Security Basics for Your Portable Mac

CHAPTER 3

In This Chapter

- Your Mac OS X password and security
- Set your Open Firmware password
- Manage your keychain
- Encrypt your home folder
- Other encryption solutions
- Backing up your files

If your iBook or PowerBook ever gets in the wrong hands, it's important that your personal or business information isn't compromised. Security precautions and portability go hand-in-hand because a portable Mac is much easier to lose or have stolen than a desktop Mac. Also, for many of us, the data on the computer can be more valuable and irreplaceable than the computer itself, so implementing a backup strategy and keeping your data secure are important.

Your Mac OS X Password and Security

One of the most important setup tasks in getting an iBook or PowerBook ready for the road is securing it from access by unauthorized users. These Macs' portability makes them targets for theft and loss, and a Mac in the wrong hands may offer up personal, financial, and other data that you'd prefer not to share with others. Fortunately, it's relatively easy to secure your Mac and its contents from prying eyes, even if the iBook or PowerBook gets lost or stolen. It just takes a little vigilance.

Choose a good password

The first step in securing your Mac is to choose a good password for your Mac OS X user account; more than likely you selected one via the Setup Assistant that runs when you use

your Mac for the first time. When you choose a password, consider some of these key rules:

- Your password should be at least eight characters long.
- Your password should not be composed of words found in the dictionary; nonsense is better.
- When possible, use a combination of letters and numbers to make up your password.
- Change your password frequently, particularly if other people use your Mac and/or you travel with it quite often.

If you use your Mac in an office setting, it's good to change passwords every few weeks. Employees come and go, so a trusted colleague may be working for someone else the next time you see him or her at a conference.

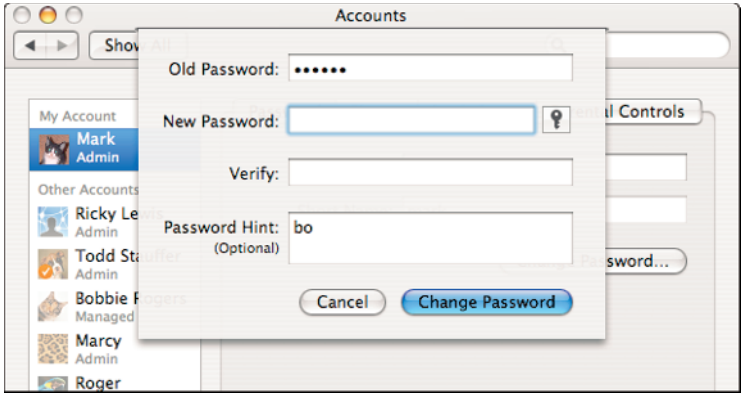
The best passwords are a string of characters and numbers that mean something to you — which helps you remember the password — while meaning nothing to other people. For example, you could use a phrase such as "It was the Fourth of July when I fell for Sally" to create the password iwt4o7wif4s or something similar. That might be easy for you to remember but hard for someone else to guess.

A truly secure PowerBook actually has a number of passwords. As you'll see in later sections, it's possible to scramble your documents and data so that someone without the proper password would need to set up some serious encryption-cracking tools to get at your files. And, the PowerBook offers a low-level password that gives you the ultimate security for a lost or stolen PowerBook, making it nearly impossible to access the drive directly.

Encryption is the process of storing files in a format that appears to be nonsense, but that can be decipher by someone who has the right tools. In the case of your Mac, we'll explore some different utilities within Mac OS X that enable you to use a password to encrypt documents that are stored on your hard disk so that their contents can't easily be accessed by someone who gets his hands on your Mac portable.

The first password you need to change to make your Mac more secure, however, is your everyday Mac OS X user account password — the one you use to log on to your Mac when you want to get some work done. Here's how:

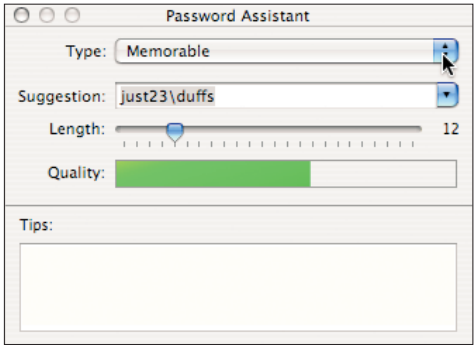
1. **If you haven't already, log on to your user account (or any Administrative user's account).**
2. **Open the System Preferences application (choose System Preferences from the Apple menu), and then click the Accounts icon.** By default, your account is selected in the Account list, and the Password tab is shown.
3. **Click Change Password to type a new password.** When you do, the dialog sheet shown in figure 3.1 appears.



3.1 You can type a new password using the dialog box that appears when you click Change Password in the Accounts pane in System Preferences.

It's also helpful to know that you don't have to come up with that extremely clever password on your own; you can get Apple to help you with it. Here's how:

1. **Open the System Preferences application if you closed it after the previous set of steps.**
2. **Type your old password in the Old Password field.**
3. **Click the small key icon to the right of the New Password field.** The Password Assistant dialog box appears. (Shown in figure 3.2; note that this feature requires Mac OS X 10.4 or higher.)
4. **Choose a password type from the Type menu.**
5. **When you're done creating a new password, close the Password Assistant.** The password is entered in the New Password field for you.
6. **Type that password again in the Verify field.**
7. **Type a hint for yourself in the Password Hint field.** This is optional. If you have trouble getting the right password when you're logging on, the hint appears after three failed attempts — or you can see it by clicking Forgot Password in the login window.
8. **Click Change Password.** Your password is changed.



3.2 The Password Assistant can help you create more secure passwords.

In the Password Assistant dialog box, you can use the Type pop-up menu to choose the different types of passwords that the Password Assistant will help you with. You can take a few different approaches:

- If you already have a password in mind, choose Manual from the Type menu, and then type the password in the Suggestion entry box. As you type, the Assistant responds by showing the length of the password and the Quality of the password. The more obscure and difficult to guess, the better the Quality rating will be.

If your password is difficult for your to remember — so much so that you end up writing it down and putting it in your wallet or on a sticky in your laptop bag — then it's less secure than one that you can remember fairly easily but that otherwise follows the rules.

- If you can't think of your own password, use the Type menu to choose a type of password. The Memorable passwords tend to be a little less secure, but they're randomly generated and easy to remember because they mix real words with numbers and symbols. The other types of passwords tend to be high quality because they are collections of letters, numbers, and/or symbols — they just might be more difficult to remember.

You don't have to use the first suggestion that appears in the Suggestion entry box. Click the down arrow next to the Suggestion entry box and you'll see a menu of other suggestions.

Administrative Accounts and Security

On the screen for each user is the option to Allow User to Administer This Computer. By default, the original account you create on your Mac through the Setup Assistant is an Admin account. If you're particularly paranoid about security, you can create a user account for which this option is turned off and then use that account for day-to-day work.

If, while working in a regular account you encounter the need for an Administrator's password, then you can type your original username and password. By working in a regular account, you don't allow access to any administrative functions to anyone who sits down and begins using your Mac while that account is active. Instead, anyone accessing an Administrative function from a regular account is forced to type a username and password for a valid Administrator account before going forward.

Setting logon options

Once you have a secure user account password, you need to make sure your Mac is configured to use that password. By default, your Mac may be set up to bypass its password screen and automatically log you on to the account that was created when you went through your Mac's Setup Assistant. That may be convenient, but it's not really the best idea if your goal is security for the important data on your portable.

