

WhoStoleMyPC

Control your laptop after it's been stolen

RemoTrieve Technologies
www.who-stole-mypc.com

WhoStoleMyPC

Copyright © 2006 RemoTrieve Technologies

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: June 2006

Table of Contents

1.0 Introduction	3
2.0 Warning!	5
3.0 Installation	6
4.0 Configuration	10
4.1 Demo	11
4.2 Machine Information	12
4.3 Configuration Screen	14
4.4 Watchdog	16
4.5 Watchdog Commands	18
Delete Files	20
Execute Application	21
Format Hard Drive	23
Simulate Hardware Failure	24
Change Windows Password	25
Purge E-Mail	25
Shutdown Computer	26
Display Custom Message	27
4.6 File Transmission	29
4.7 Advanced	31
5.0 www.who.stole.mypc.com	33
5.1 Commands	35
Log IP Locations	36
Log Screen Contents	37
Log Keystrokes	37
Log Visited URLs	38
Log Incoming E-Mail	39
Transmit Files to FTP Site	40
Delete Files	41
Purge E-Mail	42
Change Windows Password	42
Shutdown Computer	43
Format Hard Drive	43
Simulate Hardware Failure	44
Execute Application	45
Display Custom Message	46

Change FTP Information	47
Change Zip Password	48
Uninstall WhoStoleMyPC	48
6.0 In Case of Difficulty	49
Index	51

1 Introduction

Thank you for using WhoStoleMyPC! Although we hope that you'll never need to use the product, we know that there's hundreds of thousands of people that wish they had heard of us before they became a victim. Congratulations, you're not going to be one of them!

If You've Purchased a License:

We appreciate your business. If you haven't already, you should activate the license and then configure WhoStoleMyPC. Be sure to tell your friends, relatives and coworkers about your experiences with WhoStoleMyPC. If you have any ideas on how the program can be improved, please let us know. We're always interested in how we can improve the program.

If You're Evaluating the Demo:

Thanks for stopping by! If you haven't already, you should configure WhoStoleMyPC. You will have 30 days to evaluate the program, after which the program will uninstall itself (if you choose not to purchase a license). If you don't find WhoStoleMyPC to your liking, please take the time and tell us why. We'll never learn if you don't tell us.

What is WhoStoleMyPC?

You bought your laptop because it's small, light and travels well. Unfortunately, these reasons make it easy to be stolen. And as careful as you may be, if a thief wants your computer bad enough, he's going to get it.

Nowadays, laptops are relatively cheap. Although you want it back, often there's something you want back even more: **The Data.**

That's where WhoStoleMyPC comes in. In addition to providing information that can help authorities locate your laptop, WhoStoleMyPC gives you the ability to prevent data theft.

WhoStoleMyPC give you total control of your machine while it's in the thief's hands - and he's never aware:

- **Logging:** IP address, keyboard, screen content, visited URLs and e-mail.
- **Retrieval:** Transmit specified files to an FTP site.
- **Security:** Delete files, e-mail messages or format hard disk(s).
- **Control:** Change the Windows password, shut down the machine, display messages, execute applications and simulate hardware failure.

When your computer has been stolen, you can log onto www.who-stole-my-pc.com and activate WhoStoleMyPC's remote control commands. As long as your stolen computer has even occasional access to the Internet, these commands will be executed. You have complete control over these commands through the web site.

In cases where your computer has not been able to communicate with the Internet, a set of commands that you have pre-selected will be executed.

2 Warning!

WhoStoleMyPC can give you a great deal of information about the person who stole your computer. You may even be able to determine the thief's identity and/or location. Even though you may want to, you should **never confront the thief**. Remember, he is not averse to breaking the law, and may become violent if threatened in any way. You should always let the authorities do their job.

If your computer is stolen:

1. Report the theft to the police immediately. Once the police have a record of the theft, it will be easier to relay any information that WhoStoleMyPC can provide to them.
2. Immediately use WhoStoleMyPC to remove any sensitive information. The faster you do it, the less time the thief will have.
3. Report any information that WhoStoleMyPC provides to the authorities.
4. Change any user names and passwords that the thief may have access to. For example:
 - E-Mail
 - Online banking website access.
 - Credit card website access.
 - Don't forget any user names or passwords that your web browser has memorized for you.
5. If you maintained your finances with the computer, notify the bank(s), credit card companies and other financial institutions that you do business with.
6. Regard any information that was sent or received by you via e-mail as compromised.
7. Check your credit report to ensure that the thief hasn't stolen your identity in any way. Do so periodically.
8. Do not confront the thief!!!

3 Installation

System Requirements:

WhoStoleMyPC will run on Windows 2000 and Windows XP. It does not require much memory or a fast processor. If your computer capable of running Windows 2000/XP, you're all set.

Installation:

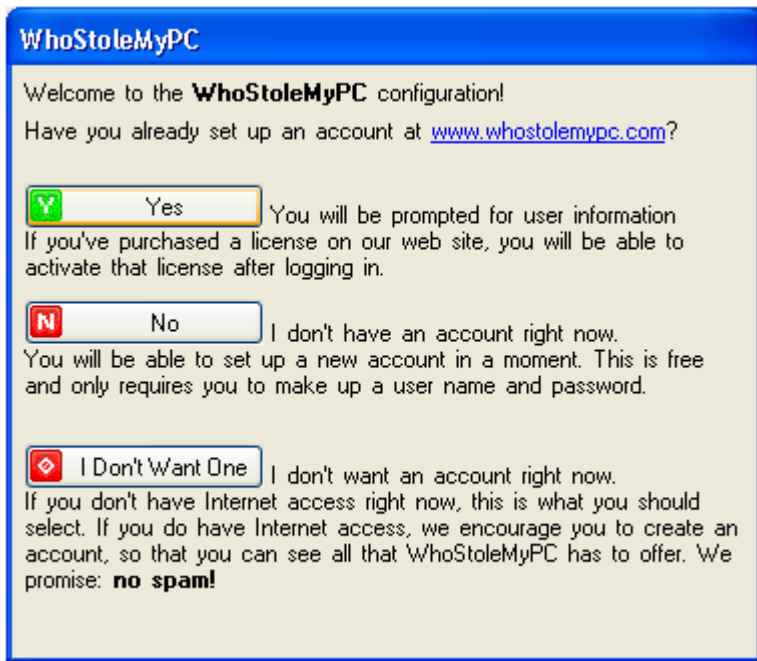
1. Download the WhoStoleMyPC installer from www.whostolemypc.com.
2. Launch the installer (click **Run** when asked or double-click **setupwsmpc.exe**).
3. Follow the installation steps.

Firewall Warnings:

After the program has been installed, it will attempt to access the Internet to determine if the computer already has a license. If your computer has a firewall, you may get two or more warnings indicating that a program is attempting to access the Internet. You should tell the firewall that this is okay, and that it should not warn you about this in the future. See the Frequently Asked Questions topic in the electronic documentation for more information on firewalls.

Activating the License or Activating the Demo:

1. After the initial program installation, you will be prompted with the following dialog:



WhoStoleMyPC

Welcome to the **WhoStoleMyPC** configuration!

Have you already set up an account at www.whostolemypc.com?

Y Yes You will be prompted for user information
If you've purchased a license on our web site, you will be able to activate that license after logging in.

N No I don't have an account right now.
You will be able to set up a new account in a moment. This is free and only requires you to make up a user name and password.

I Don't Want One I don't want an account right now.
If you don't have Internet access right now, this is what you should select. If you do have Internet access, we encourage you to create an account, so that you can see all that WhoStoleMyPC has to offer. We promise: **no spam!**

2. If you already have an account at www.whostolemypc.com, click **Yes**. You will be prompted for your user name and password:



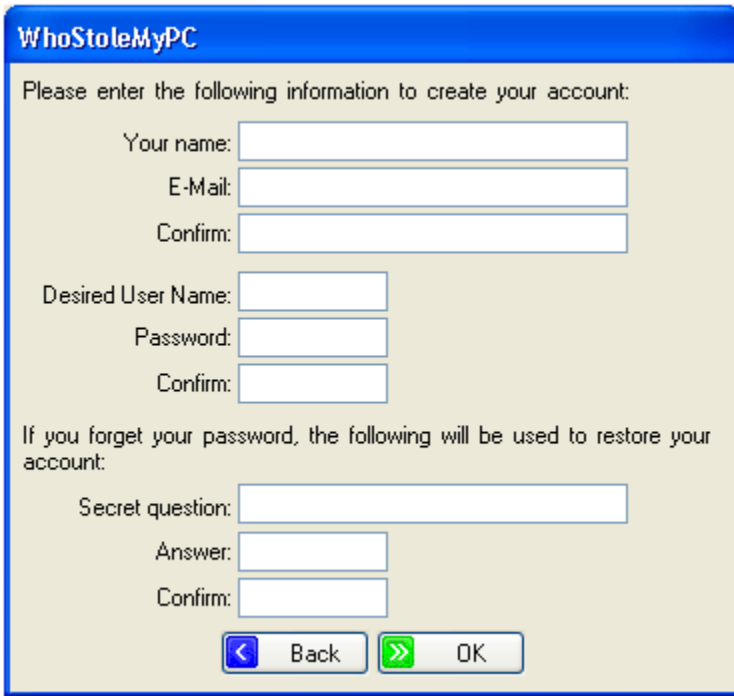
WhoStoleMyPC

Please enter your **WhoStoleMyPC** user name and password.

