

Protecting Your Data

Recommendations for Maintaining Your Computer
and Protecting Your Information

Chris Hallgren, MBA/TM

President, Helios Data Forensics

March 2004

Protection Strategy

The key to protecting your computer from the many threats in cyberspace is to remain as “invisible” as possible to the outside world. This document presents a number of recommendations that together form a multi-layered strategy for protecting your data and keeping your computer “healthy.” Keep in mind that this strategy is meant only to *minimize* potential exposure to certain threats. The only way to completely protect yourself from external threats would be to never turn on your computer. However, for most people, following the strategy outlined here will result in a significant improvement in privacy, protection and performance. This strategy consists of the following 10 recommendations:

- 1) Apply Windows Updates Regularly
- 2) Clean Out Your Startup Folder
- 3) Defend Against Viruses
- 4) Defend Against Hackers
- 5) Browse the Web Anonymously
- 6) Keep Your Registry Clean
- 7) Use a Disposable Email Address
- 8) Don't Save Passwords!
- 9) Backup Your Data
- 10) Clean-up Your Data

Note: *This document recommends a number of specific software packages. These packages are listed because the author has experience with these packages and they have performed well in the past, however no software package is 100% effective and there are many other packages available that perform the same functions. Each computer owner should take it upon him or herself to learn as much as they can about the different solutions available and make their own decision about what is best for their specific situation. This document assumes the use of the Microsoft Windows operating system but many of the recommendations presented here would be applicable to other operating systems.*

Apply Windows Updates Regularly

Once a month, download any updates available for your computer at windowsupdate.microsoft.com. This web site will scan your computer and determine whether there are any updates you need to apply. These updates are broken down into three categories: **Critical Updates and Service Packs**, **Other Windows Updates** and **Driver Updates**. Any **Critical Updates or Service Packs** that are listed should always be downloaded. **Other Windows Updates** and **Driver Updates** are optional, but it is generally recommended that, unless there is a specific reason not to, it is best to go ahead and apply all updates.

Regularly applying these updates will help keep your computer current and protected from security vulnerabilities. It is possible to configure your computer to download and apply these updates automatically. To change your Automatic Update settings, go to Control Panel >> System >> Automatic Updates.

You can also download updates for Microsoft Office, however since these updates are not released with the same frequency as Windows Updates, this does not need to be done as often – 2 or 3 times a year is fine. These updates can be found at office.microsoft.com/officeupdate/default.aspx.

Clean Out Your Startup Folder

Any program that is listed in your Startup folder (Start Menu >> Programs >> Startup) is run every time the computer is booted up and the operating system loads. Many software packages put programs in this folder and, sadly, many of these programs are unnecessary. These programs eat up valuable computer resources and can also perform actions without the user's knowledge. It is a good strategy to have as few programs in your Startup folder as possible. Here are some general tips for keeping this folder cleaned out:

- 1) Create a folder in Start Menu >> Programs called "Startup Inactive". When you remove programs from your Startup folder, put them into the Startup Inactive folder. This way, if it later turns out that you do want that program to run at startup, you can easily move it from the Startup Inactive folder back to the Startup folder.

- 2) When in doubt, you probably don't need it! If you do not know what a program is or whether you need it, move it to your Startup Inactive folder for a while and see if you miss it. You probably won't, but if you do, move it back.
- 3) Once you have cleaned out your Startup folder, keep it clean. Anytime you install a new software package, check the Startup folder and see if it put anything in there. If it did, you will need to decide if you want to keep it there, but most of the time it will probably be unnecessary.
- 4) Some common programs found in the Startup folder that do not need to be there: Microsoft Office, Office FindFast, Real Player, Quicken Billminder, etc. These programs may provide some additional functionality to the program they are associated with, but it is not necessary to have them running to utilize the basic functions of the software package and they come at a heavy price by way of taking up computer resources.
- 5) There are many Windows Startup management software packages available that can give you even greater control over the startup process. A list of some of those can be found here:
www.spychecker.com/software/startup.html.

The Startup Folder is only one of several places where programs can get loaded automatically when Windows starts. For those who want greater control over how Windows starts, and are brave enough to venture beyond the Startup Folder, a utility exists that can help manage these programs. That utility is called MSConfig and it comes with some versions of Windows. You can find more information about MSConfig at the following web site:

<http://www.perfectdrivers.com/howto/msconfig.html>

Defend Against Viruses

Everyone knows this by now, right? Use an anti-virus software package and keep it updated! Computer viruses are so prevalent today that, if you are not using anti-virus software, you almost certainly have viruses on your computer (possibly many!) The important thing to remember about anti-virus software is that it must be kept up to date to be effective. New viruses are created everyday, so anti-virus companies must update their software on a regular basis. Norton and McAfee are both excellent programs and each can be configured to automatically download virus updates. These updates should be done at least once a week.

