MacPhoneHome™

Tracks & Locates Missing Computers

INSTALLATION GUIDE

OS X Ver 3.0

Tiger Compatible

Brigadoon Software Inc
143 Main Street
Nanuet, New York 10954
Tel: +1-845-624-0909 _ Fax: +1-845-624-0990
Website: www.brigadoonsoftware.com

INSTALLATION GUIDE FOR MacPhoneHome™

THEFT RECOVERY SOFTWARE

INTRODUCTION

This manual will help authorized users track and locate Apple computers protected with MacPhoneHome™ software. The proper installation and configuration of MacPhoneHome™ is critical to the recovery process.

OVERVIEW: HOW MACPHONEHOME™ WORKS

Every computer connected to the Internet has its own Internet address called an "IP Address." An IP Address is a set of four numbers separated by 3 decimals. (*i.e., 255.255.255.255*) Your ISP (Internet Service Provider) controls a group of IP Addresses that it, in turn, assigns to its customers.

Dynamic IP Addresses

Most people receive a "dynamic IP Address" when they dial up their ISP. A dynamic IP means that every time you connect to the Internet, your ISP "loans" you an IP address for the duration of that connection. The next time you connect to the Internet through that same ISP, you will receive a new IP Address.

Static IP Addresses

If you connect to the Internet via an ISDN, DSL, Cable, Satellite, T1, T3 or some other type of high-speed connection, you probably have a "Static IP Address." A static IP Address means that your ISP assigns you the same IP address every time you connect to the Internet. It does not mean you "own" the static IP Address (it's still controlled by your ISP); it means you have the right to its ongoing use.

ISP Logs

ISPs keep records of who uses what IP Address and at what time (if it's a dynamic IP Address), and to whom they assign a static IP Address. MacPhoneHome™ contains a stealth email application that sends your pre-configured recovery information via proprietary protocol to an email address of your choice (including web-based email).

Included in that email sent by MacPhoneHome™ is your ownership and contact information, as well as the IP Address from which that stealth email was sent. From that information, it is possible to trace the message back (via the IP Address) to the ISP that controls that IP Address and obtain location information for the lost computer. With this information, law enforcement can obtain the necessary warrant to recover your stolen computer.

INSTALLATION

This section covers proper installation and configuration. The examples used here are for the installation of MacPhoneHome Pro™ for MAC OS X. The MacPhoneHome™ install wizard is a menu-driven application. Simply follow the directions provided by the installer.

IN ORDER TO PROTECT YOUR PROPRIETARY DATA AND TO PROVIDE YOU WITH THE HIGHEST PROBABILITY OF RECOVERY OF YOUR COMPUTER SHOULD IT BE LOST OR STOLEN, WE RECOMMEND THAT YOU USE THE SECURITY PROTOCOLS LISTED IN THE APPENDIX OF THIS DOCUMENT.

Image1 MacPhoneHome™ Installer.

MacPhoneHome™ uses a Sit archive. To begin Installation double click the macph_v3.0.sit file. This will unstuff the installer file called MacPhoneHome – V3.0.mpkg in the same folder.

Double Click on MacPhoneHome – V3.0.mpkg to begin installation.

Image 2 Welcome Screen.

Click on the Continue button to continue installation.

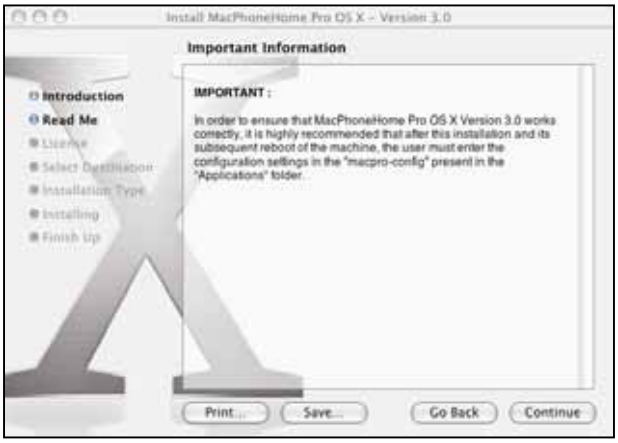


Image 3 Information Screen.

This Information Screen will appear.

