



## About the Author

Mike Burstein is a principal and an IT Consultant with Dominion Repair Service, Inc. in Northern Virginia. He has many years experience installing, configuring and supporting computers and networks in commercial and residential settings.

The battle with spyware/malware has grown over the years as more and more people connect to the Internet. His expertise in fighting this problem is well known within the industry and this Ebook is designed to help the average computer user combat this problem in a cost effective manner.

Much of the work that Dominion Repair Service performs is related to cleaning up the damage that spyware./malware has created and has lead to our developing extensive skills in this fight.

Hopefully the information contained herein will provide you with the information that will help you surf the Web and process your email safely and without disastrous consequences to your computer and data.

## 1. What is spyware?

As you surf the Internet, aka the World Wide Web, many times you encounter offers that seem to be harmless. Programs, screensavers, backgrounds, ringtones and a multitude of other computer related items are available to download from the Internet for “Free”.

Are they really free? Maybe free of cost but if people took the time to read the licensing agreement (EULA), they would find that many offers are not free of strings. Of course, not all authors of spyware/malware include the information in their EULA that even warns the user of the additional programs that come with the “free” download.

These strings can include tracking programs to determine the sites you visit on the web, Trojans, worms and other malware that can be used to call “home” and run continually on your PC, key loggers that will steal your passwords and call home with the info, programs that will provide unscrupulous marketers with all of the email address in your address book so they can be spammed, annoying pop-up ads, dialers, browser hijackers that will redirect your browser to a new home page or search engine, and many other nefarious malware programs that bog down or crash your computer.

Email is another common way that spyware/malware enters your computer. Never, never, never open attachments on email from people that you don’t know. Even if the email is from a known person, if you aren’t expecting an email attachment from them, you should check with them first to verify the authenticity of the email attachment. This one simple, safe computing practice can eliminate most dangers that you encounter on the Internet.

Links in spoof email are another common source of spyware/malware. Never, never, never (did we say never) click on links in an email purportedly from a bank, company or other organization claiming that your account has a problem, no matter how clever and convincing the spoof email may be. If you aren’t sure of the validity of the email, simply go directly to the company’s website, type in the URL and log in to your account. If there really is a problem, it will show up immediately upon entering your account area.

Pornographic sites and gambling sites are the absolute worst offenders in the spread of spyware/malware. If your surfing activities take you to these types of sites, there probably isn’t any defense strong enough to protect your computer from the inevitable infestation that will occur. The enormous infections that occur when browsing these types of sites usually require a nuke and pave approach to remove the infections – format the drive and reinstall all software – a time consuming and expensive cure.

Another side effect of spyware/malware is that much of the code is poorly written and is the most prevalent reason for computing problems on PC's today. System lockups, unexpected reboot, the blue screen of death, the inability to shutdown, extremely slow processing speeds, the inability to connect to the Internet and a host of other problems can be directly traced to spyware.

What can you do to protect yourself and your PC? Are there tools available to help repair and protect your computer and your personal information from these spyware pirates?

Fortunately, these are numerous ways to protect your computer, most of which are truly free! No strings attached!

The trick is knowing which tools to use and how to use them. You also must be willing to invest the large amount of time necessary to run all of these tools.

This Ebook was written for precisely that purpose – to allow you to protect yourself and your computer from spyware/malware. If you will take the time to read this Ebook completely and implement the strategies offered, your time on the web is not likely to be spoiled by spyware.

The majority of these free tools require an Internet connection to use them effectively.

If you are fairly tech savvy, the most functional use of these tools to clean up your computer is to run them all in Safe Mode. Pressing the F8 key while the motherboard splash screen is showing during computer boot up will take you to the Safe Mode menu – use Safe Mode with Networking.

Additionally, a lot of spyware/malware hides in the System Restore area on your computer so it makes cleanup more effective if you turn off System Restore while running these tools.

System Restore can be accessed from the Control Panel, select System and then select the System Restore tab.

Be sure to turn System Restore back on after your cleanup scans are complete.