User Name:

Password:

3. If you don't already have an account at www.whostolemypc.com and would like to create one, click **No**. You will be prompted for some user information:



The screenshot shows a dialog box titled "WhoStoleMyPC" with a blue header. The main area is light beige and contains the following text and form fields:

Please enter the following information to create your account:

Your name:

E-Mail:

Confirm:

Desired User Name:

Password:

Confirm:

If you forget your password, the following will be used to restore your account:

Secret question:

Answer:

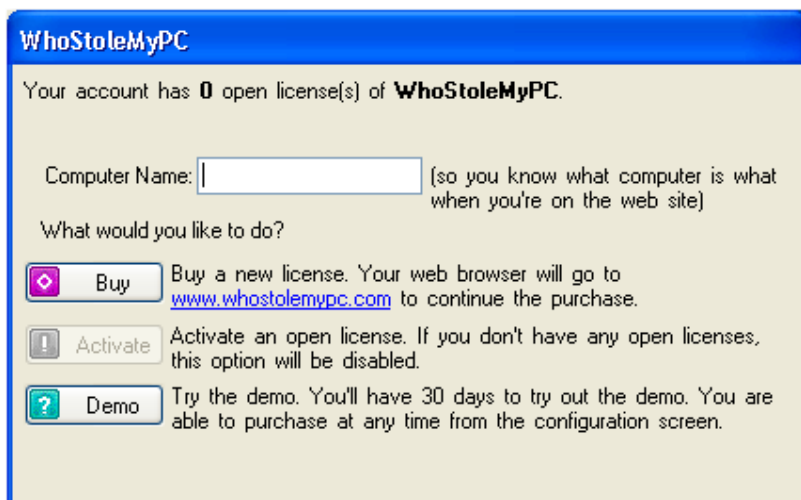
Confirm:

At the bottom, there are two buttons: "Back" with a blue left-pointing arrow icon, and "OK" with a green right-pointing arrow icon.

4. If you would rather not set up an account at www.whostolemypc.com, click **I Don't Want One**. If you have purchased a license, you should not choose this option, but rather log in with the user name of the account.

If you are evaluating the product, creating an account is still a good idea, as you will be able to see how you can control your computer from www.whostolemypc.com after it has been stolen. Without a user account, you can only evaluate the Watchdog functionality. Accounts are free and no personal information is gathered.

5. Finally, the following dialog is displayed:



At the top, the number of open licenses will be indicated. If this number appears to be incorrect, you should double-check by logging into www.whostolemypc.com and going to My Account. Click **Buy** if you would like to purchase a license at this time. You will be taken to www.whostolemypc.com, where you will be stepped through the purchasing process.

If you've already purchased a license(s), you can click **Activate** to activate that license for this machine. If you don't have any open licenses, this option will be disabled.

If you aren't ready to buy, you can click **Demo** to try out the product for 30 days. You will be prompted from time to time if you decide to purchase.

6. At this point, you will be taken to the configuration screen.

4 Configuration

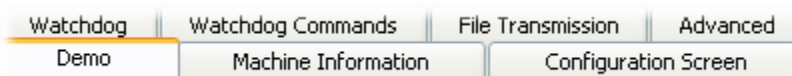
WhoStoleMyPC has a set of configuration options that can be changed at any time. They fall into the following categories:

- **Machine Information** Details about your computer, which can be very useful for recovery.
- **Configuration Screen** How the configuration screen is to be called up, as well as the password and prompt message.
- **Watchdog Settings** The watchdog password and prompt, as well as commands that will execute if the computer has been stolen and loses contact with the Internet for an extended period.
- **FTP Settings** If you plan on instructing WhoStoleMyPC to transmit logs or files to you, you will need to specify your FTP server details.
- **Advanced Settings** A few settings that you probably don't need to worry about.

When you first install WhoStoleMyPC, you are immediately taken to the configuration screen after installation. At that opportunity, we strongly urge you to change the **Configuration Screen** settings (particularly the activation keystroke, prompt, and password).

You can enter the configuration screen at any later time by pressing the activation keystroke that you specified earlier. If you ignored our advice and left the default settings, the activation keystroke is **CTRL+ALT+SHIFT+F10**. The password is **password**. See how obvious they are? Now go and change them!

The configuration screen contains the following tabs:



- **Demo** (if you're evaluating the product) Details on how to purchase the product, etc.
- **Machine Information** Details about your computer.
- **Configuration Screen** How to call up the configuration screen.
- **Watchdog** The watchdog timeout, password and prompt.
- **Watchdog Commands** The commands that will be executed if your computer is stolen and loses contact with the Internet.
- **File Transmission** FTP server details.
- **Advanced** Advanced settings, update and uninstall options.

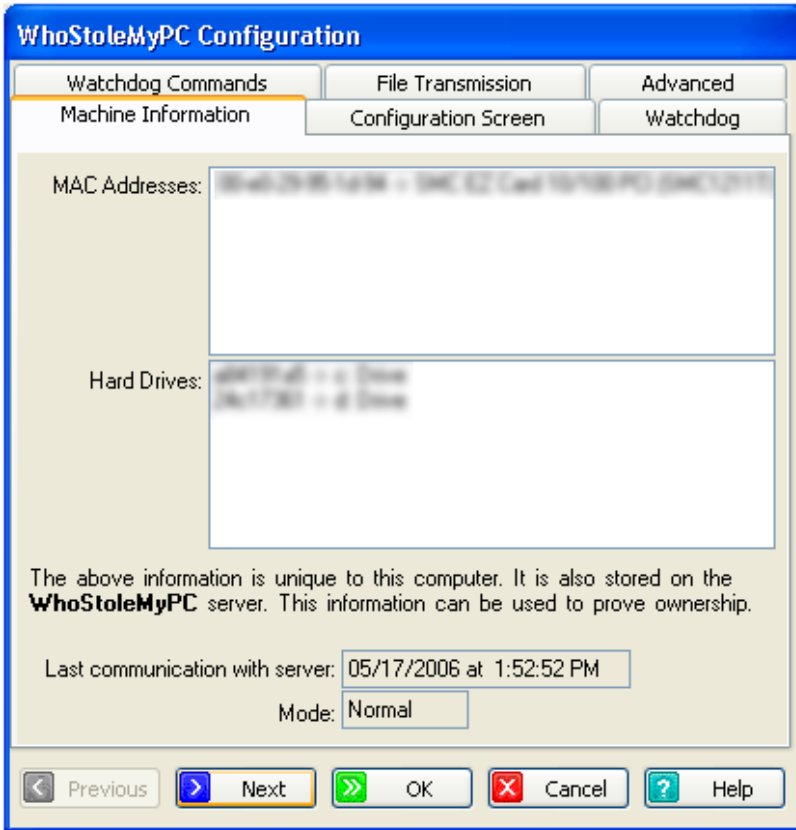
4.1 Demo



This screen appears if you are evaluating WhoStoleMyPC. The **Purchase** button will open your web browser and take you to our purchasing site (so you'll need an Internet connection).

During normal operation, WhoStoleMyPC contacts the server every day or so for instructions (if the computer has been stolen, contact is more frequent). Often people trying out the demo would like to see an instantaneous response to the instructions they've set up on our web site. The **Contact Server** button will tell the program to retrieve instructions from the server immediately after you leave the configuration screen.

4.2 Machine Information



This screen lists information unique to your computer. The **MAC Address** list lists the network adapters present in the computer along with their corresponding MAC addresses. MAC addresses are unique and can be used to positively identify your machine if it is stolen.

The **Hard Drive** list lists the internal hard drives present in the computer along with their corresponding serial numbers. Like MAC addresses, drive serial numbers are unique.

In addition to being presented here, this information is recorded in the WhoStoleMyPC server. If your computer is stolen, you can retrieve this information to prove ownership.

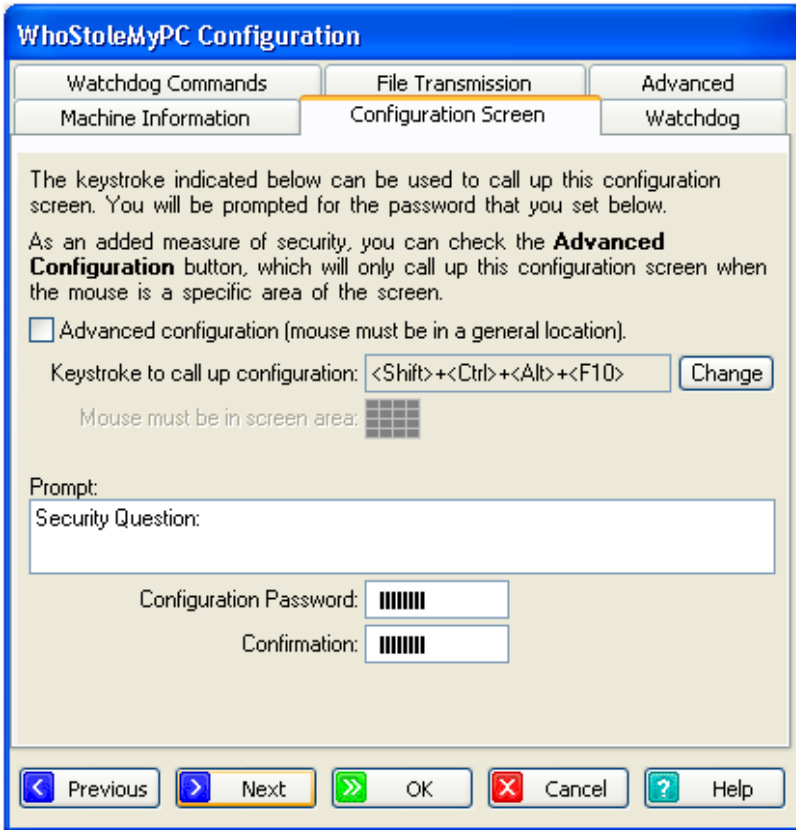
Although MAC addresses and serial numbers are a good 'digital fingerprint', the computer's physical serial number (usually stamped on the case or chassis) is still a preferred way of proving ownership. So while it's still fresh in your mind, record those numbers right now!

