PC PhoneHome™

Tracks & Locates Missing Computers

Version 3.5

Windows

XP – Vista - Seven

Brigadoon Software, Inc
119 Rockland Center, Suite 250
Nanuet, New York 10954
Tel: +1-845-624-0909 Fax: +1-845-624-0990
Website: www.brigadoonsoftware.com

APPENDIX: "HARDENING" YOUR HARDWARE

Disclaimer & Warning: While we recommend that you "harden" your computer to third party intrusion, the information provided in this Appendix **is advisory in nature only**.

All the hardening techniques of your computer's operating system rely on your Windows operating systems features. **THEREFORE, IF YOU HAVE ANY QUESTIONS, YOU SHOULD CONSULT MICROSOFT TECH SUPPORT DOCUMENTATION.**

Any actions involving computer firmware, such as changing your boot sequence in your computer's BIOS, is done so at your own risk. **IF YOU HAVE ANY QUESTIONS ABOUT YOUR COMPUTER'S BIOS OR FIRMWARE, YOU SHOULD CONSULT YOUR COMPUTER MANUFACTURER'S TECH SUPPORT DOCUMENTATION, OR (IN THE CASE OF YOUR BIOS SETTINGS) CONSULT YOUR BIOS MANUFACTURER'S TECH SUPPORT DOCUMENTATION.**

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. The message from PC PhoneHome will be sent immediately with your computer's location. This provides MAXIMUM opportunity to recover your stolen computer.
4. Utilize **your computer's BIOS settings** to change the boot sequence to prevent booting the computer from an external drive without authorization. With this activated, an unauthorized party can NOT reformat your hard drive. Refer to your computer's documentation on how to do this.
5. Use encryption software to protect your proprietary data in protected folders.

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. We suggest STRONGLY that you make your computer boot into the guest account so a thief will have access and be able to get internet access which is required so PC PhoneHome can send it's location details. If your computer is password protected, a thief won't be able to boot and get internet access.

III. Utilize your computer's BIOS settings

Anyone can change your Administrator password if they start your computer up with a Windows Installation CD. We recommend you prevent the possibility of someone unauthorized from 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 unauthorized booting from external drives, we recommend you change the boot sequence in your BIOS settings to only boot from the main (C:/) hard drive, and then password protect that BIOS setting.

IMPORTANT: Changing the boot sequence is a function of your hardware settings, NOT PCPHONEHOME™. You should consult your computer's manual for specific information on using the CMOS setup program. An incorrect setting in this critical area of the computer can make the computer non-operative.

Enable your computer's setup password to prevent someone from accessing the computer's CMOS settings and changing the boot sequence. But **DO NOT** enable to boot password!!! Make sure your computer boots into a non-password protected account.