

# Mac Security Essentials

See what software you *really* need to keep your data—and your Mac—safe

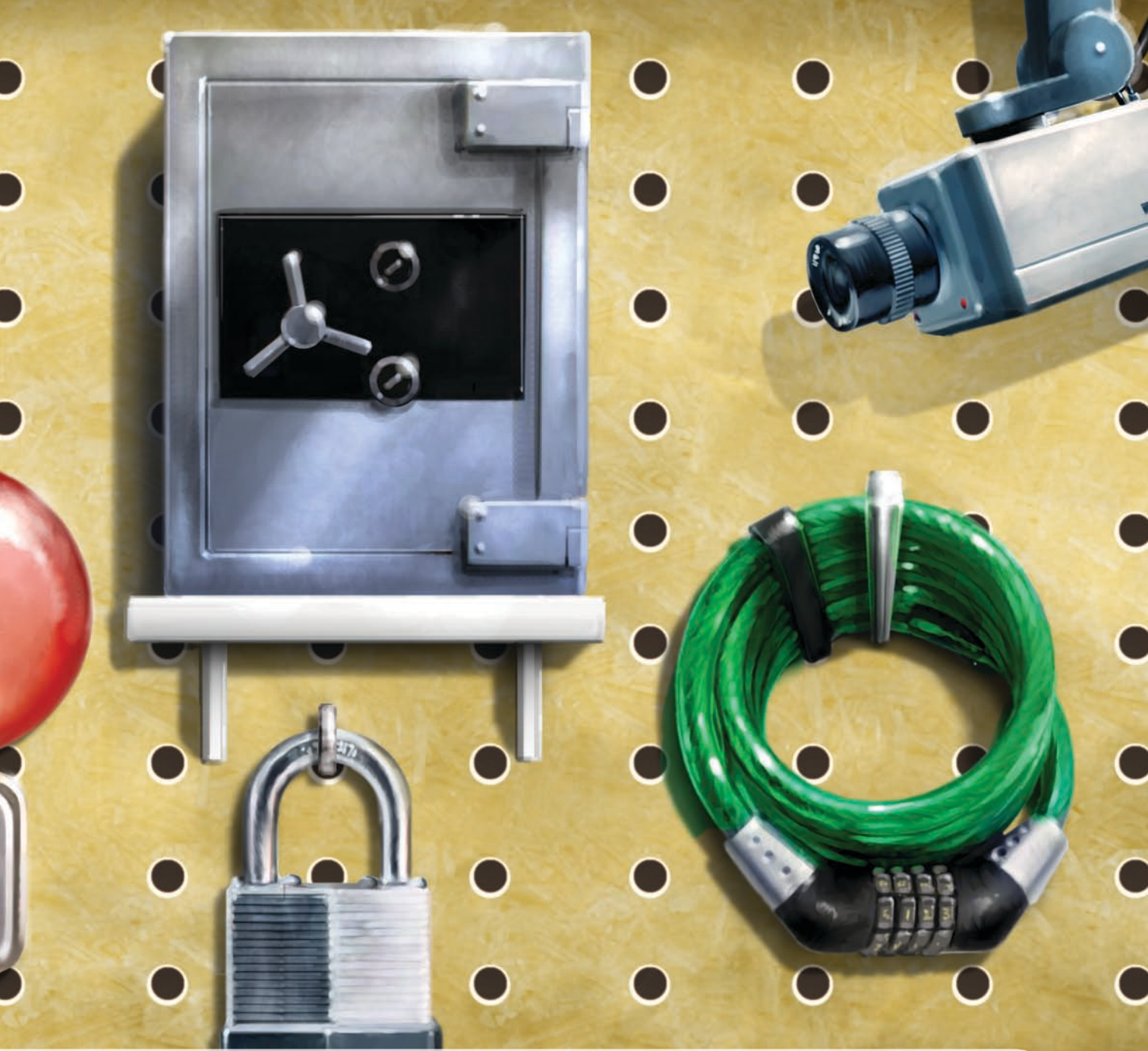
## Are Macs really more secure than PCs? The answer isn't as simple as you might think.

Technically, Macs are not inherently more secure than Windows PCs—by some measures, they are actually less so. Over the past five years, Microsoft has made huge improvements in the security of its Windows operating system, and Apple now lags behind Microsoft in implementing library randomization, data-execution protection, and other

advanced security features. To its credit, Apple continually releases OS X security updates to patch vulnerabilities as they're discovered.

Still, OS X faces fewer security threats than Windows. In part, that's because malicious hackers no longer write viruses and take down Web sites just for the fun of it. Now they do it for money. And since the vast majority of computers run Windows, focusing efforts on that platform is just a more profitable use of a hacker's time. Also, there





aren't many Mac-compatible hacker's tools, and fewer attackers know OS X programming. All those factors add up to fewer Mac attacks.

Could that change? Absolutely. Most security experts agree that as the Mac's popularity and market share increase, so will the risks.

