

# Protecting Your Computer

by

**Jack Pelling**

1. Fighting Spam
2. What is Spyware
3. Phishing for your Identity
4. Spam Buster
5. Just what is Intelligent Explorer? For your safety, you really need to know
6. Computer Viruses that Come a Calling
7. Spyware Beware
8. Antivirus Software
9. Trojan Horse...Greek Myth or Computer Nemesis?
10. Website Security Rules of the Road
11. Who are the Players in the Antivirus Industry?
12. Why Do I Feel Like Somebody's Watching Me?
13. Name, Rank and Social Security Number
14. Conclusion

## **Fighting Spam**

How prevalent is Spam? According to Scott McAdams, OMA Public Affairs and Communications Department ([www.oma.org](http://www.oma.org)):

"Studies show unsolicited or "junk" e-mail, known as spam, accounts for roughly half of all e-mail messages received. Although once regarded as little more than a nuisance, the prevalence of spam has increased to the point where many users have begun to express a general lack of confidence in the effectiveness of e-mail transmissions, and increased concern over the spread of computer viruses via unsolicited messages."

In 2003, President Bush signed the "Can Spam" bill, in December of 2003 which is the first national standards around bulk unsolicited commercial e-mail. The bill, approved by the Senate by a vote of 97 to 0, prohibits senders of unsolicited commercial e-mail from using false return addresses to disguise their identity (spoofing) and the use of dictionaries to generate such mailers. In addition, it prohibits the use of misleading subject lines and requires that emails include and opt-out mechanism. The legislation also prohibits senders from harvesting addresses off Web sites. Violations constitute a misdemeanor crime subject to up to one year in jail.

One major point that needs to be discussed about this: spam is now coming from other countries in ever-greater numbers. These emails are harder to fight, because they come from outside our country's laws and regulations. Because the Internet opens borders and thinks globally, these laws are fine and good, but do not stop the problem.

So what do you do about this? Here are the top 5 Rules to do to protect from spam.

Number 1: Do what you can to avoid having your email address out on the net.

There are products called "spam spiders" that search the Internet for email addresses to send email to. If you are interested, do a search on "spam spider" and you will be amazed at what you get back. Interestingly, there is a site, WebPoison.org, which is an open source project geared to fight Internet "spambots" and "spam spiders", by giving them bogus HTML web pages, which contain bogus email addresses

A couple suggestions for you: a) use form emails, which can hide addresses or also b) use addresses like [sales@company.com](mailto:sales@company.com) instead of your full address to help battle the problem. c) There are also programs that encode your email, like **jsGuard**, which encodes your email address on web pages so that while spam spiders find it difficult or impossible to read your email address.

Number 2: Get spam blocking software. There are many programs out there for this. (go to [www.cloudmark.com](http://www.cloudmark.com) or [www.mailwasher.net](http://www.mailwasher.net) for example). You may also buy a professional version. Whatever you do, get the software. It will save you time. The software is not foolproof, but they really do help. You usually have to do some manual set up to block certain types of email.

Number 3: Use the multiple email address approach.

There are a lot of free email addresses to be had. If you must subscribe to newsletters, then have a "back-up" email address. It would be like giving your sell phone number to your best friends and the business number to everyone else.

Number 4: Attachments from people you don't know are BAD, BAD, BAD.

A common problem with spam is that they have attachments and attachments can have viruses. Corporations often have filters that don't let such things pass to you. Personal email is far more "open country" for spammers. General rule of thumb: if you do not know who is sending you something, DO NOT OPEN THE ATTACHMENT. Secondly, look for services that offer filtering. Firewall vendors offer this type of service as well.

Number 5: Email services now have "bulk-mail" baskets. If what you use currently does not support this, think about moving to a new vendor. The concept is simple. If you know someone, they can send you emails. If you don't know them, put them in the bulk email pile and then "choose" to allow them into your circle. Spam Blocking software has this concept as well, but having extra layers seems critical these days, so it is worth looking into.

### **How many spyware items are infecting your computer?**

I just had, by mistake, a plug-in called Intelligent Explorer attach to my browser. What a nightmare! I have another article on this topic, but this brings home a point. Spyware or adware items are continually infecting computers. Most computers have no protection from them. Most frightening is the frequency of them. From the InfosecWriters web site, "According to a 2004 survey by America Online and the National Cyber Security Alliance, 91% of users questioned were familiar with the term spyware. Only 53% believed their computers were infected, but a scan found that 80% of their PCs had some type of spyware installed on them." It goes on to

say, "...The average number of spyware components per computer was 93 with one computer having well over a thousand."

