MAKE YOUR MAC MORE SECURE

IN A WORLD WHERE SECURITY IS BECOMING INCREASINGLY IMPORTANT, WE'LL SHOW YOU WHAT TO DO TO KEEP YOUR MAC SAFE **BY CORY BOHON**

Apple already has a lot of security features baked into the Mac. From its strong, well-tested Unix foundation to the built-in privacy features of OS X, it's one of the most secure operating systems available to consumers. A lot of users, however, make mistakes in their daily usage that can severely compromise the security of their Mac. We'll show you these pitfalls and help you lock down your Mac to make your privacy, digital information, and even your hardware less likely to be compromised. We'll cover everything from user accounts to the physical security layer of your computing workflow—and we'll even throw in some iOS safety tips for good measure.

SECURING YOUR USER ACCOUNTS

It has been said that a computer is only as secure as the user. That's why we begin our journey of making your Mac more secure here: if the user level of your Mac is left unsecured, then you are vulnerable to unwanted access to your machine. Let's look at how we can make this part of your computing workflow safer.

SETTING PASSWORDS

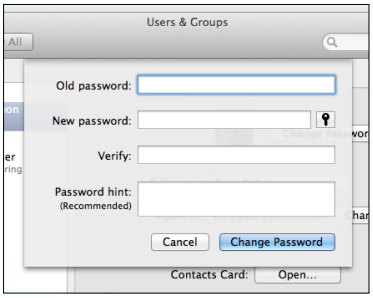
The first line of defense in any computer system is to secure your user account with a strong password. When someone has access to your user account, they have access to all of your files, your browsing history, your applications, and sometimes even your online accounts and passwords (if they are not stored securely). This is why it is very important to create good passwords and rotate them frequently.

Rotating (or changing) your passwords ensures that if someone were to get your password, it will not work once it has been changed. For system account passwords, we recommend changing them anywhere between every six months to a year.

If you have never set a user account password in OS X, then your system can be easily accessed by just specifying your username. This can be fixed by setting up your password for the first time. To do this, open System Preferences by going to the Apple menu and selecting "System Preferences." Next, navigate to Users & Groups > Your User Account > Password. Once there, click on the "Change/Set Password" button.

In the dialog that appears, enter your old password (if there is no old password, then leave this field blank), then type in your new password and verify it. You can optionally set a password hint, but ensure that the password hint only jogs your memory about the password you've set and does not include any information about the content of your password.

When you're ready to secure your account, click on the "Change Password" button. Remember this password, as you'll need it to log into your computer and to make changes to your system.



Setting a password in OS X is a sure-fire way to curb unauthorized access to your computer.

FileVault starts off by giving you a recovery failsafe passcode that can be used in the event you forget your user account password.

ENABLING FILEVAULT

Setting a password is essential, but there's another oft-forgotten piece of the puzzle: your hard drive. Even though you've got a password set on your account, it controls only your login and access to your account. Files in your account are still written to the hard drive in plain sight. If someone is able to get physical access to your Mac, then they can easily read the files from the internal drive by connecting it to another machine while your Mac is in Target Disk Mode (http://bit.ly/ml_targetdisk), or by removing the drive and placing it in another computer.

To solve this, Apple introduced FileVault. This feature of OS X encrypts your entire drive, files and all. This means that if someone were to gain access to your hard drive, they would not be able to read your files. The only way that the drive can be unencrypted is if someone had access to your OS X user password or had access to the recovery key.

Setting up FileVault to encrypt your Mac is an easy process. To enable it, visit System Preferences > Security & Privacy > FileVault. Once here, click the "Turn On FileVault..." button. After doing this, you will be presented with a "safety net" passcode. Write down and keep this passcode in a safe place. If you forget your user account password, this passcode can be used to decrypt your Mac's hard drive.

On the next screen, you have the option to store your recovery key with Apple. If you choose to store your password with Apple, then you will be able to contact Apple to retrieve the passcode should you forget it in the

future. This added level of safety means that you can still access your files, even in the worst-case scenario. After selecting your options and filling in the security information, you will be prompted to restart your Mac. This will begin the encryption process.

