



Internet Preventative Maintenance

or

How to Maintain a Safer Computer and Have More Fun Online

(Last Update January 2009)

Introduction

It is the desire of TaosNet to provide you with the very best Internet experience. Recent events have shown us that many of the problems that are routinely experienced by our clients can be attributed to whether a computer has been protected against attacks by Malware — malicious software.

This document is intended for Windows computers since this operating system is the most widely used and the most vulnerable. In the past two years alone the number of threats our recommended tools remove has increased by a factor of ten! We are now in the unfortunate position of having to assume that every Windows computer we encounter is infected — the average infection comprising 100 to 300 instances. Keeping your machine clean is now a necessary maintenance issue. Ignorance is *not* bliss when it comes to malware.

The information presented in this document will help you maintain your own computer and alert you to the dangers of the “dark side of the Internet.” The Internet can be a very cool place if you remember to follow some basic precautions.

Maintenance is the Key

Just as when you own or use a car, there are some responsibilities involved in owning or using a computer. Because of the growing problem of malicious software, we must recommend strongly that your machine be cleared of potential malware on a regular basis. We suggest weekly for our customers who have high-speed connections, because your computer is connected all the time that it is on.

When you own an automobile, you are responsible for changing the oil on a regular basis. Some owners feel comfortable doing this themselves; others are not so inclined and must hire someone on a regular basis to do the work for them. If the oil is not changed, eventually it will kill the car. This same effect can happen with computers that are not properly maintained.

The purpose of this document is to empower you to “change your own oil” or perhaps allow you to decide that you’d rather hire a computer technician to help you maintain your system. The last thing you want is a computer worth hundreds of dollars lying around useless.

Even more closely parallel is our saying “You can’t keep the mud off your truck when you go out in the woods, so if you want a nice truck, you wash it when you get home.” This is just what happens to our computers on the Internet, and the tools we’re talking about allow you to do the washing.

An important point is that avoiding “bad” websites will not linger guarantee your computer stays clean. Good sites do get compromised and new vulnerabilities get exploited to infect computers even when the owners have done everything right.

Why do people write malicious software?

Why do people do anything that harms others? Well, like in many other endeavors, sometimes the mantra “Follow the Money” will give some kind of an answer. Other times, the old adage about climbing Mount Everest - “Because it’s there” is more apt.

Examples of money motivators include much of the spyware that is designed expressly to track your habits online, maintain a record that gets sent back to someone somewhere, for the purpose of targeting you with junk email or worse. This type of malware is certainly money-motivated, when the number of “hits” a site gets directly relates to advertising revenue. If the “hits” are generated artificially with the help of malicious software, we all lose. One method that has become more popular in recent years is the spam-generating “work at home” businesses that are advertised on daytime and late night television. These are often referral services that connect you to an agent that will charge you (!) to get involved in a spamming scheme.

An example of the latter effect is the childish behavior of certain so-called “script kiddies” who use malware toolkits (yes, there are even toolkits to help these jerks) to develop viruses and other malware for the express purpose of bragging rights. One recent example of this was the “war” between the writer of Netsky, who is now in jail in Germany, and the writer of Bagel (Beagle). They actually cursed at each other in the code hidden in various competing versions of their respective viruses!

The main thing to remember is that you can’t get rid of bad people’s actions, so you’d better anticipate them and be prepared to fight them!

Ya Wanna Buy a Watch??

If somebody on the street opens his trenchcoat and utters that famous phrase, you’re likely to kick them or laugh at them. You should have the same reaction to offers online, especially any popup window or balloon that appears. Many infections now operate through these popups.

Even if you do avoid the more obvious tricks, you’re still not home free. While you are turning down fake watches, someone could be stealing your car stereo. Some threats are just there to distract you from others. This means that your computer *can* get infected if you connect to the internet. You need to protect it and check regularly that it *stays* clean.

Recommended Software...