IMPORTANT: This screen reminds you that YOU MUST ENTER THE CONFIGURATION SETTINGS IN THE "macpro-config" IN THE APPLICATIONS FOLDER AFTER YOU RESTART THE COMPUTER AFTER INSTALLATION.

Click on the lock to login as "Continue".

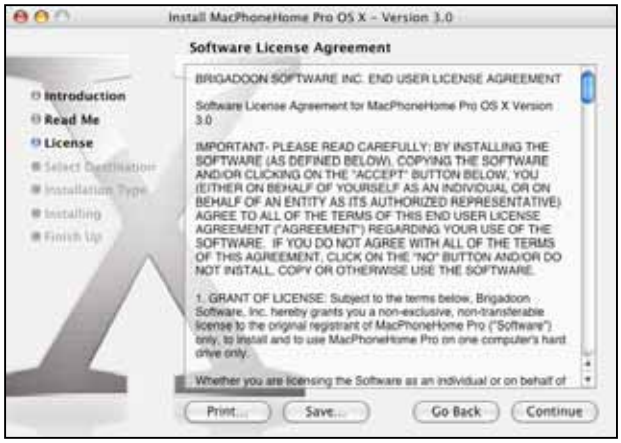


Image 4 License Agreement

The MacPhoneHome™ license agreement should be read in its entirety to insure that the registrant understands the legalities of using MacPhoneHome™ and agrees with the terms and conditions of using MacPhoneHome™ software.

Click "Continue" to bring up the Acceptance Screen.

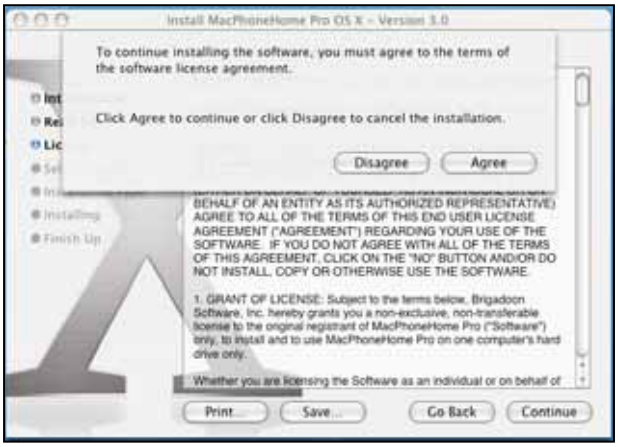


Image 4A License Agreement Acceptance

You must then click on "Agree" in order to install MacPhoneHome™ and continue the setup process.

If you do not agree with the End User License Agreement, click "Disagree" and the installation with terminate.

Image 5 Destination Select

You must then choose where to install MacPhoneHome™ (the default hard drive), and then click on "Continue" in order to install MacPhoneHome™ and continue the setup process.

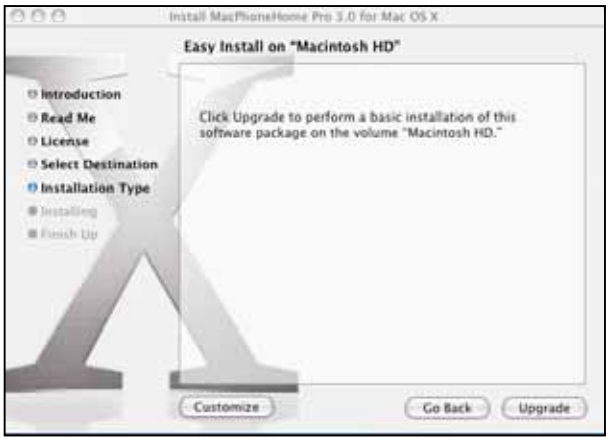


Image 6 Install/Upgrade Select

You must then complete the installation of MacPhoneHome™ by clicking on "Install" in order to install MacPhoneHome™ and continue the setup process.

NOTE: If you are performing an upgrade of MacPhoneHome™, an "Upgrade" button will appear in lieu of the Install Button. This is an acceptable variation.

