

THE SECURITY ISSUE

Welcome to the third issue of the new TekJournal. We are currently converting the first two issues into PDF format to add to the archive section and hope to be able to dual post in the near future. In other words, you will be able to read it online, or download it for later. We are also working on labels so that the Algerian headings look as they should.

This issue hopefully will get everyone asking themselves the same question. If I lost my hard drive immediately, how much information would I lose, and how would it affect me? before you read any more, think very hard about that question. I'll wait...

We all seem to take our computers for granted. We know, or assume, they are well built, but what guarantee do we have that they are infallible. In a word, NONE! Your present hard drive is approximately 3.5 inches in diameter, and is spinning at either 5400 rpm or 7200 rpm. I was once told that is the equivalent to about 300 miles per hour. Whether it is or not, it is really fast and therefore we are at the mercy of this device which can actually crash at any time. A minutely small particle not visible to the naked eye, mere microns in size, can irreparably damage the surface of your drive causing you to lose everything. Think about the question in the last paragraph again, and then I will tell you a story...

Recently, one of our clients called to say his system wouldn't start and he didn't know what was wrong. Upon inspection of the system, the troubleshooting began. It could be a power issue, or it could be a hard drive, or it could be a motherboard. Other components could cause a system to hang in the POST mode, but it is unlikely. Let's hope this was a power supply or a motherboard. Unfortunately, Not! This time it was the hard drive. The solution is generally fairly simple. Install a new hard drive, add the operating system, restore the data and you are back in business. But what happens if you don't have a backup?

There are companies who specialize in recovering your lost data, but they are expensive. Costs begin at \$ 400 and quickly escalate to \$ 2000, \$ 4000. and beyond. When you consider backup systems can be as low as 80 cents a day for do it yourself burners, or \$ 24.95 /month for automated backups, it is a wonder why more people don't do it. Do you? If not, why not? We will help you out shortly with various ways to help yourself.

BITS, BYTES, & NIBBLES

The corporate powers that control what we watch, listen to, and are entertained are still enraged. First they killed Napster, and now have set their sites firmly on Morpheus, KaZaA, et al. We thought they had already won when the little guys said in May they were just about broke and ready to give up. But it still rages on... MPAA and RIAA are after Kazaa and it parent company Sharman Networks again in the never ending battle of file sharing. Weren't we all taught to share as children? The latest is Sharman claiming they can't be held accountable to US law since they are based in Australia and therefore beyond the US reach. The battle continues...

AMD has introduced is Barton core and will add the XP3000+ CPU to it's lineup soon. Although rated at 2.167 GHz it actually competes head to head with Intel's 3.06GHz processor. The Barton core adds another 256K to the on die cache.

32% of all Americans with Internet access use it for Banking. The only other application with higher usage, by 1%, is Instant messaging.

SURFING THE NET

Staying in the vein of Security, here is a download you may want to consider. [Microsoft Baseline Security Analyzer](#) will probe your PC from the Internet. It detects patchable holes in the operating system and alerts you to any fixes or upgrades available. I have just installed and tried this program. It does identify security risks on your system. Fixing them maybe a slight more difficult as it directs you to Windows Update or to white papers on where you might find solutions. It is possible to nail everything down though.

Another freebie from Microsoft is [Bootvis](#). This program runs in the background when Windows XP starts and logs every program that is initiated during startup and identifies how long it takes to load. This is a program to use to shave a few seconds off the starting of you system. Again, there is probably a fair bit of reading associated with this, but it may be beneficial.

Adding and removing programs from your system on a regular basis can make for a cluttered registry and disk. Tools like Norton System Works have utilities to keep track of these changes, but why buy a whole suite for one utility. Here is a free one. [Add/Remove Pro 2.06](#) will analyze your system and tell you which ones in the Add/Remove box still exist and which ones don't. It will then help you remove the ones you don't want and get rid of the bad ones for good. It even lets you hunt down and repair broken links to the correct uninstall routine.

Windows XP has a refresh rate problem which can make for severe eye strain if you are in front of your computer for as many hours each day as I am. The refresh rate determines how often the screen is repainted and the higher the rate the less flicker your eyes will perceive. Even if you are not aware of the flicker, it may still be there. [RefreshForce 1.10](#) is a neat little program that helps determine the top refresh rates your monitor can achieve for each major display setting, and then locks them in, even for 3D modes. If you are working on an LCD or TFT screen, this program won't change anything. It is designed for CRT's only.