Mozilla Firefox and Thunderbird

Because of Microsoft’s domination of the industry, almost all attacks against your computer are actually directed at Microsoft software product vulnerabilities. In order not to give the malware authors a chance in the first place, you may want to consider using an alternative browser and email program! We even recommend these programs to our Macintosh users because of their features.

The internet browser we recommend is called Mozilla Firefox. We also recommend their excellent companion email program called Mozilla Thunderbird. You can get them when a machine is brought to us for cleanup, or they are available free at either:

<http://www.mozilla.com>

or *<http://www.getfirefox.com>* and *<http://www.getthunderbird.com>*

The Mozilla Foundation also offers a combined internet browser and email program called the SeaMonkey suite. It has the advantage of a what-you-see-is-what-you-get (WYSIWYG) HTML editor for those brave enough to try their own web page editing. Get it from:

<http://www.seamonkey-project.org/releases/>

Types of Trouble to Prevent

Although there is a short glossary in this document, the following definitions are direct from Symantec's Security Response system where there is a great discussion of the types of malware that we are all trying to address.

This link has great descriptions of the main types of malware, what they are and why people write them. Each description has a "more info" link, and we recommend checking out their site:

http://www.symantec.com/business/security_response/threatexplorer/risks/index.jsp

In short, the general malware categories are:

Adware: Programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purposes. This is often accomplished by tracking information related to Internet browser usage or habits. Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger adware by accepting an End User License Agreement from a software program linked to the adware.

Dialers: Programs that use a system, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.

Hack Tools: Tools used by a hacker to gain unauthorized access to your computer. One example of a hack tool is a keystroke logger — a program that tracks and records individual keystrokes and can send this information back to the hacker.

Joke Programs: Programs that change or interrupt the normal behavior of your computer, creating a general distraction or nuisance.

Remote Access: Programs that allow another computer to gain information or to attack or alter your computer, usually over the Internet. Remote access programs detected in virus scans may be recognizable commercial software, which are brought to the user's attention during the scan.

Security Risks: Threats which do not conform to the strict definitions of Viruses, Trojan horses, Worms, or other expanded threat categories, but which may present a threat to your computer and its data.

Spyware: Stand-alone programs that can secretly monitor system activity. These may detect passwords or other confidential information and transmit them to another computer. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.

Viruses, Worms and Trojan Horses: A **Virus** is a program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though, many do a large amount of damage as well.

A **Worm** is a program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

A **Trojan Horse** is a program that neither replicates nor copies itself, but causes damage or compromises the security of the computer. Typically, an individual emails a Trojan Horse to you, it does not email itself, and it may arrive in the form of a joke program or software of some sort.

Tools and How to Use Them

Because of the complexity of the tools we recommend, we can't include comprehensive instructions for each of them. However, we will give you a link that helps you find out more about each program.

In general, the tools we recommend here are preventative maintenance tools that attack the issue of malware from multiple directions. Just as you can get a different perspective on a problem by approaching it differently, these tools work separately and together to give a comprehensive set of protection that you can feel confident using and that we feel confident recommending.

Each of the programs here **MUST BE UPDATED AND RUN ON A REGULAR BASIS**. This is because new threats are always being written. The tools all include update functions that allow you to keep them current. Going back to our analogy of a car, if you are using an old map, you may not get there very efficiently. Worse yet, you may not get there at all!

In general the procedure for using each of these pieces of software follows the same process (remember that each program also has an excellent Help feature, some with tutorials, for you to check out and learn more about its workings): Download updates, then run scans and/or immunize.

One Time:

We will also make some changes in your Internet Options control panel that we recommend to make your internet experience safer, quicker and more rewarding. Then, we'll Download, Install and Register the recommended software that will be described in the next section.

