

Basic Digital Officer Safety

May 2008

Creating a protected online investigation environment in the Windows Operating Systems

Todd G. Shipley, CFE, CFCE
CEO and President
Detective Sergeant (Retired)
Reno, Nevada Police Department



www.veressoftware.com

Copyright Notice

Copyright© Vere Software 2008.

The information contained in this document is protected by copyright under the laws of the United States of America and any applicable International laws. Users of this document are authorized to redistribute and reproduce the document without the written permission of Vere Software as long as the document is distributed or reproduced in its entirety along with this notice. Users of this document are not authorized to modify, or make public or commercially use the information without the written authorization of Vere Software. The registered marks referenced in this document are the property of their respective companies and imply no association with those companies and are used as a descriptive nature only under the “Fair Use” laws.

Special thanks to Stephen Turner, Detective Sergeant (retired) who provided the inspiration for this guide.

May 2008

Table of Contents

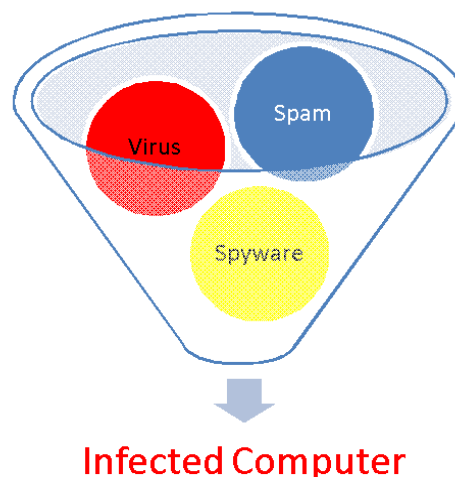
Digital Officer Safety	4
Online Investigative Computer Protection Process.....	5
I. Basic Investigative Computer Protection	6
Fire Walls	6
Hardware Firewalls.....	6
Basic steps to consider for securing a SOHO router	7
Software Firewalls	8
Virus Protection	9
Spyware Protection	10
Installing and updating browsers	12
Blocking Cookies	12
Windows Operating Systems and Application Changes	13
Disable file sharing	13
Antispam for Outlook.....	13
Windows Updates	13
II. Keeping your investigative computer secure	14
Encryption	14
Keeping your System Clean.....	15
Testing Your Security.....	15
Anonymizing your activities	16
Using the Vere Software Investigative Tool Bar	16

Digital Officer Safety

Conducting investigations on the Internet are not without general computer security problems. Anyone going on the Internet should take basic precautions to prevent the problems associated with viruses, spyware and malware. This document is not intended to deal with undercover situations. Instead, it should prepare the basic investigator with the various tools needed to ensure successful online investigations by limiting the investigators exposure to the dangers of the Internet.

All products mentioned in this paper are property of their respective companies. This is not an exhaustive list of potential software applications available in each category, merely suggestions for the investigator new to online investigations. We have found the following products useful in the prevention of your investigative computer becoming ineffective due to its compromise by either a virus or malware.

The intent of this paper is to provide the investigator with some consideration for the various protective tools available. Obviously, the installation of these tools will depend on the investigators administrative control over the operating system used for the online investigations. Many government owned computers require the user to obtain permission to load any additional software onto the government owned system and require administrative access to do so. In most cases, an agency's IT department will be protecting their system and the attached computers with many of these same types of applications. These suggestions are for the investigative computer not generally attached to an agencies network or behind existing firewalls. The online investigator needs to be aware of the potential Internet threats in order to help protect against data leakage, loss and potential system compromise.



The online threats to an investigator continue to be those commonly reported, such as viruses, malware, and other malicious code and external attempts to access your computers. Each of the thousands of types of threats can be protected against if the investigator understands the requirements and the tools to do so. It is important for the investigator to protect

his system to keep viruses and other threats from spreading to other agency controlled systems. It is also important to protect the validity of the investigation conducted and ensure that any Internet based evidence ultimately collected is protected from these potential threats.