If you prefer to have the information and programs referenced in this Ebook on CD (or you are not able to connect your computer to the Internet), you will find the CD available at <http://RepairCD.DominionRepair.com> .

This self-running CD contains all of the tools discussed in this Ebook in addition to other critical preventative resources and recommendations to make your time on the Internet safer from intrusion.

## 2. Microsoft Windows Defender

Microsoft finally joined the fray against spyware when they purchased a leading anti-spyware tool developed by Giant Software.

Currently, this extremely effective tool is being offered for free by Microsoft for Windows XP and is included in Windows Vista.

The tool offers real time protection against infections from spyware/malware in addition to being an effective program to help remove existing spyware from your computer.

Updates can be configured to automatically download and install daily and a scan can also be scheduled to run daily, all with no user intervention.

Download the tool at (copy and paste the URL into your browser if necessary):

<http://www.microsoft.com/athome/security/spyware/software/default.mspx>

Before you run this scan, download the TCP/IP repair tool from chapter 7 in case you are unable to connect to the Internet after scanning.

### 3. The Ad-aware Weapon

If your computer is already infected with spyware, you will need to use additional programs to clean up the mess. No one program can remove all of the infected files from your computer.

After installing the tools described in this Ebook and updating all of them to the current definition files, turn off System Restore and re-boot into Safe Mode to run the scans individually.

One of the easiest to use spyware removal tools is Ad-aware by Lavasoft Software. This program can be downloaded from the LavaSoft USA website at no charge.

The URL is: [http://www.lavasoftusa.com/products/ad\\_aware\\_free.php](http://www.lavasoftusa.com/products/ad_aware_free.php)

After you download and install Ad-aware, be sure to use the *Check for Updates Now* utility before you scan for problems; this will download the most current definition file.

After running Ad-aware and removing all spyware entries that were identified, verify that you are able to connect to the Internet.

Before you run this scan, download the TCP/IP repair tool from chapter 7 in case you are unable to connect to the Internet after scanning.

## 4. The SpyBot Search and Destroy Weapon

After running Ad-aware, the next step to clean up your PC and protect it in the future is to scan with SpyBot Search and Destroy.

Patrick M. Kolla offers this outstanding free tool at: <http://www.safer-networking.org/en/download/index.html>

Once again, after you download and install SpyBot Search and Destroy, use the update utility to get the latest definition file.

After running SpyBot Search and Destroy and removing all spyware entries that were identified, verify that you are able to connect to the Internet.

Before you run this scan, download the TCP/IP repair tool from chapter 7 in case you are unable to connect to the Internet after scanning.

Another nice feature is the immunize program that will block a large database of known spyware sites in your browser – both Internet Explorer and Firefox. It is recommended that you immunize your computer after each definition file update.

Many of the authors of the free tools recommended in this eBook accept and appreciate donations for their tools (Donationware).

## 5. Online Scans

There are numerous online scanners to remove spyware/malware at no charge. You must be able to connect to the Internet to utilize these tools but you should run at least one of these if you are in the process of cleaning up your computer, however, more is better – feel free to run them all!

- Trend Micro HouseCall - <http://housecall.trendmicro.com/>
- BitDefender Online Scanner - <http://www.bitdefender.com/scan8/ie.html>
- Ewido antispware - <http://www.ewido.net/en/onlinescan/>
- Panda ActiveScan - [http://www.pandasoftware.com/activescan/activescan/ascan\\_2.asp](http://www.pandasoftware.com/activescan/activescan/ascan_2.asp)

Once again, if your computer is already infected, run them all in Safe Mode!

Before you run these scans, download the TCP/IP repair tool from chapter 7 in case you are unable to connect to the Internet after scanning.

## 6. Rootkit Infections

The most difficult spyware/malware infections are in the form of rootkit attacks. Rootkits use sophisticated techniques to avoid being detected by antivirus solutions.