### The Tools You Need

So what should you do to keep your Mac safe? We've told you before about basic security precautions you can take (see "Lock It Up" at

[macworld.com/3356](http://macworld.com/3356) and "Protect Your Mac" at [macworld.com/2536](http://macworld.com/2536)). Many of those suggestions require using OS X's built-in security tools—particularly the firewall and programs like FileVault and Disk Utility that can encrypt your data.

But are those built-in tools enough? Or do you need one of the many third-party security programs to truly keep your Mac safe?

To answer those questions, we looked at three categories of security software: firewalls, antivirus appli-

cations, and privacy programs. We looked at the threats they protect against, the tools built into OS X, and the third-party alternatives.

In the pages that follow, you'll find our conclusions. At the same time, we urge you to go back to our earlier security stories and be sure that you're following their advice, too. By educating yourself about the real risks and taking a few basic precautions, you can stay safe, even if the Mac world becomes a little riskier.






# FIREWALLS

**OS X has two firewall apps built in. Do you need another?** By Rich Mogull and Chris Pepper

**S**imply put, firewalls monitor and regulate the data moving on and off of your computer or network. They can keep villains out while allowing legitimate network traffic in. OS X comes with not one but two firewalls of its own. However, those two aren't always enough.

## The Threat

 Sneaking up on your computer through a network connection is a much more effective way for an intruder to gain access to it than, say, waiting for you to click on a virus-infected e-mail attachment. For example, a long-fixed bug once let attackers send Macs a so-called “ping of death”—specially designed network traffic that could crash a system.

With millions of computers in the world, it may seem as though the odds of your Mac being targeted for attack are awfully long. But in fact there are computers out there that do nothing all day but probe Net-connected machines for vulnerabilities; it's certainly possible that one will find yours. And don't forget that any time you're on a network—a coffee shop's Wi-Fi system, for example—you're exposed to anyone else on that network.

The risks—the loss of private data and the hijacking of your Mac's computing power—are great enough, and the cost of prevention low enough, that implementing a good firewall on your Mac and your local network is a no-brainer.

## OS X's Firewalls

All versions of OS X through 10.4 (Tiger) have included a Unix-based firewall called *ipfw*. In security parlance, *ipfw* is a



*packet-filtering* firewall: it checks each packet coming or going through the Mac's network interfaces against a set of rules, and allows it to pass or blocks it.

Packet-filtering firewalls like *ipfw* classify network traffic two ways: by type, using port numbers; and by origin and destination, using IP addresses. For instance, a packet-filtering firewall could accept file-sharing connections from IP addresses of your work network but not from other addresses on the Internet.

To *ipfw*, Leopard adds a new *socket-filter* firewall (also known as an application firewall). Rather than using network ports and IP addresses to decide whether to allow a packet, it bases its decision on the application making the network request. When a program asks to accept network traffic, a socket filter checks a list of programs that have been autho-

rized to do so. If the program is on the list, the firewall allows the connection. If the program isn't on the list—as in the case of new or upgraded software—OS X asks you whether to allow the program to accept incoming traffic.

You access Leopard's socket firewall in System Preferences: Security: Firewall by selecting Set Access For Specific Programs And Services. When you select that option, you'll see a list of allowed and blocked programs. If you'd like to block *all* nonessential traffic, you can select Allow Only Essential Services, but beware: doing so will break some applications. You'll still be able to browse the Web and use e-mail, but other inbound connections will be blocked.


Socket filters are less flexible than a packet filter like *ipfw*. Applications that are allowed to accept network connections will accept them from anywhere on the Internet; they can't be told to distinguish trusted from untrusted Net addresses. The Leopard firewall also blocks only *inbound* connections; it won't prevent programs from making outbound connections. This has become a big problem in the Windows world: spyware programs lodge themselves on hard drives and then attempt to “phone home” with sensitive private information.

## TIP

### Stay Current with Software Update


Malicious hackers exploit software flaws to gain access to or control of your Mac—these flaws are called *vulnerabilities* in the security business. The speed with which Apple releases fixes for those vulnerabilities, and how quickly you install those fixes, is key. So keeping your software up-to-date is the most valuable thing you can do to protect your Mac. To make sure you stay current, go to Preferences: Software Update and make sure it's enabled. (By default, it is.) I recommend setting it to check for updates daily,





While OS X 10.5 still includes ipfw, it's effectively disabled by default. But you can enable and configure it from the command line or using a third-party application such as Hanynet's free WaterRoof 2.0 or NoobProof 1.1 (both ; [macworld.com/3734](http://macworld.com/3734)). And ipfw is compatible with Leopard's socket filter, so you can combine the two to block untrusted applications from accepting connections and simultaneously restrict inbound and outbound traffic by ports and IP addresses.

### Third-Party Firewalls

So why would you want to buy and install a third-party firewall when OS X's seem to cover the bases pretty well? The primary reasons are more flexibility and better protection.

For example, a tool like Intego's \$50 NetBarrier X5 (; [macworld.com/ttkk](http://macworld.com/ttkk)) will let you set multiple rules based on where connections are coming from. NetBarrier also includes privacy features that protect you when you're browsing the Web. You can get similar firewall control from free tools such as WaterRoof, but they don't offer those extra privacy features.

