

MBTS TekJournal

Volume 4, Issue 4

April 2005

It's great to be back in the writer's chair after so long an absence. My Spring Break holiday was great in that we were someplace warm and not great because we were ill for the first three days. Even now, after being back at work for about three weeks we still aren't feeling 100%. Sometimes I wish I was a computer so that I could fix myself quicker than modern medicine seems to be able to do.

Since SPRING has come to Winnipeg and warm weather, and everyone is anticipating a nice summer, I think it is time to do some Spring Cleaning. Now is the time of year that I go through all my Future Column folders and clean disk. It is sort of a hodgepodge of articles, but it gets everything off to a great start.

I get questions all year long and I do my best to address them as they come up and many of them make it into the newsletter. However, some answers are harder to find and when the answer reveals itself it gets put into a Future Articles folder and gets slotted into a future edition. But questions and answers build up and every Spring I find that I have quite a few unrelated articles to patch together into a quilt of useful information that never really found a home.

Some of the articles in this issue include:

- How do you tell if your system is infected?

- How to backup your DVD's
- Is Shaw Secure better than what you have now?
- Is your system cool enough?
- Do you leave your computer on all the time?

Next issue we will look at software licenses and what you can legally do with the software you purchase. Thank you for your business and I look forward to your comments about this issue.☺

Are You Infected?

When you first got your computer you probably marveled at how FAST it was. Today, however, you may feel it isn't quite as fast as it was and you are not sure why. Here we will look at some of the ways that your system can be slowed down, sometimes to a crawl.

Most users today have high speed Internet connections that are always on. If your system is not protected by hardware firewall and anti virus software and possibly anti Spyware software your system is at high risk for infection. Now your primary question is probably going to be "How do I know if I am infected?"

If your computer starts to suddenly slow down or you begin to see pop-up windows, even when you're not browsing the Internet, you may be the victim of Spyware and other unwanted software. Spyware is software that is automatically downloaded, or installed, to your computer generally without your approval, and is often attached to another file you have chosen to download or install. Spyware can also be downloaded to your computer when you click on banner ads on Web sites.

Types of downloads that may contain Spyware

- Free games downloaded from the Internet
- Music, movies, and other software file-sharing programs downloaded from the Internet or from other computers
- Animated characters for your desktop
- Free screen savers downloaded from the

INSIDE THIS ISSUE

- 1 Welcome
- 1 Are You Infected?
- 3 Should you leave your system On or Off?
- 4 Is your System Cool enough?
- 5 F1 – Backup DVD's
- 6 Shaw Secure vs. Windows XP

Infected continued on page 2

Internet

- Toolbars for your Internet browser
- Free pop-up blockers that appear on your computer when you are online

A very common method of getting your system infected is by using Peer to Peer sharing software like KaZaA or Limewire. Even if you have all the protection listed above, you may not be completely safe from infection via these other sources. You know your system is safe, but what about the computer you are getting your "shared" files from? Are they taking the proper precautions?

There are two types of "free" software. The first is a truly altruistic form written by programmers who really love what they do and want to offer alternative solutions to procedures they feel are lacking in today's computers. The other type is written purely for monetary gain and is to be avoided. But how do you tell the difference?

Software costs money to be created. It takes many hours to write a simple application and can take months or years to write complex applications like P2P sharing. So how do these people, or companies, get paid for "free" software? The answer is in bundling their application with other applications that you don't necessarily want.

Bundling is done by most software creators, including Microsoft. A really good example of bundled software is Microsoft's latest version of MSN Messenger. When you begin the installation of the software a dialog box pops up and asks if you also want to install the MSN Toolbar, MSN Desktop Search, and if you would like to change your search engine to MSN and set you home page to MSN. Most users don't take the time to read this dialog box and simply click next. By asking for one application, MSN Messenger, you are actually getting three applications by way of the bundled software that comes with it. The MSN Toolbar is not really needed since Windows XP SP2 does a great job of stopping pops up from appearing and that is the main function of the MSN Toolbar. The Desktop Search is a specialty search feature that can actually slow down your system. If you have Indexing turned on as a service you are already performing some of the tasks involved to make Desktop Search work properly. Desktop Search takes the Indexing service one step further by

including not only all files and folders (including temporaries and backups) but also email, and chats, The premise is that indexing everything will make finding information faster, but every time you change (or add/delete) a file on your computer, the index gets updated first. Desktop Search plus the Indexing service duplicates the effort and overhead and can only slow down your system. How important is it really to find something on your system when most likely it will be in My Documents or your Inbox?