Upon restarting, your Mac will begin the lengthy process of encrypting your hard drive and all of its files. This process can take quite a while, so you may want to start this in the morning and let it run all day. Depending on the size of your drive, it can take upward of 12 hours or more. The wait is worth it: your Mac will be better protected once the encryption process has completed.

One difference with your Mac that you will notice is the startup: on the Apple boot screen, you will now be prompted to sign into your Mac's user account. This is due to the fact that your Mac must now decrypt the hard drive before booting into OS X.

You will need to restart your Mac for the changes to take effect.

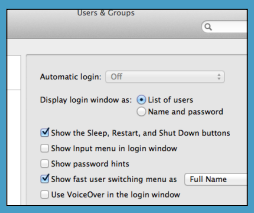
After restarting, your Mac will begin encrypting the internal drive, which can take quite some time.

3 SYSTEM PREFERENCES TO PROMOTE SECURITY

With a little help from System Preferences, you can further lock down your Mac to prevent unauthorized access to your computer.

TURN OFF AUTO LOGIN

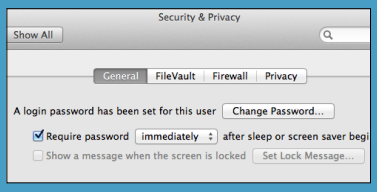
Having your Mac automatically log into your user account poses a huge security risk. You can reduce this security risk by visiting System Preferences > Users & Groups > Login Options. Once there, ensure that the drop-down menu option for "Automatic Login" is set to "Off." Note that if you've turned on FileVault, then Auto Login will be turned off by default.



Turning off Automatic Login limits unauthorized access to your Mac to those with knowledge of your user account password.

TURN ON PASSWORD REQUIREMENTS

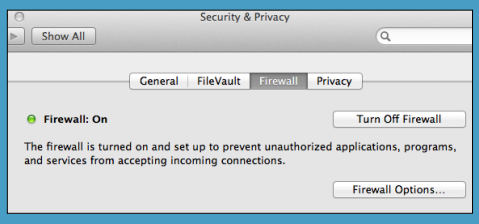
When you leave your Mac unattended without any password requirements, then anyone can easily walk up to your machine and access the entire computer, files and all. To curb this issue, OS X features password requirements that can be set in System Preferences > Security & Privacy > General. Ensure that the checkbox for "Require password immediately after sleep or screen saver begins" is checked so that you'll be required to enter your password in order to start using your Mac again.



Block unauthorized access by automatically locking down your Mac when you've stepped away from it.

TURN ON FIREWALL

While the router on your network provides a firewall to the outside world via the Internet, whenever you're on a public network, your Mac (just like all other computers) is vulnerable to network trickery. To enable the firewall, visit System Preferences > Security & Privacy > Firewall. Once there, click on "Turn On Firewall." From this point on, any unauthorized incoming network connections will be blocked. We especially recommend turning this on when using a portal Mac over an open, shared Wi-Fi network connection.



Enable the OS X Firewall to turn away unauthorized incoming network connections.

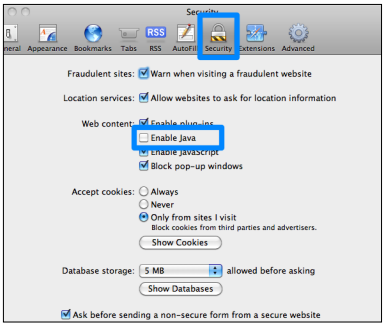
SECURING YOUR WEB BROWSING

Obviously, web browsing is one of the biggest uses of modern computing. We shop online, listen to music online, and even communicate with friends online. Most online vulnerabilities on the Mac come from social-engineering tactics designed to make you believe something is legitimate, even though it's not. We'll walk you through ways to battle these tactics and remain safe online.

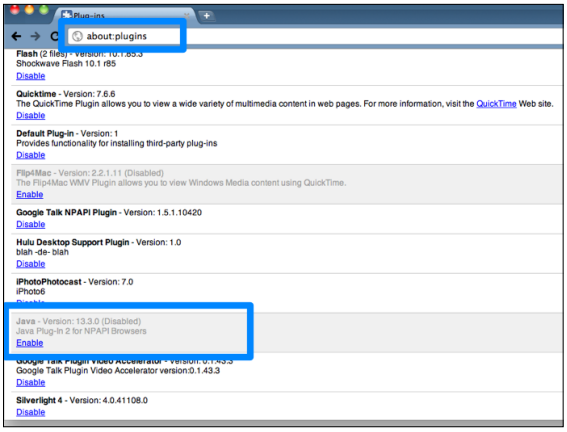
DISABLING JAVA

The Mac has had very few bouts with viruses or trojans/malware (applications designed to look like something they're not), but those that have sprung up have often originated from Java running in a web-browser environment.