To check whether the password screen is bypassed, you can check it in the Accounts pane of System Preferences. Follow these steps:

1. **Choose System Preferences from the Apple menu, and then click the Accounts icon in the System Preferences window.** That causes the Accounts preference pane to appear.
2. **Click Login Options.** You'll see the window reconfigure with a series of options.
3. **If the Automatically Log In As option is selected, deselect it and turn the option off (see figure 3.3).**

Other options in the Login Options window are interesting for security. Under Display Login Window As, you can choose to show a List of Users (the default) or just the Name and Password. If you choose the Name and Password option, someone accessing your Mac's logon screen won't see a list of the

3.3 Turning off automatic login is an important security measure, as it requires anyone who starts up your Mac to log on with a valid user account.

existing users — and, hence, won't be able to simply select a user and then start guessing his or her password. Instead, any potential user needs to know a valid username first that can be typed into the Name field.

Another option under Display Login Window As that is interesting for security is the ability to turn on and off the Password Hints option. If you feel strongly that you can remember your password and no one else accesses your iBook or PowerBook, just deselect that option.

Need to know how to change a password that you've forgotten? If you can, log on as a user who has Admin privileges, and change the password for the account that you've forgotten. If you don't have a user with Admin privileges, you need to restart your Mac from a Mac OS X installation CD, and then choose Reset Password from the Utilities menu. See Chapter 7 for more on recovering from a forgotten password.

Require your password often

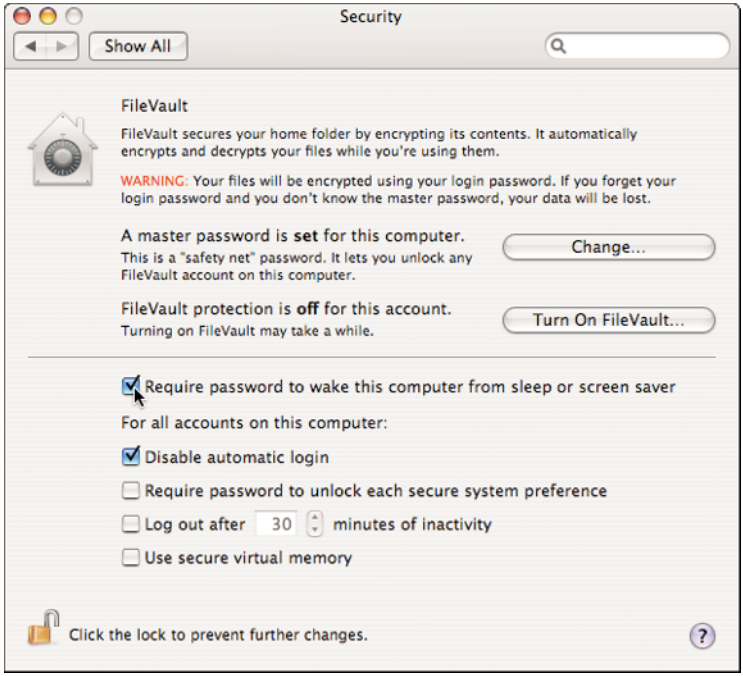
After establishing a better, more secure user account password, you are ready to enact more security measures. A good place to start is in the Security pane of System Preferences. Launch System Preferences (or, if it's already open, click Show All to view all of the preference panes), and then click the Security icon. That reveals the Security pane (see figure 3.4).

In the Security pane, you see important security items under the heading For All Accounts On This Computer. Here's a look at those items:

- **Require Password to Wake This Computer From Sleep or Screen Saver.** I pretty much always have this one turned on, particularly on my Mac portables. That's because it's a great first line of security for situations where you don't want others to have even casual access to your files. With this option turned on, you can put your Mac to sleep with the Sleep command from the Apple menu (or allow it to go to sleep or into screen saver mode) and your Mac is instantly password protected, requiring your login password before it will allow you or another user access to your account and any open applications and/or documents.
- **Disable Automatic Login.** This option forces a user to use the logon window to access the Mac from startup, restart, or after an account is logged out.

Setting Up a Screen Saver

In order to use a screen saver for security, you need to turn the screen saver on first. You do that via the Desktop & Screen Saver pane in System Preferences. Open the pane, and then click the Screen Saver tab. Select a screen saver from the list. Use the Start Screen Saver slider to determine how long the computer should be idle before the screen saver kicks in. There you'll also find the Hot Corners button, which you can use to activate the screen saver when you place your mouse point in one of the corners of the screen. When combined with the Require Password to Wake option, using a hot corner for the screen saver means instant security for your account.



3.4 The Security pane of System Preferences gives you options focused specifically on keeping you data private.

- **Require Password to Unlock Each Secure System Preference.** This option slows the access to your Mac down somewhat, but it means you have to type the password for an Administrative user in order to change important settings in the System Preferences application.
- **Log Out After ___ Minutes of Inactivity.** Select this option and choose a length of time if you want accounts to be automatically logged out when the computer is not in use. (Note that applications with unsaved changes or those that have other issues can blog the Log Out After command from finishing the log out process.)
- **Use Secure Virtual Memory (Mac OS X 10.4 and higher).** When this option is active, items that are swapped to temporary files as you're working in multiple applications are stored in a secure, encrypted manner.

With all those options turned on, you can be assured that your Mac is reasonably secure for day-to-day use. But you're not totally secure yet.

While the casual unauthorized user will be deterred by requiring logins and password-protecting sleep or screen saver waking, someone who gains access to your Mac and who wants to get at your data has other options. That person may still be able to

restart it in Target Disk Mode, for instance, which allows unfettered access to your files. And, an unattended Mac can be restarted with a Mac OS X installation disc, which gives the user access to the Reset Password utility — your passwords can be changed and your files accessed.

Fortunately, there's a way to lock people out of these features, too, with a special Open Firmware password.

Later in this chapter you see how to encrypt the data on your hard drive so that it's not easily read even if the Mac is taken apart and the hard drive removed.

Set Your Open Firmware Password

After you press the power button on your Mac, a small set of instructions is responsible for starting up the computer, testing its vitals, and then handing control off to the Mac OS. Those instructions, called *Open Firmware* on a modern Mac, are stored on a special type of static memory chips that maintain data even without electrical power. And aside from getting your Mac started up and tested, Open Firmware also checks to see if you're holding down any special keys on the keyboard. Certain keys send a signal to the Mac that you want to start up the Mac in a different way than usual.

That's why — even if you're diligent with your account password — it's still possible for someone to gain access to your Mac. One technique is to restart with a Mac OS X installation disc and use the Reset Password function to change an accounts password. (All you do is insert an optical disc in the drive and restart the Mac. After the startup tone, press and hold C and the Mac attempts to boot from the disc instead of the internal hard drive.)

Or, a person can press and hold T to boot your Mac into Target Disk Mode, connect it to another Mac through FireWire, and access your files.

Target Disk Mode is discussed in Chapter 2.

Fortunately, there's a way to lock down your Mac so that these startup keys are ignored and a special password is required to change a setting in Open Firmware, including these startup options. It's called, appropriately enough, the Open Firmware Password, and you set it using a special utility application.

It's imperative that you remember this password once it's set. Not even Apple can retrieve it if you forget it.

Here's how to set this special Open Firmware password:

1. **Launch the Open Firmware Password application that's located in the Utilities folder inside your Mac's main Applications folder.** The Open Firmware Password window appears.
2. **Click Change to move to the next screen.**
3. **Select the Require password to change Open Firmware settings option and then type a password twice in the entry boxes provided and click OK.** Figure 3.5 shows a new password being created in the Open Firmware Password window.

3.5 Use the Open Firmware Password utility to change the password that blocks access to startup keyboard shortcuts.

4. **Type the name and password for an Administrator on this computer and click OK.** If the admin account name and password are accepted, a message appears saying that the password has been updated.