The mode indicates WhoStoleMyPC's current state:

- **Normal** Normal operation; (not stolen).
- **Stolen!** The computer has been reported to the WhoStoleMyPC server as stolen.
- **Demo** You are using the evaluation version of the program.

In the above illustration, we've intentionally blurred the computer's MAC address and serial numbers. Your results will be legible.

4.3 Configuration Screen



This screen allows you to specify how you would like to call up WhoStoleMyPC's configuration in the future. We strongly encourage you to visit this screen and change the default options. If you don't and your computer is stolen, a suspecting thief can easily call up the configuration and remove WhoStoleMyPC.

If **Advanced configuration** is checked, not only is the keystroke combination validated, but also the location of the mouse. Only if the mouse is located in the specified area of the screen will the keystroke work. Mouse placement is divided into 16 sections of the screen (4 rows by 4 columns), so your placement doesn't have to be exact.

When the **Change** button is clicked, you will be prompted to press the keystroke combination. If Advanced configuration is checked, you should position your mouse in the appropriate area before pressing the keystroke combination.

During normal operation, a prompt is displayed when the user has pressed the correct keystroke combination (and, if necessary, the mouse is in the proper location). The user must specify the correct answer or the configuration screen will not appear.

The **Prompt** can be changed here. You can make this question anything you like, and it does not have to accurately describe the **password** that it is prompting for. For example, the prompt could be "What is 4+5?", and the password could be "germany".

Important Note: When you are using the demo, the configuration screen appears every few days to remind you that you are using the evaluation version of WhoStoleMyPC. However, once you purchase the product, the configuration screen will *never* appear without your asking (for obvious reasons). So be sure to make the keystroke and password something that you will remember!

4.4 Watchdog

WhoStoleMyPC Configuration

Watchdog Commands File Transmission Advanced
Machine Information Configuration Screen Watchdog

If this machine cannot (or is prevented from) communicating with the **WhoStoleMyPC** server for an extended period of time, a set of pre-selected commands will be activated.

Activate commands after days.

After this period of non-communication, you will be prompted for the password below. A limited number of failed password attempts is allowed (one attempt per day).

Allowable failed password attempts:

Prompt:
Security Question:

Configuration Password:

Confirmation:

(**Watchdog Commands** can be specified on the next tab).

Previous Next OK Cancel Help

If the computer cannot communicate with the Internet for an extended period, a set of pre-selected instructions will be executed. On this screen, you set several of the parameters that determine how this is done.

The **Activate commands after** prompt allows you to specify exactly how long the computer should go without communication before it starts to wonder what's happened.

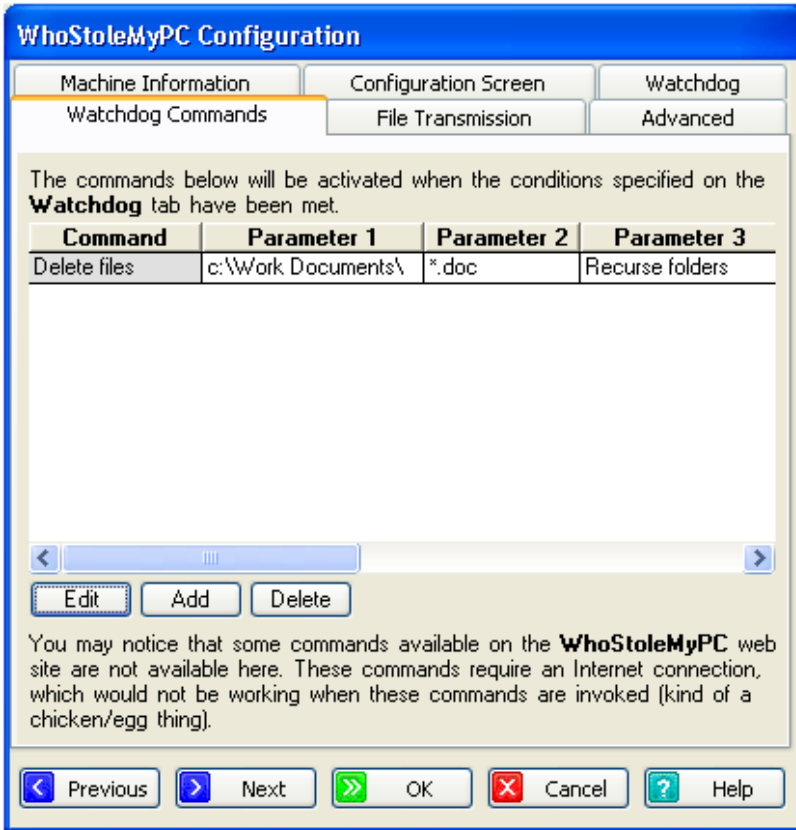
Once the computer has determined that it hasn't been able to talk to the internet for a long time, it will prompt the user with a question. This **Prompt** and **Password** are specified here. Although the prompt and password may look similar to the ones on the Configuration Screen, they are used in a completely different situation. You may or may not want to use the same prompt and password (it's up to you).

The **Allowable failed password attempts** tells the program how

many incorrect attempts should be allowed before the computer is deemed stolen. If you don't trust your memory, you may want to increase this number.

After the specified number of failed attempts, WhoStoleMyPC will initiate Watchdog Mode. In this mode, the commands specified on the Watchdog Commands tab will be executed.

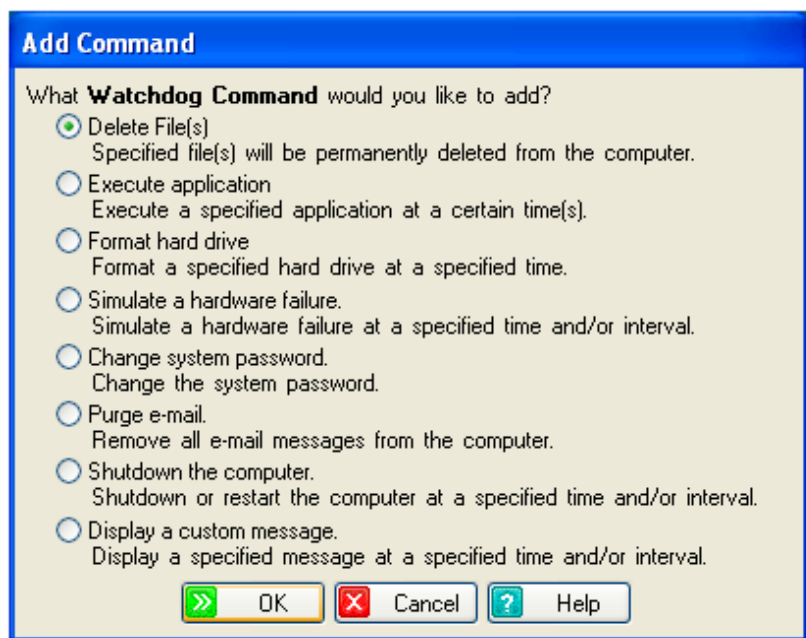
4.5 Watchdog Commands



As discussed on the Watchdog screen, if the computer cannot communicate with the Internet for an extended period, a set of pre-selected instructions will be executed. On this screen, you specify what those instructions will be.

The list at the top of the screen will list the commands you have specified. When you first install WhoStoleMyPC, this list will be empty. Once you have added commands (below), you can edit them by clicking the **Edit** button. Not surprisingly, you can delete them by clicking the **Delete** button.

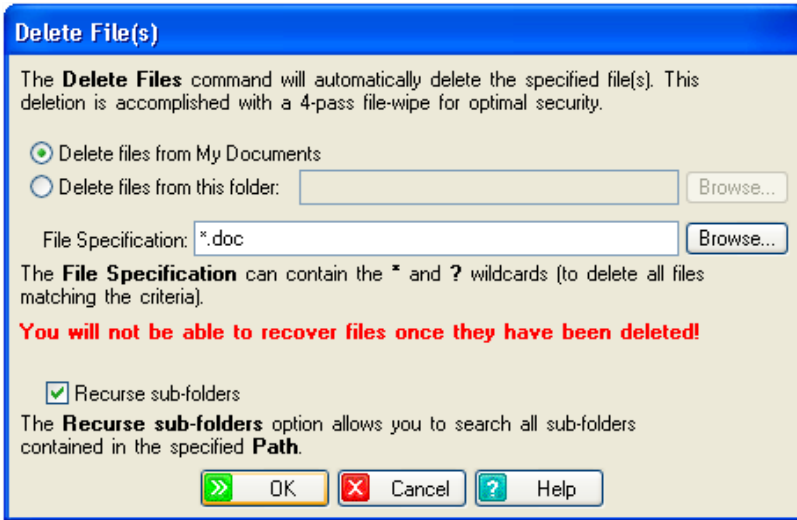
Click the **Add** button to add a new watchdog command. When you do this, the following screen will appear:



Here you can select the command to be added:

- **Delete Files** Permanently remove file(s) from the computer.
- **Execute Application** Execute an application at a certain time.
- **Format Hard Drive** Format a hard drive at a certain time.
- **Simulate a Hardware Failure** Simulate a hardware failure at a certain time and/or interval.
- **Change System Password** Change the Windows password.
- **Purge E-Mail** Remove all e-mail messages from the computer or an account.
- **Shutdown the Computer** Shutdown or restart the computer at a certain time and/or interval.
- **Display a Custom Message** Display a message at a certain time and/or interval.