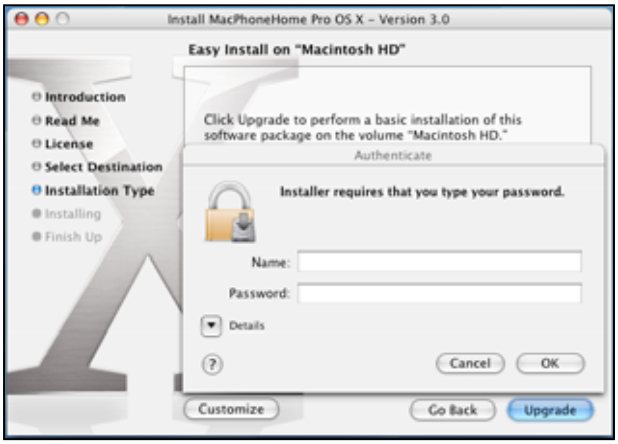


Image 7 Authentication Screen

MacPhoneHome™ requires that you use your regular Administrator Name and Password to allow installation.

[NOTE: The previous versions of MacPhoneHome™ required you to log in and install from the "Root" or "System Administrator" account. This is no longer required in Version 3.0]

Click "OK" in order to continue the installation process.

Image 8 Restart Notification Screen

MacPhoneHome™ will restart your computer after installation. BE SURE YOU'RE READY TO RESTART YOUR COMPUTER IMMEDIATELY AFTER THE INSTALLATION.

Click "Continue Installation" in order to continue the installation process.

Image 9 Restart Screen

MacPhoneHome™ will now complete the installation process and provide this screen indicating that installation was successful.

Click "Restart" in order to restart your computer and begin the configuration process.

CONFIGURATION

IMPORTANT!!

The ownership information you provide in the MacPhoneHome™ configuration box is the information that is sent to your designated email address. It is also the same information you will turn over to the police in the event your computer is lost or stolen. It is important that you enter accurate and truthful information in the configuration process. The police will use this information as a basis to attain a court ordered search warrant to retrieve your property. Less than accurate information may result in a search warrant application being denied.

AFTER INSTALLATION, YOU WILL NEED TO REBOOT AND CONFIGURE MACPHONEHOME™.

How MacPhoneHome™ Works

MacPhoneHome™ contains a stand-alone stealth email application that sends your pre-configured recovery information via proprietary protocol to the email address of your choice (including a web-based email address).

Configuration involves two tasks: (i) providing the email address to which you want the information sent; and (ii) ownership information essential to the recovery process. Therefore, it is important that you obtain all the information required prior to beginning the configuration process.

Figure 10 MacPhoneHome™ OS X Configuration.

In order to configure MacPhoneHome™, launch "macpro-config" (/MAC HD/Applications/)

NOTE: Your will need to use your Administrative account Name and Password in order to access this file.

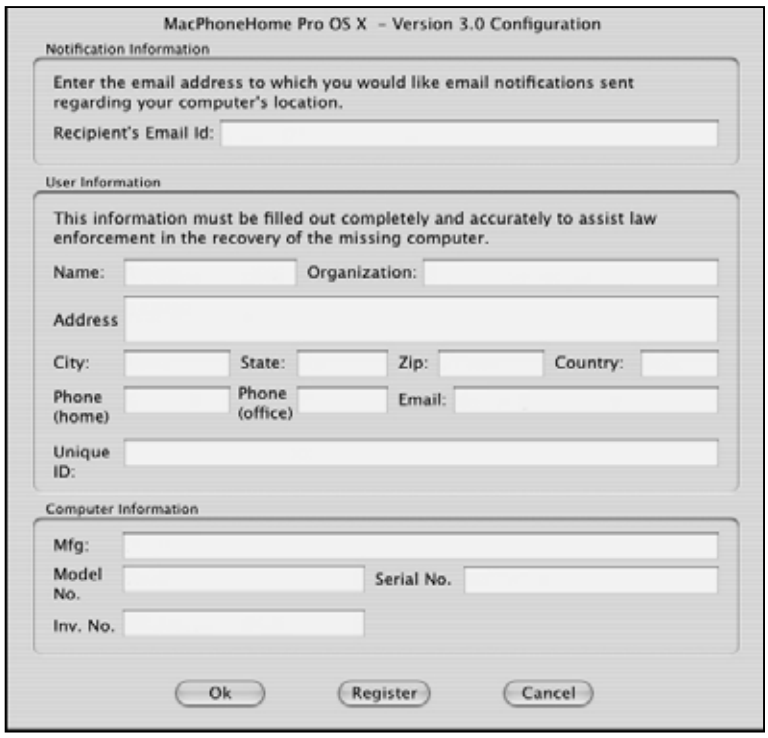


Figure 11 MacPhoneHome™ OS X Configuration.