5. **Choose Open Firmware Password ➪ Quit Open Firmware Password to quit the utility application.**

Once you successfully set the Open Firmware password, you have another layer of security active. Now, the keyboard shortcuts for starting up from a CD/DVD or starting into FireWire Disk mode are disabled. To change the way the Mac starts up, you must use the Startup Disk pane of System Preferences and type an administrator's account and password.

To boot into the open firmware operating system itself (where there's actually a text prompt), restart your Mac and press and hold ⌘+Option+O+F. At the Open Firmware prompt you'll need to type your Open Firmware password before you can move on to any other commands.

Manage Your Keychain

If you're like most computer users, you have many passwords that you use with your Mac — both within the operating system interface and on the Internet — and you find it's tough to keep up with them in a secure way. With your PowerBook or iBook, if you have your passwords written down anywhere in the vicinity, such as in your wallet, in the computer bag itself, in your luggage, and so on, then you increase the risk that someone who gains access to your portable can access the data it contains.

Apple's solution to that issue is called the *keychain*, a technology built into Mac OS X that can help you manage your mountain of passwords by giving you a central repository that you can access with a single password in order to unlock all of your other passwords. Ultimately, your keychain is a special, secure database that stores automatic login information for certain resources (such as local network logins and some Web-based login information) as well as any scrap of information that you'd like to keep password protected, such as login information, credit card numbers and details, and so on.

Understand your keychain

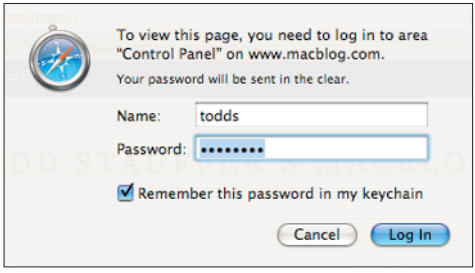
A keychain is created for you when your user account is created, and this default *login* keychain has the same password as your user account. When you log in to your user account, the keychain is unlocked and left unlocked; your applications can access passwords that they store in the keychain, so that, for example, Mail can access e-mail

servers or a stored password can be accessed by Safari. That sort of thing is handled automatically; the only indication that you sometimes get from an application is a request, in the form of a dialog box, to access that item (see figure 3.6).

3.6 Occasionally a dialog box appears while you're working that asks if an application can have access to your keychain.

If you see this dialog box, you can choose to deny the application access to your keychain database, you can give it one-time access, or you can tell it that that application can always access that particular item.

As you work in your applications, you find different opportunities to store passwords in the keychain. Figure 3.7 shows an example in Safari; in general, you work with the keychain by selecting an option in a dialog box where you typed the password for network or Internet resource.



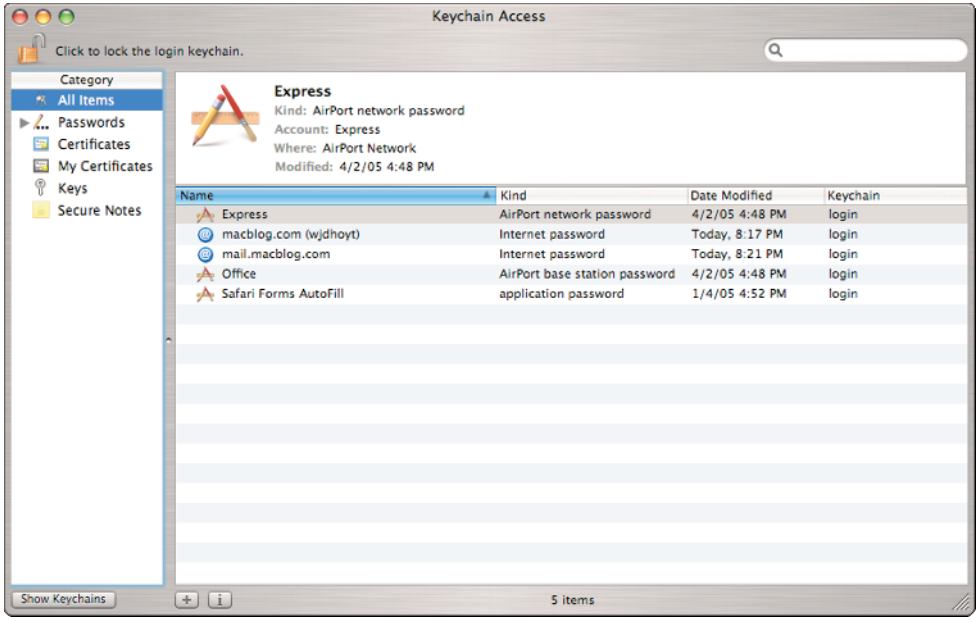
3.7 In this example, Safari allows the password for an online account to be saved in the keychain.

As long as you're logged in to your account and your keychain password is the same as your user account password, then your applications have access to those keychain items. This is worth noting because if you change your user account password, your keychain password is not changed along with it. As a result, you'll be asked by your applications for your keychain password (see figure 3.8) as well as permission to access the keychain. Your keychain password, in that case, will be the password that you had for your user account when the user account was created.

3.8 Occasionally you'll see a dialog box that asks for the password to your keychain, particularly if your keychain is locked or if the password is different from your login password.

Manage your keychain

You can manage your keychain in a hands-on way, and there are some benefits to doing that. To get to your keychain and its preferences, launch the Keychain Access application found in the Utilities folder inside your Mac's main Applications folder. When you do, the Keychain Access window appears, as shown in figure 3.9.



3.9 The Keychain Access application is used to manage your keychain.

The first thing to notice about the Keychain Access application is the padlock icon at the top-left of the window. If it's open, then your keychain is open, meaning applications can access the keychain and its contents, in some cases without your typing a password or making any choices. If the padlock is locked, then your keychain password is required before any of the items on that keychain can be accessed.

So, one thing you can do with your keychain in Keychain Access is lock it if it's unlocked or unlock it if it's locked. To do either, click the padlock icon. If the keychain is unlocked, then it will be locked immediately; if the keychain is locked, a dialog box appears that requests your keychain password. If you type it correctly, the keychain is unlocked.

Once you unlock your keychain, it stays unlocked until you log out of the account (or switch to a different user account). So, if your Mac stays logged on to your account and is accessible to other users, they can conceivably use data stored on your keychain, such as Internet account names and passwords.

It's more secure to lock your keychain when you're not using your Mac, but leaving it logged on to your account. The easiest way to do that is to set the keychain to lock automatically. Choose Edit ➪ Change Settings for Keychain. In the dialog box that appears (see figure 3.10), select the Lock after ___ minutes of inactivity and/or Lock when sleeping option(s). In the blank, type the number of minutes or use the arrow controller to change the number of minutes you want your Mac to wait before locking your keychain.

3.10 The Change Keychain Settings dialog box can be used to automate the locking of your keychain.

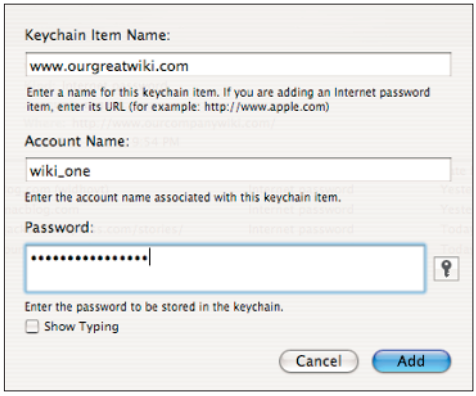
The Keychain Access window is designed to give you quick access to different categories of items that can be stored on your keychain, each of which is shown in the Categories list. By default, the All Items category, which shows you all of the keychain items you have stored at once, is displayed. But the Categories list can also be used to show specific items, such as passwords that have been stored for various reasons. Click the disclosure triangle next to Passwords in the list to see the types of passwords — AppleShare, Application, and Internet — that are stored.

