the menu bar and select Login Window from the drop-down menu. The login window will appear. When you return to your Mac, log in as you usually do. All your applications will be just as you left them—even your iTunes music will start up again where it stopped playing.



**No Waiting** When you specify a hot corner in the Screen Saver preference pane, you can instantly hide your files by simply dragging your mouse to that corner of the screen.

## SAFEGUARD YOUR DATA

by, press a key to wake your computer, and access your files.

**AUTO-LOCK YOUR MAC** Prevent this easy access by requiring a password when anyone deactivates the screen saver or wakes your computer from sleep.

To do this, go to the General tab of the Security preference pane and make sure Require Password To Wake This Computer From Sleep Or Screen Saver is enabled. (For ways to quickly lock your screen without waiting for your screen saver to kick in or putting your Mac to sleep, see “Instant Lockdown.”)

**MANUALLY LOCK YOUR SCREEN SAVER** But what if you don’t want to *always* lock your screen when the screen saver activates or your computer wakes from sleep? (After all, it can be a pain to have to enter your password over and over again throughout the day.) Keychain Access holds the key. You can use this application (in your Applications/Utilities folder) to quickly activate your screen saver from the menu bar *and* require a password to turn it off—even if the Security pane option isn’t enabled.

Open Keychain Access and then go to Keychain Access: Preferences. Click on the General

tab and select the Show Status In Menu Bar option. A small lock icon will appear in your menu bar. Close the Preferences window and quit Keychain Access. Now click the lock icon in your menu bar and choose Lock Screen to start your screen saver.

**SET MORE OPTIONS** But you’re not done yet. In that same window you’ll find several additional safety measures that can help keep your data secure.

The Require Password To Unlock Each Secure System Preference option prevents changes to systemwide settings without an administrator password. The Log Out After X Minutes Of Inactivity logs you out of your account—locking up any encrypted disk images in the process (see “Encrypt Sensitive Files” later in this chapter for more on encryption)—if you step away for an extended period of time.

You should also consider turning on the Use Secure Virtual Memory option, which encrypts portions of your RAM as they’re swapped out to your hard disk. That way, if someone were to examine the virtual memory files written to disk as you use your Mac, they wouldn’t find any unencrypted traces of your data.

# Protect Your Privacy Online

Battle Snoops, Spammers, and Phishers to Keep Your Personal Information Private

Every e-mail you send, online purchase you make, instant message that you have, and spam e-mail you receive puts you and your personal information at risk. It's surprisingly easy for Webmasters, your boss, or hackers to see what you've been up to online.

If you only use your browser to look at LOLCats, and all online communication is limited to Sunday conversations with your grandmother on iChat, you probably don't need to be super strict about guarding your information from prying eyes. However, chances are you make purchases and manage your finances online, e-mail private information, and chat about business matters you'd rather not have seen by others. For users who are concerned about privacy, here are some ways to protect online activities and communications from snoops, identity thieves, and other online invaders.



## TABLE OF CONTENTS

- 30 Surf Safely
- 34 Secure Your Communications
- 43 Fight Spam and Phishing

# Inoculate Your Mac Against Viruses

Learn How to Keep Your System Safe from Malware, and How to Back Up and Recover Just in Case

**A**pple computers are not somehow magically immune to malware, such as viruses, spyware, worms, Trojan horses, and adware. However, thanks to a lack of incentive for hackers and smart design by Apple, Macs have been remarkably free of these pests for most of their history.

Unfortunately, as Apple becomes more popular and more Mac users run Windows on their machines, the risk of infection increases. Actual attacks might be few and far between, but they are a very real threat to your system that will only increase over time.

The key to not becoming a paranoid basket case is to know your enemies and protect yourself accordingly. In this chapter we'll learn about the history and current state of malware threats to your Mac. Then we'll compare anti-virus software for OS X, Windows on a Mac, and e-mail. Finally, we'll show you how to find and eliminate any suspicious programs from your system.



## TABLE OF CONTENTS

- 54** Know the Dangers
- 57** Prevent Infection
- 61** Locate and Treat It

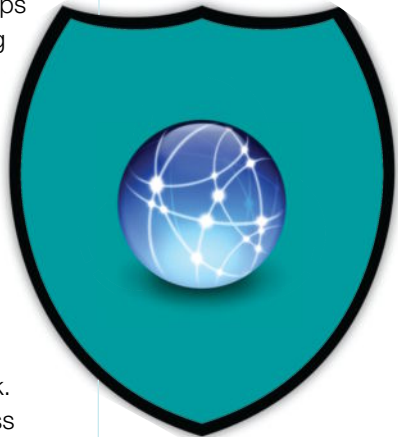
# Shield Your Network

Connect with Others Safely and Secure Your Wi-Fi Traffic

**B**ad guys don't need physical access to your Mac to do you wrong. They can snoop on your network traffic (unencrypted Wi-Fi connections at coffee shops and airports are especially easy), looking for strings of characters that might be passwords, account numbers, and the like. There's no way to know the exact likelihood of your network traffic being intercepted while you're out and about. But anecdotal evidence suggests it is quite common.

Luckily, you can stack the deck in your favor. Thieves, hackers, and spies have only so much time to do their work. The harder you make it for them, the less likely they'll keep at it.

In this chapter we'll show you how to make your Mac invisible to outside intruders by setting up a good firewall, how to give trusted others access to specific parts of your Mac without giving them free rein, and how to protect yourself when working on a wireless network at home, at the coffee shop, and from your iPhone.



## TABLE OF CONTENTS

- 64** Set Up a Firewall
- 73** Let Outsiders Access Your Mac
- 79** Secure Your Wireless Connections



Nobody spends more time with Apple's computers and software than the writers and editors at *Macworld*, the world's foremost Mac authority.

Now *Macworld's* team of experts has used its knowledge to create this essential guide to keeping your computer, your network, and your personal information safe and secure. It's common knowledge that Mac users have a head start when it comes to malware, but that doesn't mean they can afford to be lax about security. *Macworld's Mac*

*Security Superguide* has must-read tips for even the most vigilant of Mac owners.

In this book we show you how to keep your Mac and everything on it safe from thieves and prying eyes. We share easy tweaks you can make to your security habits that will greatly decrease the chances of sensitive files falling into the wrong hands. And since bad guys (or girls) don't need to be nearby to hack into your Mac, we cover everything you need to know about setting up a firewall. One of the biggest threats to Mac users is phishing. We have step-by-step instructions on how to keep your online communications and personal information private using encryption and common sense. Finally, we'll give you the tools you need to protect your system from malware infections.

Let *Macworld's* team of experts teach you how to keep your system and information secure.

