



PC PhoneHome™
Tracks & Locates Missing Computers

INSTALLATION GUIDE



Version 3.3.1



95/98/ME/NT/2000/XP

Brigadoon Software_{inc}

© 2001-2005 Brigadoon Software, Inc. All rights reserved.

INSTALLATION GUIDE FOR PC PhoneHome™

THEFT RECOVERY SOFTWARE

INTRODUCTION

This report will assist authorized users to track and locate computers protected with PC PhoneHome™ software. The proper installation and configuration of PC PhoneHome™ is critical to the recovery process.

OVERVIEW: HOW PC PHONEHOME™ 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. PCPhoneHome™ 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 PC PhoneHome™ 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 PC PhoneHome™ for Windows 95/98/ME/XP/NT/2000.

IMPORTANT!
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.



Please Note: For the Vista operating system log in as the Administrator and then turn off "Account User Control" before installation. After installation you can turn Account User Control back on if you wish. To turn off Account User Control: Go to Start Menu..."Settings"..."Control Panel"..."User Accounts"..."Turn User Account Controls On or Off" ...and change the setting to "off".

Image1 PC PhoneHome™ Installer.

PC PhoneHome™ uses a Zip archive. To begin Installation **double click the pcph3.3.1.zip** file. This will extract the installer file called **pcph3.3.1.exe** in the same folder.

Double Click on **pcph3.3.1.exe** to begin installation.

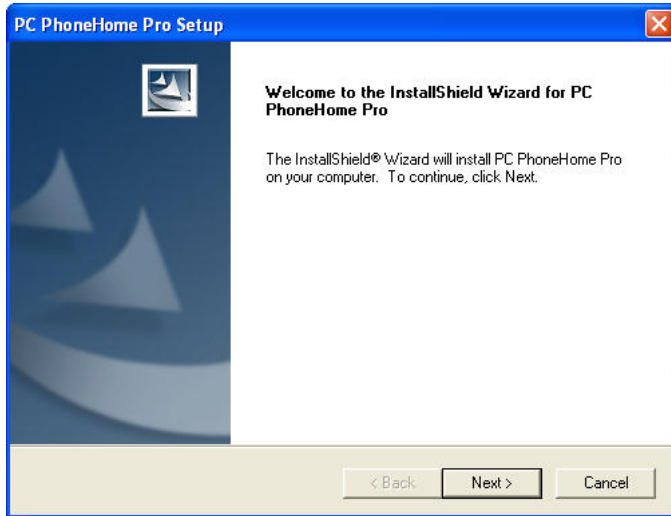


Image 2 Installation Setup

At the start of the install you will see this:

The PC PhoneHome™ install wizard is a menu-driven application. Simply follow the directions provided by the installer.

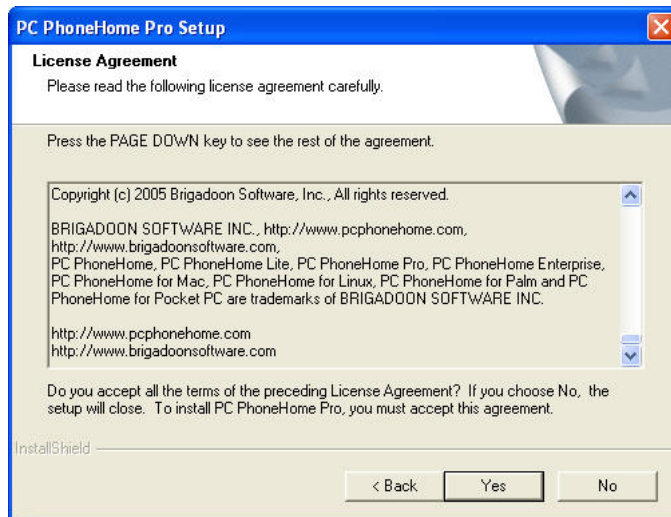


Image 3 License Agreement

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

IMPORTANT!!