To open your Internet Properties window, choose your Start menu, then go to Settings -> Control Panel in Windows 2000 or directly to Control Panel in XP or Vista. Open the Internet Options control panel. In XP and Vista, you may not immediately see the Internet Options control panel, if you are using the new (default) views it will appear after choosing Classic View on the left side. Once opened, the Internet Properties dialog box will show a series of tabs across the top that will vary according to which version of Internet Explorer you have installed. You should see the following: General, Security, Privacy, Content, Connections, Programs, and Advanced. The changes we want to make are in the General and Privacy tabs - the other tabs can be left alone. If you don't have a Privacy tab, we strongly recommend updating your Internet Explorer version using Windows Update to get to a newer version that includes this very useful tab. Better yet, follow our recommendation to stop using Internet Explorer (except for the Windows Update and other ActiveX-based sites which require it) and switch to Mozilla Firefox as your browser.

General tab settings

Home Page Section - The settings we want to make here are to the Home Page setting, which should be set to where you want to go when you first get online. Many clients prefer about:blank (a Blank page since we often go different places each time we're online) or a favorite page such as My Yahoo or the TaosNet home page. Another very useful option would be your favorite search engine since that allows you to find what you need from there. During the cleanup TaosNet offers our customers we normally set our home page and the Postini anti-spam login page to be your home page tabs.

Temporary Internet Files Section - We want to choose the Settings button here to change the size of the temporary area to something more reasonable than we find on most machines. This setting basically controls how much of the Internet is stored on your machine for future reference. Although this can speed returns to your favorite pages, there's no reason to use up lots of your hard disk space storing something that is available on some other computer somewhere and has to be checked each time. We recommend setting the Check for newer versions of stored pages to Automatically, and the size of the Temporary Internet files folder to 20 to 40 MB. If you have it much higher than that, you're actually wasting hard disk space and perhaps even slowing the machine down.

Privacy tab settings

This tab allows us to better control Cookies, those little files that know so much about you. Here we recommend the change to Override Cookie Handling and opt to Allow First Party Cookies but to Block Third Party (Advertising) Cookies. Also check the Always Allow Session Cookies box to allow one-time cookies to function normally.

Periodic Maintenance (Recommended weekly - expected time 1-3 hours*):

Run your Windows Updates!!! The Critical ones, especially, are usually security related. We normally *Pin* Windows Updates to the *Startup Menu* (find it in All Programs and Right Click to get this command).

In order to effectively run Windows Update, you will need to have at least Version 5 of Internet Explorer. When you examine the Tools menu, you will see the entry Windows Update. When you choose this, your computer will automatically go to the Microsoft web page where initially your Windows Update software itself will be version checked and if necessary updated. From here you will click the one of the buttons that appears to Check for Updates. The Express button will automatically download and install all Critical updates. The Custom button allows you to choose which updates to install of those offered. The site will inform you as to the progress of the check.

When it is done, you will often get the recommendation to download what are called Critical Updates. Because these often have to do with the security of your system, as a rule you should always choose to install them. This is done with the Download and Install button that will appear. Windows may then inform you that one or more downloads may have to happen first relative to the others. Always let these downloads progress according to Microsoft's recommendations. This may require you to restart the machine as part of the process. If this happens, IMMEDIATELY RETURN to Windows Update if the computer doesn't take you there itself. You may have to perform this restart more than once as a part of the normal update process.

When Windows Update completes, it will inform you that there are no more Critical Updates, but that there may be additional updates available. These updates are feature related, and you should review them and decide for yourself. It is possible that a Critical update or one of the additional updates could make your computer worse instead of better. Knowing this, some experts choose to only install the Critical updates.

*A good habit to develop since there are a number of tools is to run one of them each day in round-robin fashion. In that way they will be run often enough and you'll get used to doing it.

Recommended Software

Your choice of backup software should be regularly run to prevent the loss of your data should the computer or the cleanup fail. Some infections are too severe to be cleaned.

Next, run the following recommended anti-malware programs and be sure to update the definitions before scanning:

Spybot Search & Destroy - Preventative (Immunization feature) and Curative for Spyware

Ad-Aware - Curative for Adware

~~**AVG AntiSpyware**~~ - Unfortunately no longer offered by Grisoft nor supported by TaosNet

Avira AntiVir - Curative for Viruses, Trojans and such

Spyware Blaster - Preventative for Spyware (prevents access to over 11,000 malicious sites)

*A good habit to develop since there are a number of tools is to run one of them each day in round-robin fashion. In that way they will be run often enough and you'll get used to doing it.