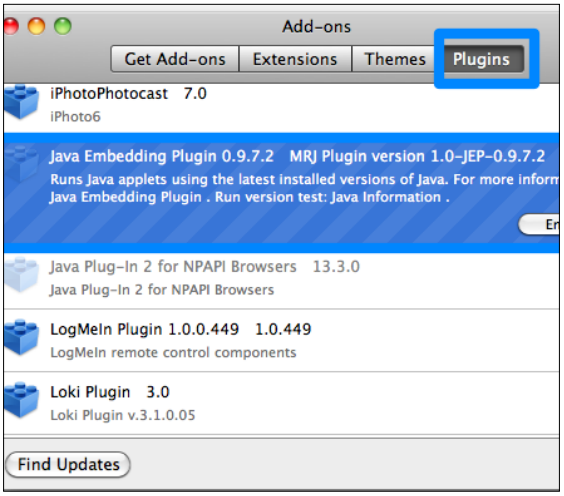
Java is a programming language that has been all but phased out by many mainstream websites, but the Java Applets (small web programs) that Java executes in the browser can pose a security risk as websites could install malware or other harmful pieces of software onto your Mac. After disabling Java, any applets that try to load a Java-based program in the browser will be denied access. You can always re-enable this feature for trusted websites, but it's best to leave it off for normal web browsing.



IN SAFARI: To prevent Java applets from executing on pages when browsing the web in Safari, simply head over to Safari > Preferences > Security, and uncheck the box labeled "Enable Java."



IN CHROME: Google makes disabling various plugins easy with Chrome, as well. To start, open Chrome, and type in "about:plugins" into the Omnibox (address bar). From the page listing all of the installed plugins, locate the plugin called "Java" that has a description of "Java Plug-In 2 for NPAPI Browsers." Click the Disable link and Java will be disabled in Chrome.



IN FIREFOX: In Firefox you'll need to navigate to Tools > Add-ons > Plugins. Once there, locate the plugin called "Java Embedding Plugin." Click it, and then select the Disable button that appears. Depending on the version of your browser, there may also be a plugin called "Java Plug-In 2 for NPAPI Browsers" that will also need to be disabled.

DOWNLOADING FILES

Before downloading any file, it's important to keep two rules in mind: first, always check the address bar of your browser to ensure that you trust the site you're downloading the file from.

The next rule of thumb is to not download software via torrent websites. Doing this can greatly compromise the security of your system. In fact, one of the main causes of Mac malware is sites offering downloads of pirated software. With torrents, you cannot verify the validity of the source, and can therefore not trust the download.

Most Mac malware spreads through torrent sites offering pirated software. You cannot verify the validity of files downloaded through torrent files.

MAXIMIZING PRIVACY

When browsing the web and entering your personal information, it's always a good idea to know how to maximize your privacy and security. Just remember that anyone, in any location, can easily set up and operate a website. This is both good and bad: good because it allows a free market where anyone can express their creativity, but bad because social engineers can take advantage of that to create fake or fraudulent sites that can steal your information. Here are two ways to greatly increase your privacy and security when browsing sites.

HTTP vs. HTTPS

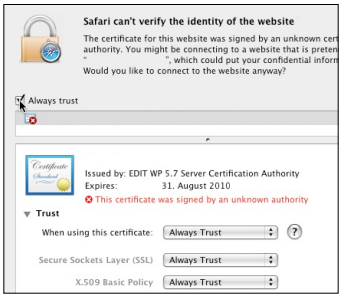
Before entering any personal or confidential information (credit card info, social security numbers, etc.) on a site, you should always look to the address bar in your browser.

If the address begins with HTTP, then this means that your browsing session with that particular server is *not* secured. However, if the address begins with HTTPS (HTTP + Secure), then your connection is encrypted end-to-end. Usually banks and online stores operate over HTTPS because they transmit sensitive information, such as account numbers. You should never submit sensitive information over an HTTP connection.