Another limitation of Leopard's built-in socket filter is that it can't change rules when you change locations. For example, you might want to leave your laptop's iTunes sharing on at home but shut it off when you use your laptop on the road. Open Door Networks' \$80 DoorStop X Security Suite (; [macworld.com/2657](http://macworld.com/2657)) lets you define locations and quickly set the firewall to preset rules for where you are. NetBarrier also allows you to create different rules for local network addresses and for addresses on the Internet—a remarkably simple and useful distinction.

If you want fine-grained application control—defining not only which applications can send and receive information to and from the Internet, but also which Net addresses they can contact—you can use Objective Development's \$30 Little Snitch (; [macworld.com/3693](http://macworld.com/3693)); it's particularly effective against spyware.



**Set Access** The Security preference pane lets you configure OS X's built-in socket-filter firewall, which filters network traffic by application.

### Our Advice

For most users, the firewalls built into OS X are enough. Enable OS X's basic socket-filter firewall via the Security preference pane (we recommend that you choose Set Access For Specific Services And Applications); if you want the extra protection of OS X's ipfw

firewall, use the excellent and free NoobProof to configure it.

**Rich Mogull** is a contributor to TidBits ([db.tidbits.com](http://db.tidbits.com)) and runs Securosis LLC ([securosis.com](http://securosis.com)), a security consulting practice. **Chris Pepper**, a systems administrator, writes about security issues.

## Third-Party Firewalls

PRODUCT	PRICE	RATING	FIND CODE <sup>A</sup>
<b>DoorStop X Security Suite 2.2</b> Open Door Networks <a href="http://www.opendoor.com">www.opendoor.com</a>	\$79		<a href="http://macworld.com/2657">macworld.com/2657</a>
<b>Flying Buttress 1.4</b> Brian Hill <a href="http://www.ttkk.com">www.ttkk.com</a>	\$25		<a href="http://macworld.com/1312">macworld.com/1312</a>
<b>Intego SentryX 2.2</b> Intego Software <a href="http://www.intego.com">www.intego.com</a>	\$60		<a href="http://macworld.com/ttkk">macworld.com/ttkk</a>
<b>Little Snitch 2.0.3</b> Objective Development <a href="http://www.obdev.at">www.obdev.at</a>	\$25 (multiuser and upgrade licenses available)		<a href="http://macworld.com/3693">macworld.com/3693</a>
<b>NetBarrier X5</b> Intego <a href="http://www.intego.com">www.intego.com</a>	TK		<a href="http://macworld.com/ttkk">macworld.com/ttkk</a>
<b>NoobProof 1.1</b> Hanynet <a href="http://www.hanynet.com">www.hanynet.com</a>	free (payment requested)		<a href="http://macworld.com/3734">macworld.com/3734</a>
<b>Norton Personal Firewall 3.0.3</b> Symantec <a href="http://www.symantec.com">www.symantec.com</a>	\$50		<a href="http://macworld.com/1314">macworld.com/1314</a>

<sup>A</sup> Typing in find codes after [macworld.com/](http://macworld.com/) directs you to a product's review or overview. For example, [macworld.com/3693](http://macworld.com/3693) takes you to our review of Little Snitch 2.0.3. <sup>B</sup> Version 2.0 reviewed.





# VIRUS PROTECTION

**If there are no Mac viruses, who needs an antivirus program?** By Scott McNulty

Although Apple computers are not somehow magically immune to viruses and other malware, they've been remarkably free of such pests for most of their history. But does that mean you can ignore antivirus software?

## The Thr

In 1982, the Elk Cloner virus spread among Apple IIs by copying itself to floppy disks' boot sectors. The 50th time an infected machine was booted, a poem would appear on its screen. Elk Cloner didn't do any actual damage, but it certainly perplexed many 1982 computer users, who had never experienced a computer virus before.

Twenty-four years after Elk Cloner, Leap-A emerged. Disguised as an image file, Leap-A modified files on an infected Mac and, when iChat was opened, would send infected files to the victim's iChat buddies.

Many people thought at the time that Leap-A signaled the end of OS X's bug-free idyll. But Leap-A managed to infect a grand total of 49 Macs ([macworld.com/tktk](http://macworld.com/tktk)), and in the two years since, the Mac virus floodgates have yet to open: A few proof-of-concept viruses have cropped up, but almost none have been observed in the wild. Question is, why?

Security expert Bruce Schneier credits the Mac's small market share: "If you're looking for the masses of naive users, Windows is where to go," he says. Adam O'Donnell, director of emerging technologies at Cloudmark, agrees. He's applied applied game theory to the question and concluded that producing



Mac malware won't be economically viable until the Mac's market share hits 16 percent (it's now 8.5 percent). O'Donnell says, "There is no economic benefit to investing the time in compromising a Mac when you can compromise 10 to 20 times more systems for the same level of effort by going after PCs."

But that doesn't mean you should keep your guard down entirely. Running Windows on an Intel-based Mac—in either Boot Camp or with virtualization software such as Parallels Desktop or VMware Fusion—exposes you to the same security risks as if you were running it on a Dell. And while your Mac might not suffer any ill effects from virus-laden e-mail attachments, you can still pass those dangerous files to your Windows-using friends.