Not everything is free, but some things are still worth having. The defrag utility that comes with Windows is okay but there are better utilities available. Probably the best comes from Executive Software and is called [Diskeeper 7.0](#). Defragging is something we should do on a regular basis, but never get around to. This program has a "set it and forget it" option that lets you tell the system when to defrag regularly to keep your system running smoothly. The defrag routine has been clocked at approximately 50% faster than the one built into Windows, and with "Set it and forget it" it will run as a background process to help make sure your system never gets too fragmented again. The cost is a little steep, from \$ 29.95 US, but it is well worth the investment. Click on the link for a 30 day trial.

TEKQUESTIONS

This section deals with the doom and gloom at the beginning of this newsletter. It is related to security and backups.

How do I go about backing up my data to make sure I don't lose everything in a crash? How do I make sure my system is secure?

Security is one thing, backups are another. But they are related and doing one without the other is foolhardy.

Security begins with you. Who has access to you computer, with or without your knowledge? Since most of us are attached to the Internet on a possible 24/7 scenario, if you don't have a firewall of some sort, you are vulnerable. Two of the most popular software based firewall's are Zone Alarm Pro and Black Ice. These offer protection from programs accessing the Internet without your approval and also stop outsiders from accessing your system by blocking incoming traffic.

While a software solution is acceptable, a hardware solution is better, and a combination of the two may be the best. A hardware firewall is achieved by installing a router to route traffic from the Internet to your system and back again. It only lets in what you ask for. When you are connected to the Internet via high speed, you are constantly broadcasting your IP address to the world. With high speed, your IP address is not exactly attached to your computer, but to the modem used to make the access possible. You can click on the IPMonster link and see what your current IP address is. If you have a router, the IP address associated with your system will be different, probably beginning with 192.168. The 192. IP address is an internal address that is never broadcast to the Internet and the address you see at IPMonster is the address the Internet community sees. Without a firewall of some sort, the broadcast IP address is the same as having a full page newspaper ad saying that you have lots of goodies and no locks on your house. Everything is free for the taking. A router hardware firewall will always stop intruders dead in their tracks at the modem side of the connection, not allowing them near your system. But it has been identified that programs may still get into your system, usually because you let them, that can access the Internet without your permission and send valuable data to places you may not want it to go. Hence, the trend to having a software firewall in addition to the hardware firewall. In this case, the free version of Zone Alarm will do nicely for those that feel additional protection is always good.

More on securing your system continues with the use of a good Anti Virus product. Many people still use and swear by McAfee, but our preference is Norton Anti Virus. The latest edition is 2003, and protects your system from viruses via email, downloads, Internet access, and Instant Messengers. Again, on the frugal side, there is a free anti virus product from AVG. The free version checks for incoming viruses including e-mail.

Once your system is secure, or at least as secure as you can possibly make it, the question of backups is raised. You have collected a lot of information from various sources and generally would be hard pressed to recreate it from scratch. Especially if your system is your business system. How many can honestly say that if they lost their entire accounting system that they would know to the penny who they owe money to, and how much is owed to them. Including PST and GST which don't accept the excuses of my system crashed as being valid for having your remittances come late.

Backing up your data, like defragging your drives, is something we all know we should do, but seldom accomplish. If it so important, why don't we do it? We're lazy. We want something to do it for us, or constantly remind us, and then we want it done quickly. It may never be quick, but some options have reminders and some are quite automated. Here are a sample of available backup solutions, which is by no means complete...

Windows Backup utility. This option is built in, free, and located in the System Tools area. Available media to backup to is your hard drive, floppies, or removable media attached to your system. It also has a scheduler to help automate when your backups will be completed. The easiest method to use is probably to your existing hard drive, and hopefully your system has at least partitioned a portion of your drive into drive D: so if you lose the operating system, when it is reformatted and replaced your data will be recoverable. But this option is akin to putting all your eggs in one basket. If the drive fails, all partitions are lost.

Removable Media Backup: At one time, tape drives were the norm for backing up data. Today, it seems that optical drives (Burners) have replaced this type of media. CD-R disks are cheap, generally less than \$ 1.00 each, and two or more backup sessions will fit on one disk. The media also seems to last forever, unless it gets too close to fire. Also, when we used tapes, it was generally for a DOS based system and we backed up everything, including programs. With Windows, all we back up is data, so there is generally less need to backup GB's and GB's of stuff.