The ownership information you provide in the configuration box for PC PhoneHome™ is the information that is sent to your designated command center. 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 data field of the configuration window. 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.**

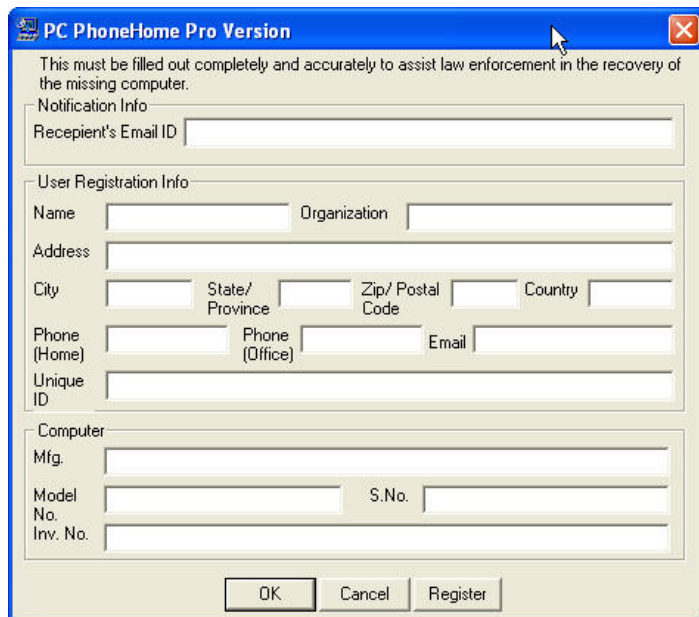


Image 4 PC PhoneHome™ Configuration Window

SMTP Details

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

Example: your-email-address@your-isp.com (web email addresses are OK too)

User Ownership Info

Name: Your name

Organization: Your organization (if any-or else put in "None")

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)

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

Unique ID: The Unique ID is user defined and can be anything you choose. It is useful when you are protecting more than one computer and want to easily differentiate between the archived emails from your different computers.

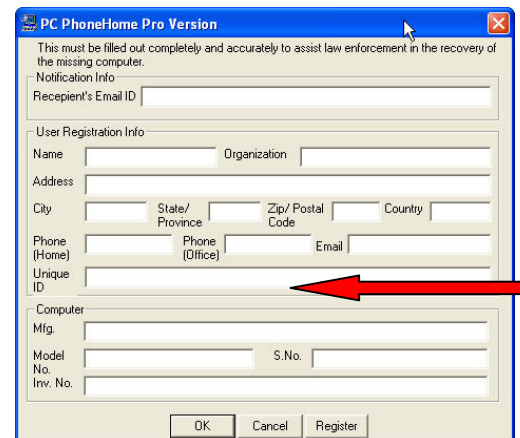
Computer Info

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?



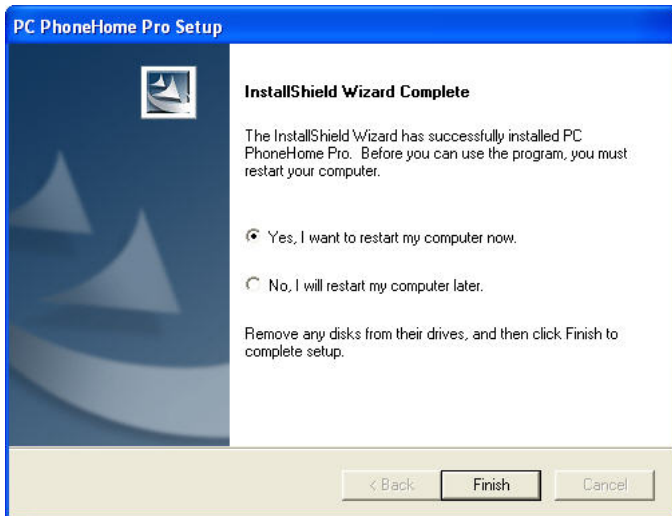


Image 5 Installation Complete

The PC PhoneHome™ installation is then complete. You will need to restart the computer to activate the software.

ONCE YOU COMPLETE YOUR CONFIGURATION, REBOOT THE MACHINE. FROM THEN ON (PROVIDED YOU CONFIGURED YOUR APPLICATION PROPERLY) YOU NEED NOT DO ANYTHING MORE. PC PHONEHOME™ 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 PC PhoneHome™ 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 PC PhoneHome™ is on it and logs into the Internet, allowing PC PhoneHome™ to report its location through a stealth email. Therefore, any file left on the computer, such as "**pcph3.3.1.zip**" 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 **pcph3.3.1** folder and a **pcph3.3.1.exe** 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 PC PhoneHome™. We suggest that you keep a copy of pcph_v3.0.zip off your computer and archived.