The screen (figure 11) shows the configuration and identification information that is embedded into MacPhoneHome™.

Email Details

Recipient's E-Mail ID: Enter the E-Mail address to which you want your computer's location coordinates sent.

Example: your-email@your-isp.com

User Ownership Info

Name: Your name

Organization: Your organization (if any)

Address: Your address

City: Your City

State/Province: Your state or province

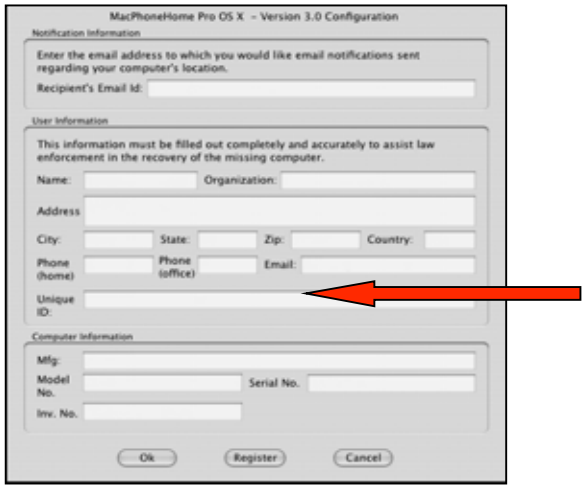
Zip/Postal Code: Your zip code or postal code

Country: Your country

Company Phone: Your company phone (if owned by organization)

Home Phone: Your home phone (for notification of recovery)

Figure 11A MacPhoneHome™ Unique ID Field



Email: Your E-Mail: (for notification of recovery)

Unique ID: If you purchase MacPhoneHome™, you are provided with a Unique ID. Insert that Unique ID code here.

Computer Info

Manufacturer: What company made this computer?

Model Number: What model number is this computer?

Serial Number: What is the serial number on the back or bottom of this computer?

Inventory Number: What is the organization's inventory or asset tracking number of this computer?

Note: for individuals users who don't have anything to put in there, you should still fill it with some other information, or just put in n/a, none, etc. (you get the picture.)

TO COMPLETE YOUR CONFIGURATION, ENTER THE CORRECT DATA IN THE FIELDS PROVIDED AND THEN REBOOT THE MACHINE. FROM THEN ON (PROVIDED YOU CONFIGURED YOUR APPLICATION PROPERLY) YOU NEED NOT DO ANYTHING MORE. MACPHONEHOME™ WILL SEND A STEALTH EMAIL TO THE EMAIL ADDRESS YOU ENTERED IN THE "RECIPIENT EMAIL" FIELD ONCE A DAY OR EVERYTIME THE PROGRAM SENSES YOU HAVE INTERNET CONNECTIVITY AND YOUR IP ADDRESS HAS CHANGED.

WHAT TO DO WITH YOUR INSTALLATION FILES

The beauty of MacPhoneHome™ is in its stealth: that is, you have a better chance of retrieving your lost or stolen computer if the person who has it doesn't know MacPhoneHome™ is on it and logs into the Internet, allowing MacPhoneHome™ to report it location through a stealth email. Therefore, any file left on the computer, such as "macph_v3.0.sit" might tip off the thief that MacPhoneHome™ is on the computer. Therefore, we recommend that you keep a copy of the installation file OFF YOUR COMPUTER AND IN A SAFE PLACE AWAY FROM YOUR COMPUTER.

In addition, there is a macph_v3.0 folder and a MacPhoneHome – V3.0.mpkg file that were created when you extracted the .sit during the installation process. We highly recommend you delete this folder and file off your computer as well. NOTE: Under the End User License Agreement, you are allowed to make an archive copy of MacPhoneHome™. We suggest that you keep a copy of Macph_v3.0.sit off your computer and archived.

NOTES

REGISTERING YOUR SOFTWARE

IMPORTANT! Even though you have a paid single user version of MacPhoneHome™, it is not fully operational until you register the software and receive a User Name and Password.

Why? There is a legal basis for this: Remember, this application is primarily designed to track and locate missing and stolen computers. As such, the software is designed to (1) locate the computer; and (2) provide law enforcement the necessary tools they need to both (a) obtain a search warrant to recover the computer; and (b) prosecute the perpetrator.

