Lock Down Your Mac

by Mike Sullivan | Cove Apple Club | April 9, 2014

You can take some quick, easy steps to help protect your Mac in case of physical theft and to aid in its recovery if it is lost or stolen.

These procedures are a must for any portable Mac (MacBook Air or MacBook Pro), and are strongly recommended for Mac desktops as well (iMac, Mac mini and Mac Pro).

Enable boot-up and sleep/wake password:

1. On your Mac, click the Apple menu and choose System Preferences

2. Click the Security & Privacy pane, then click the General tab

3. Click the little padlock icon at the lower left corner of the General pane, then enter your Mac's admin password and click Unlock. (The admin password is the password you must sometimes enter when updating or installing software.)

4. Tick the checkbox for "Disable automatic login." This requires you to enter your Mac's admin password whenever your Mac boots up.

5. Tick the checkbox for "Show a message when the screen is unlocked."

6. Click the "Set Lock Message…" button.

7. In the dialog box, enter your name on the first line followed by "— REWARD FOR RETURN."

8. **Hold down the Option key and press Enter to start a new line**, then enter your contact phone number and email address.

9. Click OK to close the Set Lock Message dialog box.

10. Tick the checkbox for "Require password…," and choose "immediately" from the pop-up list for "after sleep or screen saver begins."

11. Click the little padlock icon at the lower left corner of the General pane to lock in your new settings.

Make sure to keep a secure, replicated, encrypted, off-site, backed-up copy of your Mac's admin password. Ideally, this will be kept in a Secure Note inside the 1Password app on your Mac, iPhone or iPad.

If you lose this password, it will be very difficult to regain access to your Mac, to install or update new software, or to make some System Preference settings changes, so keep this password safe, secure and backed-up *somewhere OTHER* than on your Mac.

Enable Find My Mac

Apple's iCloud service can help you locate your Mac if it is lost or stolen. The iCloud service Find My Mac uses geolocation and remote telemetry over the Internet to help you or law enforcement personnel find your Mac if it is stolen, so long as it is able to connect to a Wi-Fi network and Internet connection.

To enable Find My Mac:

1. On your Mac, click the Apple menu and choose System Preferences

2. Click the iCloud pane. If you don't already have an iCloud account, follow the prompts to create a new iCloud account along with an iCloud email address. Be sure to use a strong, long, unique password for your iCloud account, and memorize it.

3. In the iCloud preferences, scroll down to Find My Mac.

4. Tick the checkbox for Find My Mac, then click Allow.

5. Quit System Preferences.

6. To test the Find My Mac feature, open Safari and go to **www.icloud.com**. Log in to iCloud using your Apple ID (or iCloud email address) and password, then click "Find My Mac." Use the drop-down menu under "All My Devices" along the top of the screen to view the location information for each of your Apple devices.

Enable Firmware Password

If your Mac is lost or stolen, a bad guy with enough Apple knowledge and resources may be able to boot up your Mac and gain access to your data even if you have a boot-up password enabled as described above. This is possible using an advanced technique Apple has built into OS X through a feature called "Recovery Partition," or by booting your Mac from an external hard disk.

However, you can enable a second, *unbreakable* level of boot-up protection on your Mac by enabling the use of a **Firmware Password**, which prevents access to your Mac via the Recovery Partition or an external boot drive. Here's how:

1. Shut down your Mac. From the Apple menu, choose "Shut down…," then click Shut down

2. Wait five seconds, then press the power button to start up your Mac.

3. As soon as you press the power button, *press and hold down* Command-R. That means you should press the Command key (⌘) and the "R" key at the same time.

4. Continue holding down Command-R while your Mac boots. After the Apple logo is displayed for about 10 seconds, your Mac will boot into the Recovery mode and the OS X Utilities menu will be displayed.

5. From the OS Utilities menu, click Utilities, then choose "Firmware Password Utility."

6. A dialog box will appear stating "Password protection is off." Click Turn On Firmware Password…

7. Enter your Mac's admin password, the same password you had set and used in the first section of this guide. There's no point in trying to create and remember another unique password for this one unlikely-to-ever-be-used function, so just re-use your Mac's admin password.

8. Re-enter your Mac's admin password in the Verify field of the dialog box, and then click "Set Password."

9. Click Quit Firmware Password Utility.

10. From the Apple menu, choose Restart to force the settings into effect. Your Mac will boot up normally.

Make sure to keep a secure, replicated, encrypted, off-site, backed-up copy of your Mac's Firmware password. Ideally, this will be kept in a Secure Note inside the 1Password app on your Mac, iPhone or iPad.

For more information:

Protect your Mac with a Firmware password (The Instructable):

> `http://goo.gl/9QRVCg`

How to protect your Mac from potential theft (Jeff Reifman):

> `http://goo.gl/1KKLG5`

Add a custom lock message in OS X (OS X Daily):

> `http://goo.gl/x90RIo`