

FREE Consumer 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:
MOOSE LOGIC
1415 Western Avenue, Suite 205
Seattle, WA 98101
<http://www.mooselogic.com>



From The Desk of: Scott Gorcester, President
Moose Logic

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 hear from people 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 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 computers running normally 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 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 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 (because most of the time you actually *consent* to installing it – the language is buried in the license agreement that no one ever reads but that you have to agree to before you can download whatever it is you wanted), 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 (and sometimes to *anything* it finds anywhere on your system that looks like an e-mail address) without your knowledge or consent. It can also cause your computer, without your knowledge, to participate in coordinated, distributed attacks on third party systems (like a Web site that the bad guy wants to take down by flooding it with traffic).

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. Some hackers have actually created "kits" that make it easier for other people to create malware, and some of the most dangerous people out there are the "script kiddies" who use these kits to create malware that is far more sophisticated than they would be able to create from scratch – and for no more reason than to see if they can do it!

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

Since most malicious programs are designed to hide themselves, detecting their existence is 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. (Note, however, that having an email "bounced back" to you that you don't remember sending, or having someone contact you to say, "Hey, you sent me a virus!" may not necessarily mean that *your* computer is infected. It may be that someone with whom you've exchanged email in the past has had *their* computer infected, and that the virus discovered your email address on *their* computer and used it as a fake "From" address so the copies of itself it sent out would look like they were coming from you!)
- 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 Five 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 to create individual computer “security policies” that were tailored to prevent a particular executable from running, regardless of its filename or directory location, and in a few 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 *most* cases, malware, spyware, and viruses are a result of some action taken by the *user* (you or an employee or family member who 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, search toolbars, screen savers, and just about any of the “cute” programs you come across that are free to download. Always read the terms and conditions of the license agreement before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer.

Of course, if your computer doesn't have the latest security updates installed, it's vulnerable to exploits regardless of what else you do or don't do. (That's why we stated that in *most* cases the problems are the result of actions taken by the user.) We've read of experiments where unpatched Windows XP machines were connected to the Internet without

any kind of firewall protection just to see how long it would take before the machines were discovered and compromised. In most cases, it took only minutes.

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.

TECH NOTE: We find that it's very common for users to have administrative rights to their own workstations. In many cases, that's the path of least resistance for the network administrators, because it eliminates problems and user complaints – some applications won't run properly under an account with limited privileges, and users complain if control of the workstation environment is taken away from them. But it's dangerous. Limiting user accounts to the least privileges possible also limits the users' ability to accidentally delete critical files, or to inadvertently install malware.

#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 computers 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's built-in firewall 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.

#5: If I Don't Use Internet Explorer, I Don't Have to Worry About Security.

Everybody loves to beat Microsoft up on the subject of security. But there's a simple reason why most security exploits target Microsoft products: it's all about the return on investment for malware developers! To put it simply, if Linux or Macintosh had the kind of market share at the desktop that Microsoft has, all the bad guys would be writing exploits for Linux or Macintosh. The fact is that just in the latter part of 2006 and early 2007 there were a number of vulnerabilities identified that affected applications such as QuickTime (affecting both Windows and Mac), Sun's Java implementation (affecting Windows, Mac, and Linux), the Firefox browser, the WinAmp media player (affecting Mac's OSX) and the Macintosh OSX Operating System itself. You can bet your bottom dollar that as alternatives to Microsoft applications and Operating Systems become more popular, more exploits will be written to target them. So if you prefer Firefox, by all means, use it. But don't fool yourself into thinking that using Firefox means you don't have to worry about security. No matter what browser or email reader you use, you still need to make sure you have the latest updates.

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...

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

1. **Keep up-to-date anti-virus and anti-spyware software running at all times.** If you are one of our *MooseGuardTM* Platinum customers, you don't have to worry about it – because we're making sure your systems are protected using *two different* scanning

engines to make sure nothing slips through the cracks. And if you're a *MooseGuardTM* Silver or Gold customer, you can add this to your plan as well. For customers who want to own and manage their own anti-virus software, we recommend the Trend Micro product line, which can cover the complete range of needs from workstations to file servers to email servers. If you or someone you know needs anti-virus software for *private, non-commercial* use, and can't really afford a commercial product, try the AVG product, which you can download from <http://www.grisoft.com>.