Since, in most cases, MacPhoneHome™ was the PRIMARY instrumentality that provided the information used to find and prosecute a thief, the METHOD on how that instrumentality is used is subject to legal scrutiny.

The recovery process must withstand a defense's challenge on "can you prove that you used this software on your computer legally?" A good defense lawyer may challenge the software as being "illegally used" (i.e., bootlegged, or used in violation of the user license). He/she will challenge the prosecution to prove that it wasn't used illegally (proving a negative is always difficult).

But with MacPhoneHome™'s registration procedure, we can.*

When an end-user purchases the program, the purchase is verified by a number of methods:

1. Electronic download: usually by the Unique ID OR by the Invoice from the download; or

2. CD media: by the Unique ID that accompanies each paid disk.

Therefore, registration provides the basis for proving that the software is legally installed on the computer (remember, the license is for ONE computer for the length you own the computer).

30-Day Registration Period

The end-user is required to "Register" the software in order to continue to use it after the first 30 days. IF YOU DO NOT REGISTER YOUR SOFTWARE IN THE FIRST 30 DAYS AFTER INSTALLATION, IT WILL STOP SENDING LOCATION INFORMATION.

When Brigadoon Software receives your request for the registration codes, the request is cross-referenced against records (either download receipts or validly-issued Unique IDs). If everything checks out (i.e., valid purchase) the registration User Name and Serial Number are sent to the bona fide end-user. No further registration User Names and Serial Numbers are now issued for that software license.

How do you register your paid single user version of MacPhoneHome™?

Once you install MacPhoneHome™, you may request your Registration Codes by emailing your request, along with identifying information (i.e., such as your name, address and privacy code/Unique ID from the configuration screen when you installed MacPhoneHome™ to support@brigadoonsoftware.com. Brigadoon Software will then check your Unique ID or electronic download invoice to determine if you are a bona fide licensee, and will then send you your User Name and Serial Number by email.

* Remember, Enterprise Editions have none of these issues, so the registration protocol is not required.

Here's how you complete the registration process

1. Go into the application's folder. (/Macintosh HD/Applications/)

2. Open up "macpro-config".
This should bring up the configuration window.
[Remember you will need to use your Administrator Name and Password to access this file]

3. Click on the "Register" button on the configuration window.

4. Enter your Username and Password (provided to you by Brigadoon Software) and then click "OK".

If you correctly completed the registration of your software license by correctly entering the Username and Password, you should then see the following window:

TECH SUPPORT

If you need technical support or have any questions regarding your software, here is how you contact us:

Email (usually the fastest response): support@brigadoonsoftware.com

Fax: +1-845-624-0990

Telephone (during normal business hours-New York time): +1-845-624-0909

Every time the computer has Internet access, MacPhoneHome™ has the ability to send an identifying stealth email to the Recipient's email address for location and recovery purposes. An example of how the message appears is as follows (color added for emphasis):

The information that is sent back to the recipient email address you provided contains two major bodies of information:

Return-Path: <tech@brigadoonsoftware.com>
Received: from mailer.pcphonehome.com (69.54.139.38) by mail.mcf.com with ESMTP (Eudora Internet Mail Server 3.1) for <tech@brigadoonsoftware.com>;
Fri, 22 Feb 2002 12:04:57 -0500
Received: from localhost (209.118.221.88) by mailer.pcphonehome.com with
SMTP (Eudora Internet Mail Server 3.1) for <tech@brigadoonsoftware.com>;
Fri, 22 Feb 2002 12:04:08 -0500
From: sparky@somewhere.com
To: sparky@somewhere.com
Subject: Information
Date: Fri, 22 Feb 2002 12:04:08 -0500
Message-ID: <1194435048-494213613@mailer.pcphonehome.com>

MacPhoneHome Pro OS X - Version 3.0
Date: 02-21-2002
Time: 23:36:17
Machine name: localhost
Processor serial number:
<4c4943000000000000000000000524e31595741386400000000000000000000000000000000000000000000000000>
IP information:
inet 127.0.0.1 netmask 0xff000000
inet 192.188.1.125 netmask 0xffffff00 broadcast 192.188.1.255
Ethernet Information:
ether 00:03:93:16:43:e2
Currently logged in users:
user console Feb 20 23:31