### **What is Spyware?**

Butte College ([www.bctv.butte.edu/support/spyware.html](http://www.bctv.butte.edu/support/spyware.html)) offers this definition:

"The term 'spyware' is broadly defined as any program that gets into your computer without permission and hides in the background while it makes unwanted changes to your user experience.

Spyware is generally not designed to damage your computer. The damage it does is more a by-product of its main mission, which is to serve you targeted advertisements or make your browser display certain sites or search results.

At present, most spyware targets only the Windows operating system (Internet Explorer)."

To be fair, spyware can be harmless, for example tracking cookies don't do much. While such things infringe on your privacy, they don't really harm anything. Others, however, are extremely dangerous.

### **So what do you do about it?**

No spyware program seems to do everything, but there are a lot of good solutions out there that can help. Here is a list of some of the top Spyware tools to look at:

- 1) Try Ad-Aware 6.0 Professional from LavaSoft (there is also a free version with less functionality)
- 2) Spybot Search & Destroy from PepiMK Software
- 3) Xoftspy from Pareto Logic
- 5) Spyware Guard from Javacool Software is a free program
- 4) Pest Patrol (now part of Computer Associates by acquisition)
- 5) McAfee Anti-Spyware

One thing is for certain: you do need to take spyware seriously. For some reason, too many people out there think anti-virus solutions are the end-all solution. They are not.

### **And, when all else fails?**

Finally, as drastic as it seems, if your computer has been infected with a large number of spyware programs, the only solution you may have is backing up your data, and performing a complete reinstall of the operating system.

### **Phishing For Your Identity**

Who hasn't received an email directing them to visit a familiar website where they are being asked to update their personal information? The website needs you to

verify or update your passwords, credit card numbers, social security number, or even your bank account number. You recognize the business name as one that you've conducted business with in the past. So, you click on the convenient "take me there" link and proceed to provide all the information they have requested. Unfortunately, you find out much later that the website is bogus. It was created with the sole intent to steal your personal information. You, my friend, have just been "phished".

Phishing (pronounced as "fishing") is defined as the act of sending an email to a recipient falsely claiming to have an established, legitimate business. The intent of the phisher is to scam the recipient into surrendering their private information, and ultimately steal your identity.

It is not as easy as you think to spot an email phishing for information. At first glance, the email may look like it is from a legitimate company. The "From" field of the e-mail may have the .com address of the company mentioned in the e-mail. The clickable link even appears to take you to the company's website, when in fact, it is a fake website built to replicate the legitimate site.

Many of these people are professional criminals. They have spent a lot of time in creating emails that look authentic. Users need to review all emails requesting personal information carefully. When reviewing your email remember that the "From Field" can be easily changed by the sender. While it may look like it is coming from a .com you do business with, looks can be deceiving. Also keep in mind that the phisher will go all out in trying to make their email look as legitimate as possible. They will even copy logos or images from the official site to use in their emails. Finally, they like to include a clickable link that the recipient can follow to conveniently update their information.

A great way to check the legitimacy of the link is to point at the link with your mouse. Then, look in the bottom left hand screen of your computer. The actual website address to which you are being directed will show up for you to view. It is a very quick and easy way to check if you are being directed to a legitimate site.

Finally, follow the golden rule. Never, ever, click the links within the text of the e-mail, and always delete the e-mail immediately. Once you have deleted the e-mail, empty the trash box in your e-mail accounts as well. If you are truly concerned that you are missing an important notice regarding one of your accounts, then type the full URL address of the website into your browser. At least then you can be confident that you are, in fact, being directed to the true and legitimate website.

### **Spam Buster**

Spam. Nobody likes it. Nobody wants it. No, we aren't talking about the canned meat, but those unsolicited, unwanted, irrelevant, or even inappropriate messages that hit our email in mass quantities. While most mailboxes have some type of spam filtering software built into their system, they never seem to do a very good job of catching what you want them to catch, and letting through what you want them to let through. Therefore, it becomes increasingly important to turn to some type of additional spam filtering product. One such filtering system, designed for Outlook and Outlook Express users, is receiving rave reviews for its superior detection and low rate of false positives (i.e., what you want to get through does).