Invalid Certificates

With HTTPS traffic, websites must install an SSL (secure sockets layer) certificate that promotes encryption and decryption of information sent to and from the server and your web browser. These certificates are given out by a certificate authority after the website owner has been verified.

Safari (and other browsers) include checks to make sure that the SSL certificate that a website presents over an HTTPS connection is valid and not expired. If the certificate has expired, you will be alerted. When a certificate has expired, it is usually a good indication that the website you are trying to browse is fraudulent, except in rare cases where the website owner forgot to renew the certificate. Either way, you should never submit sensitive information to a website with an expired certificate.



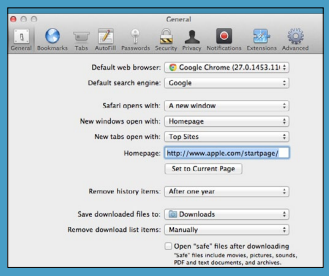
When an SSL certificate on a website has expired, Safari and other browsers will alert the user.

3 SAFARI SETTINGS TO PROMOTE SECURITY

Are you using Safari to surf the web? If so, here are a few extra precautions you can take.

OPEN "SAFE" FILES

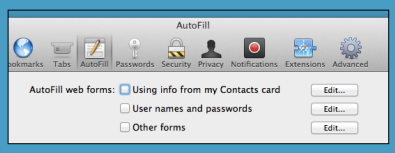
By default, Safari will automatically open files that have been downloaded from the Internet. According to this Safari preference, only "safe" files will be opened automatically. However, we always prefer to have the last word over which files are opened on our system. You can disable this feature by visiting Safari > Preferences > General, and unchecking the box labeled "Open 'safe' files after downloading."



Disable the Safari feature that causes "safe" files to be opened after download completes.

TURN OFF AUTOFILL

It has been shown in the past that websites can steal your data using hacks that trick Safari (and other browsers) into submitting user data through its AutoFill feature. To combat this, you can disable the AutoFill feature of Safari by visiting Safari > Preferences > AutoFill, and unchecking the boxes for "Using info from my Contacts card," "User names and passwords," and "Other forms." For passwords, we've found that it's best to use a password manager like 1Password or LastPass instead of the browser's built-in password manager. You can learn about using 1Password to manage your usernames and passwords at http://bit.ly/ml_1pass and learn about LastPass at http://bit.ly/ml_lastpass.

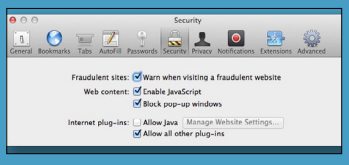


Disable AutoFill in the browser so that fraudulent websites won't have a chance to capture of your personal data.

FRAUD WARNING

Safari (and most modern web browsers) includes a feature that periodically checks an online database of fraudulent websites and compares the sites you visit against the database. If a website you visit appears on the list of phishing (or other scam) websites, then you'll be alerted, and the page will not automatically be loaded.

We recommend turning on this feature by going to Safari > Preferences > Security, and checking the box labeled "Warn when visiting a fraudulent website." Note that this only protects against known fraudulent websites.



When visiting a website that is on Safari's list of fraudulent websites, you'll be alerted to your actions.