Note

AppleShare passwords are generally stored when you log on to network resources, and Internet passwords are stored when you use a Web browser, FTP application, e-mail application, or something similar to access an Internet server. An application password is used to get into the secure portion of an application — for example, you might password-protect documents or diary entries in some applications, or use a password to get into your financial software. If the application is capable of it, you might be able to automatically store those passwords in your keychain.

You've already seen how you can use options within your keychain-aware applications to add passwords to your keychain; you can also add them manually. Follow these steps:

1. **Choose File➪New Password Item if you have an Internet or similar password that you want to store.** A dialog sheet appears.
2. **In the dialog sheet (see figure 3.11), type the name or URL for the item, the account name, and password.**



3.11 You can create new password items from within Keychain Access.

3. **Click Add.** The item is added to your keychain for safekeeping.

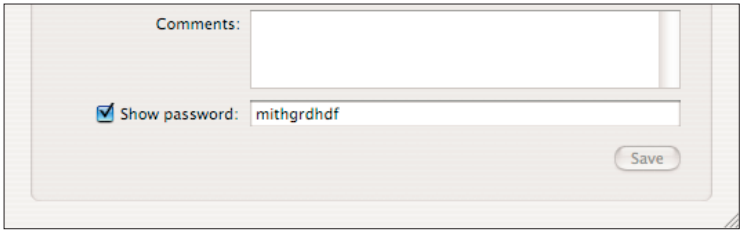
Not every Internet password that you type results in your being able to log in automatically using your browser. The keychain can only communicate with Web sites that use the browser's own authentication methods; in most cases, if you find that you're actually typing the username and password for a site on the Web page itself (instead of in a dialog box generated by your Web browser) then you probably can't use the keychain for login, but simply for safely storing the password so you can refer to it later.

If you ever need to jog your memory about this (or any other) account password, it's simple — just double-click the item to open its information window. Then, select the Show Password option on that screen. Most likely, a dialog box appears asking you to allow Keychain Access to access your keychain. Type your keychain password and click Allow Once or Always Allow. If the dialog accepts your password, you're returned to the information window for that item and you should see the password now in plain text (see figure 3.12).

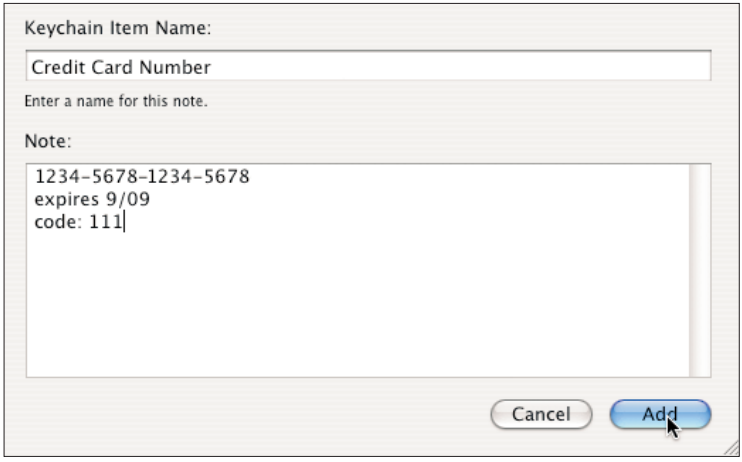
Along with passwords, another important use of your keychain is to store secure notes that can only be accessed by someone who has your keychain password. A note can be used for a variety of reasons — it can be a list of passwords you lock away, credit card or financial information, or even a small diary entry or other pasted text that you just want to keep to yourself. Whatever it is, to create a secure note, follow these steps:

1. **Choose File ➪ New Secure Note.** A dialog sheet appears.
2. **Type a name for the note in the Keychain Item Name field, and then type your note.**
3. **Click Add.** The note is added to your keychain (see figure 3.13).

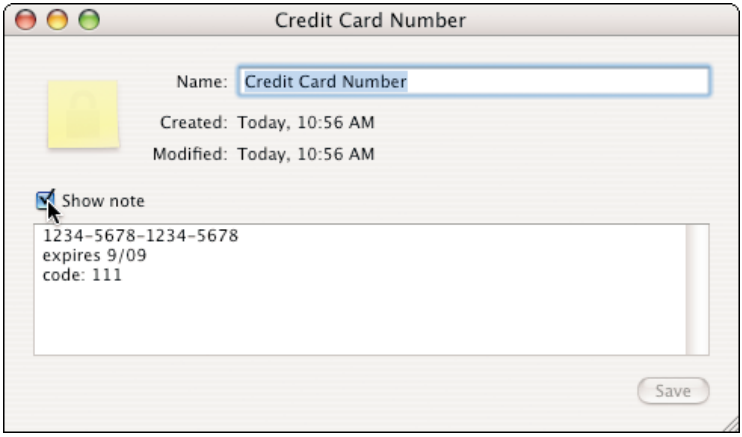
Back in the keychain window, double-click a note to view it, and then select the Show note option to see the portion that is secure (see figure 3.14). Keychain Access consults your keychain and asks you for your keychain password. Type it and choose either Allow Once or Always Allow; the contents of the note appear in the text area.



3.12 You can use a keychain item for a quick reminder of the password you stored.



3.13 You can add secure notes to your keychain that can only be accessed by someone with your keychain password.



3.14 Once the note is stored, you can access its contents only if it's been authorized through your keychain password.

The keychain also manages other items, such as information that your Mac uses to access encrypted Web sites and keys that can be used for sending encrypted messages.

Cross-Reference

Because some aspects of the keychain are little more focused on security when you're literally on the Internet, they are covered in more detail in Chapter 6.

Encrypt Your Home Folder

Ready to take file security to yet another level? How about securing against data access even if someone not only gains access to your portable Mac, but also is able to remove the hard drive? By encrypting the contents of your home folder using FileVault, a feature built in to Mac OS X, you can all but ensure that anyone but the most intrepid hacker is unable to read the data files that can be accessed by spelunking into your Mac's case. And, frankly, even that intrepid hacker would have an extremely difficult and likely unsuccessful job on his or her hands. This is because encryption essentially turns your files into a completely unintelligible string of characters based on an *encryption algorithm* (mathematical formula) that's set in motion by your personal password. That's another reason why the password should be a good one that is not easily guessed.

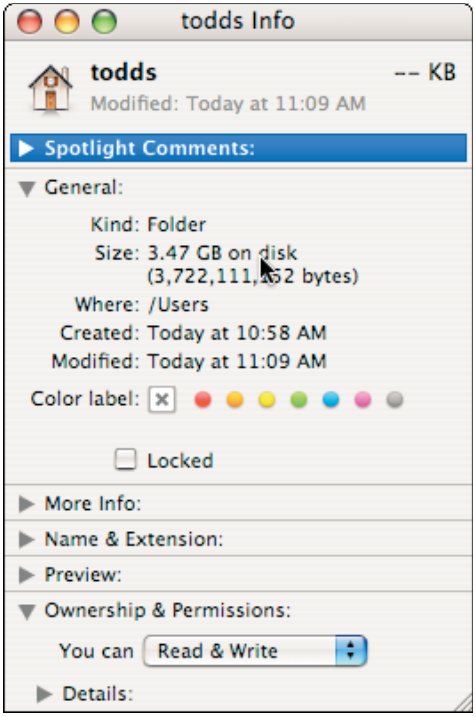
If there's a downside to encrypting your home folder, it is this: If you forget your password — and you forget the safety Master Password that Apple builds in — you've all but lost your data. The other issue to at least be aware of is the home folder encryption uses your login password as the key to decryption, so the whole encryption scheme is only as secure as your logon password.