Name: Sam Smith
Organization: XYZ Co
Address: 100 Center St
City: New York
State: NY
Zip: 10004
Country: USA
Home phone: 212-555-1234
Office phone: 212-555-4321
Email: sparky@somewhere.com
Unique Id: my-unique-identifier-goes-here
Manufacturer: apple
Model No.: imac g3 600mhz
Serial No.: QT 9423 SE Y6
Inventory No.: bsi 34224

1. Information regarding ownership of the computer that is vital for its recovery (see example of an email received from MacPhoneHome™, left, in blue); and

2. Information pertaining to the location identifiers in order to track the location of the computer at the time the computer was on the Internet and was able to send the stealth email message (data in email, left, in red).

The information included (left, in blue) above is vital in order to provide the court with probable cause so that the law enforcement agency in charge can obtain a search warrant necessary in order to recover the computer.

Section II - Recovering the Computer

If your computer is lost or stolen, report the incident to the applicable local law enforcement agency. Law enforcement should then provide a case number, and assign the case to an investigating officer. The investigating officer will serve as the contact point in the recovery efforts. At that point, contact Brigadoon Software and provide as much information about the loss, including the case number and the contact information for the investigation officer. We will then provide you with recovery technical assistance at no extra cost.

[NOTE: We provide a form called "Computer Loss Data_form.pdf" with your software for you to use if your computer is lost or stolen. Keep a copy of it in a safe place.]

Your Mac "Phones Home"

The next time your lost or stolen computer has any kind of Internet access, it will send a new message. Once that new message is sent, a Brigadoon Software recovery technician can extract the IP address (the address on the Internet from which the message was sent) from the email and determine the Internet Service Provider that assigned that IP address.

Internet Service Providers log the telephone numbers (or, in the case of broadband service, the access point) of the incoming call BEFORE assigning an IP address. This telephone number or static access point is stored at the Internet Service Provider. This telephone number or access point provides the exact location of the missing computer. Internet

Service Providers provide this telephone number or the access point information to the investigating law enforcement agency, which in turn uses this information to acquire a search warrant to retrieve the missing computer.

What is the "IP Address?"

In an IP network, each computer is allocated a unique IP address. The IP address is assigned to a computer once it makes a connection to a network. The Internet is composed of thousands of networks all connected together.

Each physical network has to have a unique Network Number, comprising some of the bits of the IP address. The rest of the bits are used as a Host Number to uniquely identify each computer on that network. The number of unique Network Numbers that can be assigned in the Internet is therefore much smaller than 4 billion, and it is very unlikely that all of the possible Host Numbers in each Network Number are fully assigned.

An address is divided into two parts: a network number and a host number. The idea is that all computers on one physical network will have the same network number - a bit like the street name, the rest of the address defines an individual computer - a bit like house numbers within a street. The size of the network and host parts depends on the class of the address, and is determined by address' network mask. The network mask is a binary mask with 1s in the network part of the address, and 0 in the host part.

Because IP addresses are a scarce resource, most Internet Service Providers (ISPs) will only allocate one address to a single customer. In majority of cases this address is assigned dynamically, so every time a client connects to the ISP a different address will be provided. Big companies can buy more addresses, but for small businesses and home users the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time. With an NAT gateway running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

Client computers label all packets with unique "port numbers". Each IP packet starts with a header containing the source and destination addresses and port numbers:

Source address	Source port	Destination address	Destination port

This combination of numbers completely defines a single TCP/IP connection. The addresses specify the two machines at each end, and the two port numbers ensure that each connection between this pair of machines can be uniquely identified.

Each separate connection is originated from a unique source port number in the client, and all reply packets from the remote server for this connection contain the same number as their destination port, so that the client can relate them back to its correct connection.

Turnaround Time and Monitoring/Recovery

Once a message is received from a lost or stolen computer, it generally takes mere minutes to get enough information to either contact the ISP directly or provide law enforcement with the information necessary for them to contact the ISP and proceed with the inspection of the ISP's log records. From the ISP's log records, law enforcement obtains enough information to determine the exact address of the lost or stolen computer when it "Phoned Home."