Spybot Search & Destroy

[Right Click and Run As Administrator if you have Vista]

Spybot S&D specializes in finding and removing Spyware. Spybot S&D is a free program whose authors encourage you to donate if you find it useful. It is a free download when starting at the following link:

<http://www.safer-networking.org>

How to use it is well-described at this link

<http://www.safer-networking.org/en/tutorial/index.html>

as well as in their Tutorial which is under the Help menu. Understand how to Immunize!

Have we mentioned Help files in general are very helpful...? ;-)

In Spybot, as with most anti-malware programs, there is an Update feature that allows the downloading of the latest definition file that will provide protection against the latest threats. Your responsibility involves starting the program, then choosing the Search for Updates button and letting it download any newer definition file that may exist. If you get a Bad Checksum error when trying to do the download, try choosing another server first. If you still get a bad checksum error, you might have some spyware that is intentionally interfering with the operation of Spybot. Run it as is, and hopefully the problem will improve on the next try.

After the definitions have been updated you will want to Immunize against any infections Spybot knows how to avoid. Click the Immunize button in the left panel (icon like a shield), and let it count up the tally. If there are any items unprotected, click the Immunize button above the work section (icon with a green plus sign) to protect those items.

After immunizing, choose the Search and Destroy button on the left and click on the magnifying glass button that says Check for problems. Spybot will then do its magic and if problems are found it will present you with a list of things that need to be fixed. If Spybot says that it couldn't fix something and offers to run again at startup, answer Yes and immediately restart the computer. It will automatically run again, and chances are very good that the problems will be fixed on the second pass.

Spybot should be run repeatedly (updating not necessary after the first time) until it tells you Congratulations, No Problems Found. This assures that any hidden, layered threats are exposed.

Lavasoft Ad-Aware

Ad-Aware specializes in finding and removing Adware. It is also available in a pay version that lets you avoid the manual update/run process. They continue to offer the fully functional free version, but keep in mind that you trade responsibility of manual updating for dollars by using it.

Ad-Aware and information concerning its use and upgrades to the pay version can be found at this link:

<http://www.lavasoft.com>

In Ad-Aware, as with most anti-malware programs, there is an Update feature that allows the downloading of the latest definition file which determines what's new and bad with the software on your computer. Your homework involves starting the program, then choosing the Check for Updates Now link and letting it download any newer definition file that may exist. If the program checks for updates quicker than normal, maybe not even making an Internet connection if you normally dial up, you probably have some spyware that is intentionally interfering with the operation of Ad-Aware. Run it as is, and hopefully the problem will improve on the next try.

Ad-Aware should be run repeatedly (updating not necessary after the first time) until it tells you No Problems Found. Remove Critical infections and Spyware Cookies, but we generally Ignore MRU's (Most Recently Used item lists). This assures that any hidden, layered threats are exposed.

~~AVG AntiSpyware~~

AVG AntiSpyware is no longer offered by Grisoft nor supported by TaosNet. We have no replacement. If you have it from one of our cleanups in the past, go to the Control Panel -> Add/Remove Programs and Remove AVG AntiSpyware to remove the purchase popups. We do not suggest you pay for the AVG Suite for several reasons. The most important reason is that it includes an antivirus component, and you should only have one antivirus program installed. Trying to be extra safe by having multiple antivirus programs installed will create more problems for your computer and you.