NOTE: Before you download any software to your computer, be sure to read the software's instructions. Additionally, make sure that any software you add to your system is compatible with your version of the Windows operating system. Some software in this paper may not be compatible with the Windows Vista operating system.

Online Investigative Computer Protection Process

To protect your online activities, the following process is recommended. This, of course, depends on your current computer configuration and the protection you already have employed. The process is broken-down into two sections: 1) Basic investigative computer protection; 2) Keeping your investigative computer secure. The following process is a recommendation for securing your investigative computer:

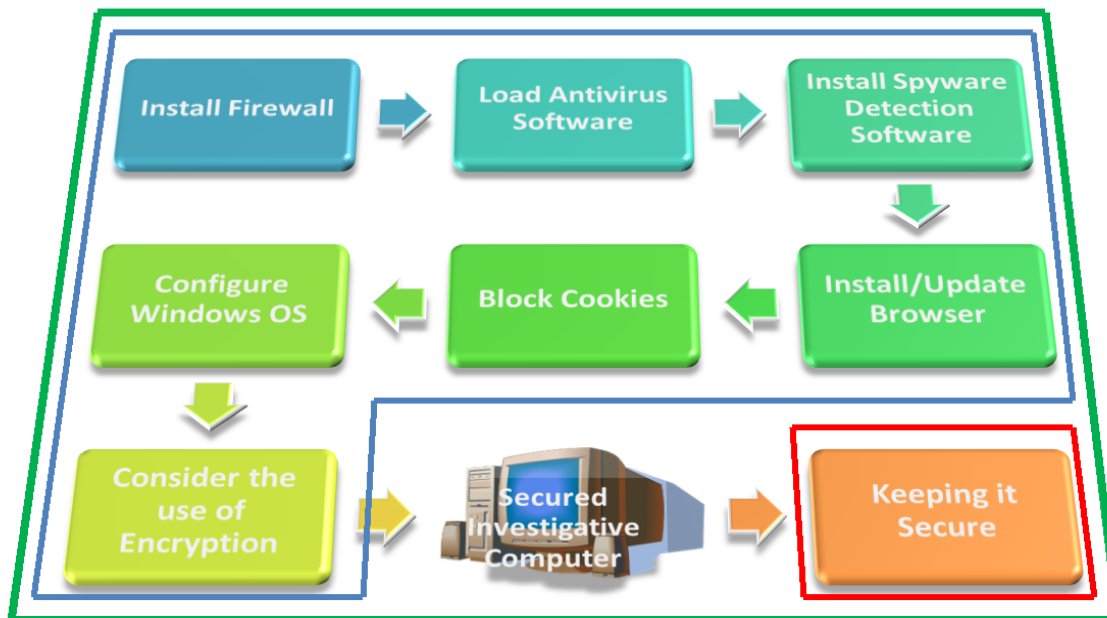


Figure 1 Online Investigative Computer Protection Process

I. Basic Investigative Computer Protection



Fire Walls

One of the most important aspects of controlling traffic to and from your computer is the use of firewalls. According to Wikipedia, a fire wall is "... a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules." Firewalls are another essential tool in controlling what happens to your computer while conducting investigations on the Internet. For our purposes, fire walls come in two general types, the hardware firewall and the software firewall.

You should have both a software firewall running as well as a hardware firewall in place. They protect against different things and each has their strengths/weaknesses. When you set it up, make sure to check the box to be notified of updates, otherwise, check their website for periodic upgrades. The program will notify you when a new version is available. If you do not install it, the firewall may cease to function or may be compromised by viruses. Listed below are several varieties of available hardware and software firewalls.



Hardware Firewalls

Hardware firewalls come in a variety of types. There are commercially available systems that cost thousands of dollars and are used by network administrators to control any size network. The most commonly available router for general use is the types that connect to the average SOHO network. They are small configurable routers which contain firmware that allow for user configuration and are intended for use with DSL or cable modem connections.