Finally, some malicious hackers have turned their talents from writing viruses to setting up phishing sites on the Web, where they hope to dupe you into handing over your credit card information, social security numbers, and so on.

## Antivirus Programs

By buying a Mac, you've already taken the first and best step toward keeping malware off your computer. (It's striking how many of the security experts interviewed for this article are Mac users.)

Both Norton and Intego sell Mac antivirus programs: Norton AntiVirus 11 (\$50; [macworld.com/tktk](http://macworld.com/tktk)) and VirusBarrier X5 (\$70; [macworld.com/3728](http://macworld.com/3728)), respectively. But if you don't run Windows and you don't mind passing along virus-laden e-mail attachments to your Windows friends, you don't need either one.

If you do run Windows on your Mac, you should install a Windows antivirus program on your virtual PC. Our confederates at *PC World* recommend Symantec's \$70 Norton Internet Security 2008 ([macworld.com/3797](http://macworld.com/3797)), the \$80 Kaspersky Internet Security 7.0 ([macworld.com/3798](http://macworld.com/3798)), McAfee Internet Security Suite (\$70 for a three-seat

## TIP

### Pick E-mail Services with Antispam and Antivirus Features

E-mail is a favorite tool of digital miscreants; it's the perfect distribution mechanism for viruses and other malicious software. If you don't see the sense in installing antivirus software on your Mac (and for many users, that's probably the right decision), consider using an e-mail service, such as Google's free Gmail ([macworld.com/3524](http://macworld.com/3524)), MobileMe ([macworld.com/3774](http://macworld.com/3774)), or Yahoo Mail ([macworld.com/3523](http://macworld.com/3523)), that scans e-mail and blocks viruses and spam before they ever hit you.—RICH MOGULL



license; [macworld.com/3799](http://macworld.com/3799)), and BitDefender Internet Security 2008 ([macworld.com/3800](http://macworld.com/3800)), which costs \$50 for three PCs. Each of these general-purpose security suites can protect your virtual Windows machine against all sorts of threats.

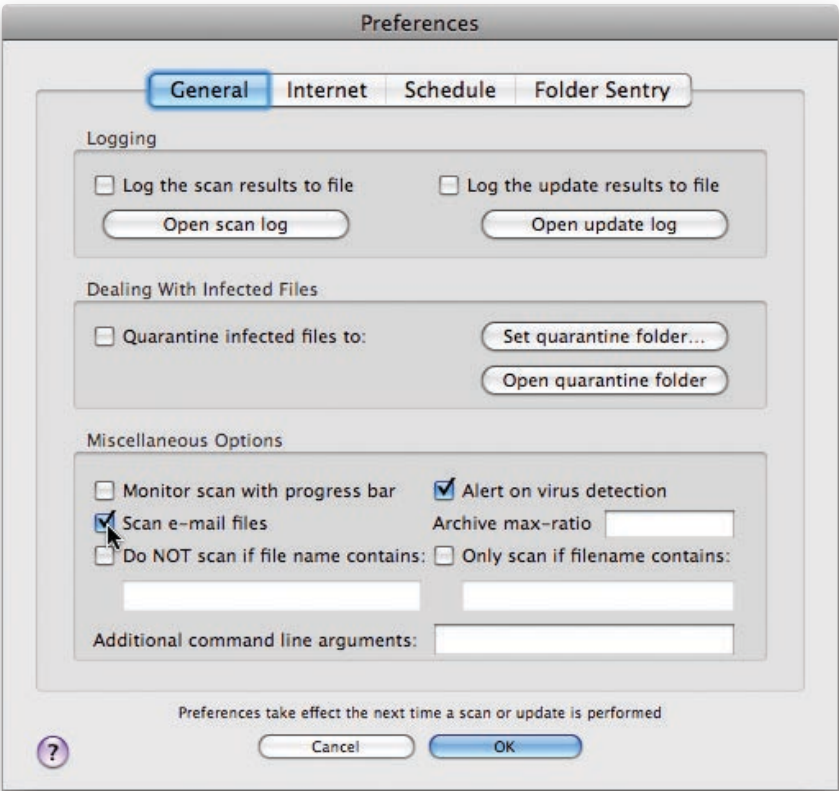
Both Norton ([www.symantec.com](http://www.symantec.com)) and Intego ([www.intego.com](http://www.intego.com)) offer dual-protection products for users who run both Windows and OS X on their Macs. These bundles give you Windows and Mac antivirus apps. Norton's package costs \$70 and includes Norton AntiVirus 11 for Mac and Norton AntiVirus 2008 for Windows while Intego's package costs \$80 and includes VirusBarrier X5 for Mac and BitDefender Antivirus 2008 for Windows. Each of these packages costs far less than its two programs bought separately; you have to install the Mac program and the Windows program on their respective operating systems.

If you're worried about passing along infected e-mails to friends, these bundles or one of the stand-alone Mac apps can also scan your inbox for malware attachments. The free, open-source ClamXav ([www.clamxav.com](http://www.clamxav.com)) will do so, too, but it's slow.