2. **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, even if the message claims to be from someone you know!
3. **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. Aside from the questionable legality of file sharing, 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.
4. **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 – and, no, the Windows Firewall is *not* sufficient by itself.

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 know the Internet Protocol address ranges that major Internet Service Providers use for their high speed Internet customers, and have programs that automatically and regularly scan those address ranges looking for computers connected via a cable modem or a DSL connection without a firewall. They can even detect someone whose system is *temporarily* vulnerable because of maintenance activities such as upgrading their firewall software. In routine tests our engineers have performed on their own high speed Internet connections, we have found that hackers can detect and connect to an open computer on a high speed Internet connection in as little as **90 seconds!** Once they find one, they immediately start trying to access your computer, download vicious programs, and even use YOUR computer to send viruses to your friends and other computers, all without your knowledge or consent.

D-Link makes a variety of "broadband routers" with basic firewall functionality that are adequate for consumer use – you can find them at your local computer superstore for as little as \$50.00. Business use is generally a bit more demanding, and for those applications we recommend the Watchguard product line. We'd be happy to give you a recommendation for a specific model that would meet your business needs.

- 5. 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 enough the importance of backing up your files. 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 choose will depend on the amount or size of the data you need to back up. Sometimes a simple zip drive or CD burner will do the trick. If you have a lot of data to back up, you may want to consider an external hard disk drive that you can attach to one of the USB ports on your computer. If you want to know what is best for your specific situation, call our offices and we will be happy to discuss the best system backup plan for you. Our *MooseGuardTM* customers can even take advantage of our centrally-managed backup service where we just take care of it for you.

In a business network, you have to consider not only the files that are stored on your file server(s), but also databases, email servers, *and* the business-critical files that your employees store on their individual PCs (even though you've told them to store everything on a file server). We offer our customers a range of solutions that can insure that critical files are backed up *constantly*, each and every time they are changed and saved, and can automatically transmit your most critical data to a secure, encrypted, off-site location.

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

Introducing The “Ultimate Peace of Mind” Computer Security Pack 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 *MooseGuardTM* support plans are designed to take the guesswork out of securing your computers from data loss, viruses, spyware, downtime, and expensive computer repairs so you never have to worry that you are not protected.

Silver Level Includes:

✓ Initial Site Survey (27-Point Network Audit)

A senior engineer will come on site to create initial network documentation, as well as to audit your network for potential problems areas including:

- Network security
- Data back-ups
- Virus protection
- Spam filtering
- Hardware integrity (check for pending failures)
- System performance and trends
- Overall network design and layout

Moose Logic will review the results of the network audit with you and recommend remedial action for any problems that may be identified.

✓ Network Monitoring:

This 24-7 network monitoring service will allow us to watch every aspect of your network to detect and report problems before they escalate into downtime, data loss, or expensive repair issues. Some of the items we will monitor include:

- Server traffic and load
- Hardware integrity and reliability
- Storage space and availability
- Back up success and failures
- Anti-virus and spyware monitoring (of Customer's anti-virus or anti-spyware software)
- Uninterruptible Power Supply (UPS) Monitoring (requires intelligent UPS, e.g., APC SmartUPS or equivalent)

✓ Patch Management:

Unlimited remote monitoring and installation of Microsoft critical patches and updates.

✓ Annual On-Site Consultation

Once a year, we will come on site to perform an extensive analysis of your network's trends, security, and performance, as well as to review your company's goals and technology issues. This review will allow us to make specific recommendations for improving your network performance, office productivity, and help you to plan and budget for future IT needs.

✓ Guaranteed Same Business Day Response To Critical Issues¹ during regular business hours.

✓ A Preferred Client Discount on Standard Technical Support Rates.