DLINK and Netgear make good routers and allow you to use one DSL or Cable modem to distribute your broadband between multiple computers as well as wirelessly. Additionally, you are able to network your computers to back up each computer's files on other network computers. They make inexpensive combo hardware/wireless routers which also allow the use of a laptop anywhere within 300 feet of the WIFI router. The routers offer firewall features that can be of great use to the online investigator. However, certain security steps should be considered prior use. Each router and its configuration are different. Be sure to read the manufacturers manual to identify

individual specific device security features. At a minimum, the following basic steps should be considered for the security of your router.

Basic steps to consider for securing a SOHO router

1	Enable Encryption	Enable the available encryption on your router. Current SOHO routers generally have WEP (an older encryption system), WPA (Wi-Fi Protected Access) preferable, or WPA2 encryption. Ensure you turn on the encryption and use a strong password/passkey, otherwise anyone with a wireless card could connect to your wireless access. If available, choose WPA-PSK (pre-shared key) and use a strong password/key.
2	Change the SSID/Disable Broadcast	The default SSID for your router needs to be changed to something unique to your system. The default SSID name makes it easier for hackers to identify and exploit. Disable the SSID broadcast so it cannot be seen. This will make your system stealthier and harder to discover.
3	Remote Management	Turn off remote management. Sometimes called WAN Management. This feature lets you change the router's settings from the Internet. It's an excessive risk.
4	Change the access password	Change the access password to your router to a strong password. Most hackers know the default passwords for most commonly sold routers and it has become an exploit. A strong password is at least 8-12 characters, including letters, numbers, and symbols. The longer the better. Do not use words in the dictionary or common names.
5	Disable Universal Plug and Play	Disable Universal Plug and Play on the router.

6	Media Access Control	A good security option is MAC (Media Access Control) addressing. This ties hardware device addresses for each computer to a specific network subnet address (as assigned by your router) associated with your machine in order to validate the devices.
7	Ping	Uncheck any options that allow the router to respond to a ping command from the internet.



Software Firewalls

Windows XP SP2 and Vista each come with a firewall. If you use them, ensure that you have the latest version. If you use one of the firewalls listed below, be sure to check its compatibility with Windows firewall. Most systems do not operate well when two software firewalls are running at the same time. Disable the Windows firewall before loading any other firewall to prevent any conflict between the software firewalls.



Zone Alarm www.zonelabs.com



Sun Belt Personal Firewall

<http://www.sunbelt-software.com/Home-Home-Office/Sunbelt-Personal-Firewall/>



CA personal firewall

shop.ca.com/downloads/free_trial_software.aspx



Virus Protection

Protecting your investigative computer from viruses is a basic step towards conducting investigations online. Having a proper virus application will help to prevent a virus from compromising an internet investigation.

The following virus application manufacturers provide products that will assist the investigators in the prevention of computer virus infections. Beware that a common problem with virus applications is their incompatibility with each other. Installing multiple virus applications on the same computer can cause unexpected problems. Before installing any new virus program, un-install any existing program first so that there is no conflict between the programs. You should update the programs/definitions periodically (manually or use the automatic update features) and do full manual scans, otherwise the programs are as worthless as if you never installed them.



Avast www.avast.com

This program updates frequently, sometimes 2-3 times a day when a lot of changed viruses are going around. It also automatically updates itself multiple times a day.



AVG www.grisoft.com

AVG updates more often than most commercial virus programs but is an effective antivirus program.



Norton Antivirus www.symantec.com

Symantec, maker of Norton Antivirus, is a major player in the antivirus community. Their product has been a standard for computer users for many years.



McAfee VirusScan www.mcafee.com

McAfee is another mainstay in the antivirus community.



LavaSoft Personal Fire Wall www.lavasoftusa.com

Lavasoft also makes a good Ad ware removal program.