The entire scheme is also based on the security of a Master Password, which you set the first time you attempt to initiate FileVault. Pick the most un-guessable password you can come up with. See the section "Your Mac OS X Password and Security" earlier in this chapter for advice.

I recommend you back up any and all important files in your home folder before encrypting because it's really uncool if something happens to your Mac during the encryption process and you can't get your important documents back. Also, note that your home folder should have the same name as your accounts' official short name (which is specified when creating your account and used to name your home folder) or you may run into trouble with FileVault.

One point is worth noting before you attempt to encrypt your home folder — you need enough free space on your hard drive to create an entire copy of that home folder. If your home folder takes up 50MB, then you'll need at least 50MB of free space. If it takes up 5GB, you'll need at least 5GB free. If you're not sure how much space your home folder takes up, locate its icon in the Finder, highlight that icon, and choose File ➪ Get Info. In the General section you can see how much space your home folder takes up by looking at the Size entry (see figure 3.15).

If you don't have enough room or if you're simply surprised to find that your home folder is taking up a ton of space (like I was) then consider moving some items out of your home folder's hierarchy, such as movie, music, or photos that don't really need encryption. You can move them elsewhere on your Macintosh HD (or whatever name you've given your Mac's internal hard drive) or, perhaps, to the Shared folder instead of your main Users folder.



3.15 Check the size of your home folder in the Get Info window, and then make sure you have enough room on your hard drive.

Turn on FileVault

Once you know you have enough space and you're otherwise ready to encrypt your home folder, here's how:

1. **Make sure no other users are logged in to your Mac using the Fast User Switching feature.** You can't turn on FileVault unless you're the only active user.
2. **Launch the System Preferences applications (choose Apple menu, System Preferences) and click the Security icon.** That opens the Security pane.
3. **If a Master Password has not yet been set, click the Master Password button.** That reveals the Master Password dialog sheet.
4. **Read about the Master Password; then type one in the Master Password field; type it again in the Verify field.** If desired, type a hint for yourself if you forget the password that will jog your memory without revealing the password.
5. **Click OK.**
6. **Click Turn On FileVault.** A dialog sheet appears requesting your user account password.
7. **Type your user account password and click OK.** Another dialog sheet appears warning you about FileVault.
8. **Read the dialog sheet, and then click Turn On FileVault.** You can also choose to turn on Use Secure Erase if you want your unencrypted files erased securely by your Mac. (The files will be overwritten after being erased, which makes them very difficult to recover.)

When you click Turn On FileVault, your Mac logs out and the FileVault dialog box appears showing the progress of the operation. After what may be a while, you return to the login window and asked to log in again. When you log in, you are working with an encrypted home folder; in fact, if you check out your home folder icon, you see it has a new icon that looks a little like a combination safe in the shape of a house.

Note that FileVault makes it impossible for you to log in to your account from a remote Windows computer and access files through file sharing when you're not logged in to your Mac; that's because your Home folder is, for all intents and purposes, one large, encrypted disk image. That image is *mounted* (meaning that it's made available for access by the Mac's underlying file system) when you log in to your account with the appropriate password.

Interestingly, although FileVault is a relatively new feature in Mac OS X, this is mostly a clever use of Apple's existing disk image technology that you can use for a variety of reasons. For more on disk images and encryption, see the section "Other Encryption Solutions" in this chapter, as well as more discussion of disk images in Chapter 6.

Turn off FileVault

If you find that FileVault is unworkable or if you simply don't need the extra level of security or the file sharing hassles, you can turn it off. Follow these steps:

1. **Make sure no one else is logged on to the computer using Fast User Switching.**
2. **Open the Security pane of System Preferences and click Turn Off FileVault.**
3. **After confirming that you want to turn off FileVault in the dialog box that appears, your account logs out and the FileVault dialog box appears.** You see the progress of decrypting. When FileVault is done, you return to the logon screen, and you should be able to log on to your newly decrypted home folder.

FileVault password recovery

So what happens if you encrypt your home folder and then forget your login password? That's when the Master Password kicks in.

Generally speaking, when someone on your Mac forgets his or her login password, one solution is to log on using another administrator-level account and change the password. But with FileVault, one admin user can't change the password of a user who has FileVault active. That's because you sever the link between the user's login password and FileVault password, which means you can't access your files even if you logged in.

Instead, you need to attempt to log in to your account — and fail. After three attempts, you are asked for the Master Password. Type that (or have someone else type it if it's a password you don't know or control) and click Log In. You are then walked through the process of changing the password for the encrypted account. This messes up the account's access to its keychain, which uses the same (forgotten) password as the logon, unless you change it.

As you can see, the Master Password is pretty powerful. You need to make sure that it's a high-quality password that is not easy to guess or defeat — otherwise, there isn't much point in going to the trouble of encrypting your home folder.

Other Encryption Solutions

FileVault is handy because it's built in to your Mac, but it isn't the only solution to maintaining data integrity. Another clever

way to add encryption to your overall security arsenal is something already mentioned. In fact, it's the same technology that FileVault is based on — an encrypted *disk image*. A disk image is really just a special kind of file that, when double-clicked, appears to mount a volume on your Mac as if you'd inserted a CD or DVD or attached an external hard drive. (Mounting simply makes the disk's contents available for access in the Finder.) The difference is that, once unmounted, the disk image continues to be a typical file that can be stored, transmitted to others, burned to disc, or, in this case, encrypted so that it can only be accessed via password.

Using the Disk Utility that comes with Mac OS X, you can create an encrypted disk image that's then used for storing files that you want to secure using a password. Here's how:

1. **Launch Disk Utility, which you find in the Utilities folder inside your main Applications folder.**
2. **Click the New Image button in Disk Utility's toolbar. A dialog sheet appears.**
3. **In the dialog sheet, type a name for the disk utility, and choose a place for it to be stored.** Then, choose a size for the image from the Size menu.
4. **In the Encryption menu, choose AES-128 and choose Sparse Disk Image from the Format menu.** A sparse disk image only takes up as much storage space as is required by the files you add to it; a read/write disk image takes up the amount of space you specify in the Size menu, regardless of the storage requirements of the files on the disk.
5. **Click Create.** The Disk Utility progress dialog box appears. Soon after, the Authenticate dialog box appears (see figure 3.16).

3.16 The Authenticate dialog box is used for creating a password to secure your encrypted disk image.

6. **Type a password for the disk image's encryption in the Password field, then repeat that password in the Verify field.** You also have the option of adding this password to your keychain so that the disk image can retrieve the password from your keychain instead of asking you for it every time you mount it.
7. **Click OK after typing the password twice.** That's it. The progress window continues until the image is created and mounted.

With a disk image, you see two things — the disk image file, and, when mounted, the disk image itself (see figure 3.17), which appears on your desktop by default as well as in the Sidebar of Finder windows. It's the disk image where you drag any files that you want to store; the disk image file is what you double-click to mount the disk image.

To unmount the disk image, simply select it in the Finder and choose File ➪ Eject, or click and drag the disk image (not the disk image file) to the Trash.

3.17 The disk image file (top icon) is what you double-click in order to mount the disk image, which is the volume you work with as if it were a removable disk.

As you're dragging, you see the Trash icon turn into an Eject icon, which is a helpful reminder that you're dragging the right item.

Now, the next time you double-click the disk image file to mount its disk image, a password will be required. If you access the disk image from your own account, and you stored the password in your keychain, then the disk image will use your keychain to retrieve the file. If not, you need to type the password before you can access the disk image and retrieve the files; otherwise, it remains encrypted.

Backing Up Your Files

Backing up important documents is a key part of data security for any computer user; for those of us who rely on a portable computer to conduct personal or professional business, backup is critical. Fortunately, it doesn't have to be terribly difficult or time consuming, particularly if you come up with a system for managing it.

