

Computer User Awareness Guide:

How To Keep Your Computer Safe From Crippling Pop-ups, Viruses, Spyware, & Spam, While Avoiding Expensive Computer Repair Bills

- Do you constantly get hammered by pop-up ads that come from nowhere and interfere with using your computer?
- Does your computer run slow, act funny, or crash unexpectedly?
- Are you getting tons of spam from unknown senders?

If so, then your computer is probably infected with malicious programs that could end up destroying your files, stealing your personal and financial information, and rendering your computer useless.

Don't Be A Victim To Online Crime!

Cyber criminals lurk everywhere and are constantly finding new ways to harm you. Even legitimate websites have sophisticated methods of snooping into your private information using cookies and spyware. If you want to make sure you aren't their next victim, read this guide and discover:

- ✓ Computer scams, threats, and rip-offs that you **MUST** be aware of.
- ✓ Surefire signs that you are infected with spyware, malware, and viruses.
- ✓ Sneaky, underhanded ways cyber criminals access your computer, and how you can stop them dead in their tracks.
- ✓ The absolute worst type of program to install for your computer's health; go to these sites and indulge in these seemingly innocent activities and you're practically guaranteed to get infected with vicious spyware and destructive viruses.
- ✓ The single biggest cause of expensive computer repairs – and how to avoid it.
- ✓ 7 Simple steps to keep your computer safe from pop-ups, viruses, spyware, malware, and expensive computer repair bills.

Provided as an educational service by:

Tim Shoemaker, President
Synectics, Inc.
2210 Bryan St. PO Box 537
Melbourne, FL 32902-0537
Phone: (321) 733-7310 Fax: (321) 733-1709

From The Desk of: **Tim Shoemaker**
President, Synectics, Inc.

Dear Fellow Computer User:

If you own a computer that has access to the Internet and e-mail, then it is only a matter of time before you fall victim to a malicious spyware program, virus, worm, or hacker. Every day we get customers coming in who are experiencing computer problems due to these threats, *and it is only getting worse.*

What is even more frustrating is that many of these computer users are back in my office a few days or weeks later with the EXACT same problems and end up having to spend ANOTHER hefty fee for restoring their computer back to normal.

You see, unless you learn how to ward off these evil cyber criminals and beat them at their own game, you will constantly fall victim to their pranks and criminal intent and end up spending hundreds – possibly even thousands – of dollars to get your computer running normal again.

Just recently we have seen a sharp increase in the number of computer users falling victim to these attacks and that is why I decided to write this report. I wanted to arm my customers with the facts so they could avoid problems and expensive repair bills.

The information in this Guide will not only educate you as to WHY you are experiencing these problems, but also what you **must** do now to guard against the unethical actions of these cyber criminals.

Three Dangerous Threats You Must Be Aware Of

One of the most dangerous aspects of online threats is their ability to cloak their existence. Hackers and the authors of malicious spyware and malware programs go to great lengths to create programs that are difficult to identify and remove.

That means a malicious program can be downloaded and doing its dirty work on your computer long before you are aware of it. Below are the two most common threats you'll need to guard against with a brief explanation of what they are:

Spyware: Spyware is Internet jargon for hidden programs advertisers install on your PC without your permission to spy on you, gather information, and report this information about you and your online activities to some outside person.

Spyware is NOT harmless; it can be responsible for delivering a boatload of spam, altering your web browser, slowing down your PC, and serving up a bounty of pop-up ads. In some of the more extreme cases, spyware can also steal your identity, passwords, e-mail address book, and even use your PC for illegal activities.

Most spyware finds its way onto your computer via file downloads including free programs, music files, and screen savers. While you *think* you are only downloading a legitimate program to add emoticons to your e-mails, you are unknowingly also downloading a heaping spoonful of spyware programs.

Spyware piggybacks the download and runs undetected in the background collecting information about you and sending it back to its originator until it is removed. Although spyware has malicious components, it is not illegal, and it is not considered a virus because it doesn't replicate itself or destroy data.

Malware: Malware is short for **malicious software** and represents all programs, viruses, Trojans, and worms that have malicious intent to damage or disrupt a system. Malware is harder to remove and will fight back when you try to clean it from your system. In some extreme cases, we have had to completely wipe out all of the information on the computers' hard disk and start with a complete re-install of the operating system.

Among other things, a malware infection can corrupt your files, alter or delete data, distribute confidential information such as bank accounts, credit cards, and other personal data, disable hardware, prevent you from using your computer, and cause a hard drive to crash. Frequently, malware is also designed to send itself from your e-mail account to all the friends and colleagues in your address book without your knowledge or consent.

Hackers: Hackers are computer programmers turned evil. They are the people who design the spyware and malware programs that attack your computer.

Some of them have criminal intent and use these programs to steal money from individuals and companies. Some have a grudge against the big software vendors (like Microsoft) and seek to harm them by attacking their customers (you). Others do it purely for fun. Whatever the reason, hackers are getting more intelligent and sophisticated in their ability to access computer systems and networks.