- **Norton AntiVirus** from Symantec – www.symantec.com – \$50
- **McAfee Virusscan** from Network Associates – www.mcafee.com – \$35/\$50

Defend Against Hackers

No one would consider buying a house that did not have locks on the doors. Likewise, a good personal firewall program should be considered just as essential as anti-virus software. A firewall stands between your computer and the rest of the world and controls the communications that go in and out. It might take a while to get used to running a firewall because it may restrict some of the things you normally do, but a firewall is critical to protecting your computer from hackers and some types of viruses, such as Trojan Horses (viruses that can appear to be a legitimate program but that give a hacker “back door” access to your computer). Some firewalls can also protect your computer from spyware, programs installed on a computer that monitor the activities of the user (while there are legitimate uses for spyware, these programs can also be used maliciously – see “*Use Anti-Trackware Software*” later in this article).

There are several personal firewall packages available. Here are a few:

- **Norton Personal Firewall from Symantec** – A popular firewall, it costs approximately \$50, but it is probably more “user friendly” so you may consider this cost justified. It can be purchased online: www.symantec.com.

- **BlackICE from Internet Security Systems** – Another popular firewall, it costs approximately \$40 for a single license. It can be purchased here: blackice.iss.net.
- **ZoneAlarm from Zone Labs** – This firewall comes in three versions: ZoneAlarm, ZoneAlarm Plus and ZoneAlarm Pro. The basic package is freeware. ZoneAlarm Plus and Pro each must be purchased but provide more functionality. ZoneAlarm can be downloaded and/or purchased online: www.zonelabs.com.

The above products are *software* firewalls. If you have more than one computer, you may want to consider a *hardware* firewall. Many of the network routers sold today include firewall functionality and are relatively easy to configure. Numerous companies sell network hardware. Linksys (www.linksys.com) makes hardware targeted for home or small business users that is reliable and reasonably priced.

Configuring a firewall can be a bit confusing and, if done wrong, you can end up allowing access to the very threats you are trying to keep out. Make sure you read the directions for your firewall software carefully and, if you're feeling unsure, consider hiring a computer technician to setup your firewall for you.

Browse the Web Anonymously

When you go shopping at the mall, you would never leave your wallet or purse out in the open for someone to look through or steal, and the same type of precautions should be taken while browsing the web. The goal is to remain as anonymous as possible while still enjoying the great benefits and opportunities available on the Internet.

Pop-up Blockers/Cookie Managers

As you surf the Internet, web sites are regularly placing files and other bits of information on your computer. Some sites also use a method of advertising called a pop-up window. Web site behaviors like these can range from annoying to invasive and even malicious. Unprotected, surfing can result in all kinds of problems on your computer. Not only can it expose personal information such as your email address, street address, phone number, credit card numbers, browsing behavior, etc. but it can also cause your computer to perform poorly.

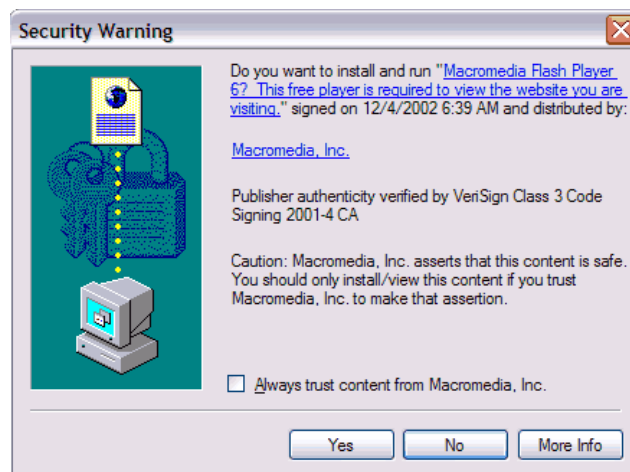
A pop-up blocker/cookie management program acts like a bouncer at a bar. It protects you and your information while you surf by keeping some items out while allowing through items from web sites on your "VIP list." Like a personal firewall, using a pop-up and cookie blocking program can be frustrating at first because it may interfere with things you normally do on the web, but once you get the hang of it you will find browsing the web much easier and safer.

AdSubtract (www.adsubtract.com – \$30) is a popular ad blocking and cookie management application available, but there are many. Whichever program you chose, here are some features you should look for:

- Pop-up and banner ad blocking
- Cookie blocking
- Ability to identify favorite or friendly web sites where ads or cookies will be allowed
- Ability to delete unwanted cookies and other temporary web files

ActiveX Controls

As you browse the web, you may occasionally get a message that looks like this:



ActiveX is a set of technology that allows interactive content on the Internet. ActiveX controls often enhance web browsing, but not all ActiveX controls are harmless. If your browser presents you with a security warning like the one above, play it safe! If you are not familiar with the company that made the control, or if you don't understand why you need the control installed on your computer, just say "No."