4.5.1 Delete Files



The specified files will be deleted from the computer. If there's sensitive information on the computer, it may be best to get rid of it ASAP. This deletion is a 4-pass file-wipe, which will prevent all but the most sophisticated hackers from recovering your files.

You can elect to delete files in your "My Documents" folder by selecting **Delete files from My Documents**, or you can specify the location of the file(s) to be deleted by selecting **Delete files from this folder**. Click the **Browse** button if you need assistance locating the folder.

Specify the name of the file(s) to be deleted in **File Specification**. Click the **Browse** button if you need help locating the file. The * and ? wildcards can be used to specify ranges of files. This can be very useful as it allows you to specify several files in a single command. For example:

- *.* will delete all files in the specified path.
- *.mp3 will delete all MP3 music files in the specified path.
- *.jp*g will delete all JPEG images (files with the .jpg or .jpeg extensions).

If **Recurse sub-folders** is checked, then WhoStoleMyPC will not only delete files matching the file specification in the specified path, but will also delete any files matching the file specification in any child folders (and their child folders, etc). This feature makes the Delete Files command even more powerful.

For example, if you want to ensure that all JPEG images are removed from your machine, you would specify `c:\` as the path, `*.jp*g` as the file specification, and check the recurse button.

Note that multiple instances of this command are allowed, so you can be selective about what files you want to delete.

Using the `*` wildcard and a file extension is usually a pretty reliable way to remove all files of a certain type.

4.5.2 Execute Application

Execute Application

The **Execute Application** command will automatically launch a program at a specific time or after a delay.

Execute at a specific time (hh:mm:ss): 10:00:00 AM

Execute after a set delay (hh:mm): 0:05

The application can be repeatedly launched at a specified interval (if a prior occurrence of the application is still running, it will not be launched a second time).

Repeat at time interval (hh:mm): 0:30

Remove this command after first operating session.

Start in Folder: c:\Program Files\UltraVNC

Application: c:\Program Files\UltraVNC\WinVNC.exe

Parameters:

The Execute Application command will execute the specified application. Why would you want to do this?

- To launch a virtual network server program so that you can try to access the machine over the Internet.
- To run a program that could provide more tracking information (maybe a GPS tracker, phone dialer, etc).
- Other things that we never thought of.
- Just to have a little fun with the thief.

You can either launch the application at a specific time (**Execute at a specific time**) or launch the program after the computer has been running for a certain amount of time (**Execute after a set delay**).

If the program usually runs for a little while before self-terminating, you may want the program to re-launch after a specific interval of

time (**Repeat at time interval**). Note that if the previous occurrence of the application is still running, then it won't be launched a second time (not until the first occurrence terminates).

If you would like the program to only execute a single time (and never again), check **Remove this command after first operating session**.

Specify the folder where the application should be launched in **Start in Folder**. The **Browse** button can be used to help you locate this folder.

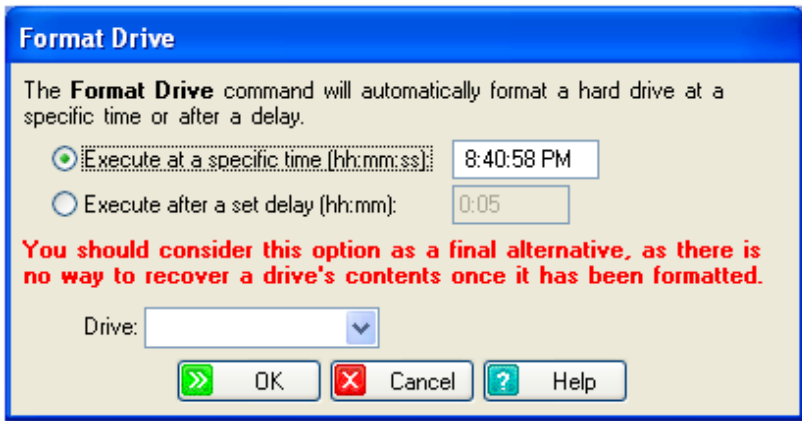
The executable (and optionally path) should be specified in **Application**. Again, the **Browse** button can be used to locate this file.

Any command line parameters should be specified in **Parameters**.

Hint: If you are unsure how to set up a particular application, there's an easy way to find out:

1. Locate the shortcut to the application on the desktop or **Start** menu.
2. Right-click the shortcut and click **Properties**.
3. Click the **Shortcut** tab.
4. Use the **Start in** entry for the **Start in Folder** (remove starting and ending double-quotes).
5. Use the **Target** entry for the **Application** (remove starting and ending double-quotes). Any text after the .exe in this entry should be moved to Parameters.

4.5.3 Format Hard Drive



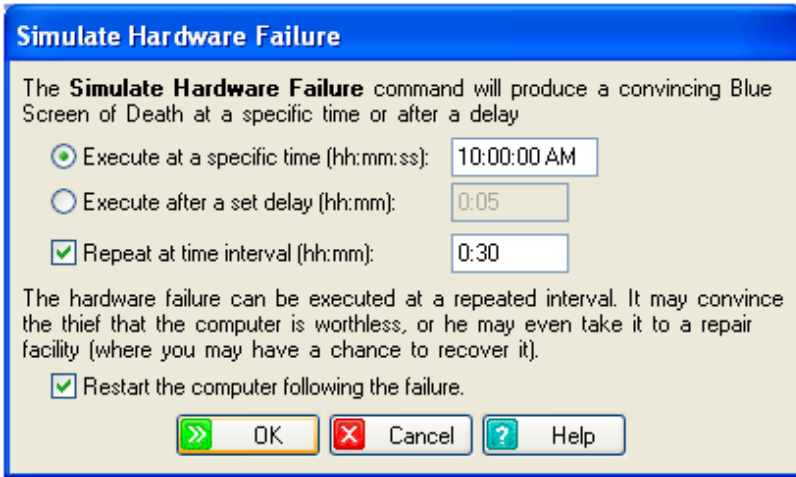
The Format Drive command will format a hard drive.

As noted on the dialog box, this is an extreme measure and should only be done when you've decided to wipe a drive clean. Once this is done, the drive's contents are nearly impossible to recover.

You can either format the drive at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a set delay**).

Specify the drive to be formatted in **Drive**. Note that the Windows drive (usually the **c:** drive) usually cannot be formatted. This would be akin to Windows committing suicide, which is not possible.

4.5.4 Simulate Hardware Failure



The Simulate Hardware Failure command will produce a Windows Exception screen (a.k.a. 'Blue Screen of Death').

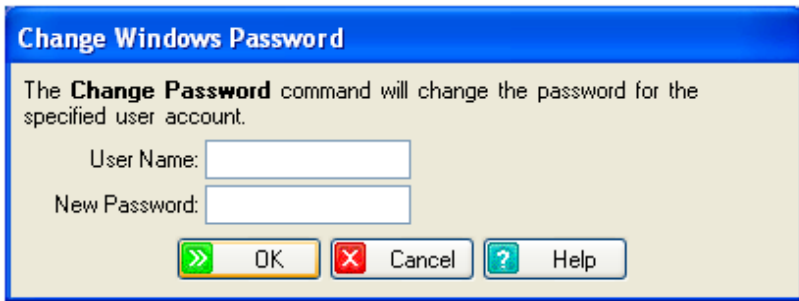
If you've used Windows for any amount of time, you've probably crossed paths with this screen once or twice. Think how annoying it will be to your thief if it appears every 30 minutes. He may even decide that there's something wrong with the computer and take it to a local PC repair shop. Maybe a repair shop that you've told to be on the lookout for your stolen machine...

You can either simulate the failure at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a set delay**).

The hardware failure can be repeated after a specific interval (**Repeat at time interval**).

Normally, the hardware failure will be displayed for a few minutes and then Windows will return to normal. However, you can opt to **Restart the computer following the failure**.

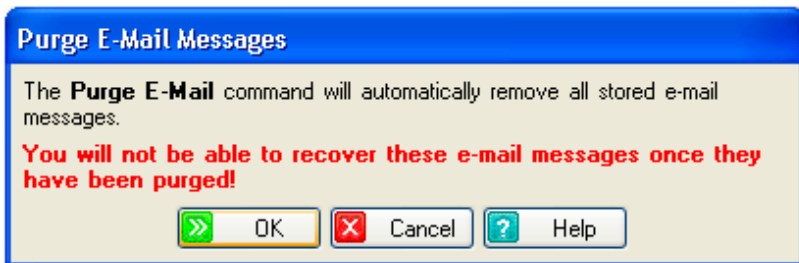
4.5.5 Change Windows Password



The Change Windows Password command will change the computer's Windows password. If you change the Windows password, it'll be harder for the thief to steal information. However, be warned that the Windows password is not very secure; there are several well-known methods to crack it.

Changing the password will usually trigger the **Enter Password** login dialog upon starting Windows, even if you've disabled it in the past.

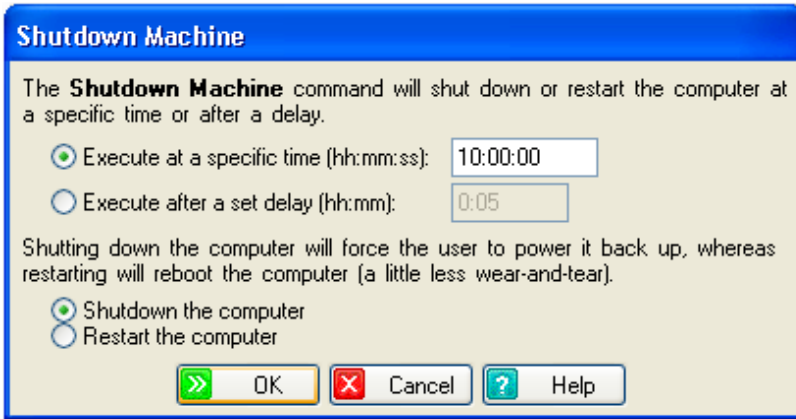
4.5.6 Purge E-Mail



The Purge E-Mail command removes all e-mail messages from the computer. If there's any e-mail messages with personal information, you probably will want to get rid of them before the thief can use this information.