SECURING YOUR FILES

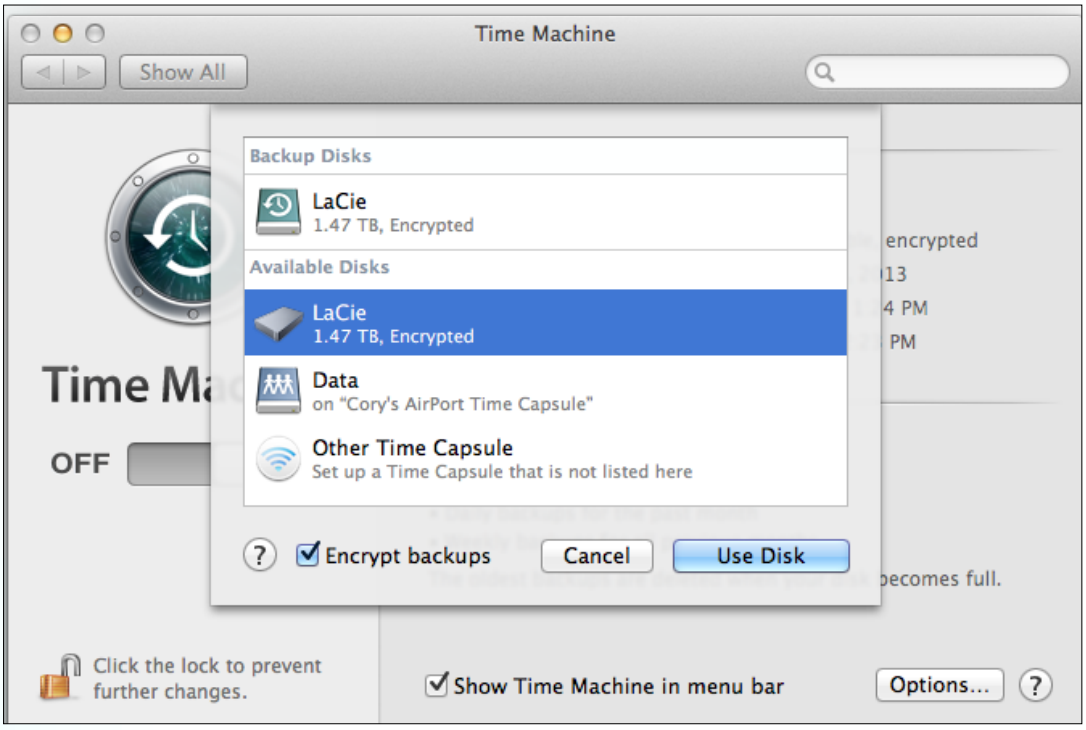
We've shown you how to secure your user account and how to protect yourself from fraudulent website trickery, but you keep files on external drives as well, be it on a Time Machine backup or a thumb drive that you carry around.

PROTECTING YOUR TIME MACHINE BACKUPS

Even if you have enabled FileVault on OS X, your Time Machine backups will not be encrypted. For OS X to encrypt your Time Machine backups, you'll need to opt-in; unless you explicitly tell Time Machine to encrypt your backups, then the files from your Mac will be backed up in a way that lets anyone access your files should you lose or misplace your Time Machine backup drive.

To turn on this feature, visit System Preferences > Time Machine > Select Disk. Once here, select your Time Machine backup drive (or select a new drive, if you haven't set up Time Machine before), and ensure that the "Encrypt backups" option is selected before clicking "Use Disk."

With encryption turned on, Time Machine will encrypt the drive that your backups are stored on, securing your backup files secured with a password that only you know. Time Machine will automatically remember this password so that you don't have to re-enter it each time a backup is created.



With Time Machine, you can encrypt the backup files that are created on an external drive.

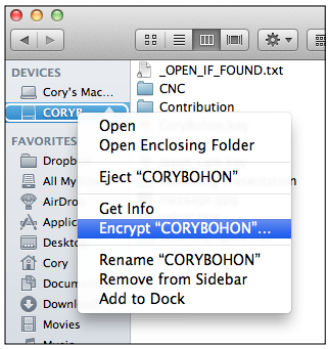
ENCRYPTING YOUR EXTERNAL DRIVES

If you're like us, then you've got a ton of USB thumb drives lying around with gigabytes of data stored on them. These drives can contain sensitive documents, or other information that you don't want to fall into the wrong hands. OS X includes a feature that can help protect your data no matter what type of external drive you have—whether it's a thumb drive or an external hard drive.

To begin, plug the external drive into your Mac and wait for it to be mounted in the Finder. Once it appears in the Finder, right-click on the drive and select "Encrypt [drive name]."

In the dialog that appears, you'll enter an encryption password (this is the password that you'll need to enter in order to unencrypt and mount the drive in the Finder). Next, verify that password, and type a password hint. The password hint is required in this case. When you're ready to encrypt your drive and all the files on it, select "Encrypt Disk."

After the encryption process is complete, you'll be able to eject the drive. When reconnecting the drive to your Mac, the drive will not be mounted automatically. Instead, you'll need to click on it in the Finder, then enter the password you entered during the encryption process.



Encrypt any drive by right-clicking it in the Finder and selecting "Encrypt [drive name]."