NOTES

REGISTERING YOUR SOFTWARE

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

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, PC PhoneHome™ 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 PC PhoneHome™'s registration procedure, we can. 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.

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

Manual Registration

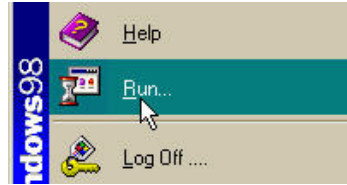
When you purchase PC PhoneHome you will receive a confirmation email (within 24 hours Monday through Friday), which will contain a USERNAME and SERIAL NUMBER/PASSWORD to use with this copy of the software. You can then use them to register and complete the process.

Here's how you complete the manual registration process:

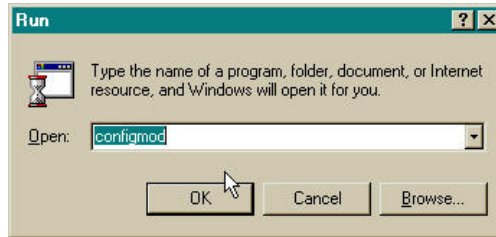
1. Click on "Start"



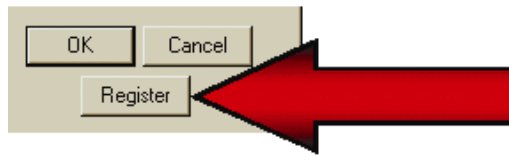
2. Click on "Run"



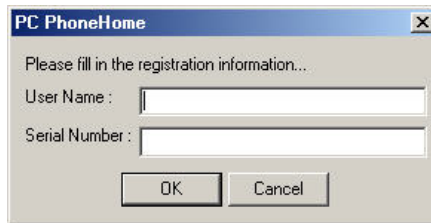
3. Then type "configmod" in the "Open" data field. This should bring up the configuration window.



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



5. Enter your **User Name** and **Serial Number/Password** (sent to you by email after you purchase the software) and then click "OK".



If you correctly completed the registration of your software license by correctly entering the User Name and Serial Number, you should then see the following window:



NOTES:

MONITORING, TRACKING, LOCATING AND ASSET RECOVERY

How PC PhoneHome™ Works

PC PhoneHome™ 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).

Laptop or Desktop with
PC PhoneHome™ Installed



Check your email for computer
identification and location information



PC PhoneHome™ sends location and ownership
information by stealth stand-alone email via the Internet

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

```
X-Persona: <BrigTech>
Return-Path: <sender@brigadoonsoftware.com>
Received: from mail.brigadoonsoftware.com (66.84.179.38)
by mail.mcf.com
with SMTP (Eudora Internet Mail Server 3.1b1);
Thu, 18 Oct 2001 11:10:21 -0400
From: sender@brigadoonsoftware.com
To: tech@brigadoonsoftware.com
Subject: Information
Date: Thu, 18 Oct 2001 11:10:21 -0400
Message-ID: 1208704675-101666554@mail.mcf.com
```

PCPH Pro For Win 95/98/ME/NT/2K

```
Date: 10-18-2001
Time: 11:10:21
Computer Name: SPARKY3223
User Name: Sparky3223
IPAddress : 66.84.179.38
Mac Address: 44-45-53-54-61-6F
Mac Address: 44-45-53-54-61-70
Mac Address: 00-80-C7-98-D6-9F
Serial Number: 392D12D8
```

```
Registrants Name: sammy
Organization: bsi
Address: 100 main st
City: nyc
State/Province: ny
Zip/Postal Code: 10002
Country: usa
Work Phone: 212-555-1234
Home Phone: 212-555-4321
E-mail: sparky@somewhere.com
Unique Identifier: my-unique-identifier-goes-here
Computer Manufacturer: ibm
Computer Model Number: 570
Computer Serial Number: 1231VF2937121-92
Inventory Number: bsi-34234
```

Sample of Received email including header

The information that is sent back to the monitoring email address provides two major bodies of information:

1. Information regarding **ownership** of the computer that is vital for its recovery (data in image 4 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 image 4 in **red**).

The information included (data in image 4 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

During the normal course of monitoring, the owner and Brigadoon Software's redundant emergency backup system archive the information received from the computer in case there is a theft by saving the stealth email sent to the Recipient Email address by PC PhoneHome™.