Monthly Pricing (\$295/month minimum):

\$20.00/Workstation or laptop

\$100.00/Server

\$10.00/Other device (e.g., UPS, router, firewall, thin-client device, etc.)

¹ "Critical Issues" are those that cause, or are reasonably anticipated to cause, a significant loss of computer functionality, data, or connectivity to Customer's network where such loss would reasonably be expected to cause a material impairment to Customer's computer equipment, data, or ordinary business operations.

Gold Level Service Includes:

✓ **Initial Site Survey (27-Point Network Audit)**

A senior engineer will come on site to create initial network documentation, as well as to audit your network for potential problem areas including.

- Network security
- Data back-ups
- Virus protection
- Spam filtering
- Hardware integrity (check for pending failures)
- System performance and trends
- Overall network design and layout

Moose Logic will review the results of the network audit with you and recommend remedial action for any problems that may be identified.

✓ **Network Monitoring:**

This 24-7 network monitoring service will allow us to watch every aspect of your network to detect and report problems before they escalate into downtime, data loss, or expensive repair issues. Some of the items we will monitor include:

- Server traffic and load
- Hardware integrity and reliability
- Storage space and availability
- Back up success and failures
- Anti-virus and spyware monitoring (of Customer's anti-virus or anti-spyware software).
- Uninterruptible Power Supply (UPS) Monitoring (requires intelligent UPS, e.g., APC SmartUPS or equivalent)

✓ **Patch Management:**

Unlimited remote monitoring and installation of Microsoft and Citrix critical patches and updates.

✓ **Software Asset Management:**

Monitoring of exactly what software applications are installed on which computers, to allow you to insure that you are in licensing compliance for all your applications.

✓ **FREE Break-Fix Services**

In the RARE event that covered equipment goes down due to equipment failure, virus outbreaks, or operating system problems, our team of senior technicians will troubleshoot and resolve the issue at NO ADDITIONAL SERVICE FEE to you. This includes telephone and, if necessary, on-site support for Critical Issues as defined above. You can consider this as a "network insurance plan". (Cost of replacement hardware is not included. Also please note that many laptops and/or tablet PCs require special tools and manufacturer certification in order to repair the laptop hardware. If it is determined by our support team that a laptop or tablet PC has a hardware problem, it will be your responsibility to have it repaired by a factory-authorized service center.) In the event that a workstation must be rebuilt (e.g., after a hard drive failure), Moose Logic's liability is limited to installing the Operating System, Operating System updates, and *MooseGuardTM* client utilities **unless** workstation is covered by Moose Logic's managed backup option, in which case the most recent image of the workstation will be restored.

✓ **Semi-annual Network Tune Up**

Twice a year, a senior network engineer will come on-site and conduct a thorough audit and "tune up" of your network to:

- Review and update available security patches & service packs
- Check status of Anti-Virus Clients
- Test peripherals, such as UPS(s)

- Perform a test restore to ensure back ups are functioning properly
- Review Hard drive space, memory, CPU utilization
- Review network documentation and make changes as necessary
- Review routers, firewalls, switches for failure or problems
- Optimize server for maximum performance and reliability
- In-depth review of server logs for errors and potential problems

✓ **Guaranteed 2-Hour or Less Response to Critical Issues during regular business hours.**

✓ **We Will Act On Your Behalf With 3rd Party Vendors**

At your request, we will act as a liaison between your company and other 3rd party vendors to manage projects or take care of problems. This includes hardware vendors, your ISP, your accounting software vendor, or other line of business applications.

✓ **A Preferred Client Discount on Standard Technical Support Rates.**

Monthly Pricing (\$495/Month Minimum):

\$35.00/Workstation or laptop

\$300.00/Server

\$50.00/Other *manageable* device (e.g., router, firewall, managed switch, etc.)

\$20.00/Thin-client terminal (e.g., Wyse Winterm)

\$10.00/Monitor-only devices (e.g., APC SmartUPS)

\$25.00/Workgroup Printer

\$10.00/Personal Printer

Platinum Level Service Includes:

Best Value

✓ **Initial Site Survey (27-Point Network Audit)**

A senior engineer will come on site to create initial network documentation, as well as to audit your network for potential problem areas including:

- Network security
- Data back-ups
- Virus protection
- Spam filtering
- Hardware integrity (check for pending failures)
- System performance and trends
- Overall network design and layout

Moose Logic will review the results of the network audit with you and recommend remedial action for any problems that may be identified.