APPENDIX: "HARDENING" YOUR HARDWARE

Disclaimer & Warning: While we recommend that you "harden" your hardware to third party intrusion, the information provided in this Appendix **is advisory in nature only**. Any actions involving computer firmware, such as enabling the Open Firmware password protection feature, is done so at your own risk. Brigadoon Software, Inc. will NOT be held accountable or responsible for the result of your actions. Any hardware/firmware/operating systems issues that may arise are under the aegis of the computer manufacturer.

Introduction

Out-of-the-box, Mac OS X is reasonably secure. Apple installs a fairly secure default configuration, and provides regular Security Updates. However, to protect your proprietary data and to provide you with the highest probability of recovery of your computer should it be lost or stolen, we recommend that you take the following steps:

1. Set up different user accounts on your Mac:
    a. For personal use: two accounts: Administrator and Guest (Managed);
    b. For organizations: three accounts: Administrator, Standard and Guest (Managed);
2. Password protect access to your Administrator and Standard accounts, but not your Guest account;
3. Have your computer boot directly into your Guest Account.
4. Utilize Apple's Open Firmware Password application to allow you to enable security features in Open Firmware;
5. Use Apple's File Vault to protect your important data.

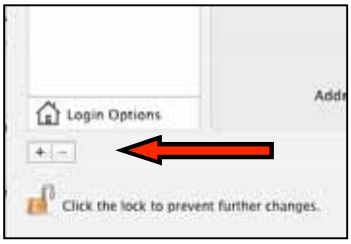
I. Accounts and users

By default, the account created when installing OS X is an Administrator account that has the equivalent of "root" access. It's not secure or necessary to use that account for routine work.

Recommendations:

Have several accounts for special purposes on your Mac OS X system. Be in control of all access to your system by other users. Here's how:

A. Create (i) a Standard account for daily work; and (ii) a Guest (Managed) account.
While logged in as the administrator, use the "Accounts" System Preference tool to create two non-administrator user accounts.
    a. Create a Standard Account (with a password) for daily tasks (especially in a multi-user or organizational situation); and
    b. Create a Guest (Managed) Account (without a password)
        i. go to "System Preferences";
        ii. click on "Accounts", and click on the "+" sign

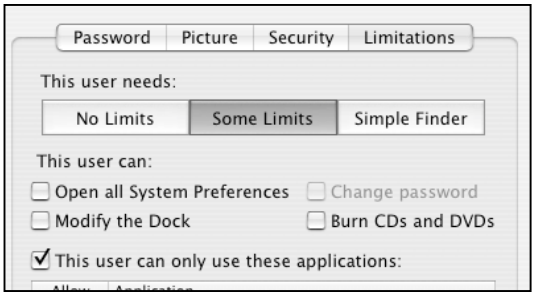


iii. type in “Guest” in the Name field

iv. DO NOT PUT IN A PASSWORD

v. Click “OK” when prompted that there is no password

vi. Click on Limitations and click only on “This user can only use these applications” and select a minimum of applications (see below).



B. Change Log in to a show Users as startup.

By default, OS X logs in automatically after a restart, using the first account created during installation and this account's saved password. As previously noted, this is an administrator account, so anyone can start it up and make changes to it. To fix this,

a. go to “System Preferences”;

b. click on "Accounts", and click on “Login Options”

c. be sure "List of users" is selected instead of "Name and password."

[NOTE: Do not enable Personal File Sharing unless you need to, because it doesn't allow you to require an account and password. It's a bad idea to allow guest or anonymous access to any service, folder, or file unless you understand what you're doing.]

II. Have your computer boot directly into your Guest (Managed) Account.

We recommend that you have your Mac automatically log in to the Guest (Managed) account you created. From there you can log out and then log in to either your Administrative or Standard account, as needed. Here’s how:

A. Open System Preferences and click Accounts.
B. If some settings are dimmed, click the lock icon and type an administrator name and password.
C. Click Login Options.
D. Select the way you want users to log in (a list of users).
E. Select "Automatically log in as" if you want the computer to log one user in automatically each time it starts up. Then choose the Guest (Managed) user from the pop-up menu when prompted.

III. Utilize Apple’s Open Firmware Password

Anyone can change your Administrator password if they start your Mac up with an OS X Installation CD. If your Mac is started up from an OS 9 (Classic) System Folder, there is no protection or security at all for the OS X files in the same disk partition We recommend you prevent the possibility of someone booting it from an external hard drive, DVD, or CD, and then changing your administrator password, erasing your disk, or accessing your private documents.