Cloudmark Desktop, formerly known as SpamNet and SafetyBar, uses a unique community-based filtering process. This community-based filtering system relies on users to report any new spam. Within minutes of a spammer being reported, they are placed on a blacklist. At that point, no other member will receive that particular spam. Cloudmark also applies the same basic process to phishing email scams.

What is interesting is how Cloudmark creates a digital reputation model of reporting spam. Each user starts with a neutral reputation. A user's reputation will rise if they are among the first to identify undesirable content. On the flip side of the coin, a user's reputation falls when they falsely reports spam. The result is a system that is automated, highly scalable and resistant to tampering.

An added bonus is that because the software doesn't depend upon the user to configure its settings, it installs in minutes and is easy to use. Cloudmark blocks over 98% of spam from reaching your inbox and boasts over one million users worldwide.

The cost of program is \$39.95 for a one-year subscription. The subscription is renewable annually. For those wanting to test drive the product, a free 15-day trial period for either your Outlook or Outlook Express is available.

### **Just what is Intelligent Explorer? For your safety, you really need to know**

I recently hit, by mistake, what I thought was an Explorer upgrade option. It turned out to be a pop-up appearing legitimate but really was not. It uploaded a product called Intelligent Explorer on my machine. What a nightmare!

I did some research on the web and found messages like this one from a BullGuard Antivirus Forum,

"PLEASE HELP!!! I HAVE A SPYWARE, TROJAN AND HIJACKER ON MY COMPUTER. I HAVE RUN BULLGUARD, CWSHREDDER AND AD-AWARE. ALL HAVE PICKED UP THE VIRUSES AND SAID THAT THEY HAVE BEEN MOVED/REMOVED BUT WHEN I LOG ONTO THE INTERNET THAT DAMN INTELLIGENT EXPLORER TOOLBAR IS SHOWING"

Another message from spywareinfo Forum goes something like this:

"Hey I'm having issues with something called Internet explorer toolbar - Intelligent explorer. I can't find a way to remove it from my comp and I really don't want to reinstall windows. I've used spybot, ad-ware, and cw shredder but nothing seems to work."

It appears that Intelligent Explorer allows other software to be downloaded to your machine and this is where the problem occurs. What is even more remarkable is that by downloading Intelligent Explorer, their license grants them the right to install software add-ins on your computer at their will. Take a look at what the software license for Intelligent Explore says (go to <http://www.ieplugin.com/terms.html> to read it all):

"You grant to us the right, exercisable by us until you uninstall the Software or this agreement is otherwise terminated, to provide to you the Service of downloading and causing to be displayed advertising material on your computer, through 'pop-up' or other display while you use your browser. You acknowledge and agree that installation of the Software may automatically modify toolbars and other settings of your browser. By installing the Software you agree to such modifications."

The company, IBC incorporated, is incorporated in Belize. I really can't believe this license!

One end user found highly objectionable pop-up advertisements generated by this software bundled with Intelligent Explorer in the form of extreme pornography.

I have yet to break this.

Intelligent Explorer is a plug-in, which can create a new home page, as well as start up and endless loop of pop-ups. You can remove the view bar, but then starting up Internet Explorer will cause it to reappear. I asked some friends to help, and no one could tell me what to do.

### **This is what I did:**

I bought a copy of a program called XoftSpy and it removed the software. It took two scans and a reboot to do it. This is not an advertisement for this product. They advertised it was free, which it was to run, but then I had to buy it to actually fix anything. It cost me \$40 and I am sure that there are freeware products out there as well, but that is what ended the nightmare for me. Other spyware products I have seen out there include spybot, NoAdware, Spyware Eliminator, Pal Spyware Remover, and Spyware C.O.P.

Let the buyer beware!

### **Computer Viruses that Come a Calling**

Every day new computer viruses are created to annoy us and to wreck havoc on our computer systems. Below are ten viruses currently cited as being the most prevalent in terms of being seen the most or in their ability to potentially cause damage. New viruses are created daily. This is by no means an all inclusive list. The best thing you can do is to remain vigilant, keep your anti-virus software updated, and stay aware of the current computer virus threats.

#### **Virus: Trojan.Lodear**

A Trojan horse that attempts to download remote files. It will inject a .dll file into the EXPLORER.EXE process causing system instability.

#### **Virus: W32.Beagle.CO@mm**

A mass-mailing worm that lowers security settings. It can delete security-related registry sub keys and may block access to security-related websites.

