

FREE Consumer Awareness Guide:

How to Keep Your Computers 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:

Larry Owens, President
IntegrIT Network Solutions, Inc.
PO Box 2458
Lynnwood, WA 98036-2458
www.integrit-network.com

Please turn over...

Dear Colleague,

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...

Please turn over...

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

#1: Spyware and Malware are 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. 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 DOWLOAD 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.

Please turn over...

Want To Be Absolutely Certain That Your Computer Network Is Safe From Spyware, Malware, and Other Threats Including Inappropriate Employee Online Activities?

FREE Problem Prevention Assessment for All New Customers

As a prospective customer, we would like to offer you a \$495 Problem Prevention Assessment of your company's network for FREE.

During this Assessment, we will do a comprehensive inspection of your computer network to look for potential problems, security loopholes, spyware, and other computer problems that will cause your computers and network to run slow, act funny, crash, and lose data.

We will:

- ✓ Diagnose any computer problems you are experiencing
- ✓ Check your network's security against hacker attacks and viruses
- ✓ Review your network and data backup processes to ensure they are working properly
- ✓ Check that your computer and network equipment does not have any service failures or critical alerts
- ✓ Provide system utilization reports to pinpoint current and potential service interruptions including a list by employee and by system to help you identify installed viruses, malware and spyware
- ✓ Provide written documentation of all critical systems for asset tracking and disaster preparedness purposes

All you have to do is contact us for ANY computer repair or service and we'll do this comprehensive assessment for FREE!

How to Secure Your Free Network Security Assessment

1. Fill in and fax back the enclosed request form.
2. Call us direct at 866-578-6220
3. Via our Web site at www.integrit-network.com/freeoffer
4. Send an e-mail to info@integrit-network.com with the words, "Network Security Assessment" in the subject line. Be sure to include your company name, address, and phone number so I can follow up with you.

There is absolutely no obligation or pressure for you to buy anything, or to ever use our services again. This is simply an easy way for us to demonstrate how we can help your business at no risk to you.

Good Networking,
Larry Owens, President
IntegrIT Network Solutions, Inc.
1-866-578-6220
www.integrit-network.com

“Yes! I Want To Make Sure My Network And Company’s Data Is Safe From Harm”

Please sign me up for a FREE Problem Prevention Assessment so I can make sure I am doing everything possible to secure my network.

I understand that I am under **no obligation** to do or to buy anything by requesting this assessment.

Please Complete And Fax This Page Back To 425-787-0124

Name: _____
Title: _____
Company: _____
Address: _____
City: _____ ST: _____ Zip: _____
Phone: _____ Fax: _____
E-mail: _____
Number of PCs: _____
Operating System: _____

The IntegrIT Network Solutions, Inc. Customer Bill Of Rights

Here is what we promise to deliver if you choose IntegrIT Network Solutions, Inc. to service your computers or company network:

1. When you call us with a computer problem, we guarantee that your phone call will be either answered immediately or returned within 60 minutes or less by an experienced technician who can help.
2. You should not have to wait around all day for your computer to be repaired. We understand how important your computer is to you; that is why we offer specific appointment times for repair services.
3. You deserve to get answers to your questions in PLAIN ENGLISH. Our technicians will not talk down to you or make you feel stupid because you don’t understand their “geek speak.”
4. You deserve complete satisfaction with our products and services. We will do whatever it takes to make you happy. No hassles, no problems.
5. You should EXPECT that no damage will be done to your machine or your data. Before we start working on your computer or network, we will evaluate your problem and alert you to any potential risks involved in fulfilling your job. If there are any risks, they will be explained in full, and your authorization and agreement will be obtained before the work commences. You can also choose to have your data backed up before we start any work on your machine.

A large proportion of our business comes from referrals from happy, satisfied customers. We want you to recommend us and we know that you will only do this if you are happy with the services we provide. That is why we work so hard to go above and beyond the call of duty.

Please turn over...

But... Don't Take Our Word For It; Just Listen To What Some Of Our Customers Have To Say...



"CG Engineering contracted with IntegrIT Network to take on some of the day-to-day management tasks of the existing IT systems. IntegrIT installed new state of the art hardware and software to meet the intensive demands of an engineering office. **With IntegrIT Network Solutions Chevy and Greg are able to put their focus on the business side of the company and know that the computer system is being efficiently monitored.**" ~ C. Chevy Chase, PE, SE, C G Engineering, Edmonds, WA



"Your **Rest Assured proactive maintenance plans have saved me at least \$3,000 in IT support costs** and I love the fact that I don't have to worry about security issues any more." ~ Roy Cats, Fire Protection, Inc., Everett, WA



"We have been working with IntegrIT Network Solutions, Inc. for over 3 years and they continue to provide outstanding service to us. **We rely on them for all of our IT needs and to monitor our network, which helps us provide the type of service to our patients that they demand.** Their proactive monitoring service provides me with great comfort!" ~ Dr. Heidi Rendall, Anchor Medical Clinic, Mukilteo, WA



"Your prompt service and ability to get things running smoothly are terrific. Not only did you correct the servers allocation, **you ensured the data backup process was secure and correct.** That gives me plenty of **peace of mind.**" ~ Fred Desimone, owner of SIR Construction, Mukilteo, WA



"You provided 100% service during a very frustrating situation with a local telecom firm. But you stuck with it and even helped provide an "out of the box" solution so I could still continue working. **You've given me much peace of mind, knowing my sensitive client data is safe and secure** within my wireless network plus having a solid plan for future business growth." ~ Jennifer Russell, Jenderuss Forensics Accounting, Lynnwood, WA



"**Responsiveness, clarity, and remote access - key benefits we enjoy by contracting with IntegrIT Network Solutions.** In short, we have a bigger, faster, more reliable system with backup and better customer service, for less money that we were paying previously. You can't beat that!" ~ Manny Rios, Rios Cruz, PS, Seattle, WA