Once a computer is reported as lost or stolen, report the incident to the applicable local law enforcement agency. Law enforcement should then generate a case number, and assign the case to an investigating officer. The investigating officer will serve as the focal 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.

Your PC "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 a 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:



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."

TECH SUPPORT

For questions or technical support you can either contact the manufacturer, Brigadoon Software or contact us at SecurityKit.com and we will get the answers for you. Here is contact information for both companies:

Brigadoon Software (Monday – Friday 9:00 AM to 5:00 EST)
Email – support@brigadoonsoftware.com
Phone – 845.624.0909
Fax – 845.624.0909

SecurityKit.com (Monday – Friday 9AM – 4:30 PM PST)
Email – customercare@securitykit.com
Phone – 323.822.0382
Fax – 323.822.1342

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 changing your boot sequence in your computer's BIOS, 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/operating systems issues that may arise are under the aegis of the respective manufacturer.

Introduction

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 computer:
 - 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 **your computer's BIOS settings** to change the boot sequence to prevent booting the computer from an external drive without authorization;
5. Use encryption software to protect your important data.

I. Accounts and users

Creating a User Account

You should not use your administrator account for everyday tasks on your computer. Your administrator account allows you to install software, but using it all the time is dangerous because viruses and Trojan horses accidentally run from the administrator account can cause greater harm to your computer. To prevent damage to your system, you should create a user account for every day use.

Windows XP

To create a user account in Windows XP:

- 1 Click the **Start** button in the lower left corner of the desktop.
- 2 Click **Settings**, then click **Control Panel**.
- 3 In the **Control Panel** window, click **User Accounts**.
- 4 In the **User Accounts** window, click **Create a new account**.
- 5 Enter the user account name in the **Account Name** field and click **Next**.
- 6 Select the **Limited** radio button, then click **Next**.
- 7 Click **Create Account**.
- 8 In the **User Accounts** window, click on the new account.
- 9 Click **Change the password**.
- 10 Enter the desired password (this should be different than the administrator password).
- 11 Verify the password and add a password hint.
- 12 Click **Change Password**.
- 13 Log out of the administrator account by hitting CTRL-ALT-DEL and selecting **Log Off**. Then log back in as the new user account.

Windows 2000

To create a user account in Windows 2000:

- 1 Click the **Start** button in the lower left corner of the desktop.
- 2 Click **Settings**, then click **Control Panel**.
- 3 In the **Control Panel** window, click **Users and Passwords**.
- 4 In the **Users and Passwords** window, select the **Users must enter a name and password to use this computer** check box.
- 5 Click **Add**.
- 6 Enter the **User Name** and **Full Name**, then click **Next**.
- 7 Enter the desired password (this should be different than the administrator password).
- 8 Click **Next**.
- 9 Select the **Standard User** radio button, then click **Finish**.
- 10 Click **OK**.
- 11 Log out of the administrator account by hitting CTRL-ALT-DEL and selecting **Log Off**. Then log back in as the new user account.

Windows NT

To create a user account in Windows NT:

- 1 Click the **Start** button in the lower left corner of the desktop.
- 2 Click **Programs**, then **Administrative Tools** (Common), and then **User Management**.
- 3 In the **User Management** window, click **New User**.
- 4 Enter the **User Name** and **Full Name**.
- 5 Enter the desired password (this should be different than the administrator password).
- 6 To allow the user to select a new, private password, select the **User Must Change Password at Next Logon** check box.
- 7 Click **OK**.
- 8 On the **Start** menu, click **Shut Down**, select the **Close all programs and log on as a different user** radio button, then click **Yes**.

=====

By default, the account created when installing Windows 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 Windows computer. 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, Windows 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 computer 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 your computer's BIOS settings

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.

IV. Use Encryption Software to protect your important data.

About the Encrypting File System

Microsoft Windows includes the ability to encrypt data directly on volumes that use the NTFS file system so that no other user can use the data. You can encrypt files and folders if you set an attribute in the object's **Properties** dialog box. For Windows XP Professional and Windows 2000 Professional Edition.

See: <http://support.microsoft.com/?kbid=223316>

You can use Encrypting File System (EFS) to:

- Encrypt their files
- Access their encrypted files
- Move or rename their encrypted files
- Copy their encrypted files
- Decrypt their files

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_SEconceptsI mpEncrypt.htm