Other places where Spyware hides and you are most likely to install it without notice include: Date Managers, Time Managers, Peer to Peer software, cute animations that display on your screen, some screen savers, ... The list is almost endless. All of these applications have the potential to infect your system with, but generally without, your knowledge or approval. Looking in your Add/Remove options of the Control Panel could be the starting point for identifying unwanted software. Casino software is rampant and generally gets installed as a tagalong application. The same is true for Points Managers, some Shop at home services, New.net Domains, P2P services, etc.

Other forms of Spyware however do not announce themselves in the Add/Remove options. These include infections like About:Blank, CWS, Cool Web Search, and vx2 Transponder. These forms of infection require special software tools to be removed from your system.

What Happens when your system gets infected?

You are happily surfing the internet and a banner pops up and asks if you would like a calendar displayed on you desktop to help to see what the current date is. Your immediate thought is probably, "What's the harm?", so you click the banner and download and install the software.

First the original application gets installed, but if you don't ready the fine print (and sometimes there isn't any) the additional software also gets installed. Also, since your system environment is changing the System Registry gets updated with the new changes, and the Startup folder may change if the application is supposed to start every time your computer does. However, these are the simple areas that most people can track.

Behind the scenes more files are added to your system and not always in places you would normally look. Every time you access the Internet you add hundreds to thousands of temporary files in the Cookies, History, and Temporary Internet Folders. You also add folders to hidden cache folders, and infections can also be added to a Prefetch folder. Remember I said the System Registry gets updated: Many infections add code to the registry which tells their application to propagate itself to other hidden folders and back into the registry if any part of the infection is only partially removed. So, you find an unknown software component in the Add/Remove section of the Control Panel and remove it from your system. But it doesn't get rid of all of it. The next time your system starts, the infection is only partially available so it finds the hidden part that wasn't deleted and reinstalls itself bypassing the Add/Remove section making it harder to find. Sometimes these infections create folders in the Windows using plausible system names so you think they are really supposed to be there while in fact you have an infection hiding in plain sight. Other forms of infection attack your browser by changing the search criteria or your home page. If your default home page is MSN or Google or something familiar and you start your Internet browser and the page you expect to see has been replaced, your system is probably infected. When you do a search and instead of showing the search results you are transported to a unique search page, this is another indication that your system may have been infected.

If you think your system is running slower than normal, or you see pop ups when you're now actively accessing the Internet, or your search results are appearing as you have come to expect them to, or your home page has been replaced, your system may need professional help. If any of these symptoms can be found on your system, Call us for an appointment clean out the infection and make it run properly again.☺

On or Off?

Probably every third service call I get asked the question: Is it better to turn my system off every night or is it okay to leave it on?

For many people the perfect answer is "Do whatever

you're comfortable with." However I have heard of horror stories where a computer left on during a family vacation shorted out and burned down the house; a buildup of dust caused a static discharge that fried everything in its path; a power failure cause one client to lose all data without a current backup due to a power spike from lightning; and the list is seeming endless. But these rare cases and simple answer don't really answer the question, so here we will explore the real answer.

The real answer is it is a matter of choice relating to cost and security. If you make proper and regular backups that are tested, and your system is in peak form, and you have proper power conditioning, an excellent security system, and cost is not a factor, you may opt leave it on.

Power consumption related to cost for leaving a computer running 24/7 was recently studied at the Iowa State University. They found that the average computer running 'all the time' cost about \$65 per year. If you were to shut your monitor off on nights and weekends but leave the computer running, the cost would drop to about \$40 per year. If you turn everything off at night and on weekends, the cost would drop to about \$21 per year for operation of approximately 12 hours per day. Saving \$ 44 per year may not seem like a lot of money, but if you watch your pennies the dollars will take care of themselves. Cost conscious users turn everything off.

Some other factors to consider before making your own final decision include: Is your system operating at a cool enough temperature or does it overheat? (see our cooling article for more information) What is the MTBF (Mean Time between Failure) of the internal components? Do you really have a choice?

Component manufacturers use a rating of MTBF to estimate when their respective devices will stop working as originally designed. However, this rating is only a guide and an estimate based on studies each manufacturer has done in a scientific environment while testing each component they make. Since their testing facilities are always state of the art (just like the ones used to estimate your car's fuel consumption which you will never duplicate) the figure they come up with are probably over estimated. For example, many

power supply's have ratings of 50,000 hours (or about 6 years) while hard drives have been known to be as high as 300,000 hours (or just over 34 years). From my own personal experience over the last 35 years in the computer industry the actual MTBF for most components is significantly less.