Spyware Blaster

While other tools do damage control after it happens, Spyware Blaster is designed to *deflect* potential infections in the first place, acting as a *preventative* tool. You can now surf more confidently knowing that over 11,000 types of infection are actively prevented. It is similar to the other Anti-Malware tools in that it should be updated and run on a weekly basis. It too has a pay version which allows for automatic updates. The manual version is free from:

<http://www.spywareblaster.org>

Popular Commercial Anti-Virus Software vs. Avira AntiVir

Commercial products are well developed and generally well supported. However, their subscription service must be used to stay current against new threats and requires an annual fee, and they are not completely effective by themselves. If you don't already use Norton or McAfee products, we don't recommend you start, as the four programs we currently recommend will do the job more effectively AND more cost-effectively. If you'd like a very good antivirus program that is freeware, we'd recommend going to Avira for their excellent Anti-Vir antivirus program (the Personal Edition), which is FREE to home users only. Business users should visit the website and click the Products link to find the appropriate paid product. You can get them at the following link:

<http://free-av.com>

Although AntiVir will keep itself up-to-date, it does so at the expense of a pop-up window that may or may not entertain or irritate you as time goes on. If you invest in one of their pay versions of the program, this annoyance will go away. It will be your responsibility to scan your computer regularly if you do not choose to upgrade to a pay version. This is done by opening the program

through the red umbrella icon near the clock or on your desktop, and then going to the “Scanner” tab that appears in the control window. To perform a complete system scan, choose the first icon below labelled “Local Drives” and then click the magnifying glass icon to start the scan. When the Luke Filewalker window appears, the progress of the scan and anything found will be indicated - allow it to delete or quarantine anything it finds. As with all the scanning programs, rescan after a restart to be sure you cleaned it all.

Glossary (also see malware glossary in Types of Trouble to Prevent section)

backup - extra copies of your work stored away from the computer to serve as a replacement in the case of a tragic event such as weather or viral damage

broadband - a high-speed internet connection, types include fixed wireless and DSL which TaosNet offers and satellite and cable which TaosNet cannot offer

browser - the program type used to view web pages on the internet

byte - a unit of storage on your computer, prefixed in Greek to show greater orders; kilo=thousand, mega=million, giga=billion, tera=trillion etc.

CD-ROM - acronym for Compact Disc Read Only Memory. See ROM.

client - a computer that typically downloads information from a server

control panel - the way to change settings and preferences for your computer including how it works and appears

cookie - a temporary file on your computer in which a web site or sites store information about you. First party cookies are like those that allow you to communicate securely with your bank or other vendors. Third party cookies are used by advertisers to track your habits and build demographic profiles for marketing purposes. Session cookies are one-time use cookies for e-commerce and other real-time transactions.

CPU - the Central Processor Unit, actually the computer brain inside the main housing on the motherboard

dialog box - the tabbed boxes which appear in which settings are made and changed (you talk to the computer, it talks to you)

domain - the ultimate type of website you are visiting is expressed by its top-level **domain** designation, some examples of which are .com for commercial, .gov for government, .org for organizations, .de, .fr, .ca, etc. for specific countries and so on

DSL - acronym for Digital Subscriber Line, a method of broadband connection using the phone lines

encrypted - when information is sent over a connection, it is converted to a more secure code that only the two computers speaking to each other can understand - contrast with unencrypted

ethernet - the “fat phone plug” carries high-speed broadband internet and networking signals between your computer and others either directly or over DSL or wireless connections

file extension - the last three or four characters of a file name determine which program that type is associated with, e.g. .doc for Word type documents, etc. This extension may be shown/hidden in the Folder View Options Control Panel.

firewall - a method for allowing only certain network or internet traffic to get to your machine to help achieve better security

ftp - the File Transfer Protocol and programs that use it facilitate the transfer of larger files than email will support (typically 5 megabytes maximum depending on the mail systems involved)

giga- - prefix meaning billion, as in gigabyte and gigahertz

hard drive (hard disk) - the long-term storage in your computer, likened to a filing cabinet for your work and programs. Needs to be backed up regularly; every hard disk will eventually fail.