✓ **Network Monitoring:**

This 24-7 network monitoring service will allow us to watch every aspect of your network to detect and report problems before they escalate into downtime, data loss, or expensive repair issues. Some of the items we will monitor include:

- Server traffic and load
- Hardware integrity and reliability
- Storage space and availability
- Back up success and failures
- Anti-virus protection
- (UPS) Uninterruptible Power Supply Monitoring

✓ **Quarterly Network Tune Up**

Every quarter a senior network engineer will come on-site and conduct a thorough audit and “tune up” of your network to:

- Review and update available security patches & service packs
- Check status of Anti-Virus Clients
- Test peripherals, such as UPS(s)
- Perform a test restore to ensure back ups are functioning properly
- Review Hard drive space, memory, CPU utilization
- Review network documentation and make changes as necessary
- Review routers, firewalls, switches for failure or problems
- Optimize server for maximum performance and reliability
- In-depth review of server logs for errors and potential problems

✓ **Patch Management:**

Unlimited remote monitoring and installation of Microsoft and Citrix critical patches and updates.

✓ **Software Asset Management:**

Monitoring of exactly what software applications are installed on which computers, to allow you to insure that you are in licensing compliance for all your applications.

✓ **FREE Unlimited Telephone Support for Microsoft Operating Systems and Productivity Applications + Unlimited On-site Support for Critical Issues**

This plan is for the organization that is looking for full outsourcing of all of their IT Support needs, including end-user help desk support for Microsoft productivity applications. And, in the RARE event that covered equipment goes down due to equipment failure, virus outbreaks, or operating system problems, our team of

senior technicians will troubleshoot and resolve the issue at NO ADDITIONAL SERVICE FEE to you. (Cost of replacement hardware is not included. Also please note that many laptops and/or tablet PCs require special tools and manufacturer certification in order to repair the laptop hardware. If it is determined by our support team that a laptop or tablet PC has a hardware problem, it will be your responsibility to have it repaired by a factory-authorized service center.)

✓ **Guaranteed 1-Hour Priority Response To Critical Issues during regular business hours.**

✓ **We Will Act On Your Behalf With 3rd Party Vendors**

At your request, we will act as a liaison between your company and other 3rd party vendors to manage projects or take care of problems. This includes hardware vendors, your ISP, your accounting software vendor, or other line of business applications.

✓ **FREE Managed Anti-spam, Anti-virus, and Anti-spyware software and filtering**

This includes both anti-spam and anti-virus screening powered by Postini – which will keep most spam and viruses from even reaching your email server – *and* workstation- and server-level anti-virus and anti-spyware software.

✓ **Unlimited Remote Software Installation and Upgrades**

✓ **User Account Maintenance**

Creation and deletion of user accounts, shared folder permissions, and email accounts.

✓ **Acceptable Use Policies and Procedures**

We will work with your organization to draft a set of Acceptable Use Policies and Procedures for your employees, if you do not already have them.

✓ **Hot-Spare “Loaner” PC.**

✓ **A Preferred Client Discount on Non-Covered Technical Support**

This would include network upgrades, installation of new hardware or software, special projects, or any other type of service we offer outside of this plan.

✓ **FREE Year-End Technology Review** to help you plan how to use technology to increase productivity, cut costs, gain competitive advantages, and support your company’s growth.

Monthly Pricing (\$1,495/Month Minimum):

\$100.00/Workstation

\$300.00/Server

\$50.00/Other *manageable* device (e.g., router, firewall, managed switch, etc.)

\$50.00/Thin Client Terminal (e.g., Wyse Winterm)

\$50.00/Citrix or Terminal Services User not permanently associated with a covered terminal device.