In the encryption dialog, type your password, and verify it.

In order to mount an encrypted disk in the Finder, you'll need to enter your encryption password.

CREATING STRONG PASSWORDS

Use these handy hints to come up with passwords that cyber-scoundrels are less likely to crack.

The more convoluted your password is, the harder it is to crack. Most passwords being cracked today rely on sophisticated computer programs that utilize dictionaries containing common words. Good passwords (or passwords that are harder to guess for both computers and humans) follow some pretty simple rules.

Your password should be at least eight characters long. Longer passwords mean that computer password-cracking programs take longer to crack them. This is a deterrent from all but the most sophisticated cracking programs.

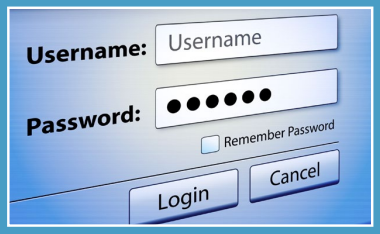
Your password should not contain your real name, company name, or username. This information is easily obtainable from websites, social networks, and through social engineering. Ensuring that your passwords don't contain this information is one step toward creating a more secure password.

Your passwords should not contain dictionary words or complete words. Dictionary words and complete words are easy to guess. If you insist on using complete words, then vary the casing (making random characters of the word upper or lower case), or mix common characters with numbers. Example: cookie could be c0Ok1E, where the Os are replaced with zeros, and the l is replaced with a number one.

Each of your passwords should be significantly different. This is a common mistake among users: using one password across multiple accounts and online services. This lessens your security, even if you have a strong password. If one account is compromised, then all of your accounts can easily be compromised.

Your passwords should contain characters from four different categories. These categories are: uppercase letters, lowercase letters, numbers, and special symbols (like ~ , @, !, etc.).

Remembering passwords can be difficult, but you can create strong and easily remember-able passwords by creating an acronym from an easy-to-remember piece of information. For example, "My anniversary is 19 August 2010." Guided by that phrase, you could come to the password of "mAi19/Aug10."



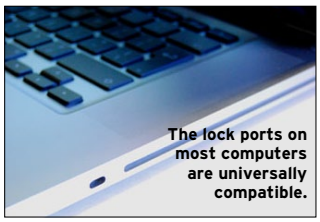
PHYSICAL SECURITY

We've covered all our bases in terms of data security, but what about the physical security of our machine? What happens if we lose it, misplace it, or it gets stolen? Fortunately, there are a few things you can do to combat these scenarios, as well. Let's take a look at the options.

LOCK IT UP

Most all Macs include what's known as a "Kensington Lock" port. This security port allows you to lock down your Mac using a simple cable that's similar to a bicycle lock. You can get very fancy locks with all kinds of bells and whistles, but simple combination or key-access locks work just fine.

To lock your Mac down, just insert the lock into the lock port, then follow the instructions for closing the lock. Most locks feature long cables that will need to be wrapped around a sturdy surface (such as a table leg), making it difficult for a thief to easily untether your Mac and walk away with it.



The lock ports on most computers are universally compatible.

HARDWARE PASSWORDS FOR MAC

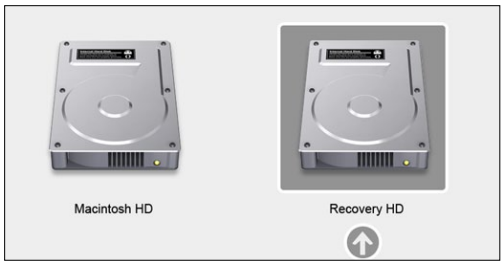
We've locked down the user account in OS X, encrypted the hard drive, and even encrypted the Time Machine backup from our Mac. What more could be done? Well, there is one other area that is still vulnerable to a physical theft: the thief could erase the hard drive, leaving them with a shiny new Mac.

"How can we combat this?" you might ask. Fortunately, Macs have a feature called Firmware Password Protection. This is a password that can be enabled to keep thieves from booting to another startup disk, booting into recovery mode, or even from accessing other firmware-based utilities like target disk mode.

To enable the use of a firmware password, you'll need to boot into the Recovery partition on your Mac (or the install DVD if you have an older Mac) by pressing the Option key on boot. Once you see the "Recovery HD" partition listed (or your Install DVD), select it.