Recommendations: To prevent booting from external drives, use the Open Firmware Password utility to set a firmware password. See http://docs.info.apple.com/article.html?artnum=120095 for complete instructions and a copy of the utility.

Open Firmware Password Application

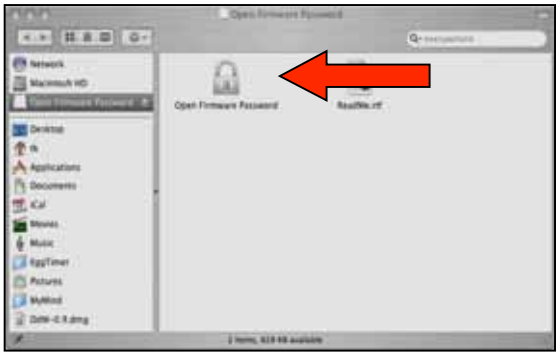
Version 1.0.2

The Open Firmware Password application allows you to enable security features in Open Firmware. You can use it to prevent others from starting your computer using a CD or other disk with an operating system on it. You can use Firmware password protection to enhance access security to your computer.

When you set a Firmware password, it prevents others from starting up the computer from a volume other than the one you have chosen as the startup disk (chosen in the Startup Disk preference panel within the System Preferences.) Once security is enabled, you cannot startup from other devices such as an external FireWire disk, a CD-ROM drive, or another partition or disk inside the computer.

Requirements

This application requires Firmware update 4.1.7 or a later version and Mac OS X 10.1 or later.

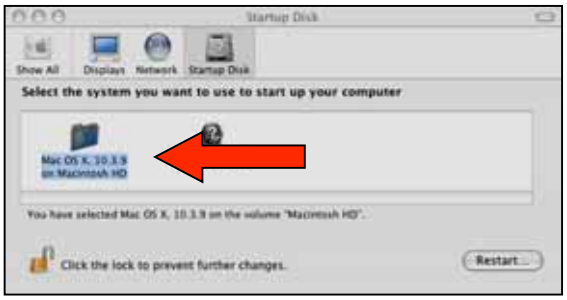


Installing the Firmware Password Application

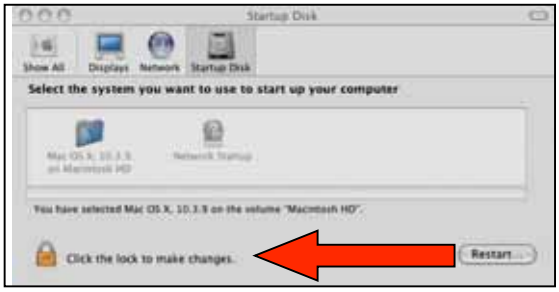
1. Drag the application icon from the disk image (.dmg file) to your hard disk (Macintosh HD). (see example, right)

Using the Application

1. Make sure that you have selected the Mac OS X System folder for your startup device that your plan to protect. If your startup device is correctly selected, you should be able to
    a. Click on "System Preferences"
    b. Click on "Startup Disk" preference pane
    c. Show "Mac OS X, 10.x on Macintosh HD" (see example, right)



    d. Be sure to lock your settings to prevent further changes (see example, right)



2. Double click the "Open Firmware Password" icon to open it. (/Macintosh HD)

3. Click the "Change" button to modify the security settings. (see right)

4. If you are enabling the security features, enter a password into the Password and Verify boxes. (see right)

5. Click OK. (see right)

6. Follow the prompts to enter your Administrator account information. You should then see a successfully saved window. (see right)

IV. Use Apple's File Vault to protect your important data.

About FileVault

Mac OS X includes FileVault, which allows you to encrypt the information in your home folder. Encryption scrambles the data in your home folder so that your information is secure if your computer is lost or stolen. FileVault uses the latest government-approved encryption standard, the Advanced Encryption Standard with 128-bit keys (AES-128).

When you turn on FileVault, you also set up a master password for the computer that you or an administrator can use if you forget your regular login password.

WARNING: If you turn on FileVault and then forget both your login password and your master password, you will not be able to log in to your account and your data will be lost forever.

Because of the amount of disk space required, we recommend that you use File Vault with the account in which it essential to protect your important data only.