Rootkits are programs designed to hide processes, files or Windows Registry entries. This type of software is used by hackers to hide their tracks or to insert threats surreptitiously on compromised computers. There are types of malware that use rootkits to hide their presence on the system.

There are a number of free tools to detect and remove these infections but most require an in-depth knowledge of the operating system files to use. Panda Security has one that detects and removes rootkits with an easy to use interface and is the only program that is recommended.

Panda Security Anti-Rootkit - [http://research.pandasecurity.com/archive/New-Panda-Anti\\_2D00\\_Rootkit-2D00-Version-1.07.aspx](http://research.pandasecurity.com/archive/New-Panda-Anti_2D00_Rootkit-2D00-Version-1.07.aspx)

Before you run this scan, download the TCP/IP repair tool from chapter 7 in case you are unable to connect to the Internet after scanning.

## 7. TCP/IP Stack Repair Tool

Many of the poorly written spyware programs end up corrupting the TCP/IP stack on your PC – this is the networking protocol that allows your PC to connect to the Internet.

This handy tool can get you back online quickly after you have removed spyware from your PC.

WinSockFix by Explicit Software Solutions can be downloaded from the following sites:

<http://www.tacktech.com/display.cfm?ttid=257>

<http://www.itc.virginia.edu/desktop/central/display/versions.php3?softwareID=67&nav=title>

After downloading the program, click WinsockFix.exe and then click the Fix button.

After the program finishes running, reboot your computer and you should be able to connect to the Internet.

## 8. On Patrol with WinPatrol

WinPatrol is another layer in the defense systems you need to use on your PC. This neat little intrusion detection program will alert you to any changes that occur to critical system resources on your computer without your knowledge.

Download this free tool at: <http://www.winpatrol.com/download.html>

Scotty is the tool in this program that will alert you to a nefarious program's attempt to install itself on your PC. Scotty's bark is an invaluable defender of your computer.

WinPatrol's author also offers an enhanced version for a nominal cost.

## 9. Preventative Measures

After you finish cleaning the spyware off of your computer, it becomes an easy task to keep it that way.

Begin a weekly preventative maintenance schedule to run Ad-aware and SpyBot Search and Destroy (run them immediately if you stumble into a hornets nest of spyware) in addition to the daily scan run by Microsoft AntiSpyware. Always download the most current definition files before scanning.

Pay attention to any alerts that Scotty (WinPatrol) brings to your attention – unless you are installing a program, you should always answer no to Scotty’s question, “Is it OK to install \_\_\_\_\_”.

Using these tools, in conjunction with an updated *Anti-Virus* program, will allow you to enjoy your Internet experiences with few or no problems.

You can find outstanding free anti-virus programs from the following links but be sure to read the licensing terms carefully – most do not allow commercial use and some limit use to one computer at home only:

- AVG Antivirus - <http://free.grisoft.com/doc/downloads-products/us/frt/0?prd=aff>
- avast! 4 Home Edition - [http://www.avast.com/eng/avast\\_4\\_home.html](http://www.avast.com/eng/avast_4_home.html)
- PC Tools Antivirus - <http://www.pctools.com/free-antivirus/>
- Avira AntiVir Personnel Edition - <http://www.free-av.com/>

If you prefer to have the information and programs referenced in this eBook on CD, you will find it available at <http://RepairCD.DominionRepair.com> .

This self-running CD contains all of the tools discussed in this eBook in addition to other critical preventative resources and recommendations to make your time on the Internet safe from intrusion.

## 10.Reprint Information

You are invited to use this eBook, in its' entirety, in your publication or website. The only requirement is the inclusion of the following at the end of this article:

*Mike Burstein is a principal in Dominion Repair Service Inc. in Northern Virginia and an IT Consultant who has been helping the Small/Medium Business community, SOHO's and Independent Professionals grow & prosper for over 20 years by selling and servicing computers and networks while using technology to get things done.*

Visit <http://www.DominionRepair.com> for the latest FREE tips & tricks.  
Email: [Info@DominionRepair.com](mailto:Info@DominionRepair.com)