Spyware Protection

Spyware has become one of the most pervasive threats when using the Internet. The simple act of accessing a website can put the web surfer at risk. Spyware has become a common method by which to attack computers. Spyware can also add the leakage of data from the infected computer. Spyware will make your machine slow to a crawl and often compromises security. Spyware infections can get so bad that you may have to reformat your hard drive to remove the offending programs.

As with virus protection, you should update the programs/definitions periodically (manually or use the automatic update features) and do full manual scans, otherwise the programs are as worthless as if you never installed them. Installing and using the listed software will remove most spyware and keep your system clean. However you have to use them all to get rid of most of these threats.

Some examples of programs that add in the detection and removal of spyware are:



Ad-Aware www.lavasoftusa.com

A freeware program that helps to protect you from spyware.



Spybot www.safer-networking.org

A freeware program that helps to protect you from spyware.



SpywareBlaster www.javacoolsoftware.com

A freeware program that helps to protect you from spyware.

**Microsoft Windows Defender**

www.microsoft.com/athome/security/spyware/software/default.mspx

Microsoft's spyware program. It's currently free as long as you validate your Windows XP operating system with Microsoft. Defender comes standard on Windows Vista. It doesn't work with earlier versions of the OS.



No Spy Mail www.belshe.com/nospymail

If you use HTML mail in Outlook, you should be aware that many spam senders embed spyware that notifies them if someone opens/deletes their spam. This lets them know your address is valid and you will get more of the same. HTML looks better but text only is safer.



McAfee Site Advisor www.siteadvisor.com

This is a free plug-in program for both IE and Firefox that lets you know if you're on an unsafe site with spyware.

**Rootkit Revealer**

www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.msp

This free program from Microsoft scans for a very nasty category of spyware called rootkits. Rootkits are a very stealthy form of spyware written to hide within the operating system.



Spy Sweeper www.webroot.com

The freeware version is very good but upgrade to the pay version for current updates.



Installing and updating browsers

A browser is an application that provides a way for users to access and interact with text documents, graphics and other computer files on the World Wide Web. Two of the most popular browsers are Microsoft's Internet Explorer and Mozilla's Firefox.



Internet Explorer www.microsoft.com/downloads

Internet Explorer is the web browser that comes standard with Windows Operating System. The current version of Internet Explorer that is available from Microsoft is version 7. This version is much better at protecting the user while online than previous versions.



Firefox www.mozilla.com/en-US

Firefox is a free, open source Web browser for Windows, Linux and Mac OS X. It offers customization options and various features including pop-up blocking, tabbed browsing, privacy and security measures. The Firefox user interface is designed to be easily customizable by adding "extensions". Firefox is one of the most popular browsers and has many extensions to expand its functionality.

Useful Internet Explorer and Firefox Extension¹

**Internet Explorer
URL Spoofing**

Spoofstick www.spoofstick.com

This extension verifies that the visible web address is actually where the user thinks they have surfed. If they match, you're good. If not, it identifies the true location.



Blocking Cookies

The purpose of cookies is to identify website users and potentially prepare customized Web pages when the user returns. A Web site using cookies, may ask the user to

¹ A great review of investigative Firefox Extensions can be located at www.search.org. The document, Firefox for Investigators, was written by Keith Daniels. It covers a wide variety of Firefox extensions useful to the online Investigator.

complete certain information about themselves or simply record information about their computer and their incoming Internet address. This information is saved in a “cookie”, sent through your Web browser, then stored on your computer. The next time you go to the same Web site, your Web browser will send the cookie previously downloaded to the Web server. This Web server can then use this previous information to present you with custom Web pages, such as “Hello Bob, thanks for returning to our web site”.

Cookies represent a potential security risk. The following article explains it in further detail: <http://www.grc.com/cookies.htm>



Windows Operating Systems and Application Changes

Disable file sharing

If you do enable it to share between two or more computers, enable it for a DMZ shared files folder only and make sure you have a strong password. A strong password is at least 8+ characters of random letters, numbers, and symbols. Never open up more folders than you need and **never** share the c:\ (root) drive.