The key to successful backup is two-fold: redundancy and distance. The process of backing up files gives you, by definition, copies to which you can refer if you have trouble with your Mac or trouble with that file. A backed-up document can even be handy in cases where you have no trouble with the file except that you saved over it or made a change that you later regret. If you have a previous version available as part of your backup scheme, you can grab it and start over.

The other thing that's important to do with a backup is to get it away from your computer. Putting discs of important data in fireproof safes or safety deposit boxes is always a good idea. Backing up to an online service can be a handy way of accomplishing both, which is one reason that Apple includes the option with its .Mac subscription service. By backing up online, you have both redundancy and distance; but the data isn't so far away that you can't get to it quickly over an Internet connection. The downside is that online storage is a lot more expensive than recordable CDs or DVDs, so it's only ideal for data that you're in serious need of backing up.

So, one good choice is .Mac and the Backup software that comes with it. If you don't want to pay for the .Mac subscription, however, you can opt for third-party backup software, or you can cobble together a system for yourself using the Mac OS and a tool such as Automator, a new tool in Mac OS X 10.4 that enables you to create automatic workflows to make your Mac take steps on its own, such as perform backups.

Backup and .Mac

Backup is software that comes with your .Mac subscription; if you are a subscriber and haven't yet downloaded it, you can get at it in a few different ways — log on to www.mac.com and click the Backup icon, or access your iDisk and open the Software folder. The Software folder is actually a link to downloadable items that Apple offers — it doesn't take away from your storage space on your iDisk. In the Apple Software folder you should find a Backup, which you can copy to your hard drive by clicking and dragging it to the Desktop or another Finder window. Double-click the disk image file and you gain access to the Backup disk image; you should see the Backup.pkg file that you can double-click to install the software.

The version of Backup at the time of this writing does not offer encryption of the data that you back up from it, even if you've encrypted your home folder. So, be aware that with very sensitive information, it's theoretically a bit less secure sitting on your iDisk. You may want to opt for a third-party backup system in situations where you need top-notch file security.

When you launch Backup, it checks for a valid .Mac account (which you need to have typed in the .Mac pane of System Preferences) and it may ask for your permission to access your keychain in order to get your iDisk password (or, failing that, it just asks for your iDisk password). Once it's connected to iDisk you see the main Backup pane (see figure 3.18).

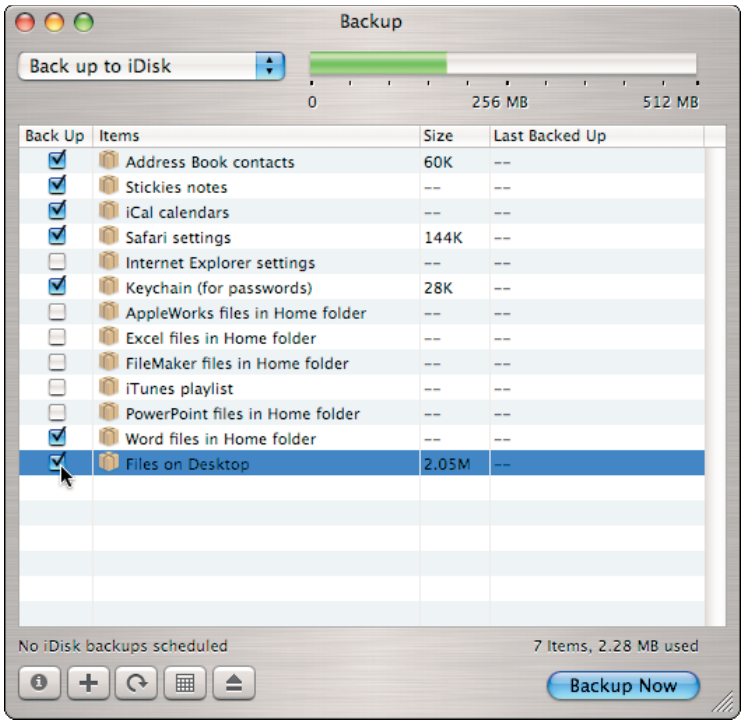
Backup understands fairly well how your Mac is organized, so it's able to be fairly specific about the items it suggests that you back up. In the Backup window, it offers a list of QuickPicks that are both convenient and suggestive. You'll notice that Backup is trying to help you pick and choose what important files you opt to back up, because it knows that the typical iDisk doesn't have a lot of space to burn.

At the time of writing, the standard .Mac account offers 256MB of space to be shared among all its tools — as you can see in figure 3.18, I paid extra to upgrade mine to 512MB.

Begin by selecting the categories of items on your Mac that you want to back up. To learn more about what's being backed up in a certain category, select it and click the information icon at the bottom of the Backup window. A drawer appears (that's the window portion that slides out from the side of the Backup window), showing you the items that Backup intends to back up.

If you don't see a category, click the plus (+) icon at the bottom of the Backup window and an Open dialog box appears; here, you can select a particular folder that you want to back up or you can even add a particular file that you want Backup to track. (For example, you might want to back up your accounting software's main database file on a regular basis.)

Once you have Backup configured with the items you want to back up, you can immediately initiate that backup by clicking Backup Now. Backup begins the process of synchronizing your files between the iDisk and your Mac. Note that this means that items that have changed on your Mac are replaced on your iDisk, including any changes you made since the last time you backed up.



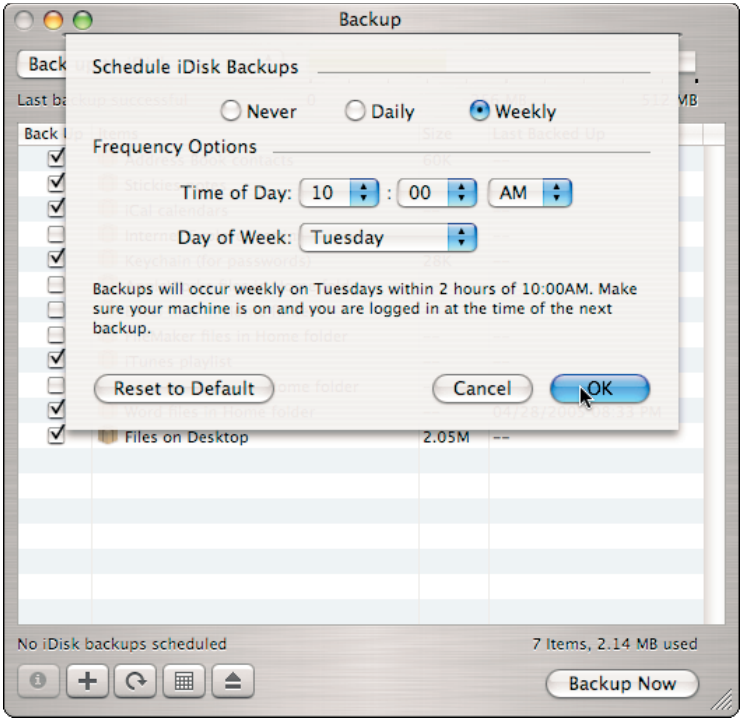
3.18 The Backup application enables you to quickly select key items you'd like to back up.

Note

This type of synchronization backup isn't always a good thing. It can overwrite files that you may prefer to have multiple versions of in different states of completion. For example, you might want to be able to access your backup version from last week because you accidentally deleted important parts of a Word document and then saved those changes. If your backup solution is exclusively the synchronization approach, then your older versions are overwritten during the backup process. So, it's a good idea to back up both online in this fashion and to disc, as described in the next section.

Along with manual backups, you can use Backup to perform scheduled backups as well. To do that, click the calendar icon at the bottom of the Backup window (actually, it looks a little like a calculator). A dialog sheet appears that you can use for scheduling your backups (see figure 3.19).