As for keeping yourself safe from Web-based phishing schemes, your own common sense is your best line of defense: Don't give out personal information on a Web site unless you're 100 percent sure it's legitimate.

Some Web browsers—notably Firefox and Opera—notify you when you visit a potentially dangerous site. Safari doesn't, which is why *Consumer Reports* and some e-commerce companies (including PayPal) recommend using something else. Studies have shown that most users ignore these warnings; they shouldn't.

Safari users can stay safer by using Agile Web Solutions' \$30 password manager iPassword (★★★★; [macworld.com/3801](http://macworld.com/3801)). It automatically fills in Web forms, but you can define how much information it'll give out when. It also compares URLs with the database at PhishTank.com (a community-based phish-tracking site) and alerts you when you visit a suspicious one. Norton



**ClamXav** ClamXav is a free way to scan Mac e-mail for Windows viruses, before you pass them along to your

Confidential (\$50; [www.symantec.com](http://www.symantec.com)) includes phishing-protection plug-ins for both Safari and Firefox. It compares URLs you visit with Symantec's database of phishing sites and alerts you if you attempt to visit one. Norton Confidential also protects against e-mail based phishing attempts.

### Our Advice

No matter which operating system you use, there will always be people out there trying to make a fast buck by exploiting

known bugs, system vulnerabilities, or lax users. I advise spending your money not on Mac antivirus software but on a good phishing-protection application; at the very least, consider using a browser that offers built-in phishing protection. Your Mac's file system is probably safe from malicious hackers, but your identity may not be.

**Scott McNulty** is a senior contributor for MacUser ([www.macuser.com](http://www.macuser.com)) and blogs at blankbaby ([blog.blankbaby.com](http://blog.blankbaby.com)).

## Third-Party Antivirus Applications

PRODUCT	PRICE	RATING	FIND CODE <sup>A</sup>
ClamXav 1.10 open source	free (payment requested)	★★★★½ <sup>B</sup>	<a href="http://macworld.com/1307">macworld.com/1307</a>
Norton AntiVirus 11 Symantec <a href="http://www.symantec.com">www.symantec.com</a>	\$50; upgrade, \$30	★★★★½	<a href="http://macworld.com/3727">macworld.com/3727</a>
VirusBarrier X5 Intego.com	\$70; upgrade, \$45 (includes a one-year virus update subscription)	★★★★½	<a href="http://macworld.com/3728">macworld.com/3728</a>

<sup>A</sup> Typing in find codes after [macworld.com](http://macworld.com) directs you to a product's review or overview. For example, [macworld.com/3728](http://macworld.com/3728) takes you to our review of VirusBarrier X5. <sup>B</sup> Version 1.03 reviewed.





# PRIVACY SAFEGUARDS

**Keep your personal information personal with OS X and third-party apps.** By Joe Kissell

**A**t the very least, losing your wallet to a thief is a major pain in the neck: you lose your cash and (possibly) some precious mementos, and you have to cancel your credit cards and replace your driver's license. More seriously, the thief could steal your identity, using your personal information to make purchases, get loans, or cause you all kinds of grief by pretending to be you.

All that and more could also happen if your Mac's data were to fall into the wrong hands.

Privacy software addresses concerns like these by making sure that any confidential information you keep on your computer or send across the Net can be seen only by you and the people you designate. In most cases, that means using some form of encryption.

## The Threats

Threats to computer privacy—and the software tools that address those threats—fall into two broad categories: threats from physical loss and threats from electronic snooping.

**Physical Loss** Computer theft is unfortunately quite common. Thieves are certainly interested in your Mac, either to keep or to sell. But anyone with a bit of curiosity and a few minutes could discover all kinds of useful things about you by examining your files—especially if your keychain is unlocked or has an easily guessable password.

A laptop is more likely to be stolen than a desktop, especially if it spends a lot of time outside your home or office. A Mac Pro in a locked room of an



isolated house with a big guard dog is certainly less likely to be stolen than a MacBook Air you carry with you all the time as you walk around a big city.

Also, laptops are frequently simply lost—left on restaurant tables or at bus stops, forgotten at airport security checkpoints, or otherwise misplaced. Although an honest person might locate and return your lost computer, you might not be so lucky.

Even if your computer is right where it's supposed

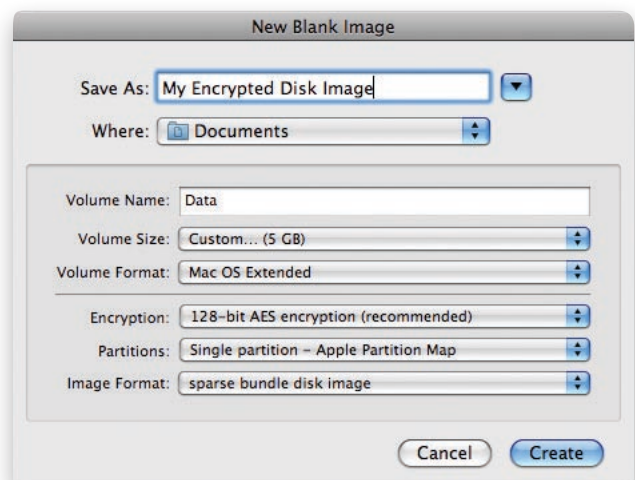
to be, other people can still get to your personal information. Family members, friends, or coworkers, say—any of them could, in theory, snoop around on your hard disk. And if your Mac breaks down, any repair technician could potentially see your private data.