However, you may not have a choice about turning off your system. Web servers don't get shut down every night; ATM's and traffic lights only stop working in a power failure. There are lots of reasons to leave your computer running.

There is no perfect answer to this question, but if you do decide to leave everything running 24/7 here is a list of things to do to help ensure your system has a long life.

- Keep the environment as dust free as possible
- Use a recognized UPS device
- Have the system internals cleaned regularly
- Replace components at the first sign of excessive wear
- Utilize Redundant Power Supply's and RAID backup devices. ▣

Is your computer Cool enough?

As computer processors get more and more circuits stuffed on the chip, and as die sizes continue to get smaller, the heat factor of the CPU will always increase. As the temperature inside your case, and on the CPU itself, increases, your system becomes more unstable. What other factors must be considered when calculating how hot your computer is getting?

What actually generates heat inside a computer? The CPU generates the most heat, but also the chipsets on the motherboard, graphics and sound cards. The hard drive generates more heat when you are looking for data or transferring large amounts of data, but still generates heat in a quiet state. To some degree the optical drives also generate heat when you are reading or burning a disk. Anything else inside a computer that you can think of that generates heat? I would almost bet that no one suggested DUST! But dust is an insulator and therefore a film of dust on your components will increase the heat factor significantly. So how do you keep you system cool?

FIRST: Count the fans and the direction they are spinning that are incorporated into your computer system. There must be one more fan expelling air than bringing air in to create a negative airflow which is required for proper cooling. You may need to use a short light thread stuck to a pin to help determine the air flow direction of the fan you are testing. If your system doesn't have negative air flow, it could be running hotter than it needs to be.

SECOND: Is your CPU cooler really effective? This is generally where a major amount of the heat generated by a computer system originates. The fan/heat sink assembly is designed to draw heat away from the CPU through the heat sink coils and then extract and distribute the air away from the coils with the fan. The better the fan on top of the heat sink the better the cooling, but also the better the material which makes us the heat sink the better the dissipation of heat. A simple method available for estimating how hot your CPU gets is to touch the cooler as close to the base as you can get while your system is running, being careful not to wiggle it. The following scale will give you a rough idea of how hot your processor is.

- 70C = Burnt Fingers
- 60C = Painful
- 50C = Hot
- 40C = Pleasantly Warm

If your CPU temperature is much over 50 degrees Celsius then it is probably running too hot and will shorten the life span of the processor or run the risk of damaging the on die memory.

THIRD: Is your power supply rated high enough for the number of components you have installed? Almost every system built pre Windows XP could exist on a power supply from 250 to 350 watts. Now, it really does depend what you have in the box, but 400 watt and higher is becoming the norm. Multiple hard drives, multiple optical drives, high end graphics cards, and USB peripherals are all driving up the power requirements of every system. If your power is under-rated for the components it has to feed, it will generate considerably more heat than necessary to perform its function properly.

FOURTH: Are the cables connecting the devices to the motherboard and/or the power supply loose or bundled

together and cabled? Fans in the front of your computer case will bring cooler air into your system. Exhaust fans on the top, side and rear of the case will expel hot air from inside the case. If the cables are not tied effectively and impede this air flow, the extra fans used to create a negative air flow are wasted.

FIFTH: and probably most important! DUST will cause heat to build up on components which will severely shorten their lifespan and effectiveness. Using compressed air to “blow out” the dust buildup inside your computer may no longer be enough protection. Periodic disassembly and vacuuming of components before reassembly is the only truly effective cleaning method. If you do this yourself, you take full responsibility and risk for any components that may be damaged during the cleaning.

DUST is a great source of irritation to your computer and can cause serious problems. It is an insulator which causes heat buildup and can also create a static discharge. In order for you to receive a shock when you ground yourself, your body requires a minimum static buildup of 3000 volts. On 15 volts are required to damage a computer circuit and render it useless.

Computer systems should be professionally cleaned at least once per year. If your computer is near a window that is open frequently, or you have pets (dogs and/or cats) in your house, or your computer area is dusty, or smokers are nearby, you may require more frequent cleaning. Call us for an appointment today to protect your investment. ☺

F1 – Backing Up DVD’s

Making copies of copyrighted material for profit or redistribution is illegal and not condoned by MicroByte TekSolutions. However, how many people have a favourite CD or DVD that they left in the car on a really hot day and it warped and is now useless? How many have accidentally been broken? Shouldn’t you be allowed to make a copy for your own protection against your own foolishness?