There are no option settings for this command.

4.5.7 Shutdown Computer



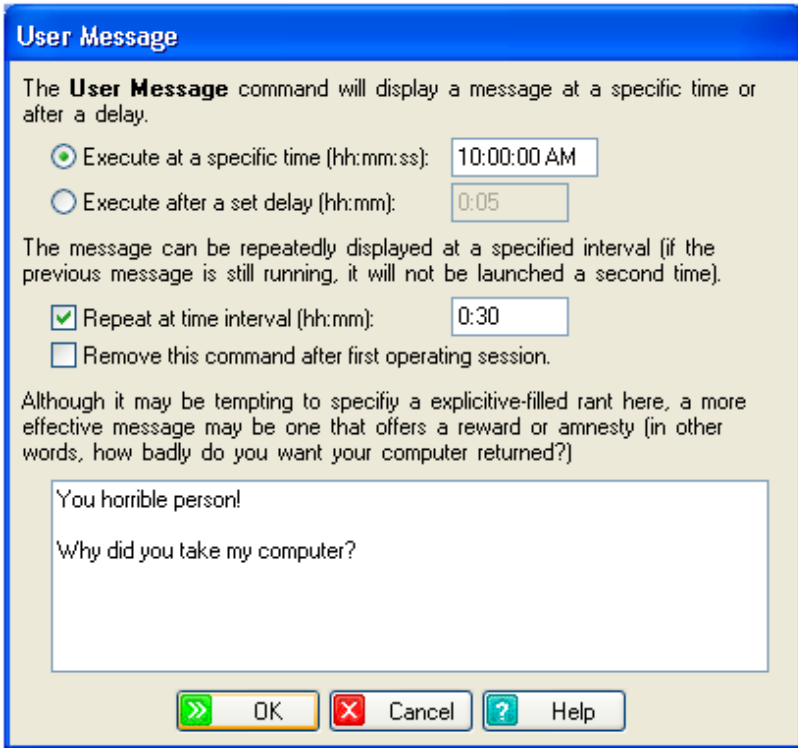
The Shutdown Computer command will shut down or restart the computer at a specific time or after being on after a delay. Not only will this be very annoying to the thief, he may decide that the computer is defective and try to have it serviced, or may give up trying to extract your information from it.

You can either shut down the computer at a specific time (**Execute at a specific time**) or after it has been running for a certain amount of time (**Execute after a set delay**).

The computer can either be shut down (turned off) or simply restarted (cycled as if you turned it off and back on).

Shutting down the computer will force the user to manually power it back up, whereas restarting will perform a reboot cycle, which causes a little less wear and tear on the computer.

4.5.8 Display Custom Message



The Display Custom Message command will display a message your choosing at a specific time or after a delay.

There's a variety of uses for this command. One tempting possibility is to unleash your wrath on the thief. Another approach may be to offer a reward and/or amnesty if he return the computer. If you think the computer's been sold, you may try to appeal to the new owner's ethics; he may even not be aware that he received stolen property.

You can either display the message at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a set delay**).

You may want the message to be displayed at specific intervals (**Repeat at time interval**). Note that if the previous message is still on the screen, the repeated message will not be displayed (not until the first one is closed).

If you would like the message to be displayed a single time (and never again), check **Remove this command after first operating session**.

4.6 File Transmission

The screenshot shows the 'WhoStoleMyPC Configuration' dialog box with the 'File Transmission' tab selected. The dialog has a blue title bar and a light yellow background. At the top, there are three tabs: 'Machine Information', 'Configuration Screen' (selected), and 'Watchdog'. Below these are three sub-tabs: 'Watchdog Commands', 'File Transmission' (selected), and 'Advanced'. The main content area contains the following text and fields:

Some FTP commands require an FTP server that will receive logs and files. See www.who stolemy pc.com if you don't have access to an FTP server (or don't know what one is).

FTP Server Address:

Target Folder:

User Name: It is a good idea to test the connection by hitting **Test FTP** below (a small file **Test.txt** is transferred).

Password:

Confirmation:

Transmitted files are compressed and protected using the password below:

Password:

Confirmation:

At the bottom, there are five buttons: 'Previous' (left arrow), 'Next' (right arrow), 'OK' (green right arrow), 'Cancel' (red X), and 'Help' (question mark).

Some commands use an FTP server to relay information back to you. Information about your FTP server access is specified here.

The **FTP Server Address** is the URL you use to connect to the FTP server.

The **Target Folder** is a folder on the FTP server where you would like WhoStoleMyPC to transfer files and logs. You don't have to specify a target folder, but if you do, it must already exist on the server (WhoStoleMyPC will not create it for you).

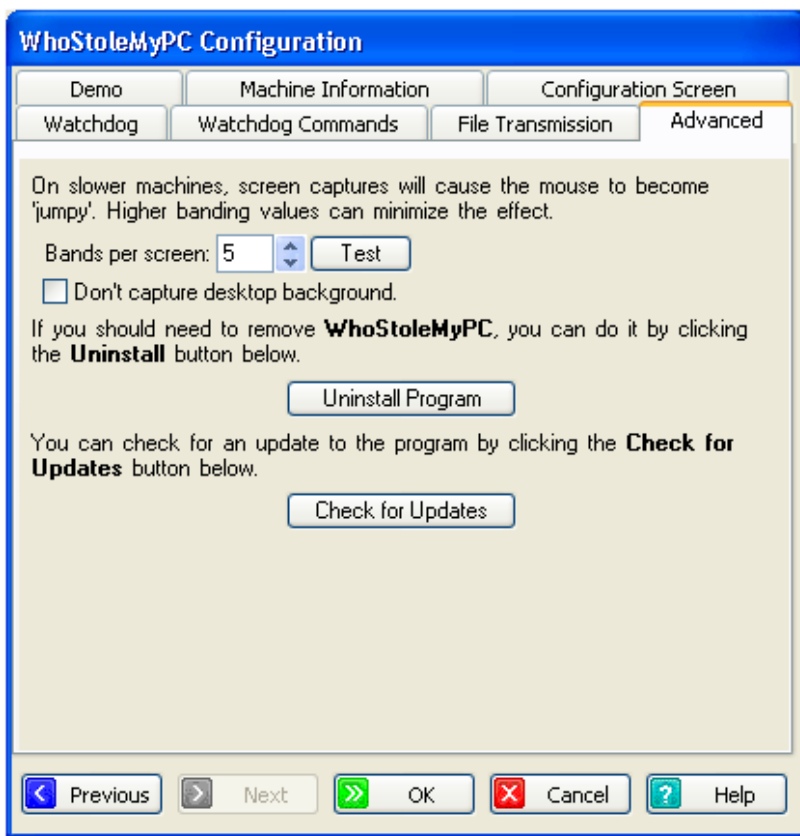
The **User Name** and **Password** are the user name and password that you use when logging in on the server.

To ensure that you have entered your setting correctly, you can click the **Test FTP** button to test the settings. A small file, test.txt will be transmitted to the server. If WhoStoleMyPC indicates that the file

could not be transmitted, you should check the FTP settings on this screen.

When any files are transmitted to your FTP server, they are first compressed using zip compression and protected with a the **Password** specified on this screen.

4.7 Advanced



The Advanced screen covers a few settings that really don't fit on any other screen. Some of them you will never need to adjust.

The **Bands per Screen** and **Don't capture desktop background** settings are used to tweak the Log Screen Contents command. This command can demand a lot of processing power, and may be noticeable to the thief as a slight 'stutter'. Adjusting these settings may cause the effect to be less noticeable. The **Test** button can be used to demonstrate what the effect will look like with the current settings.

If your computer is rather low-end, you may not find a combination of settings that can will satisfactorily. In this case, you should consider not using the Log Screen Contents command.

The **Uninstall Program** button allows you to remove WhoStoleMyPC from your computer. This is the only way to remove WhoStoleMyPC

from the machine - it is not listed in the Windows Uninstall Programs menu (that would make it too easy for the thief).

Note that you can temporarily uninstall the program and re-install it (on the same machine) at a later date. This can be useful if you are lending the computer to a friend and don't want to worry about the machine lapsing into Watchdog mode because it hasn't been connected to the Internet. On the other hand, if you don't trust your friend...

The **Check for Updates** button will check for program updates on our web server. If any are found, you will be prompted, and the updates installed.

5 www.who.stolemypc.com

In addition to the configuration settings that you can select through the Configuration screen, you can also control your PC remotely through www.who.stolemypc.com. In fact, if your computer is stolen, this will be the only way you can control your machine!

When you go to the web site, log in with your user name and password. You can then click **My Account**, which will show you information about your user account, as well as a list of computers under your control. Click **Manage** for the machine that you want to remotely control or configure.

Machine Management for "Work Computer":

Machine Name:

Last Contact: 2006-05-24 15:11:08

Machine ID Numbers:

Id 1:

Id 2:

Id 3:

Machine Status:

Normal

Stolen!

