FREE Business Advisory Guide:

How To Keep Your Computer Network 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 network run slow, act funny, or crash unexpectedly?
- ☑ Are you getting tons of spam from unknown senders?

If so, then a computer or computers on your network are probably infected with malicious programs that could end up destroying your files, stealing your company's confidential and financial information, and possibly 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 network's health; if you or your employees 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.
- ✓ 6 Simple steps to keep your computer safe from pop-ups, viruses, spyware, malware, and expensive computer repair bills.

Provided as an educational service by:
Willie Kerns, Managing Partner
SmartPath Technologies
78 Ash Street, Calvert City KY, 42029
P (270)205-4709 – F (270)205-4711 – www.smartpathtech.com

From The Desk of:
Willie Kerns / SmartPath Technologies

Dear Colleague:

If you are a business owner with a computer network connected to the Internet, then it is likely only a matter of time before you fall victim to a malicious spyware program, virus, worm, or hacker. Every day we get customers calling our office 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 clients call back a few days or weeks later with the EXACT same problems and end up having to spend ANOTHER hefty fee for restoring their computer network back to normal.

Unless you learn how to secure your network from 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 network running normal again.

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

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 malicious individuals.

Three Most Common and Dangerous Threats You Must Be Aware Of

One of the most dangerous aspects of online threats are 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. They are also highly experienced at finding tiny, overlooked loopholes in your security to access and infect your network undetected.

That means a malicious program can be downloaded and doing its dirty work on your network long before you are aware of it. Below are the three 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 network 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. All it takes is one employee downloading a questionable file to infect your entire network.

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 **mal**icious soft**ware** 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 card numbers, and other personal data; it can also disable hardware, prevent you from using your computer, and cause an entire network to crash. Malware is designed to replicate itself from one computer to the next either through a network connection or via your e-mail account 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.
- You try and go to one website and another one appears
- Mysterious files suddenly start appearing.
- Your CD drawer starts opening and closing by itself.
- You get constant runtime errors in MS Outlook/Windows Live Mail or other programs.
- 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 an employee). 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, one of your employees could innocently download 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 to your network.

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. Employees should be restricted from downloading any of these programs from the web and educated to the dangers of these programs.

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 BitTorrent or PirateBay. 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. Again, most of the infections we see come from employees accessing these websites for personal use on company machines.

#3: If my computer network 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 business owners fall victim to. Computer networks 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…

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

While it's impossible to plan for every potential computer problem or emergency, a little proactive monitoring and maintenance of your network will help you avoid or greatly reduce the impact of the vast majority of computer disasters you could experience.

Unfortunately, I have found that most small business owners are NOT conducting any type of proactive monitoring or maintaining their network, which leaves them completely vulnerable to the types of disasters you just read about. This is primarily for three reasons:

#1. They don't understand the importance of regular maintenance.

#2. Even if they DID understand its importance, they simply do not know what maintenance is required or how to do it.

#3. They are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. That means no one is watching to make sure the backups are working properly, the virus protection is up-to-date, that critical security patches are being applied, or that the network is "healthy" overall.

While there are over 97 critical checks and maintenance tasks that need to be performed on a daily, weekly, and monthly basis, I'm going to share with you the 4 that are most important for protecting your company.

Step#1: Make Sure You Are Backing Up Your Files Every Day

It just amazes me how many businesses never back up their computer network or their computers. Imagine this: you write the most important piece of information you could ever write on a chalkboard and I come along and erase it. How are you going to get it back?

You're not. Unless you can remember it, or if YOU MADE A COPY OF IT, you can't recover the data. It's gone. That is why it is so important to back up your network. There are a number of things that could cause you to lose data files. If the information on the disk is important to you, make sure you have more than one copy of it.

Step #2: Test Your Backups On A Regular Basis To Make Sure They Are Working Properly

This is another big mistake I see. Many business owners set up some type of backup system, but then never check to make sure it's working properly and never test it! It's not uncommon for a system to APPEAR to be backing up when in reality, it's not. There are dozens of things that can go wrong and cause your backup to become corrupt and useless. That is why it's not enough to simply back up your system; you have to check it on a regular basis to make sure the data is recoverable in the event of an emergency. Remember the Health Products Company that shelled out $40,000 to recover data they THOUGHT they backed up? Don't let that happen to you.

Step #3: Keep An Offsite Copy Of Your Backups

What happens if a fire or flood destroys your server AND the backup tapes or drive? This is how hurricane Katrina devastated many businesses that were forced into bankruptcy. What happens if your office gets robbed and they take EVERYTHING? Having an offsite backup is simply a smart way to make sure you can get your business back up and running in a relatively short period of time.