#### **Virus: Backdoor.Zagaban**

A Trojan horse that allows the compromised computer to be used as a covert proxy and which may degrade network performance.

#### **Virus: W32/Netsky-P**

A mass-mailing worm which spreads by emailing itself to addresses produced from files on the local drives.

#### **Virus: W32/Mytob-GH**

A mass-mailing worm and IRC backdoor Trojan for the Windows platform. Messages sent by this worm will have the subject chosen randomly from a list including titles such as: Notice of account limitation, Email Account Suspension, Security measures, Members Support, Important Notification.

### **Virus: W32/Mytob-EX**

A mass-mailing worm and IRC backdoor Trojan similar in nature to W32-Mytob-GH. W32/Mytob-EX runs continuously in the background, providing a backdoor server which allows a remote intruder to gain access and control over the computer via IRC channels. This virus spreads by sending itself to email attachments harvested from your email addresses.

### **Virus: W32/Mytob-AS, Mytob-BE, Mytob-C, and Mytob-ER**

This family of worm variations possesses similar characteristics in terms of what they can do. They are mass-mailing worms with backdoor functionality that can be controlled through the Internet Relay Chat (IRC) network. Additionally, they can spread through email and through various operating system vulnerabilities such as the LSASS (MS04-011).

### **Spyware Beware**

Spyware and Adware are not only an ever increasing nuisance for computer users everywhere, but also a booming industry. According to Webroot Software, Inc., the distribution of online advertisements through spyware and adware has become a \$2 billion industry.

The aggressive advertising and spying tactics demonstrated by some of these programs, require an equally aggressive response from a seasoned eradicator. Sunbelt Software is such a company. A leader in Anti-Spyware, Anti-Spam, Network Security and System Management tools, they have consistently remained on the cutting-edge of anti-spyware programming since 1994.

One of their more notable software applications is CounterSpy 1.5. CounterSpy is designed to detect and remove spyware that is already in your computer system. Additionally, it provides real-time protection while preventing browser hijacking and changes to your computer's Registry.

Other notable features include:

- ◆ Detection and Removal of Tracking Cookies – while it is true that applications like Microsoft AntiSpyware Beta are free, they do not include the ability to detect and remove tracking cookies like CounterSpy does.
- ◆ History Cleaner - erases any traceable trails left on your computer as you surf the Internet.
- ◆ Secure File Eraser - a powerful deletion tool that can completely eliminate all files you want removed from your computer including images, music, movies and applications.
- ◆ PC Explorer - allows you a look into files and areas that are normally inconvenient to access, such as your startup programs, browser helper objects, and ActiveX programs that are being downloaded or used.
- ◆ Support for Older Operating Systems – includes Windows 98SE, Windows ME, and Windows NT.

Recommended by PC World, ConsumerSearch, and Dell, CounterSpy holds one of the highest effective ratings for spyware removal. It also received high marks from TopTenReviews (2006) for ease of use, customization/installation, and help/support. For only \$19.95 per machine, users can receive a one year subscription with updates, upgrades, and technical support from real live humans. CounterSpy definitely provides ease of use and affordability for just about any computer user from the novice to the expert.

## **Fighting off Viruses: Advancements in Antivirus Software Suites**

Protecting your computer from a virus is getting harder and harder each day. While it may border on the paranoid, it goes without saying that you can't leave your guard down for one second. Even corporate giant Microsoft has found its own systems compromised on more than one occasion.

Remember the "good old days", before the advent of the Internet and downloadable programs? Life was simple then in terms of computer viruses. With the primary way in which a virus could be transmitted being limited to floppy disks, the ability to catch and eradicate the virus was a lot easier. By today's standards, it used to take quite a while before a virus was able to infect a computer and slow down the system. The antivirus software of that time was typically able to identify and eradicate viruses before they caused too much damage. Additionally, computer users were pretty savvy on how to protect themselves in terms of scanning all floppy disks before copying them to our desktop.

The Internet helped change all that. The Internet provided a conduit by which viruses could move from host to host with lightening speed. No longer could a computer user just worry about floppy disks as points of entry, but they now had to worry about email, email attachments, peer-to-peer file sharing, instant messaging, and software downloads. Today's viruses can attack through multiple entry points, spread without human intervention, and take full advantage of vulnerabilities within a system or program. With technology advancing everyday, and the convergence of computers with other mobile devices, the potential of new types of threats also increase.