One of the easiest programs to use that we have found, to backup to removable media is NTI Backup Now! v3.0. This product lets you specify which files to backup, where to backup to, and includes a scheduler allowing you to backup at the same time daily. All you have to do is remember to change the CD-R media once a day.

Outlook & Outlook Express Backups: Your email and address books are among the most crucial data that should be backed up regularly. But most people never do it. In the past you would have to lose your paper address book or lose it to fire to be in a position of not being able to contact anyone immediately. Today, all you need is a power strike or a drive failure. Microsoft offers a plug-in for Outlook 2002/2002 to backup your Personal Folders so that they may be saved to an alternate backup source. Outlook-express-backup.com offers an excellent product for backing up Outlook express identities for inclusion in alternate backup sources. This product has a 30 day trial period and then must be registered for \$ 39.95 US. The plug-in from Microsoft is free.

Traditionally, there are always methods to backup your data. Export utilities in most products will create comma delimited files to help save data away from the source. Compression utilities like WinZip and WinRar shrink files down to a tiny version of the original, allowing you to put your data on diskette, or squeeze more data onto a CD-R. CD-R utilities like Roxio Platinum and Nero work with your burner to make copies of your data. The common thread in all of these scenarios is you. You have to remember to do the backup and get it off site to a more secure location. Only a permanent off site location or backup procedure gets you close to the point of guaranteeing you can recover from a serious crash. Think of it as the first step in Disaster Recovery, which it is.

VIRUS ALERTS

All current virus alerts are level 1. The first four were discovered on February 14, while the last two were found on February 13, 2003. Here is the current list:

Backdoor.Bmbot is a backdoor Trojan that allows a hacker to gain control of your computer by using Internet Relay Chat (IRC). A false error message is displayed if Backdoor.Bmbot is not executed from the %System% folder.

Backdoor.SilverFTP is a backdoor Trojan that gives an attacker unauthorized access to your computer. Backdoor.SilverFTP copies itself as %Windir%\Wincfg32.exe

W97M.Tolu is a Microsoft Word 97 macro virus that infects Microsoft Word documents and templates. The virus displays an illustration with a message, as shown below, when an infected document is opened.

BAT.Junkboat.Worm is a worm that uses the KaZaA-file sharing network and mIRC to spread. It also creates the file C:\Love_Me.vbs which has the ability to email BAT.Junkboat.Worm to all addresses in the Microsoft Outlook Address Book.

Backdoor.IRC.Zcrew is a backdoor Trojan that is similar to other backdoor IRC Trojans, such as Backdoor.IRC.Aladinz and Backdoor.IRC.Flood. Backdoor.IRC.Zcrew is written as an IRC script and uses the mIRC client to connect to the Internet, where it notifies the attacker of its presence. The hacker can send various commands to the infected computer and take full control over it. An infected computer can also be used to launch a ping flood attack against another computer at a specified IP address.

W97M.Trug.A is a macro virus that infects Microsoft Word documents when they are opened or closed. W97M.Trug.A attempts to hide its malicious actions and it may delete several files from the system.

TWEAKS

Windows XP - Delete Unwanted Screen Savers

For some reason Microsoft adds a large amount of screen savers to Windows XP that they think everyone will love. Most don't. If you want to remove the unwanted screen savers, here's how to do it.

First navigate to C:\windows\system32 using Windows Explorer and delete the Screen Savers you want to remove. Next enter "C:\windows\system32\dlldata" into the address bar to get to this folder and remove the same screen savers you removed initially. They will have the same name. The reason you have to enter the above address into the address bar is this folder is hidden and this is the only method to get there. If you don't remove the screen savers in both directories, they will magically return to your system.

Windows 98 - Optimize Swap File Performance

On systems with larger amounts of memory, more than 128Mb, the hard disk based swap file is not needed as much. This tweak optimizes the use of the swap file on such systems.

Using notepad open the SYSTEM.INI file in your Windows directory.

Find the [386Enh] section and add a new line reading "ConservativeSwapfileUsage=1".

Save the file and restart Windows for the change to take effect.

Thank you for reading the MBTS TekJournal. See you next issue...