Demo

Event Log:

Date/Time	Ok?	Message
2006-05-24 15:11:08	Yes	Contacted server from 24.91.9.18
2006-05-24 15:05:50	Yes	Contacted server from 24.91.9.18
2006-05-24 15:00:34	Yes	Contacted server from 24.91.9.18
2006-05-24 14:56:43	Yes	Contacted server from 24.91.9.18
2006-05-23 10:10:26	Yes	Contacted server from 24.91.9.18
2006-05-19 15:24:07	Yes	Contacted server from 24.91.9.18

Clear: [>1 day](#) [>2 days](#) [>7 days](#) [>14 days](#) [All](#)

Commands:

Edit?	Del?	Cmd	Parameters
Edit	Delete	<input type="checkbox"/> Transmit files to FTP site	My Documents, *.sav, Don't recurse folders, Don't delete after transmission

= Task Completed
 = Task Not Completed
 = Task in Progress

[Add Task](#) [Delete All Tasks](#) [Delete Completed Tasks](#)

[Manage Another Machine](#)

The **Machine ID Number** list shows the MAC Address and Drive Serial Numbers associated with this machine. These are the same identification numbers shown on the Machine Information configuration screen (presented here so you can get them if your machine is stolen).

The **Machine Status** indicates the current status of the machine:

- Normal The machine is in your possession, no commands are executed.
- Stolen The machine has been taken, the specified commands below will be executed.
- Demo You are trying out WhoStoleMyPC, the specified commands below will be executed, but in a limited manner.

The **Event Log** lists transmissions received from the machine, as well as the completion status of any commands that have been executed.

The **Commands** section lists the commands that will be executed if the computer's status is changed to **Stolen**. This section is the heart of how you control a stolen computer.

Click Add Task to add commands to the list.

5.1 Commands

The following commands can be specified from the WhoStoleMyPC website:

- **Log IP Locations** Log the computer's current IP address at a specific time interval (sent to you via FTP).
- **Log Screen Contents** Log the computer's screen contents at a specific time interval (sent to you via FTP).
- **Log Keystrokes** Log keyboard activity (sent to you via FTP).
- **Log Visited URLs** Log visited web sites (sent to you via FTP).
- **Log Incoming E-Mails** Log incoming e-mail messages (sent to you via FTP).
- **Transmit Files to FTP Site** Transmit specific files to your FTP site.
- **Delete Files** Permanently remove file(s) from the computer.
- **Purge All E-Mail Messages** Remove all e-mail messages from the computer or an account.
- **Change Windows Password** Change the Windows password.
- **Shutdown Computer** Shutdown or restart the computer at a certain time and/or interval.
- **Format Hard Drive** Format a hard drive at a certain time.
- **Simulate Hardware Failure** Simulate a hardware failure at a certain time and/or interval.
- **Execute Application** Execute an application at a certain time.
- **Display User Message** Display a message at a certain time and/or interval.
- **Change FTP Information** Change your FTP location, user name, password, etc.
- **Change Zip Password** Change the password used during file compression on FTP transmissions.
- **Uninstall WhoStoleMyPC** Remove WhoStoleMyPC from the machine.

You will notice that many of these commands are available as Watchdog Commands on WhoStoleMyPC's configuration screen. The additional commands you see here use FTP access, which would not be available in a watchdog situation (because watchdog commands are only used when there is no Internet access).

Some commands cannot be specified more than once and are disabled if they are already in use.

5.1.1 Log IP Locations

Log IP Locations:

The computer's IP address will be recorded at a periodic time interval. The log will be sent to your FTP server every 2 hours. This information may be useful in determining the thief's location.

Frequency: Number of seconds between IP traces. 600 secs (10 mins) is a good starting point.

IP Addresses will be logged at a specified time interval. This log is sent to your FTP server periodically. IP addresses are similar to telephone numbers, in that they are unique numbers that identify a computer on a network.

However, the IP Address of your machine may not be the one that the Internet 'sees'. Often there will be one or more DHCP routers between your computer and the Internet. Because of this, WhoStoleMyPC records each address (a.k.a. 'hops') between your computer and the Internet. Each hop is listed in the log, in the format:

```
05/31/06 at 12:15:00: 192.168.0.1, 255.255.0.0,  
255.255.0.0, 255.255.255.0, 255.255.255.255
```

The first IP address listed will be the one of the your computer. Each subsequent address will be one further hop from your computer to the Internet. Some of the first few hops will be DHCP addresses assigned by local area networks (often ones starting with 192).

IP logs are transmitted to the FTP server with a filename formatted: "mm-dd-yy hh-mm-ss.rlg".

How do I Determine the Location of an IP Address?

There are a few web sites that can assist in determine an IP Address's geographic location:

- www.geobytes.com
- www.ip2location.com
- www.hostip.info

You will notice that the information provided by these sources is sometimes not entirely accurate. This is because of two reasons:

- Internet Service Providers (ISPs) often dynamically assign addresses - a user may have address 'x' one day, and 'y' the next - the geographic address usually will indicate the location of the ISP.
- There is no 'official' IP address geographic database - the sites listed above gather information from several sources to determine a probably geographic location.

When you have collected a set of IP Address logs, you should give this information to your local authorities. Once an ISP has been determined, a subpoena can be served to the ISP, who should be able to give much more exact information about who used a particular IP address at a given time, possibly leading to arrest and/or recovery.

5.1.2 Log Screen Contents

Log Screen Contents:

The screen contents will be logged at a periodic time interval and sent to your FTP server. This information may be useful in determining the thief's location, identity or intentions.

For best efficiency, screen shots are only taken when WhoStoleMyPC detects activity and they are JPEG compressed at the quality you specify below.

Frequency: Number of seconds between screen shots. 300 secs (5 mins) is a good starting point.

Quality: Compression quality (100=best, 0=worst). The higher the quality, the larger the file (75 is a good compromise).

Screen shots will be taken at the specified time interval. These shots will be saved in JPEG format with the specified compression quality. The higher the quality, the larger the file. Screen shot JPEGs are transmitted to your FTP server immediately; at times your FTP server may receive a fairly steady stream.

Although screen shots are generally not taken if no activity is detected, they can bog down your FTP server if you use a low frequency. When first starting out, you may want to try a high frequency and gradually lower it if needed.

Screen shots can give you information as to what the thief is doing with your computer. Depending on what he is doing, you may also be able to determine his name and whereabouts.

Screen shot JPEG files are transmitted to the FTP server with a filename formatted: "mm-dd-yy hh-mm-ss.jpg".

5.1.3 Log Keystrokes

Log Keystrokes:

Keyboard activity will be continually logged. The log will be sent to your FTP server every 2 hours. This information may be useful in determining the thief's identity or intentions.

<< There are no user-editable parameters for this command >>

All keyboard activity will be recorded. This log will be sent to your FTP server periodically.

Alone, a keystroke log may or may not be able to give you information regarding the thief's identity or whereabouts. When used in combination with Screen Content Logging, more information may be available.

If there has been no keyboard activity for a while, new activity will be preceded with a date and time stamp:

```
05/31/06 at 12:15:00:
```

Keystroke logs are transmitted to the FTP server with a filename formatted: "mm-dd-yy hh-mm-ss.rlg".

Synchronizing Keystrokes and Screenshots:

Screen shot JPEGs are always saved with the filename format: "mm-dd-yy hh-mm-ss.jpg". Similarly, entries in the keystroke log will have timestamps as indicated above. It is a simple matter of locating the approximate keystroke entry that corresponds to a screenshot to determine what was entered at specific prompt.

Note that the keystroke log does not take into account mouse actions. For example, if the thief typed "password", highlighted the first 's' with the mouse, right-clicked, and clicked **Cut**, the keystroke log would only have recorded "password". Your best bet in this situation is to find another incident when he entered data at the same prompt and compare the results.

5.1.4 Log Visited URLs

Log Visited URLs:

The computer's list of visited URLs will be recorded at a periodic time interval. The log will be sent to your FTP server every 2 hours. This information may be useful in determining the thief's identity or intentions.

For example, if you see visits to a particular eBay auction, it may be worth your while to check to see whether it is your computer that is being sold.

Frequency: Number of seconds between IP traces. 1800 secs (30 mins) is a good starting point.

Visited URLs will be logged at a specified time interval. This log is sent to your FTP server periodically.

This information can be useful to you in determining the identity of the thief as well as his intentions. For example, if you see several visits to a particular ebay auction, you probably should check it out to see if he is trying to sell your computer. Each visit is listed in the log, in the format:

```
05/31/06 at 12:15:00:  
www.whostolemypc.com/index.php4
```

Visited URL logs are transmitted to the FTP server with a filename formatted: "mm-dd-yy hh-mm-ss.ulg".

Keep in mind that there's no filtering performed; be warned that some of the sites visited by the thief may contain extremely objectionable content.

5.1.5 Log Incoming E-Mail

Log Incoming E-Mails:

The computer's incoming e-mails will be recorded at a periodic time interval. The log, sent to your FTP server every 2 hours, will contain the names and addresses of the senders and recipients, as well as the e-mail's content. This information may be useful in determining the thief's identity or intentions.

If your computer is stolen, we urge you to immediately change the passwords of any e-mail accounts that the computer has access to. This command is primarily intended to intercept the thief's e-mails, not to recover your own!

Frequency:	<input type="text" value="1800"/>	Number of seconds between e-mail scans. 1800 secs (30 mins) is a good starting point.
Account Profile:	<input type="text"/>	Name of profile to scan. If you have multiple e-mail profiles, specify the profile here. Most people use a single default profile, and can leave this entry blank.
Account password:	<input type="text"/>	Profile password.
Confirmation:	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

Incoming e-mail messages will be logged at a specified time interval. This log is sent to your FTP server periodically.

This information can be useful to you in determining the identity of the thief as well as his intentions. Additionally, it can serve as a way to retrieve any of your own e-mail messages that may have been received on the stolen computer (See note below)

Each e-mail is listed in the log, in the format:

```
=====
DATE: mm/dd/yyyy
FROM: support@whostolemypc.com
TO: thief@stolenpc.com
SUBJECT: Stolen Computer
```

Hello World!