hertz - the frequency of some signal in cycles per second, the speed of your computer is measured in mega- or gigahertz, normally the higher the faster

html - the language of files stored on the World Wide Web, this is an acronym for HyperText (text that has links) Markup Language (a continually evolving standard for this linking); also as a file extension (.html or .htm) normally associated with your browser

http - HyperText Transfer Protocol, the way that HTML is transferred to and read by browsers

https - Same as http but with an added "s" for Secure, this method allows transfer of encrypted information, such as to your bank and for ecommerce

internet - the INTERconnected NETwork of computers world-wide, which TaosNet helps you join

intranet - a network of computers, typically within a business or school, etc., that may or may not be connected to the internet

ISP - Internet Service Provider, or who gets you connected to the internet

kilo- - prefix meaning thousand, as in kilobyte or kilohertz

LAN - acronym for Local Area Network, a generally private network at given location such as a home, school, or business, see intranet

malware - MALicious sofWARE, see Types of Trouble to Prevent section

mega- - prefix meaning million, as in megabyte, megahertz and megapixel

memory (vs. hard disk space) - the amount of thinking space your computer has to do work in a number of programs at one time (think of this as your desk space while your hard disk would be the file cabinets that surround you...)

menu - the list of choices that pops up when clicked with the mouse or selected with the keyboard, as with the Start menu

modem - MODulator/DEModulator that allows computers to communicate over regular phone lines. Two common types are: dialup (acoustic) generally found inside the computer, and DSL which also splits the voice signal from the computer signal they convert.

motherboard - the main circuit board inside the computer that holds the CPU, memory, and other components that perform the various processing, input and output functions for your computer

network - a group of connected computers and similar devices that can communicate with each other

news groups - discussions dedicated to specific vertical topics; this feature of the internet is traditionally accessed by a newsgroup reader program

offline - the condition of NOT being connected to the internet or LAN

online - the condition of being connected to the internet or LAN

pixel - a unit of screen or display size, there are generally 72 or 96 pixels per inch at normal size

proxy - a way of distancing your connection from the internet, a proxy server acts as a sort of buffer on some corporate and ISP systems - you see a sanitized copy of the internet limited by the rules of the proxy. Proxy servers can also be used maliciously by spyware to hijack your connection and keep better track of what you do. This is called a proxy override infection.

RAM - Random Access Memory is the "space" that your computer uses to think and work in; see Memory. RAM is volatile, which means that it is wiped out when power is lost.

ROM - Read Only Memory has the basic instructions for operating your hardware, which don't change. ROM is non-volatile in that power is not needed to "keep" the memory. CD-ROMs are a portable form of this type of storage.

server - A computer that typically sends info to clients, e.g. a web host

tab - Often dialog boxes have a series of tabs across the top (think of file folders) with different layers of settings; in a browser this feature allows multiple pages to be open at once or to open at startup. The Tab key on the keyboard is often the fastest way to navigate around dialog boxes - each press moves you to the next entry.

unencrypted - when information is sent over a connection without being converted to a more secure code, allowing other devices that intercept the info to be able to read it - contrast with encrypted

WAN - acronym for Wide Area Network, a public or private network that covers a larger geographic area, see internet

web - the internet is often referred to as the web, which is short for World Wide Web, which is actually only one feature of the internet

web host or provider - the company that serves the web pages an entity owns; this company runs the computer(s) that hold(s) a particular website

webmaster - the person or company responsible for designing and maintaining the look and function of a specific web site

www - World Wide Web, the greatest source of information since the Library at Alexandria; designed to be not quite as vulnerable to fire ;-)

Contents

Introduction	1
Maintenance is the Key	2
Why do people write malicious software?	2
Ya Wanna Buy a Watch??	3
Recommended Software... ..	3
Mozilla Firefox and Thunderbird	3
Types of Trouble to Prevent	4
Tools and How to Use Them	5
One Time:	6
General tab settings	6
Privacy tab settings	7
Periodic Maintenance (Recommended weekly - expected time 1-3 hours):	7
Recommended Software	8
Spybot Search & Destroy	8
Lavasoft Ad-Aware	9
AVG AntiSpyware	10
Spyware Blaster	10
Popular Commercial Anti-Virus Software vs. Avira AntiVir	10
Glossary (also see malware glossary in Types of Trouble to Prevent section).....	11