**Electronic Snooping** A criminal doesn't need physical access to your Mac to do you wrong. He or she can snoop into your network traffic (unencrypted Wi-Fi connections are especially easy), looking for strings of characters that might be passwords, account numbers, and the like.

There's no way to determine the exact likelihood of your network traffic being intercepted. But anecdotal evidence suggests that snooping is quite common. Whenever you use an unsecured wireless network—from an office, coffee shop, airport, or park bench—someone *could* be eavesdropping.

Snooping on wired Internet connections is harder but still possible. In theory, anyone who can tap into the network at any point between you and the servers you visit (for example, an employee of an ISP, a government agent, or someone else with physical access to one of the many routers your data passes through) could pick out your passwords, account numbers, and other private data.

Whether you're talking about physical vulnerabilities or electronic ones, you do



**Bundle Up** When creating an encrypted disk image in Disk Utility, use these settings for best results (alter the name, location, and size to meet your needs).



have the odds in your favor. Thieves, hackers, and spies have only so much time to do their work. They can't attack all the computer users out there. But even if the odds are one in a million that you'll be attacked in this way, you can make it just about impossible by using encryption and other software to protect your privacy.

## OS X's Privacy Tools

Encryption software can ensure the privacy of data you're storing on your hard drive or sending to other people, by making it essentially impossible for anyone else to read. OS X itself has some built-in encryption tools that address part of the problem, and third-party software can help with the rest.

**Protecting Your Files** To protect yourself against people who have physical access to your Mac, you should consider encrypting at least some of the data on your hard disk. You can encrypt anything from a single file to the contents of an entire volume. Unless you're protecting state secrets, one of the many off-the-shelf encryption tools available for the Mac, combined with a good password, should be good enough to keep your data safe.

OS X's FileVault feature encrypts the entire contents of your user folder (`/Users/youruserfolder`). To activate FileVault in Leopard, go to the Security preference pane and click on the FileVault tab. If you haven't already done so, click on Set Master Password and specify a password that can be used to



**FileVault** If you encrypt your user folder with FileVault and then forget your regular login password, you can get to your data by providing the master password.

unlock FileVault if you forget your regular login password. Make it a good one but one that you'll remember—and be sure not to lose it. Then click on Turn On FileVault. (The process of encrypting your user folder takes time.) Remember that, before you start, you'll need at least as much free space on your disk as your user folder currently occupies. Once FileVault is on, logging out will encrypt all your files, and logging in will decrypt them again.

While you're at it, you should consider encrypting your virtual memory (select Use Secure Virtual Memory on the Security preference pane's General tab). Then if someone examines the virtual memory files written to disk as you use your Mac, they won't find any unencrypted copies of your data.

If encrypting your entire user folder with FileVault seems like overkill, you can instead store important files in an encrypted disk image created with Disk Utility.

To do so, open Disk Utility (in `/Applications/Utilities`). Choose File: New: Blank Disk Image. Enter a name for the disk-image file and choose a location; also enter (in the Volume Name

field) the name you want the mounted image to have. From the Volume Size pop-up menu, choose the *maximum* size you want your disk image to have. Select Mac OS Extended from the Format pop-up menu, choose 128-bit AES Encryption from the Encryption pop-up menu, leave Partitions set to Single Partition - Apple Partition Map, and choose Sparse Bundle Disk Image from the Image Format pop-up menu. Then click on Create. When prompted, enter and repeat a password and click on OK.

To use your new disk image, simply double-click on the file. Enter your password when prompted, and the volume will mount in the Finder. You can then copy files to it and open them directly from the image. When you eject the image, log out, or shut down, the files will be inaccessible to anyone who doesn't have the password.

**Protecting Your Communications** To protect your e-mail, you can use one or more forms of encryption. Similarly, live chats using iChat or other instant-messaging clients can be encrypted to protect them from interception. (For more advice on securely transferring files, see this month's *Mobile Mac* column, page 86.)

## TIP

### Use Parental Controls

The one time I was ever infected by malware on Windows it was thanks to my niece browsing for free online games. Even if you follow safe browsing habits, not everyone else using your computer will. Leopard's Parental Controls (in System Preferences) are a seldom-used but powerful tool for limiting risky activity on your Mac.—RICH MOGULL



The easiest way to start ensuring secure communications is to make sure you use SSL (Secure Sockets Layer). Almost all modern e-mail services (including, naturally, MobileMe) offer SSL as an option for receiving mail (using IMAP, POP, or Exchange) and for sending mail (using SMTP). SSL encrypts e-mail as it travels between your computer and your e-mail provider (in either direction); messages will still be stored unencrypted on your mail server and the recipient's mail server.