Step #4: Make Sure Your Virus Protection Is ALWAYS On AND Up-To-Date

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

Step #5: Set Up A Business Class Firewall

Small business owners tend to think that because they are "just a small business", no one would waste time trying to hack in to their network, when nothing could be further from the truth. I've conducted experiments where I connected a single computer to the Internet with

no firewall. Within hours, over 13 gigabytes of space was taken over by malicious code and files that I could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think its fun to disable your computer just because they can.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted, shutting down your hard drive. They can also use your computer as a zombie for storing pirated software or sending spam, which will cause your ISP to shut YOU down and prevent you from accessing the Internet or sending and receiving e-mail.

If the malicious programs can't be deleted or fixed, you'll have to re-format the entire hard drive causing you to lose every piece of information you've ever owned UNLESS you were backing up your files properly (see 1 to 3 above).

IMPORTANT: A router or wireless router like you'd go purchase for your home is NOT a business class firewall! This is a mistake that we see business owners make time and time again – the routers you can purchase at retail stores are designed for home networks to allow you to share internet among your home computers, tablets, X-Boxes and other gaming systems. A business class firewall contains technology that is specially designed to protect computer networks, servers, and workstations in an office. A business class firewall typically will inspect all traffic coming in from the internet to make sure it's "OK" and also check to make sure anything that comes in is virus free, isn't spam, etc. A business class firewall will also allow you to report on internet usage and block categories of websites that you may not want your employees looking at during work hours.

Step #6: Update Your System With Critical Security Patches As They Become Available

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment. A lot of people see the little notice in the lower right hand part of the screen about "Updates Available". You need those updates and there are lots of them – Microsoft regularly releases updates for Windows, Internet Explorer, Office, and other programs, plus there are also Java updates, Adobe Updates, and a multitude of other updates that need regular attention.

Not too long ago Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they become available, you were completely vulnerable to this attack.

Here's another compelling reason to ensure your network stays up-to-date with the latest security patches…

Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

In essence, the time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

When the "nimda" worm was first discovered back in the fall of 2001, Microsoft had already released the patch that protected against that vulnerability ***almost a year before*** (331 days). So network administrators had plenty of time to apply the update. Of course, many still hadn't done so, and the "nimda" worm caused lots of damage. But in the summer of 2003 there were ***only 25 days*** between the release of the Microsoft update that would have protected against the "blaster" worm and the detection of the worm itself!

Clearly, ***someone*** needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That is why we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

270-205-4709 (phone) – 270-205-4711 (fax) – www.smartpathtech.com

While we realize we've already discussed your network with you, we felt that it was of the utmost importance that you be aware of the dangers in this report. We want to help YOU with your business technology!

Please fax this form to 270-205-4711 or e-mail it to willie.kerns@smartpathtech.com so that we can discuss how we can help you secure yourself against viruses, spyware, and online threats – even if you aren't ready for our entire line of services at this time!

Please Complete This Form:

Your Name: .....

Title: .....

Company: .....

Phone: .....

E-mail Address: .....

Number of PCs: .....

☐ **Contact me immediately**! I have a project or a problem I need your help with right away.

Fax To: 1-270-205-4711

270-205-4709 (phone) – 270-205-4711 (fax) – www.smartpathtech.com

Customer Bill Of Rights

Here is what I promise to deliver if you choose SmartPath Technologies to service your computer 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 our while-you-wait priority express service where we will start working on your computer the MINUTE you bring it in. In most cases, we can fix it within 30 minutes or less.

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.

270-205-4709 (phone) – 270-205-4711 (fax) – www.smartpathtech.com

Don't Take Our Word For It;
Just Look At What Our Customers Have To Say…

SmartPath is locally owned and operated-they are my IT partner, who has my back!

"We love the fact that you are a local business, who takes care of our IT needs. I was "WOW"ed with the fact I could turn the technical computer stuff over to you and know that you have my back. This allows me to concentrate on other aspects of my job. You take the time to communicate and check in with us. I feel like a partner with SmartPath, my computer is critical to the operations of this office."

– Debbie Buchanan, Executive Administrator
Marshall County Chamber of Commerce

Always getting to speak to someone when you call

"Since SmartPath has been our IT provider, our computer/network issues are few. I credit this to their daily monitoring of our systems. All of the staff are friendly and helpful at all times, no matter big or small questions or problems. I always recommend SmartPath, because I want others to have the best and that is why I recommend the best."

- Tiffany Carlson, Legal Practice Administrator
Law Office of Donald Thomas

Day or Night, work week and weekends, SmartPath is there for me

"Forgot my e-mail password, sent an e-mail after normal business hours and was in no hurry and expected to get a reply the next day. WRONG!!! I had my password within an hour and was able to get my e-mail on my phone. Great service. Couldn't have been better..."

- Ben Noles, Chemical Operator
Estron Chemical

270-205-4709 (phone) – 270-205-4711 (fax) – www.smartpathtech.com