Surefire Signs That You Are Infected With Spyware, Malware, and Viruses

Since most malicious programs are designed to hide themselves, detecting their existence not always easy. However, there are a few surefire signs that you have been infected:

- You start getting swamped with pop-up ads that seem to come from nowhere and constantly interrupt your use of the computer.
- Your computer is unstable, sluggish, locks up, or crashes frequently.
- Your web browser's home page changes on its own and you cannot modify the settings. You may also see toolbars on your web browser that you did not set up.

- You get a second or third web browser popping up behind your main browser that you didn't open or request.
- Mysterious files suddenly start appearing.
- Your CD drawer starts opening and closing by itself.
- You get constant runtime errors in MS Outlook/Outlook Express.
- You find emails in your "Sent Items" folder that you didn't send.
- Some of your files are moved or deleted or the icons on your desktop or toolbars are blank or missing.

If you are experiencing one or more of the above when using your computer, you are infected and should seek help from a senior computer technician. Before I talk about getting rid of it, let me share with you 4 costly misconceptions about spyware, malware, hackers, and other threats that you will also need to know...

The Four Most Costly Misconceptions About Spyware, Malware, And Other Computer Threats

#1: Spyware and Malware is easy to remove.

Some spyware and malware CAN be easily removed using a program such as Spybot's Search & Destroy (you can download it for free at: www.safer-networking.org) or Ad-Aware (you can download it at www.lavasoftusa.com/support/download).

However, not all malicious programs can be removed – or even detected – using the above software. Many programs integrate so deeply into the operating system that it takes a skilled technician several hours to fully diagnose and remove the malicious program. In some extreme cases, we have had no alternative, but to wipe the hard disk clean by deleting all of the files on it and re-installing the operating system.

Obviously this is NOT an ideal situation and we do everything within our power to avoid it. Unfortunately there are some malicious programs that are so intelligent that there is simply no other way of removing them.

Of course you can use Spybot or Ad-Aware as a first attempt at cleaning your machine; however, if you continue to notice that your computer runs slow, if you continue to get crippling pop-ups, or any other of the tell-tale signs discussed earlier, you will need to seek the help of an experienced computer technician.

#2: It is my computer's fault that I continue to get attacked by spyware, malware, and viruses.

In all cases, malware, spyware, and viruses are a result of some action taken by the user (you or a family member that uses your computer). Remember, cyber criminals are *incredibly clever* and gain access to your computer via some of the most innocent and common activities you are performing; that is why it SEEMS as though it is your computer's fault.

For example, many of the clients we see simply downloaded an emoticon software program. Emoticons are the smiley faces and action characters that you see at the bottom of many people's e-mails. In doing so they also (unknowingly) downloaded a payload of spyware and malware and before they knew it, could no longer use their computer due to the instability and pop-ups.

Other deadly programs to avoid are free "enhanced" web browsers, screen savers, and just about any "cute" programs you come across that are free to download. Always read the terms and conditions before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer.

Installing programs is not the only way a hacker or malware program can access your computer. If you do not have the most up-to-date security patches and virus definitions installed on your computer, hackers can access your PC through a banner ad on the web that you accidentally clicked on or through an e-mail attachment that you opened.

Just recently, hackers have even been able to figure out ways to install malicious programs on your computer via your Internet Explorer web browser EVEN IF YOU DIDN'T CLICK ON ANYTHING OR DOWNLOAD A PROGRAM. Microsoft is constantly providing patches to their operating system software and all it takes is one missed update to leave you completely vulnerable.

Finally, you should COMPLETELY AVOID any and all peer to peer file sharing networks such as KaZaa. These sites are the absolute WORST online activities you can participate in for your computer's health because they are pure breeding grounds for hackers, spyware, malware, and other malicious attacks.

#3: If my computer is working fine right now, I don't need to perform maintenance on it.

This is probably one of the biggest and most deadly misconceptions that most computer users fall victim to. Computers are just like cars. If you don't change the oil, change the filter, rotate the tires, flush the transmission, and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance.

There are certain maintenance checks that need to be done daily (like virus updates and spam filtering), weekly (like system backups and a spyware sweep), and monthly or quarterly like checking for and installing security patches and updates, disk defrag, spyware detection and removal, checking the surge suppressor and the integrity of the hard drive, and so on.

Your computer repair technician should be adamant that you have regular maintenance done on your computer and should offer to set up automatic virus definition updates, spam filtering (to avoid viruses), and automatic system backups that are stored on an OFF SITE location (this protects the backup from fire, flood, or other natural disasters).

If your technician does not press you to let him do this for you, then RUN – don't walk – out of their office. Lack of system maintenance is the NUMBER ONE reason most people end up losing valuable files and incurring heavy computer repair bills. If your technician isn't offering you these services, you need to find someone else to support your computer or network for two reasons:

1. Either they don't know enough to make this recommendation, which is a sure sign they are horribly inexperienced, *OR*
2. They recognize that they are *profiting* from your computer problems and don't want to recommend steps towards preventing you from needing their help on an ongoing basis.