Visited URL logs are transmitted to the FTP server with a filename formatted: "mm-dd-yy hh-mm-ss.mlg".

Important Note:

If your computer is stolen, you should immediately change your e-mail password so that the thief cannot retrieve your e-mail! In fact, you probably should consider abandoning any e-mail accounts that

the thief has access to. Also, any e-mail messages on the machine should be considered compromised.

5.1.6 Transmit Files to FTP Site

Transmit Files to FTP Site:

The specified files will be compressed and transmitted to your FTP server. If there are any files on the computer that you desperately need back, this command can be a lifesaver.

The wildcard operators * and ? are allowed to make it easier to specify multiple files (for example, "*" .jpg" to retrieve all JPEG files). You can also elect to recurse sub folders, which will search all files in the specified path as well as in any folders (and sub-folders, etc). Be careful using wildcards and recursing sub folders, as you could wind up with a lot of files on your FTP server.

Note that multiple instances of this command are allowed, so you can be a bit selective about which files you want to transmit.

WhoStoleMyPC can delete files immediately after they've been transmitted. A more conservative approach would be to add the **Delete Files** command once the desired files are in your possession.

Transmit files from...

My Documents

Specific Folder:

File path (drive and directory).

File(s):

File(s) to transmit. The wildcard operators * and ? may be used to specify multiple files.

Recurse Sub Folders

Delete File(s) After Transmission

The specified files will be compressed and transmitted to your FTP server. If there are any files on the computer that you desperately need back, this may be your only chance.

You can elect to delete files in your "My Documents" folder by selecting **My Documents**, or you can specify the location of the file(s) to be deleted by selecting **Specific folder**.

Specify the name of the file(s) to be deleted in **File(s)**. The * and ? wildcards can be used to specify ranges of files. This can be very useful as it allows you to specify several files in a single command. For example:

. will transmit all files in the specified path.

*.doc will transmit all Microsoft Word documents in the specified path.

*.jpg will transmit all JPEG images (files with the .jpg or .jpeg extensions).

If **Recurse sub-folders** is checked, then WhoStoleMyPC will not only transmit files matching the file specification in the specified path, but will also transmit any files matching the file specification in any child folders (and their child folders, etc). This feature makes the Transmit Files command even more powerful.

For example, if you want to ensure that all Word documents are

transmitted to your FTP server, you would specify `c:\` as the path, `*.doc` as the file specification, and check the recurse button.

Note that multiple instances of this command are allowed, so you can be selective about what files you want to transmit.

Using the `*` wildcard and a file extension is usually a pretty reliable way to remove all files of a certain type.

5.1.7 Delete Files

Delete Files:

The specified files will be deleted from the computer. If there's sensitive information on the computer, it may be best to get rid of it ASAP. File deletion is accomplished with a 4-pass file wiping algorithm that makes it nearly impossible for the file to be recovered.

The wildcard operators `*` and `?` are allowed to make it easier to specify multiple files (for example, `"*.jpg"` to remove all JPEG files). You can also elect to recurse sub folders, which will search all files in the specified path as well as in any folders (and sub-folders, etc). Be careful using wildcards and recursing sub folders, as you could wind up accidentally deleting a lot of files.

Note that multiple instances of this command are allowed, so you can be a bit selective about which files you want to delete.

Delete files from...

My Documents

Specific Folder: File path (drive and directory).

File(s): File(s) to delete. The wildcard operators `*` and `?` may be used to specify multiple files.

Recurse Sub folders

The specified files will be deleted from the computer. If there's sensitive information on the computer, it may be best to get rid of it ASAP. This deletion is a 4-pass file-wipe, which will prevent all but the most sophisticated hackers from recovering your files.

You can elect to delete files in your "My Documents" folder by selecting **My Documents**, or you can specify the location of the file(s) to be deleted by selecting **Specific Folder**.

Specify the name of the file(s) to be deleted in **File(s)**. The `*` and `?` wildcards can be used to specify ranges of files. This can be very useful as it allows you to specify several files in a single command. For example:

- `*.*` will delete all files in the specified path.
- `*.mp3` will delete all MP3 music files in the specified path.
- `*.jp*g` will delete all JPEG images (files with the `.jpg` or `.jpeg` extensions).

If **Recurse sub-folders** is checked, then WhoStoleMyPC will not only delete files matching the file specification in the specified path, but will also delete any files matching the file specification in any child folders (and their child folders, etc). This feature makes the Delete

Files command even more powerful.

For example, if you want to ensure that all JPEG images are removed from your machine, you would specify `c:\` as the path, `*.jpg` as the file specification, and check the recurse button.

Note that multiple instances of this command are allowed, so you can be selective about what files you want to delete.

Using the `*` wildcard and a file extension is usually a pretty reliable way to remove all files of a certain type.

5.1.8 Purge E-Mail

Purge all E-Mail Messages:

Remove all e-mail messages from the computer. If there's any e-mail messages with personal information, you probably will want to get rid of them before the thief can use this information.

<< There are no user-editable parameters for this command >>

The Purge E-Mail command removes all e-mail messages from the computer. If there's any e-mail messages with personal information, you probably will want to get rid of them before the thief can use this information.

There are no option settings for this command.

5.1.9 Change Windows Password

Change Windows Password:

The computer's Windows password will be changed. If you change the Windows password, it'll be harder for the thief to steal information. However, the Windows password is not very secure; there are several well-known methods to crack it.

Changing the password will usually trigger the "Enter Password" login dialog box in Windows, even if you've disabled it in the past.

User Name:	<input type="text" value="Administrator"/>	User name. You do remember your user name, don't you?
Password:	<input type="password" value="AAAAAAAAAA"/>	New password.
Confirmation:	<input type="password" value="AAAAAAAAAA"/>	

The Change Windows Password command will change the computer's Windows password. If you change the Windows password, it'll be harder for the thief to steal information. However, be warned that the Windows password is not very secure; there are several well-known methods to crack it.

Changing the password will usually trigger the **Enter Password** login dialog upon starting Windows, even if you've disabled it in the past.

5.1.10 Shutdown Computer

Shutdown Computer:

The computer will be shut down or restarted at a specific time or after being on after a delay. Not only will this be very annoying to the thief, he may decide that the computer is defective and try to have it serviced, or may give up trying to extract your information from it.

Shutting down the computer will force the user to manually power it back up, whereas restarting will perform a reboot cycle, which causes a little less wear and tear on the computer.

- Execute at a specific time: Computer's local time in the form **hh:mm:ss**
 Execute after a delay: Delay in the form **hh:mm**

Shutdown/Restart:

- Shutdown
 Restart

The Shutdown Computer command will shut down or restart the computer at a specific time or after being on after a delay. Not only will this be very annoying to the thief, he may decide that the computer is defective and try to have it serviced, or may give up trying to extract your information from it.

You can either shut down the computer at a specific time (**Execute at a specific time**) or after it has been running for a certain amount of time (**Execute after a set delay**).

The computer can either be shut down (turned off) or simply restarted (cycled as if you turned it off and back on).

Shutting down the computer will force the user to manually power it back up, whereas restarting will perform a reboot cycle, which causes a little less wear and tear on the computer.

5.1.11 Format Hard Drive

Format Hard Drive:

The specified hard drive will be formatted at a specific time or after being on after a delay. For most people, this is overkill, and the **Delete Files** command is probably more appropriate, but if you'd like to empty an entire drive, this may be for you.

If you specify the Windows drive (ie, usually the c: drive), you will effectively remove Windows from the machine. However, you will also remove WhoStoleMyPC, so at that point, you will lose remote control over your computer.

- Execute at a specific time: Computer's local time in the form **hh:mm:ss**
 Execute after a delay: Delay in the form **hh:mm**

Drive: The drive to format in the form **x:**

The Format Drive command will format a hard drive.

As noted on the dialog box, this is an extreme measure and should only be done when you've decided to wipe a drive clean. Once this is

done, the drive's contents are nearly impossible to recover.

You can either format the drive at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a set delay**).

Specify the drive to be formatted in **Drive**. Note that the Windows drive (usually the **c:** drive) usually cannot be formatted. This would be akin to Windows committing suicide, which is not possible.

5.1.12 Simulate Hardware Failure

Simulate Hardware Failure:

A hardware failure will be simulated at a specific time or after being on after a delay. This hardware failure (a 'Blue Screen of Death') is very convincing; the thief may assume that the computer is unusable or may even take the computer to a repair center.

<input type="radio"/>	Execute at a specific time:	<input type="text"/>	Computer's local time in the form hh:mm:ss
<input checked="" type="radio"/>	Execute after a delay:	<input type="text" value="0:10"/>	Delay in the form hh:mm
<input checked="" type="checkbox"/>	Repeat at interval:	<input type="text" value="0:10"/>	Repeat interval in the form hh:mm
<input checked="" type="checkbox"/>	Reboot after Hardware Failure		

The Simulate Hardware Failure command will produce a Windows Exception screen (a.k.a. 'Blue Screen of Death').

If you've used Windows for any amount of time, you've probably crossed paths with this screen once or twice. Think how annoying it will be to your thief if it appears every 30 minutes. He may even decide that there's something wrong with the computer and take it to a local PC repair shop. Maybe a repair shop that you've told to be on the lookout for your stolen machine...

You can either simulate the failure at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a set delay**).

The hardware failure can be repeated after a specific interval (**Repeat at time interval**).

Normally, the hardware failure will be displayed for a few minutes and then Windows will return to normal. However, you can opt to **Reboot after Hardware Failure**.