Anti-Trackware Software

Even if you use an anti-virus program, a pop-up blocker/cookie manager and a personal firewall, the unscrupulous can still find ways to invade your computer. Anti-trackware helps close this loophole by looking for known data mining and tracking software and then offering the user a chance to remove it. There are two types of applications that fall into the generally category of *Trackware*:

Adware – "Any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. Adware has been criticized for occasionally including code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge."

Spyware – "Any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program."

Definitions from TechTarget, www.whatis.com.

There are many anti-trackware applications available. Here are two good anti-trackware applications:

- **Ad-aware** – www.lavasoftusa.com – The basic package is freeware. Ad-aware Plus and Ad-aware Pro each must be purchased but offer different options and functionality. More information can be found on the Ad-aware web site.
- **SpyBot** – www.safer-networking.org – Freeware

Keep Your Registry Clean

The Windows Registry is a central repository for information such as software and hardware configurations, user preferences, etc. Most programs on your computer use the Registry in some way. Unfortunately, not all programs are good at “cleaning up” after themselves. Over time, the Registry can get bloated with obsolete and unnecessary information. Because the Windows operating system frequently needs to access the Registry, this can lower performance – the larger the Registry, the longer it takes to search through it. Keeping the Registry cleaned out will help keep your computer running fast and reliably.

As with pop-up blockers, there are many applications available that will clean your Registry. Registry Mechanic (www.winguides.com/regmech – \$20) is one easy-to-use Registry cleaner.

Warning: Working with the Windows Registry can be a risky proposition, and not all Registry cleaning programs were created equal. A poorly written Registry cleaner can do more harm than good. If your Registry gets corrupted, the operating system can stop working and data can be lost or damaged. Make sure you carefully read the directions of any Registry cleaning software you use and make a backup of your Registry before running that software.

Using a Disposable Email Address

If you follow the recommendations in this paper, you should see a reduction in the spam you receive, but the only way to completely avoid spam would be to avoid the Internet all together. Even the most “respectable” web sites gather personal information, especially when you are making an online purchase. However, without spending half your life reading privacy policies, you do not know which web sites are sharing your personal information with mass Internet marketers. This is how you end up with spam in your inbox.

One strategy for helping with spam is to have a separate email address that you use exclusively for Internet surfing. You could enter a fictitious email anytime one is requested, but this can become a problem. For example, you may want to receive an electronic receipt for your online purchase. Also, some web sites require you to respond to an email to complete your registration. With a separate email address used just for browsing, you only have to check it occasionally and it will keep spam from showing up in your primary email account.

There are several places on the Internet that offer free email accounts. Here are a few:

- MSN – www.msn.com
- Yahoo! – www.yahoo.com
- GMail – www.gmail.com
- My Own Email – www.myownemail.com

Keep this in mind – the information you use to create a free email account does not necessarily have to be accurate. The less personal information you share on the Internet, the better!

Don't Save Passwords!

Most web sites that require a user to log in also give the user the option to “save” their password, or “remember” the user’s identity so that he or she does not have to log in again the next time they visit that web site. Web browsers, like Internet Explorer or Netscape, also allow the user to save web site passwords. These passwords get stored on the user’s computer, often in an insecure way. Hackers (or any dishonest person with access to the computer) can recover these passwords and gain access to web accounts. Of course, this can expose sensitive personal information and possibly lead to financial loss.

While it may be difficult or annoying to try remembering several passwords, or to always have to re-type your ID and password each time you visit a web site, it is best not to allow web sites or your browser to save your password. You should also not store your passwords on your computer yourself or write your passwords down anywhere. These can create the same kind of exposure. In fact, the same precautions should be followed with any type of password, not just those used on the Internet.

You want to use a password that you can easily remember so that you do not need to record it anywhere, but you also do not want it to be easy to guess. One good way to do this is to think of a phrase that you can remember. Then, take the first letter of each word in the phrase and make that your password. If one or more of the letters in the password can be a number or other non-alpha character, that will make the password difficult to guess or crack. And, for passwords that are case-sensitive, mixing the case will make guessing or cracking the password even more difficult. Here are a couple of examples:

The phrase "*I Love To Play Golf For Fun*" could be made into I12pG4f

or, "*One Pound Of Pasta For Two Dollars*" could be made into 1#oP£2d

Remember to keep your password only in your head – never write it down or share it with anyone else!