In most cases, you just need to turn on this option in your e-mail program—but before you do, confirm that your e-mail provider supports SSL, and find out if it requires the use of a special mail server address or other configuration changes.

To activate SSL in Mail, choose Mail: Preferences, click on Accounts, and select your e-mail account in the list on the left. To use SSL for incoming mail, click on the Advanced tab and make sure the Use SSL option is selected. To use SSL for outgoing mail, click on the Account Information tab and choose Edit Server List from the Outgoing Mail Server (SMTP) pop-up menu. Select the SMTP server associated with this account, click on the Advanced tab, and make sure the Use Secure Sockets Layer (SSL) option is selected. Click on OK.

If you use another e-mail program, consult its documentation to learn how to turn on SSL. If your e-mail provider

doesn't support SSL, you can opt to encrypt your entire Internet connection with a VPN instead.

SSL protects your messages during just part of the journey between sender and recipient. To make sure that no one but you and your correspondents can read your messages, even when those messages are sitting on a mail server, you need to encrypt their contents. Apple Mail has built-in encryption capabilities. (Again, see this month's *Mobile Mac* for more.) If you use another e-mail program, or if you want a simpler setup procedure, you can use third-party software (described just ahead) to encrypt e-mail.

Instant-messaging (IM) sessions using iChat or another client are also vulnerable to snooping. If you use IM mainly for small talk, this risk might not bother you at all. But if you exchange business plans, passwords, or other confidential information via IM, you should consider encrypting your chats.

Some IM programs (such as Skype) encrypt chats automatically. iChat can encrypt chats if you're a MobileMe member. To set this up, open iChat and choose iChat: Preferences. Select your MobileMe account in the list on the left, click on Security, and make sure the message at the bottom of the window says "iChat encryption is enabled." If it says "iChat encryption is disabled," click on the Enable button to enable it.

## TIP

### Browse Safely

After e-mail applications, Web browsers are the most commonly attacked programs. Here are two things you can do to make browsing more safe:

- > If you're using Safari, disable the General preference pane's Open Safe Files After Downloading option.
- > If you're using Firefox, install the NoScript plug-in. (Go to [addons.mozilla.org](http://addons.mozilla.org), search for and find the NoScript plug-in, and then click on Add to Firefox.) It prevents scripts from running without your permission, but you'll have to manually enable them for every site.—RICH MOGULL

## Third-Party Privacy Tools

When it comes to encrypting your files or keeping your communications confidential as they traverse the Net, there are several third-party apps that can substantially supplement OS X's built-in tools.

**Protecting Your Files** If neither FileVault nor an encrypted disk image suits your needs, you should consider a third-party encryption program instead.

Numerous Mac programs can encrypt individual files or folders (or create "vaults," sometimes in the form of proprietary disk images, for holding multiple files). Examples are Intego's \$40 FileGuard X5 ([www.intego.com](http://www.intego.com)), Marko Karppinen's \$30 Knox (★★★★; [macworld.com/2534](http://macworld.com/2534)), PGP Desktop Home (\$99; ratingtk; [macworld.com/0719](http://macworld.com/0719)), and Smith Micro's \$80 StuffIt Deluxe (★★★★½; [macworld.com/2501](http://macworld.com/2501)).

These programs typically offer greater flexibility and more features than either FileVault or Disk Utility. For example, StuffIt Deluxe not only encrypts but also compresses your files. PGP Desktop Home can also encrypt e-mail and instant messages (a new version of that program should be available by the time you read this; see Macworld.com for our review after it comes out). You can set FileGuard to

## Third-Party Encryption Software

PRODUCT	PRICE	RATING	FIND CODE <sup>a</sup>
<b>FileGuard X5</b> Intego <a href="http://www.intego.com">www.intego.com</a>	tk	TK	<a href="http://macworld.com/tktk">macworld.com/tktk</a>
<b>Knox 1.5.3</b> Marko Karppinen <a href="http://www.knoxformac.com">www.knoxformac.com</a>	\$30	★★★★ <sup>b</sup>	<a href="http://macworld.com/2534">macworld.com/2534</a>
<b>PGP Desktop Home TK</b> PGP <a href="http://www.pgp.com">www.pgp.com</a>	\$99	★★★★½ <sup>c</sup>	<a href="http://macworld.com/0719">macworld.com/0719</a>
<b>Stuffit Deluxe 12</b> Smith Micro <a href="http://my.smithmicro.com">my.smithmicro.com</a>	\$80	★★★★½ <sup>d</sup>	<a href="http://macworld.com/2501">macworld.com/2501</a>
<b>TrueCrypt 6.0</b> open source	tk	TK	<a href="http://macworld.com/tktk">macworld.com/tktk</a>

NA = not applicable. <sup>a</sup> Typing in find codes after [macworld.com/](http://macworld.com/) directs you to a product's review or overview. For example, [macworld.com/2534](http://macworld.com/2534) takes you to our review of Knox 1.1.1. <sup>b</sup> Version 1.1.1 reviewed. <sup>c</sup> Version 9 reviewed; update expected in fall 2008. <sup>d</sup> Version 11 reviewed.



securely overwrite the original versions of your files automatically when they're copied to an encrypted image.