### **Antivirus Software**

Luckily, the advancement of antivirus software has kept pace with current virus threats. Antivirus software is essential to a computer's ability to fend off viruses and other malicious programs. These products are designed to protect against the ability of a virus to enter a computer through email, web browsers, file servers and desktops. Additionally, these programs offer a centralized control feature that handle deployment, configuration and updating.

A computer user should remain diligent and follow a few simple steps to protect against the threat of a virus:

1. Evaluate your current computer security system. With the threat of a new generation of viruses able to attack in a multitude of ways, the approach of having just one antivirus software version has become outdated. You need to be confident that you have protected all aspects of your computer system from the desktop to the network, and from the gateway to the server. Consider a more comprehensive security system which includes several features including antivirus, firewall, content filtering, and intrusion detection. This type of system will make it more difficult for the virus to penetrate your system.
2. Only install antivirus software created by a well-known, reputable company. Because new viruses erupt daily, it is important that you regularly update your antivirus software. Become familiar with the software's real-time scan feature and configure it to start automatically each time you boot your computer. This will protect your system by automatically checking your computer each time it is powered up.

3. Make it a habit to always scan all new programs or files no matter from where they originate.
4. Exercise caution when opening binary, Word, or Excel documents of unknown sources especially if they were received during an online chat or as an attachment to an email.
5. Perform regular backups in case your system is corrupted. It may be the only way to recover your data if infected.

### **Recommended Antivirus Software**

There are numerous applications available to consumers. With a little research, you can pick the program that is right for you. Many programs provide a trial version which allows you to download the program and test its abilities. However, be aware that some anti-virus programs can be difficult to uninstall. As a precaution make sure to set up a System Restore point before installing.

Here are a few programs which typically receive high marks in terms of cost, effectiveness, ease of use, and customer service.

**The Shield Pro 2005™** provides virus protection and hacker security through ongoing support and updates. When a virus breaks out, The Shield Pro 2005™ promises to provide a patch within 2-3 hours and a fix for the virus within 5 hours. You can set your computer to update viruses weekly and [run a complete virus scan](#).

**BitDefender 9 Standard** provides antivirus protection, as well as Peer-2-Peer Applications protection, full email protection, and heuristics in a virtual environment. This provides a new security layer that keeps the operating system safe from unknown viruses by detecting malicious pieces of code for which signatures have not been released yet.

**Kaspersky Anti-Virus Personal 5.0** program is simple to install and use. The user only needs to choose from three levels of protection. It allows updates as frequently as every hour while promising not to disrupt your computer. The program also offers a two-tier email protection feature and round-the-clock technical support.

**PC-cillin Internet Security** combines antivirus security and a personal firewall—for comprehensive protection against viruses, worms, Trojans, and hackers. It also detects and removes spyware and blocks spam. It even guards against identity theft by blocking phishing and pharming attacks.

**[AVG Anti-Virus Free Edition](#)** is a free downloadable antivirus program that has received high marks for its reliability. In the past, free downloadable antivirus programs have been viewed skeptically because of issues relating to its reliability. However, [AVG](#) from Grisoft, remains one of the best-known free anti-virus programs available. While AVG can not be installed on a server operating system and there is no technical support, it still makes a good choice for many home computer users. The best part is that since it is free, you can try it with no further obligation necessary.

### **Trojan Horse....Greek Myth or Computer Nemesis?**

We have all heard the term Trojan Horse, but what exactly is it? A Trojan Horse is a destructive [program](#) that masquerades as a harmless application. Unlike [viruses](#),

Trojan Horses do not replicate themselves, but they can be just as destructive. One of the most dangerous examples of a Trojan is a program that promises to rid your computer of viruses but instead introduces viruses into your computer.

The Trojan can be tricky. Who hasn't been online and had an advertisement pop up claiming to be able to rid your computer of some nasty virus? Or, even more frightening, you receive an email that claims to be alerting you to a new virus that can threaten your computer. The sender promises to quickly eradicate, or protect, your computer from viruses if you simply download their "free", attached software into your computer. You may be skeptical but the software looks legitimate and the company sounds reputable. You proceed to take them up on their offer and download the software. In doing so, you have just potentially exposed yourself to a massive headache and your computer to a laundry list of ailments.

When a Trojan is activated, numerous things can happen. Some Trojans are more annoying than malicious. Some of the less annoying Trojans may choose to change your desktop settings or add silly desktop icons. The more serious Trojans can erase or overwrite data on your computer, corrupt files, spread other malware such as viruses, spy on the user of a computer and secretly report data like browsing habits to other people, log keystrokes to steal information such as passwords and credit card numbers, phish for bank account details (which can be used for criminal activities), and even install a backdoor into your computer system so that they can come and go as they please.