Choose whether you want to update the backup weekly or daily, and then set a time. Note that you need to be logged on to your account and your Mac needs to be turned on at that time, so take that into consideration. Click OK in the dialog sheet and your schedule is in place.



3.19 Backup can schedule itself to back up your files weekly or even daily.

Tip

Curious as to whether a backup occurred? Backup keeps a log. Choose File ➪ Show Log to see the log of backup operations and make sure that the most recent one happened as you expected it to.

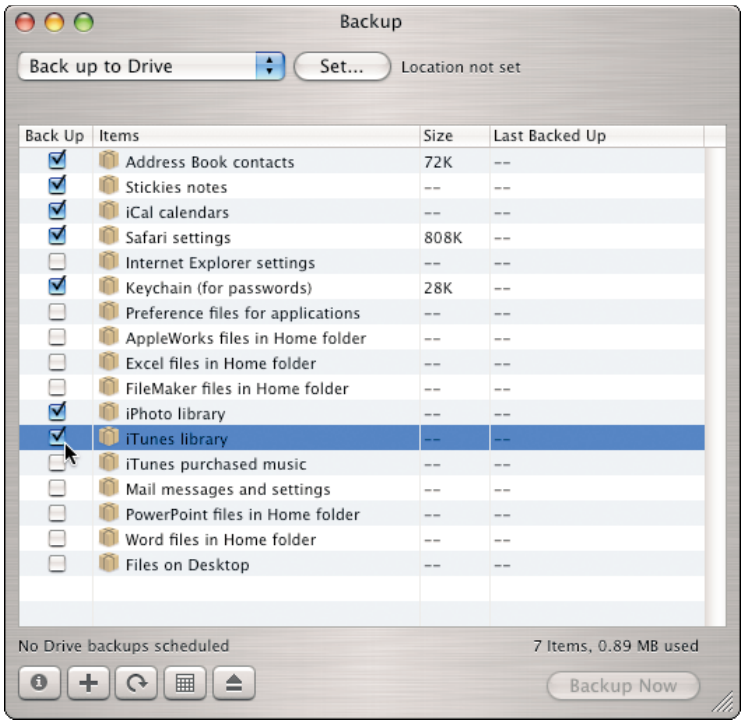
Backup to drive or disc

Backup can also back up your files either to a hard drive or to a removable optical disc if your Mac supports burning data to recordable CDs or DVDs. To configure a backup, choose the appropriate entry from the unlabelled menu at the very top of the Backup window. It may say Back up to iDisk initially. You can also, depending on the options your Mac supports, choose View ➪ Back up to CD, View ➪ Back up to DVD, or View ➪ Back up to Drive.

Note

You only see options that your Mac supports; if your Mac doesn't have a DVD-R drive, you won't see the Back up to DVD option.

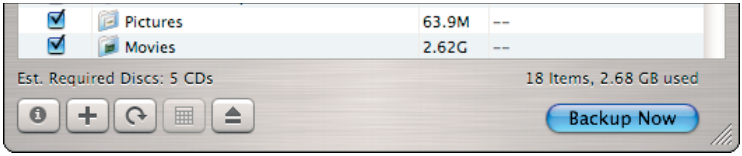
These options are all very similar; compared to back up to iDisk, you immediately find that you have a few more options in the window (such as backing up your entire iTunes library or all of your e-mail), primarily because Backup assumes that you have a lot more storage space available on a hard drive or on removable discs. Figure 3.20 shows the default options for backing up to a large external Firewire drive.



3.20 When you opt to backup to CD/DVD or hard disk, you'll see a few more default options than you did when backing up online.

For starters, look at how to back up to CD or DVD:

1. **In the Backup window, choose Back up to CD/DVD from the unlabeled pop-up menu.** You can also choose View➪Back up to CD/DVD if you prefer.
2. **Place checkmarks next to the items that you'd like to back up.** As you check items, note that the bottom of the window shows you the estimated number of discs required, as shown in figure 3.21.
3. **To add folders that aren't in the list, click the + icon.** A dialog sheet appears.
4. **In the dialog sheet, navigate to the folder that you'd like to add to your list of items to back up, highlight the folder name (or a particular document, if desired), and click Choose.** The dialog sheet disappears and you are back in the main window, with the new folder or item listed and checked.
5. **When you've made all of your selections, click Backup Now.** A dialog box appears.
6. **In the dialog box, give this backup set a name and click Begin Backup.** You see the Burn Disc dialog box.



3.21 The bottom of the Backup window shows you estimates of the discs required to store the items you want to back up.

7. **Enter a blank disc if you haven't already and, when the Burn button becomes active, click Burn.** The Backup window reconfigures to show your progress while your files are gathered and the burn process begins so that your files are written to the disc.

Note

Backup is able to use more than one CD or DVD disc if you choose more files than will fit on that single disc; it can split a file over two discs if necessary. As the backup process goes forward, you'll be prompted to insert others. Feel free to choose as many files as you want using the plus (+) button at the bottom of the Backup window.

If you choose Back up to Drive, the only difference is that you need to set the location for your backup files by clicking the Set button near the unlabelled menu at the top of the window. Here's how:

1. **In the Backup window, choose Back up to Drive from the unlabeled pop-up menu.** You can also choose View ➪ Back up to Drive.
2. **Place checkmarks next to the items that you'd like to back up.** As you check items, you'll see the total number of items and the storage space that they consume appear at the bottom right of the Backup window.
3. **To add folders that aren't in the list, click the + icon.** A dialog sheet appears.
4. **Navigate to the folder that you'd like to add to your list of items to back up, highlight the folder name (or a particular document, if desired), and click Choose.** The dialog sheet disappears and you are back in the main window, with the new folder or item listed and checked.
5. **When you've made all of your selections, click the Set button.** A dialog sheet appears.
6. **If you already have a backup location defined, you can click Open; otherwise, click Create.** The dialog sheet changes to a Save As dialog sheet.
7. **In the Save As dialog sheet, give your backup set a name (it will be a single file on the drive) and navigate to the drive and folder where you'd like the backup set stored; then click Create.** You're returned to the Backup window.
8. **Click Backup Now.** The Backup window will reconfigure itself and you'll see the progress of your backup operation. When it's done, you'll be returned to the full Backup window and you should see the message "Last backup successful" at the top of the window under the unlabelled pop-up menu.

Note

It's not terribly useful or safe to back up to your Mac's internal hard drive because that doesn't quite meet redundancy and distance requirements. However, this approach is great for backing up your files to another computer on your local network if you have a LAN, or to an external hard drive that you connect to your Mac for this purpose. Ideally, that external hard drive should be something that you leave behind, in a safe location. If not, you might want to send key files to your iDisk and back up all of your documents to a hard drive for additional redundancy.

As with online backup, you can also schedule a backup using the small Schedule button — the one that looks like a calendar page — if you want to back up to a hard drive. (Backup won't allow you to schedule a backup to an optical disc, based on the assumption that you may not be there at the prescribed time to insert one or more discs.) Again, your Mac has to be turned on and you need to be logged on to your account at the time that the backup is scheduled if it's going to happen successfully.

Restore from backup

If you get in a situation where you need to access your backed up files, you do it by switching Backup to its Restore mode. Here's how:

1. **From the unlabeled menu in the Backup window, choose Restore from iDisk, Restore from CD/DVD, or Restore from Drive in Backup, depending on which you want to do.** You can also choose those same options from the View menu, if you prefer.
2. **Then, you select the items that you need to restore in the QuickPick list; to select all items, choose Edit ➪ Check All from the menu.**
3. **With the items selected, click Restore Now.** Backup accesses the hard drive or iDisk in question (it may prompt you for a CD or DVD) and then locates your backup set. When it does, it starts asking questions about any files that you opted to restore, particularly if a matching file already exists on your hard drive (see figure 3.22).