If you want to encrypt an entire volume (other than your startup volume), consider the open-source TrueCrypt (free; TKTK mice; [www.truecrypt.org](http://www.truecrypt.org)), which can also create *hidden* encrypted volumes. Two products can encrypt an entire Mac startup volume: Check Point Full Disk Encryption (\$120; [www.checkpoint.com](http://www.checkpoint.com)) and PGP's forthcoming Whole Disk Encryption ([www.pgp.com](http://www.pgp.com)). Check Point Full Disk Encryption is geared toward rate customers who buy in volume, while PGP Whole Disk Encryption is readily available to individual consumers.

**Protecting Your Communications** If you want to be absolutely certain that a message will get to its destination without being read by anyone else, but don't want to jump through the hoops Apple Mail requires, look for a third-party option. Your best bet is software based on PGP (Pretty Good Privacy), a widely used, platform-neutral encryption system.

The commercial version of PGP, PGP Desktop Home, lets you sign and/or encrypt e-mail messages with just a few clicks; it also ensures that all your e-mail accounts use SSL. (Your correspondents must also be using some version of PGP.)

## Scrubbers

Every time you browse the Web, your browser stores information about where you've been and what you've been doing. Unless you encrypt your user folder, this information is in plain view for anyone who knows where to look.

If you use Safari, one solution is to activate Private Browsing mode (Safari: Private Browsing), which prevents most of this data from being written to your disk in the first place. Most other browsers also let you turn off these features, though doing so may require changing several settings.

You can also use a utility commonly referred to as a "scrubber" to seek out and delete all traces of your recent online activities. These programs include Maintain's \$15 **Cocktail** ([www.maintain.se](http://www.maintain.se)); Smith Micro's \$30 **Internet Cleanup** (⚙️; [macworld.com/3768](http://macworld.com/3768)); Koingo's \$20 **MacCleanse** ([www.koingosw.com](http://www.koingosw.com)); Secure-Mac's \$30 **MacScan** (⚙️; [macworld.com/1511](http://macworld.com/1511)), which also checks for spyware; and Mireth Technology's \$25 **NetShred X** ([www.mireth.com](http://www.mireth.com)).

Unfortunately, browsing in private mode and using a scrubber can still leave some traces of your Web trail behind. For example, an OS X component called Directory Services can cache some DNS information, revealing Web sites you've visited. To clear it, open Terminal (/Applications/Utilities), type **dscacheutil -flushcache**, and press return.

Also, some browser plug-ins can cache their own content, even if your browser is set to not save anything. To remove your Flash cache, drag the contents of the following folders to the Trash: *youruserfolder/Library/Preferences/Macromedia/Flash Player/Shared Objects* and *youruserfolder/Library/Preferences/Macromedia/Flash Player/macromedia.com/support/flashplayer/sys*.—JOE KISSELL

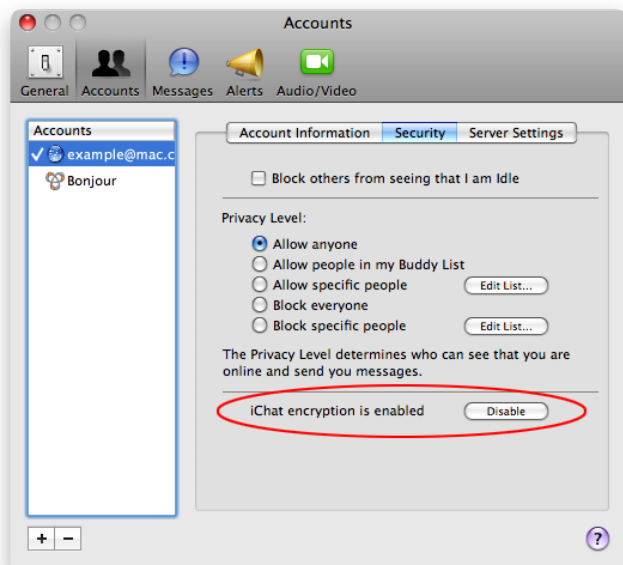
Alternatively, you might try the free, open-source Mac GNU Privacy Guard (or Mac GPG for short; [macgpg.sourceforge.net](http://macgpg.sourceforge.net)). Mac GPG lacks many

good, inexpensive way to get started with e-mail encryption.

## Our Advice

For most users, simple approaches (perhaps even using OS X's built-in software) are more than enough to protect privacy. Secure your e-mail with SSL and your iChats with MobileMe encryption, and either create an encrypted disk image to hold sensitive files or use FileVault to encrypt all your personal documents. If you need more power or flexibility, try a third-party program, but be sure to download a demo version and give it a thorough tryout before buying it. Even the most powerful encryption software does you no good if using it turns out to be so cumbersome that you avoid it.

**Joe Kissell** is the senior editor of TidBits ([db.tidbits.com](http://db.tidbits.com)) and the author of numerous e-books about OS X ([www.takecontrolbooks.com](http://www.takecontrolbooks.com)).



**Private Chat** MobileMe members can encrypt their iChats just by clicking on a button; the setup looks like this when encryption is active.