To increase your odds of not encountering a Trojan, follow these guidelines.

1. Remain diligent  
Trojans can infect your computer through rogue websites, instant messaging, and emails with attachments. Do not download anything into your computer unless you are 100 percent sure of its sender or source.
2. Ensure that your operating system is always up-to-date. If you are running a Microsoft Windows operating system, this is essential.
3. Install reliable anti-virus software. It is also important that you download any updates frequently to catch all new Trojan Horses, viruses, and worms. Be sure that the anti-virus program that you choose can also scan e-mails and files downloaded through the internet.
4. Consider installing a firewall. A firewall is a system that prevents unauthorized use and access to your computer. A firewall is not going to eliminate your computer virus problems, but when used in conjunction with regular operating system updates and reliable anti-virus software, it can provide additional security and protection for your computer.

Nothing can guarantee the security of your computer 100 percent. However, you can continue to improve your computer's security and decrease the possibility of infection by consistently following these guidelines.

### **Website Security Rules of the Road**

In 2004, online consumer spending was at a record \$65.1 billion. More and more people are attracted to the ease of online shopping and are spending higher amounts. Unfortunately, the chances of becoming a victim of Internet fraud are also increasing. The Internet National Fraud Center Watch reported that the average loss to fraud victims for just the first six months of 2005 was \$2,579. This is compared to the \$895 average for all of 2004. Complaints relating to general merchandise purchases (goods never

received or misrepresented) accounted for 30% of Internet fraud complaints, and auction purchases (goods never received or misrepresented) topped the list at 44%.

While many e-commerce Websites are reputable and have taken the necessary safety precautions to protect you, it never hurts to always proceed cautiously. If you are making an online purchase consider these easy steps:

1. Use only one credit card, preferably with a low credit limit, when making online purchases. Avoid using an ATM or debit card.
2. Be wary of unsolicited offers by sellers. The Internet National Fraud Information Center Watch reported that email, as a method of contact by Internet scammers was up 22% in 2004. While the offer may be legitimate, spammers like to use this tactic to side-step reputable sites that provide consumer protection for online purchases.
3. Use only reputable e-commerce websites that list a street address and telephone number in case you need to contact them directly.
4. Read the website's privacy policy. Some websites may reserve the right to sell/give your information to a third party. Check the document to see if they allow an opportunity to "opt-out" of receiving special offers from third-party vendors or for permission to share your personal information.
5. Check for a lock symbol in the status bar at the bottom of your Web browser window. Also, do not provide your personal information if the website address doesn't start with "https" (a sign that the site is using a secure server).
6. Choose only verified sellers. Check to see if the vendor is a verified member of a reputable third party such as the Better Business Bureau, VeriSign, or Guardian eCommerce. These third-party sites help to ensure online consumers will be protected when shopping or conducting e-commerce transactions.
7. Check that the delivery date posted is reasonable. If you have not dealt with the vendor on a regular basis, be wary of any Website that states the shipment will be delayed 20 or more days. Delivery dates of 7-10 days are more common.
8. Keep a paper trail of all online transactions. Print out a hard copy of the transaction and keep it in a file for future reference.
9. Be wary of website offers that just sound too good to be true. The Internet is littered with get rich quick scams and false advertising claims. Investigate all claims thoroughly before proceeding.
10. If you do not receive what you paid for, and the vendor will not return your emails or calls, contact your state's Department of Consumer Affairs for further assistance.

### **Who are the Players in the Antivirus Industry?**

Everyone in the United States has heard of the leading antivirus vendors Symantec, McAfee, Computer Associates, and Trend Micro. These companies have market-leading presence in the United States. Microsoft, as well, has plans become a key player in this market. Microsoft acquired intellectual property and technology from GeCad software in 2003, a company based in Bucharest, Romania. They also acquired Pelican Software,

which had a behavior based security as well as Giant Company Software for spyware and Sybari Software, which manages virus, spam, and phishing filtering.

A lot of discussion has centered on whether Microsoft will come to own a dominant position in the antivirus market by simply bundling its technologies with its operating systems at no charge. This is a similar technique applied in other markets such as word processing and Internet browsers.