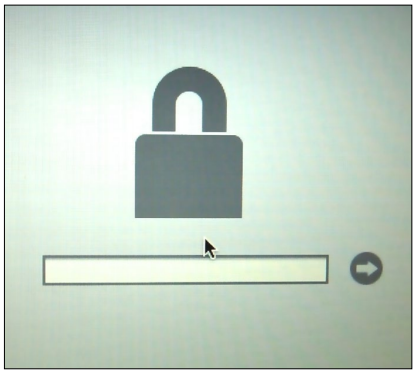
Once booted into the OS X Recovery drive (or OS X Installer), select Utilities > Firmware Password Utility. Select the button labeled "Turn On Firmware Password..." and then proceed to enter a password and verify it.

Now whenever you restart your Mac while holding down the Option key, you'll be prompted to enter your firmware password. If you wish to disable this feature, follow these instructions again, deselecting the option to "Require password to start this computer from another source" in the Firmware Password Utility.



Boot into the "Recovery HD" partition, or insert your Install DVD to proceed to the OS X installer.

The Firmware Password Utility lets you set your firmware password to control access to the firmware options on your Mac.



You'll need to enter your firmware password to boot your Mac to another source except the normal Mac volume.

USING FIND MY MAC

So, you've lost your Mac? Well, no worries—if you have iCloud and Find My Mac enabled in advance. To set up Find My Mac, visit System Preferences > iCloud, and check the box labeled "Find My Mac." If you do not have an iCloud account, you will be prompted to create one.

If you lose your Mac (or it gets stolen), then you can go to www.icloud.com and attempt to track it. On the iCloud website, click "Find My iPhone," and then wait while your devices populate the listing on the left-hand side. Once your device appears, select it. If a location has been found, then it will appear on a map; otherwise you can sign up for location alerts when your Mac reports to iCloud. In the upper right-hand corner of the screen, you'll have options for your Mac: you can make your Mac play a sound, lock it, or erase it.

Note that Find My Mac works a little differently than Find My iPhone. If your Mac is found (or a thief tries to use it), it must actively connect to the Internet in order for iCloud to report its location. Also, because Macs don't have GPS, an exact location is all but impossible. However, iCloud will do a decent job reporting the location based on the network connection your Mac is connected to.

When your Mac is lost or stolen, you can attempt to track it down by visiting www.icloud.com and signing into your iCloud account.

Enable Find My Mac in advance, otherwise you'll be searching for your Mac the old-fashioned way.

MAKE YOUR iOS DEVICE MORE SECURE

iOS devices are already pretty safe from outside meddling, but it never hurts to be cautious. Follow these steps to keep your iPhone, iPad, and iPod safe.

SETTING A PASSCODE

Just like with OS X, you can lock down your iOS device, as well. To do this, visit Settings > General > Passcode Lock, and tap on the button labeled "Turn Passcode On."

You'll then need to specify and repeat a 4-digit passcode that will be used on the Lock Screen of iOS in order to gain access to your iOS device. This can keep a thief from using your device, or a nosy person from perusing your data. It'll also keep your important stuff secret if you were to lose your phone or tablet.

Set a 4-digit passcode that will be used to unlock your device for use.

ENABLE FIND MY iPHONE

Find My iPhone is just plain useful. There's no reason that anyone should not have this feature enabled at all times; it makes finding your device super-easy.

To enable Find My iPhone, visit Settings > iCloud, and turn on the switch for "Find My [iPhone/iPod/iPad]." If you do not have an iCloud account, you'll be prompted to create one. Once this feature has been enabled, you can track your iOS device just like your Mac on iCloud.com's Find My iPhone section.

Once enabled, you can track your iOS device on icloud.com.

FRAUDULENT WEBSITE WARNING

Just like Safari on the Mac, Safari for iOS includes many security features, including the fraudulent website warning feature that is available on OS X. To enable this feature, visit Settings > Safari, and turn on the switch for "Fraud Warning."

Like OS X, iOS will periodically download a database of known fraudulent (or phishing) websites known to do harm. When you visit one of these sites in Mobile Safari, you will be warned about your action.

Fraudulent website warnings help protect unsuspecting users when visiting potentially harmful websites.