Either reason is a good one to get as far away from that person as possible!

#4: The firewall and security tools provided in the Microsoft Operating System are all the maintenance and protection I need.

Again, this is a terrible misconception. Microsoft does NOT include ALL of the security features to protect your data from viruses, hackers, and data loss or prevent your PC from running slowly.

As a matter of fact, there is no one single vendor that provides ALL of the system security features you need to keep your computer and files safe from harm.

Security and protection from these malicious attacks takes a multi-faceted, layered approach. Let me outline exactly what you need to make sure your computer is completely protected...

7 Simple Steps To Secure Your Computer From Malicious Attacks and Avoid Expensive Repair Bills

1. **Keep an up-to-date anti-virus software running at all times.** I recommend [AVG anti-virus] for two simple reasons: 1) It detects and removes spyware and malware programs that a lot of the more well-known (and more expensive) anti-virus software programs miss, and 2) It does it for about half the price.

It also has an auto scan and update feature that will make sure your computer is running the most current protection available and regularly scanning for threats. If you want a free 30-day trial of the [AVG] product, go to: www.grisoft.com.

2. **Start using an alternative web browser to Internet Explorer such as Mozilla Firefox.** Just recently, hackers have figured out a way to access and download malicious programs to your computer via a security hole in IE. What is amazing about this is that you don't even have to click on anything or download a program to get infected. You are especially vulnerable if you have an older version of Windows such as Windows 98.

Mozilla is a completely free web browser that does not have the same security problems as IE. Many of my clients even report back that they like their Mozilla browser better than Internet Explorer. Switching from IE to Mozilla is a simple and cost-free way to add another layer of security to your computer. To download this free browser, go to www.mozilla.com/en-US/products/

3. **Use an alternative e-mail program other than Outlook Express.** Outlook Express is notorious for security holes. If you don't have the latest security updates, hackers can send you e-mails with viruses that automatically open and install themselves without you even opening or previewing the e-mail and its attachments. I recommend that you either upgrade Outlook Express to a newer, more secure version of Outlook or switch to Mozilla's Thunderbird E-mail software. Thunderbird is free and you can download a copy from: www.mozilla.com/en-US/thunderbird/
4. **Never open suspicious looking e-mails or attachments.** This goes without saying because most viruses are replicated via e-mail. If it looks suspicious, delete it immediately!
5. **Stop using peer to peer file sharing sites and downloading "cute" programs.** Think of it like cyber candy. Hackers use these cute and funny programs as bait to get you to download their destructive programs. These are guaranteed ways of contracting malicious viruses, spyware, and malware. Also, peer to peer file sharing sites like KaZaa are mine fields of malicious programs. NEVER access those sites or download the programs that run them.

6. **Set up a firewall.** A firewall is simply a device that acts as a buffer between you and the big, wild world of the Internet. Many users will get a DSL or cable Internet

connection and plug it directly into their computer with no firewall in between.

The one thing you have to remember about the Internet is that it is a big open field. You have access to the world, but on the flip side, the world has access to YOU. Hackers have programs that automatically scan the Internet for computers connected via a cable or DSL connection without a firewall. Once they find one, they access your computer, download vicious programs, and can even use YOUR computer to send viruses to your friends and other computers, all without your knowledge or consent.

A simple and inexpensive firewall is Zone Alarm from Zone Labs. You can download this from www.zonelabs.com.

- 7. Backup your files every night.** Have you ever lost an hour of work on your computer due to a crash or program error? Now imagine losing all of your precious family and vacation photos, e-mails, music files, and documents. No one really thinks about losing all of the data on their computer until it actually happens. By then, it is either too late and you have lost EVERYTHING or it will take a lot of money paid to a specialist to recover your files.

I cannot stress the importance of backing up your files enough. If the files on your computer are important to you, then it is about time you got serious about protecting them by backing up every night.

The backup solution you chose will depend on the amount or size of the data you need to backup. Sometimes a simple zip drive or CD burner will do the trick. If you have a lot of data to backup, you may want to consider a tape backup system. If you want to know what is best for your specific situation, call our offices and one of our technicians will be happy to discuss the best system backup plan for you.

Want To Be Absolutely Certain That Your Computer Is Safe From Spyware, Malware, and Other Threats?

Introducing The “Ultimate Peace of Mind” Computer Security System for Small Business Owners

If your computer and the files on it are important to you, it's about time you got serious about protecting them. Our Ultimate Peace of Mind Computer Security Pack is designed to take the guesswork out of securing your computer from data loss, viruses, spyware, downtime, and expensive computer repairs so you never have to worry that you are not protected.

Call Synectics today at (321) 733-7310 and ask us about our affordable “Ultimate Peace of Mind” system for your business computers. We can tailor a program to your specific needs that will protect your systems from the threats and costs discussed in this report.

**Call us now at (321) 733-7310
We can help you get and stay safe**