3.22 When you restore files, you may be asked whether you want to overwrite existing files.

4. **Choose whether you want to overwrite the file or not.** Note the option Apply to All, which you can use so that you don't have to answer for each item.

That's really all it takes; follow the prompts in the case of CDs or DVDs that need to be swapped, but otherwise Backup automatically restores the files from your backed-up versions. When it's done, check your hard drive and you should see copies of the files that you've overwritten and/or restored.

Note

Backup doesn't have an option for extracting an individual file for recovery; however, if you know there are certain individual files that you specifically need to track in Backup, add those files as individual items in the list (for example, your accounting software database or client list documents). If you don't have the specific file in your list, use the dialog box shown in figure 3.22 to replace only the file that you're looking for.

Other backup solutions

A number of third-party backup solutions exist, but only the high points are listed here because I recommend a .Mac account for your portable computing anyway, and Backup is a solid solution, particularly for an individual user. That said, there are stronger backup applications worth considering, depending on your needs. Here's a quick look at the options:

- **Dantz Retrospect (**www.dantz.com**).** This commercial option is one of the more respected in the industry for completeness. The company offers a number of different versions from Dantz Desktop (for individual users) to Dantz Workgroup and Dantz Server. With Dantz, you're encourage to rotate your backup media, create multiple incremental backups, and take other important steps that ensure redundancy of your data, making it that much more likely that you'll recover from trouble. And the network versions are great for small or medium-sized offices where you want both server computers and individual computers — including portables that connect to your network — to be backed up.
- **Intego Personal Backup X (**www.intego.com**).** This is another commercial offering, aimed squarely at the individual user. Personal Backup will help you back up and synchronize between two different volumes, or it will back up to disks or even to an iDisk. It will also create compressed disk images that you can use for archival purposes and it will clone your Mac system so that it can be booted from another disk.

Note

While the backup approach taken by Apple's Backup is something of an online solution — meaning you always have a recent backup at your disposal — creating archives of your files can also be useful. You may, at some point, want to access a particular file as it was six months or a year ago — again, accounting software and databases come to mind. That's what an archive is for — it's a snapshot of your important files at a moment in time, which you store away until it's needed.

- **Synchronize X (**www.qdea.com**).** Another option that has grown up with Mac OS X is Synchronize, which is shareware (try-before-you-buy) software available online. But don't let the shareware moniker fool you — this is full-featured stuff, particularly the Pro version. Either version offers automatic backup or synchronization, while the Pro version can also create a bootable backup of your Mac system.

Cross-Reference

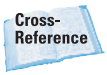
For more on synchronization of files, see Chapter 2. For more on bootable backups, see Chapter 7.

- **Dobry Backuper (www.dobrysoft.com).** It has kind of a cutesy name, but this inexpensive shareware option is a great personal backup option. It works much like Apple's Backup with the exception that you choose all your own folders and files for backing up; the software also compresses items as they're backed up so that they take up less space on the target disk.

Homegrown backup solutions

If you're not up for buying a .Mac subscription or some third-party software, that doesn't mean you should do no backup. You've still got options.

My first suggestion is to use the disk image instructions earlier in this chapter and create a special spare disk image that you can fill up with files that you want backed up. You can then take that disk image file and copy it to either a recordable disc or to an online site; if the disk image is encrypted, you can feel pretty good about copying the disk image file to any FTP location that your ISP provides for you, for example. (As a precaution, endeavor to make sure that FTP location isn't publicly available.) Or, if you have access to an external hard drive or a network, you can copy the disk image file to one of those locations.



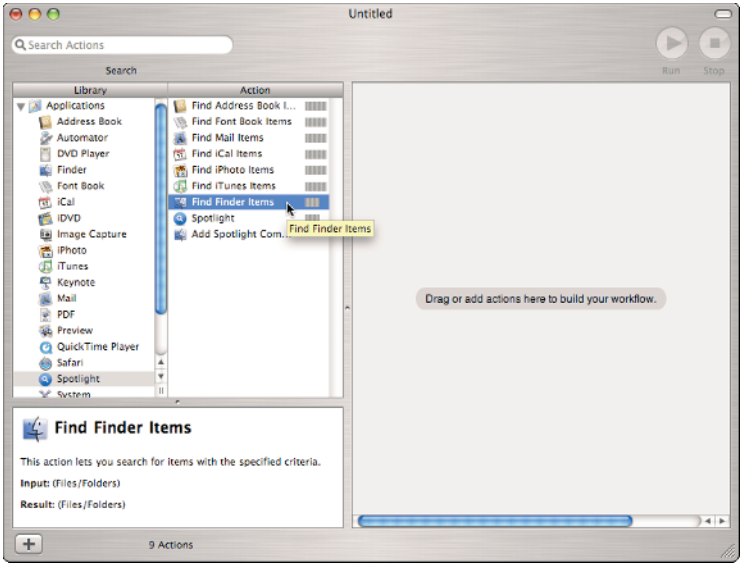
As detailed in Chapter 6, Disk Utility will create a recordable disc from a disk image, so you can create your disk image with that in mind.

Of course, what's cool about Backup and similar applications is that they automatically find files that are important to you. However, if you use the Mac OS X home folder hierarchy as it's created, you should have relatively little difficultly backing up important files — it may be as simple as backing up your Documents folder or your Photo folder and so on.

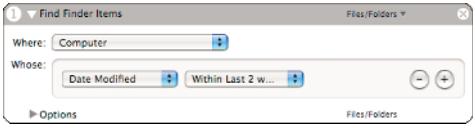
For a more sophisticated approach, you can use a tool like Automator (found in the Applications folder on your Mac if you have Mac OS X 10.4 or higher installed) to create your own impromptu backup script.

Here's one approach, which uses Mac OS X 10.4's new Spotlight search feature to gather files that have been recently modified on your Mac and then back them up to an external hard drive or a network volume:

1. **Launch Automator by double-clicking its icon in the Applications folder.** The Automator window appears (see figure 3.23), complete with a Library of items on the left side; the right side of the window is used to build your workflow, which will be the steps that Automator will undertake automatically when you run your creation.
2. **In the Library list, select Spotlight.**
3. **Click and drag the item called Find Finder Items from the Action list to the main Workflow area.**
4. **In the Find Finder Items workflow item, select where you want to search for files that have changed from the Where menu.**
5. **In the Whose menus, choose Date Modified from the first menu, and then choose a time frame, such as Within Last Two Weeks (see figure 3.24) from the second menu.**



3.23 The Automator interface includes a Library of applications; select one and a list of actions appear that you can drag into the workflow area.



3.24 In Automator, you can find files that have been recently modified.

6. **Choose Finder in the Library.**
7. **Locate the Copy Finder Items action and click and drag it to the workflow area.**
8. **In the To menu of the Copy Finder Items action, choose a location for the files you're going to back up.**
9. **Click the Run button at the top of the Automator window to see the workflow in action or choose File ➪ Save to name and save the workflow.**

This very simple example gathers all the files that have been changed in the last two weeks and copies them to a new location; you can then burn that folder to a disc, transfer it to another computer or to a network volume, and so on. You should also experiment with Automator if you go this route — there are a number of other options you can add to this script to make it more complex and complete, such as automatically creating a compressed archive, or mounting a disk image.

Save an Automator workflow as an application so that you can simply double-click it in the Finder to launch it. Choose File ➪ Save As in the Automator menu bar; then, in the Save As dialog sheet, give the workflow a name and choose Application from the File Format menu. Click Save to create an application icon for this workflow that you can use as you would any other double-clickable application.