Of course there are a number of antivirus vendors who also play in this market. There are many companies with great market presence in other countries that are beginning to become more widely known. These vendors include GriSoft out of the Czech Republic, Sophos in the United Kingdom, Panda Software out of Spain, Kaspersky in Russia, SoftWin in Romania, F-Secure in Finland, Norman in Norway, Arcabit in Poland, VirusBuster out of Hungary, and AhnLab in South Korea.

It is not clear where the industry is heading and everyone in this market faces a rapidly changing landscape. The amount of effort to find and provide fixes for viruses is staggering. Malicious programs are getting more complex and the number of them is increasing. Many companies may find themselves without the resources to match the efforts of those truly bent on creating havoc. Some virus companies are getting off hundreds of new samples a day! Moreover, the new viruses are getting "smarter" in that they propagate themselves quickly and they often hide themselves and are smart enough to move around in a system by renaming themselves in an effort to make it hard to remove them.

### **Why Do I Feel Like Somebody's Watching Me?**

Spyware is one of the fastest-growing internet threats. According to the National Cyber Security Alliance, spyware infects more than 90% of all PCs today. These unobtrusive, malicious programs are designed to silently bypass firewalls and anti-virus software without the user's knowledge. Once embedded in a computer, it can wreak havoc on the system's performance while gathering your personal information. Fortunately, unlike viruses and worms, spyware programs do not usually self-replicate.

### **Where does it come from?**

Typically, spyware originates in three ways. The first and most common way is when the user installs it. In this scenario, spyware is embedded, attached, or bundled with a freeware or shareware program without the user's knowledge. The user downloads the program to their computer. Once downloaded, the spyware program goes to work collecting data for the spyware author's personal use or to sell to a third-party. Beware of many P2P file-sharing programs. They are notorious for downloading that possess spyware programs.

The user of a downloadable program should pay extra attention to the accompanying licensing agreement. Often the software publisher will warn the user that a spyware program will be installed along with the requested program. Unfortunately, we do not always take the time to read the fine print. Some agreements may provide special "opt-out" boxes that the user can click to stop the spyware from being included in the download. Be sure to review the document before signing off on the download.

Another way that spyware can access your computer is by tricking you into manipulating the security features designed to prevent any unwanted installations. The Internet Explorer Web browser was designed not to allow websites to start any unwanted downloads. That is why the user has to initiate a download by clicking on a link. These links can prove deceptive. For example, a pop-up modeled after a standard Windows dialog box, may appear on your screen. The message may ask you if you would like to optimize your internet access. It provides yes or no answer buttons, but, no matter which button you push, a download containing the spyware program will commence. Newer versions of Internet Explorer are now making this spyware pathway a little more difficult.

Finally, some spyware applications infect a system by attacking security holes in the Web browser or other software. When the user navigates a webpage controlled by a spyware author, the page contains code designed to attack the browser, and force the installation of the spyware program.

### **What can spyware programs do?**

Spyware programs can accomplish a multitude of malicious tasks. Some of their deeds are simply annoying for the user; others can become downright aggressive in nature.

Spyware can:

1. Monitor your keystrokes for reporting purposes.
2. Scan files located on your hard drive.
3. Snoop through applications on our desktop.
4. Install other spyware programs into your computer.
5. Read your cookies.
6. Steal credit card numbers, passwords, and other personal information.
7. Change the default settings on your home page web browser.
8. Mutate into a second generation of spyware thus making it more difficult to eradicate.
9. Cause your computer to run slower.
10. Deliver annoying pop up advertisements.
11. Add advertising links to web pages for which the author does not get paid. Instead, payment is directed to the spyware programmer that changed the original affiliate's settings.
12. Provide the user with no uninstall option and places itself in unexpected or hidden places within your computer making it difficult to remove.

### **Spyware Examples**

Here are a few examples of commonly seen spyware programs. Please note that while researchers will often give names to spyware programs, they may not match the names the spyware-writers use.

**CoolWebSearch**, a group of programs, that install through “holes” found in Internet Explorer. These programs direct traffic to advertisements on Web sites including *coolwebsearch.com*. This spyware nuisance displays pop-up ads, rewrites search engine results, and alters the computer host file to direct the Domain Name System (DNS) to lookup preselected sites.

**Internet Optimizer** (a/k/a DyFuCa), likes to redirect Internet Explorer error pages to advertisements. When the user follows the broken link or enters an erroneous URL, a page of advertisements pop up.