Even though many DVD’s have copy protection applied when they are manufactured, there is still a way to make a backup copy to guard against the incidents identified above. Is it legal or not? I don’t

know, and only your own conscience can really guide you until such time that the real question is answered.

Luckily for us, there are software programs to help make the backup process easier, even though they are quite time consuming. Open your Internet access point and surf to <http://www.dvdshrink.org>

DVD Shrink is software created to backup DVD discs. You can use this software in conjunction with DVD burning software of your choice, to make a backup copy of any DVD video disc. The authors of DVD Shrink claim you can use any burning software but also expressly recommend the use of Nero. DVD Shrink is free and contains no hint of Spyware or other unwanted software.

You will need a DVD RW drive to use this software if you want to make backup copies of your DVD discs. You will first have to download and install the software from the author’s site or a mirror.

If you have more than one DVD optical drive, a Reader and a Burner, when you try to open the media it may not be automatically found. You will however be presented with a dialog box asking for the drive identifier. (Figure 1)



Figure 1

When the DVD drive is located the program will automatically begin reading the contents of the drive and you may see a preview window appear on the screen showing flashing images of what is on the DVD. This is normal and takes approximately 2 to 3

minutes to complete. The software is calculating size of the data which will be needed to calculate the size of the copy.

Once the disk has been completely read, the next step is to push the Backup button. This tells the software to decode the contents of the disk, then encode the contents of the disk onto your hard drive, and finally make a copy of the encoded data onto a blank DVD that you will put into your DVD RW drive.

If the disc has been R.C.E. protected you will be notified and if you don't change the setting the protection will be removed. The application will then ask you to identify a target location which is generally a temporary folder.

The final step is to click the OK button to begin the copying process. If your system only has one DVD optical drive, that being the burner, you will be notified and requested to insert a blank DVD before the burn process can commence. If however you have two DVD optical drives, a Reader and a Burner you may be asked if you want the application to complete the copy process without interruption.▣

Is Shaw Secure a good alternative?

The Shaw Secure products include Virus Protection, Internet Shield (Firewall), Parental Control, Automatic Updates, Spam Control, and Spyware and Pop-Up Blocking. Should you install it or use what you already have? If you are not using Windows XP, the answer is probably yes.

The FAQ on the Shaw website states that their product may not work properly if you don't uninstall similar software you are currently using. Many users today have Norton Anti Virus installed and it is known to be the premier Anti Virus software available. Does Shaw's Anti Virus software compare favourably? I personally don't know. If your Norton hasn't expired, why think about replacing it?

Windows XP Service Pack 2 (XP SP2) introduced a revamped and much better software based Internet Firewall as an integrated component of the operating system. Many users are also employing hardware

firewalls in the form of a router. Since Shaw says you can use their software free on up to three computers they are assuming you are using a router (so you can share you Internet connection) so why are they offering a software solution for something your hardware is already doing?

Parental Controls are already built into Internet Explorer (IE) and are probably available for other browsers as well. IE lets you identify Trusted Web Sites and Restricted Web Sites, and you can also Enable Content Advisor to offer Parental Controls to "Control the Internet content that can be viewed on this computer".

Automatic Updates are available on almost every application you use today. Identifying this as a feature is similar to saying that your car can be refilled with gasoline and used over and over.

SPAM Control is a major worry for most computer users and the general public even if they don't have a computer. Yes, I know it is hard to believe but not everyone has a computer and has embraced the Internet as the best thing since television. However, many current Shaw customers have told me that before the availability of Shaw Secure, they never ever received any SPAM from their Shaw email account. I wonder why it is being delivered now when it wasn't before. If you are currently using Outlook 2003, or one of the Anti Spam products from Symantec or McAfee, this option won't mean a lot to you unless your subscription is soon to expire.

Spyware and Popup Blocking are next on the list as must haves if you are going to surf the 'Net. Remember XP SP2? Popup blocking is also now an integral part of the operating system. Spyware can be blocked and removed using Microsoft's time limited free version available on their website. Or you can use Spybot or Ad-Aware (also at no charge) but the Best of the Best is Spysweeper available at www.webroot.com.

Since installing Shaw Secure means uninstalling your current security software and turning off and/or disabling the security patches in XP SP2: Is it really worth it?

That leaves a big question and a very large leap of faith, but the final choice is always yours.▣