Antispam for Outlook

Keep your Microsoft Office up-to-date and download the latest Microsoft Outlook email filters:

<http://office.microsoft.com/en-us/officeupdate/default.aspx>

A good add-on plug-in for Microsoft Outlook is a free program called Spambayes: <http://spambayes.sourceforge.net/windows.html>. You have to give the program some time and use the options to train it on your email to get it working to best efficiency.

Windows Updates

Make sure you have patched all critical Windows exploit. You can check at the following Microsoft website for those updates:

<http://v4.windowsupdate.microsoft.com/en/default.asp>

Enable automatic checking and manually check often for critical updates.

If you use Microsoft Office, Word, Outlook, or Express here's the link for critical patches:

<http://office.microsoft.com/OfficeUpdate/default.aspx>

II. Keeping your investigative computer secure



Encryption

Encryption of your working files is a recommended practice for the online investigator. Encryption prevents the unauthorized access of sensitive information. However, investigators new to using encryption should practice with the encryption tool they decide to use before ever using it on real case files. Once encrypted, if you lose the key, you have lost the files.

Encryption Programs



TrueCrypt www.truecrypt.org

TrueCrypt is a free open source encryption program.



Best Crypt www.jetico.com

Best Crypt makes several good products.



PGP www.pgp.com

PGP is the standard others compare to when making encryption decisions.



Keeping your System Clean

Your operating system needs regular maintenance to keep working at its peak efficiency. The Windows operating system stores many bits of information that over time can clog up your computer. Windows has two tools that are very useful for helping to optimize your Windows system. Both tools are located in Start Menu/Accessories/System Tools. There you will find Disk Cleanup and Disk Defragmenter. Both are tools that should be used on a regular basis to maintain the performance of your system.

There are many third party products to assist you in keeping your system running smoothly.



CCleaner www.ccleaner.com

CCleaner is one of the better all around Windows cleaning tools.



Fixit Utilities www.v-com.com/product/Fix-It_Utilities_Home.html

Another good product to help keep your system running.



Testing Your Security

Now that you have completely secured your computer you can test it to see how secure it is from the outside.

Using Shields Up!! and Leak Test by Gibson Research Corporation, you can test your investigative system to determine its security level and how much information it may be leaking. To check how stealthy your machine is to the Internet, I recommend the following site:

www.grc.com/x/ne.dll?bh0bkyd2

Other web locations for testing your system are:

www.dslreports.com/tools and

omicron.hackerwhacker.com/freetools.php

Both offer various tools to test the security of your system.

Use the Shields Up test to check for open ports and a report on your machine. This site also has a lot of useful information on compute. If you're interested in further information about securing computer systems, the author Steve Gibson's site is a good one to explore and learn about additional things to do in order to secure your computer. Check out www.grc.com/SecurityNow.htm for further.



Anonymizing your activities

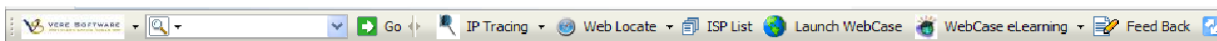
A useful program for this purpose is Anonymizer at www.anonymizer.com

This program hides your computer's IP address from the Internet and provides an encrypted tunnel (SSL) between your computer and Anonymizer's servers. SSL is the same encryption you see when you do banking or other secure business over the internet. It also reduces spam and tracking. Some sites don't like it (i.e. Google) because they think you're a hacker doing a denial of service attack. You can easily toggle the program on and off.



Using the Vere Software Investigative Tool Bar

The Vere Software Investigative Tool Bar was built to be a useful resource for the online investigator. The tool bar allows easy access for the online investigator directly from the browser to useful investigative sites, such as Internet Protocol tracing tools and websites to search for people. Investigators can easily track Internet Protocol addresses or search the various parts of the web. The tool bar also provides the users of **WebCase™**, the *Online Forensic Tool*, access to the online training and forums associated with WebCase™.



The tool bar can be located at www.veresoftware.ourtoolbar.com.