**180 Solutions** reports extensive information to advertisers about the Web sites which you visit. It also alters HTTP requests for affiliate advertisements linked from a Web site. Therefore the 180 Solutions Company makes an unearned profit off of the click through advertisements they've altered.

**HuntBar** (a/k/a WinTools) or **Adware.Websearch**, is distributed by Traffic Syndicate and is installed by ActiveX drive-by downloading at affiliate websites or by advertisements displayed by other spyware programs. It's a prime example of how spyware can install more spyware. These programs will add toolbars to Internet Explorer, track Web browsing behavior, and display advertisements.

### **How can I prevent spyware?**

There are a couple things you can do to prevent spyware from infecting your computer system. First, invest in a reliable commercial anti-spyware program. There are several currently on the market including stand alone software packages such as Lavasoft's Ad-Aware or Windows Antispyware. Other options provide the anti-spyware software as part of an anti-virus package. This type of option is offered by companies such as Sophos, Symantec, and McAfee. Anti-spyware programs can combat spyware by providing real-time protection, scanning, and removal of any found spyware software. As with most programs, update your anti virus software frequently.

As discussed, the Internet Explorer (IE) is often a contributor to the spyware problem because spyware programs like to attach themselves to its functionality. Spyware enjoys penetrating the IE's weaknesses. Because of this, many users have switched to non-IE browsers. However, if you prefer to stick with Internet Explorer, be sure to update the security patches regularly, and only download programs from reputable sources. This will help reduce your chances of a spyware infiltration.

### **And, when all else fails?**

Finally, if your computer has been infected with a large number of spyware programs, the only solution you may have is backing up your data, and performing a complete reinstall of the operating system.

### **Name, Rank and Social Security Number**

Identity theft is the fastest growing crime in the U.S. The U.S. Secret Service has estimated that consumers nationwide lose \$745 million to identity theft each year. According to the Identity Theft Resource Center, the average victim spends 607 hours and averages \$1,000 just to clear their credit records.

Identity thieves employ a variety of methods to gain access to your personal information. They may get information from businesses or other institutions by stealing it; by bribing an employee who has access to records; hacking into records; or conning information out

of employees. Once identity thieves have your personal information, they may use it to commit a fraud or theft in your name.

How can you tell if you have become a victim of identity theft? Some signs include unexplained charges or withdrawals from your financial accounts; bills or other mail stop arriving (the thief may have submitted a change of address); a credit application is denied for no apparent reason, or debt collectors begin calling about merchandise or services you didn't buy.

Your computer can be a goldmine of personal information to an identity thief. To protect yourself and your computer against identity theft consider:

- Updating virus protection software frequently. Consider setting your virus protection software to update automatically. The Windows XP operating system also can be set to check for patches automatically and download them to your computer.
- Not opening files sent to you by strangers, clicking on hyperlinks, or downloading programs from people or companies you don't know.
- Using a firewall program, especially if you use a high speed Internet connection like cable or DSL that leaves your computer connected to the Internet 24 hours a day.
- Providing your personal or financial information through an organization's secured website only. While not fool proof, a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for secure), may provide additional security.
- Not storing your financial information on your laptop, unless absolutely necessary.
- Deleting all the personal information stored on a computer before disposing of it. A "wipe" utility program to overwrite the entire hard drive is recommended.
- Checking with an anti-fraud education organization such as CardCops ([www.cardcops.com](http://www.cardcops.com)). Card Cops runs a web site designed to help consumers determine whether their credit card numbers may have been stolen. They monitor Internet "chat rooms" where identity thieves illicitly trade and sell stolen credit card numbers. CardCops turns the information over to law enforcement authorities, but also allows consumers to access their database to see whether individual card numbers may have been stolen. In the first two months of operation, the site identified more than 100,000 stolen credit cards.

As with any crime, you can not completely control whether you will become a victim, but you can take steps to minimize your risk by remaining diligent and by minimizing outside access to your personal information.

## Conclusion

Using the internet should be fun, useful and risk free. Not surprisingly it is just a reflection on everyday life. There will always be someone somewhere who is prepared to steal your cash and identity. So caution should be the KEYWORD.

Three Basic Rules to follow:

1. DO NOT click on links in emails from persons or organizations that are unknown to you.

2. DO NOT reply to Institutions that request any personal detail, they are generally fake.
3. DO NOT reply to Spam Emails requesting they delete your details as this proves that your email address is genuine, just DELETE IT.