5.1.13 Execute Application

Execute Application:

An application of your choosing will be executed at a specific time or after being on after a delay. Note that the application must already be installed on the machine before it has been stolen!

There are a variety of uses for this command. One possibility would be to launch the [VNC server](#), allowing you to operate your computer over the Internet.

<input checked="" type="radio"/>	Execute at a specific time:	<input type="text" value="10:00:00"/>	Computer's local time in the form hh:mm:ss
<input type="radio"/>	Execute after a delay:	<input type="text" value="0:10"/>	Delay in the form hh:mm
<input type="checkbox"/>	Repeat at interval:	<input type="text" value="0:10"/>	Repeat interval in the form hh:mm
<input type="checkbox"/>	Remove command after first day of operation		
Start in Folder:	<input type="text" value="c:\Program Files\UltraVNC"/>	Folder containing the application.	
Application:	<input type="text" value="c:\Program Files\UltraVNC\WinVN"/>	Executable name (ie, filename.exe).	
Parameters:	<input type="text"/>	Application-specific parameters.	

The Execute Application command will execute the specified application. Why would you want to do this?

- To launch a virtual network server program so that you can try to access the machine over the Internet.
- To run a program that could provide more tracking information (maybe a GPS tracker, phone dialer, etc).
- Other things that we never thought of.
- Just to have a little fun with the thief.

You can either launch the application at a specific time (**Execute at a specific time**) or launch the program after the computer has been running for a certain amount of time (**Execute after a set delay**).

If the program usually runs for a little while before self-terminating, you may want the program to re-launch after a specific interval of time (**Repeat at interval**). Note that if the previous occurrence of the application is still running, then it won't be launched a second time (not until the first occurrence terminates).

If you would like the program to only execute a single time (and never again), check **Remove this command after first day of operation**.

Specify the folder where the application should be launched in **Start in Folder**.

The executable (and optionally path) should be specified in **Application**.

Any command line parameters should be specified in **Parameters**.

Hint: If you are unsure how to set up a particular application, there's an easy way to find out:

1. Locate the shortcut to the application on the desktop or **Start** menu.
2. Right-click the shortcut and click **Properties**.
3. Click the **Shortcut** tab.
4. Use the **Start in** entry for the **Start in Folder** (remove starting and ending double-quotes).
5. Use the **Target** entry for the **Application** (remove starting and ending double-quotes). Any text after the .exe in this entry should be moved to Parameters.

Of course, you can't do this after the computer's been stolen!

5.1.14 Display Custom Message

Display User Message:

A message your choosing will be displayed at a specific time or after being on after a delay.

There's a variety of uses for this command. One tempting possibility is to unleash your wrath on the thief. Another approach may be to offer a reward and/or amnesty if he return the computer. If you think the computer's been sold, you may try to appeal to the new owner's ethics; he may even not be aware that he received stolen property.

Execute at a specific time: Computer's local time in the form **hh:mm:ss**
 Execute after a delay: Delay in the form **hh:mm**
 Repeat at interval: Repeat interval in the form **hh:mm**
 Remove command after first day of operation

Message:

```
You horrible person!  
Why did you take my computer?
```

The Display Custom Message command will display a message your choosing at a specific time or after a delay.

There's a variety of uses for this command. One tempting possibility is to unleash your wrath on the thief. Another approach may be to offer a reward and/or amnesty if he return the computer. If you think the computer's been sold, you may try to appeal to the new owner's ethics; he may even not be aware that he received stolen property.

You can either display the message at a specific time (**Execute at a specific time**) or after the computer has been running for a certain amount of time (**Execute after a delay**).

You may want the message to be displayed at specific intervals

(Repeat at interval). Note that if the previous message is still on the screen, the repeated message will not be displayed (not until the first one is closed).

If you would like the message to be displayed a single time (and never again), check **Remove this command after first day of operation**.

5.1.15 Change FTP Information

Change FTP Information:

Change the information about the FTP site that will receive any transmitted information. You probably set this up when you installed WhoStoleMyPC on your computer, but you may have the need to change this information (ie, your FTP server has changed locations, you've changed the password, etc).

FTP Server Address:	<input type="text" value="ftp.who stole my pc.com"/>	The FTP server's address.
Target Folder:	<input type="text" value="workmachine"/>	Optional folder where files will be stored.
User Name:	<input type="text" value="bernierm"/>	FTP User name.
Password:	<input type="password" value="*****"/>	FTP password.
Confirmation:	<input type="password" value="*****"/>	

The Change FTP Information command allows you to remotely change the FTP settings that were set on WhoStoleMyPC's configuration screen.

Some commands use an FTP server to relay information back to you. Information about your FTP server access is specified here.

The **FTP Server Address** is the URL you use to connect to the FTP server.

The **Target Folder** is a folder on the FTP server where you would like WhoStoleMyPC to transfer files and logs. You don't have to specify a target folder, but if you do, it must already exist on the server (WhoStoleMyPC will not create it for you).

The **User Name** and **Password** are the user name and password that you use when logging in on the server.

When any files are transmitted to your FTP server, they are first compressed using zip compression and protected with a the password specified on the configuration screen. This password can be remotely changed with the Change Zip Password command.

5.1.16 Change Zip Password

Change Zip Password:

Files that are transmitted to your FTP server are compressed and protected with this password. If you need to change this password, you can do it here.

Password: New password.
Confirmation:

The Change Zip command allows you to remotely change the zip compression password that was set on WhoStoleMyPC's configuration screen.

Some commands use an FTP server to relay information back to you. These files are first compressed using zip compression and protected with a the password.

5.1.17 Uninstall WhoStoleMyPC

Uninstall WhoStoleMyPC:

Uninstall the program remotely. This can be useful if you forgot to remove it before lending or selling the computer to someone.

Note that the license remains activated on our server, so if you later reinstall, the computer will automatically reactivate that license.

Be careful using this command! Once you've removed the program, you will no longer be able to remotely control it.

<< There are no user-editable parameters for this command >>

The Uninstall WhoStoleMyPC command tells the program to remove itself from the host computer. This can be useful if you forgot to remove it before lending or selling the computer to someone.

Note that the license remains active on the WhoStoleMyPC server, so if you later reinstall the program, it will automatically reactivate that license.

Note:

Be careful using this command! Once you've removed WhoStoleMyPC from the computer, you will no longer be able to control it remotely.

6 In Case of Difficulty

- Please check the documentation first. Most questions relate to information contained here.
- Use the **Check for Updates** command on the Advanced configuration screen to look for the newest version of the software.
- Visit our web site (www.whoStoleMyPC.com) and check the user forums. Other users may have experienced a similar problem and posted an answer there.
- You can contact support online.
- If you're still stuck:

Technical Support: support@whoStoleMyPC.com

Sales & Purchasing Questions: sales@whoStoleMyPC.com

OEM & Partnering Questions: oem@whoStoleMyPC.com

Press & Reviewer Questions: marketing@whoStoleMyPC.com

Mailing Address: WhoStoleMyPC
49 Garden Road
Halifax, MA 02338-1020
USA

Phone: 508-967-xxxx

Index

-A-

Advanced 31

-B-

Bands per Screen 31

Blue Screen of Death 24, 44

-C-

Change FTP Information 35, 47

Change System Password 18

Change Windows Password 25, 35, 42

Change Zip Password 35, 48

Command 47

 Change FTP Information 47

 Change Windows Password 25, 42

 Change Zip Password 48

 Delete Files 20, 41

 Display Custom Message 27, 46

 Execute Application 21, 45

 Format Hard Drive 23, 43

 Log Incoming E-Mail 39

 Log IP Locations 36

 Log Keystrokes 37

 Log Screen Contents 37

 Log Visited URLs 38

 Purge E-Mail 25, 42

 Shutdown Computer 26, 43

 Simulate Hardware Failure 24, 44

 Transmit Files to FTP Site 40

 Uninstall WhoStoleMyPC 48

Commands 33, 35

Configuration 10

Configuration Password 14

Configuration Prompt 14

Configuration Screen 14

Contact 49

-D-

Delete Files 18, 20, 35, 41

Demo 11

Demo Activation 6

Display a Custom Message 18

Display Custom Message 27, 46

Display User Message 35

-E-

E-Mail Address 49

Event Log 33

Execute Application 18, 21, 35, 45

-F-

FAQ 49

File Transmission 29

Format Hard Drive 18, 23, 35, 43

FTP Address 29

FTP Password 29

FTP URL 29

FTP User 29

-H-

Hard Drive Serial Number 12, 33

-I-

Installation 6

Introduction 3

-K-

Keystroke 14

-L-

Last Communication 12, 33

License Activation 6

Log Incoming E-Mail 39

Log Incoming E-Mails 35

Log IP Locations 35, 36

Log Keystrokes 35, 37

Log Screen Contents 35, 37

Log Visited URLs 35, 38

-M-

MAC Address 12, 33

Machine Information 12, 33

Machine Status 12, 33

Mailing Address 49

Mode 12, 33

-N-

New User 6

-P-

Purge All E-Mail Messages 35

Purge E-Mail 18, 25, 42

-S-

Screen Shot 31

Shutdown Computer 18, 26, 35,
43

Simulate a Hardware Failure 18

Simulate Hardware Failure 24,
35, 44

System Requirements 6

-T-

Technical Support 49

Transmit Files to FTP Site 35, 40

Troubleshooting 49

-U-

Uninstall 31

Uninstall WhoStoleMyPC 35, 48

Update 31

-W-

Warning 5

Watchdog 16

Watchdog Commands 18

Watchdog Password 16

Watchdog Prompt 16

www.whostolemypc.com 33

-Z-

Zip Password 29