\$10.00/Monitor only device (e.g., APC SmartUPS)

\$25.00/Workgroup Printer

\$10.00/Personal Printer

NOTE: To qualify for Gold or Platinum Level Service, your network infrastructure must meet minimum standards:

- Servers must be Windows 2000 or 2003, with current (as defined by Moose Logic) service packs and security patches.
- Workstations must be Windows 2000 Professional or Windows XP Professional, with current (as defined by Moose Logic) service packs and security patches.
- Exchange Servers must be Exchange 2000 or later with current (as defined by Moose Logic) service packs and security patches.

- SQL Servers must be SQL 2000 or later with current (as defined by Moose Logic) service packs and security patches.
- All server and workstation hardware must conform to the Microsoft Hardware Compatibility List for the installed Operating System.
- Servers must have adequate (as defined by Moose Logic) RAM and free disk space – “adequate” may vary depending on the role of each server and its installed applications.
- Servers must have some level of disk redundancy.
- Network must be connected to the Internet, and must be protected with a hardware firewall.
- Customer must have a backup system that is, in the opinion of Moose Logic, appropriate to the environment.
- Servers must be in a location that provides physical security and appropriate temperature and humidity control.
- Servers must have adequate (as defined by Moose Logic) UPS protection, and UPS equipment must be intelligent, i.e., capable of being monitored remotely (e.g., APC SmartUPS or equivalent).
- Network infrastructure must meet minimum CAT5 cabling requirements, and conform to Ethernet standards for hub/switch architecture.

The Moose Logic Customer Bill Of Rights

Here is what I promise to deliver if you choose Moose Logic 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 one business day (or sooner, depending on the response time specified in your support agreement) by an experienced technician who can help.
2. 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".
3. You deserve complete satisfaction with our products and services. We will do whatever it takes to make you happy. No hassles, no problems.
4. 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.

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

"Our business is all about process and margins; we rely on Moose Logic to install and manage network solutions that enable us to control both.

"Moose Logic created solutions that transformed our business relationships and processes. Nothing short of a revolution, we were able to make our vision a reality. With network systems that support our operations, we have lowered cost variances to less than 1%; which is unheard of in our industry.

"At Birchwood Park Homes we have developed very strict business operations disciplines. We needed a company that understood our procedures and computer systems, a company with technical expertise, and a company that would take responsibility for their work. Our network system is a mission critical tool but we didn't have the staff or budget to manage it in house, we wanted someone we could depend

on.

"Moose Logic exceeded our expectations:

- Accountability - they took ownership, we were able to focus on our business
- Business Professionals - they suggested and built systems that improved our work product, making our business more profitable
- Experience we could trust - they delivered a product that was right for our organization and budget, no surprises

"We have been with Moose Logic for 9 years; I cannot imagine trusting our business to anyone else.

"For sixty years, Birchwood Park Homes has had as its primary goal to design and build homes of the very finest quality and value. We have succeeded in achieving this goal time and time again, with thousands and thousands of satisfied homeowners who will gladly attest to it."

Ron J. Horowitz, CEO; Birchwood Park Homes

"The Moose team worked with us as an entrepreneurial partner. Scott (Moose CEO) took the time to understand the problems that were interfering with our business. He presented immediate solutions eliminating network downtime, eliminating work flow distractions. Moose offered systems that would grow with the business. Best of all, *Moose took complete ownership of our network allowing the company to focus on building business!*"

"Moose Logic eliminated the day-to-day computer problems that were interfering with operations. Moose gave me the highest level of confidence and attentiveness at each step in the project, I knew what was being done, and why. I deal with a lot of technical folks the Moose Logic teams are small business entrepreneurs who know how important it is to find trusted, efficient, expert partners. I'd recommend Moose without reservation."

"Kasala opened its first store in 1987 in downtown Seattle with a commitment to offer a unique approach to modern home furnishings. Kasala quickly became known for styles that were inspiring, fun, modern and comfortable. In 1990, a second store opened in Bellevue and later a retail outlet within the Kasala's warehouse facility."

PK Stremic, System Operations; Kasala, Seattle - Bellevue