Backup Your Data

No strategy can provide complete protection. Even if you have done everything else recommended here, you could still lose data. And if that happens, you will be extremely thankful if you have a backup of your data. Keep in mind the following tips as you plan your own backup strategy.

- How often should you run backups? That's easy – how much data are you willing to lose? If you use your computer every day, you may want to run backups nightly. If you rarely use your computer, making a backup once every week or month might be sufficient. It really comes down to how much time and effort your data is worth to you.
- In the terrible event that your office or house experiences a natural disaster, any backup data stored locally will likely be lost along with your computer. In light of this, consider storing some backup data off-site, for example, in a safe deposit box.
- You don't necessarily need to backup your entire hard drive. If you have the space to do it, great, but if not, you will need to identify the specific files you want to backup. Read the directions for your backup software, and consult a computer technician if you are not sure that you are backing up everything that is important to you.

- There are many web companies that offer backup services or “online storage” over the Internet. This is generally not recommended since it exposes the very data you have worked so hard to protect. DVD burners are relatively inexpensive these days, and a DVD’s 4 gigabytes of capacity is sufficient for most computer users.

As for backup software packages, there are many available. Windows 2000/XP comes with a standard backup utility, but this utility does not provide data compression. Here are two other backup packages that work well:

- Backup MyPC – www.stompinc.com – \$70
- WinBackup – www.liutilities.com/products/winbackup/ – \$40

Clean-up Your Data

Nearly everyone is familiar with the growing crime of identify theft. One relatively new way that these criminals are acquiring a person’s personal information is by recovering it from old computers that have been sold or discarded. The following news article discusses this new method of stealing personal information - [“Thieves Using Old Computers to Steal Identities”](#)

As the article states, deleting a file does not completely remove the data. To illustrate this behavior, think of a hard drive as a book – there are “chapters” containing data and there is a “table of contents” that lists the chapters and their location. Deleting a file removes that file’s entry in the hard drive’s “table of contents” and marks the space used by the file as available for use, but it does not remove the actual data. The data remains on the hard drive until the operating system decides to use that space. Depending on the level and types of activity performed on the computer, the data could remain for months or years. Even formatting or deleting a partition does not safely erase data. As a computer forensics specialist, I use special hardware and software tools to recover and examine this type of data. Unfortunately, identity thieves sometimes use the same tools to recover personal information for illicit use.

If you are planning to sell, donate or discard your computer, you will want to use a disk wiping utility to completely remove all data from the hard drive. A disk wiping utility removes data by actually overwriting it with "blank" data. There are many wipe utilities, but not all work equally well. The following products are well respected within the computer forensics industry.

AccessData WipeDrive – www.accessdata.com – \$40

Eraser – www.heidi.ie/eraser/ – Free

Whatever product you chose, make sure that it conforms to the US Department of Defense (DOD) 5220.22-M Standard. This level of data cleansing should be sufficient for all but the most paranoid computer users, but remember that the only way to be 100% that your data cannot be recovered is to physically destroy the hard drive.

As you can see, protecting your data is not easy. With so many threats on the Internet, one layer of defense is simply not enough. Safety and security in cyberspace requires diligence and a diverse strategy. While some level of threat will always exist, the strategy outlined here will allow you to take advantage of what the Internet has to offer while minimizing the risk to you and your data.

About the Author:

Mr. Hallgren is President of Helios Data Forensics, a company providing computer forensic services to businesses and the civil legal environment. Computer forensics involves the identification, acquisition and analysis of evidence from digital sources such as computers, personal digital assistants, digital cameras and cell phones. Forensic computer examiners use special tools and methodologies to ensure that evidence is collected in a manner that preserves its evidentiary value for use in legal proceedings. By using these tools, examiners can often find information that has been deleted or hidden.

Mr. Hallgren is a member of the High Technology Crime Investigation Association (HTCIA), an organization designed to encourage, promote, aid and affect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Mr. Hallgren is trained and licensed to use EnCase computer forensic software from Guidance Software. EnCase is widely used by local, state and federal law enforcement agencies throughout the United States. In addition to EnCase, Mr. Hallgren is trained and licensed to use the NTI Forensic Software Suite as well as the Ultimate Forensic Toolkit from AccessData. Mr. Hallgren also received a professional certificate in computer forensics from Oregon State University and NTI.

Mr. Hallgren has a Bachelor of Science Degree in Management Systems from Arizona State University and a Master of Business Administration with a specialization in Technology Management from the University of Phoenix.

Prior to starting Helios Data Forensics, Mr. Hallgren spent eleven years as an information technology consultant specializing in implementing human resources information systems and building custom technology solutions.

Contact Information:

2692 Madison Road N-1 PMB 139
Cincinnati, OH 45208
(513) 751-3333
chris@heliosdataforensics.com
www.heliosdataforensics.com