Midland Computer Club

BITS AND BYTES

The Newsletter of the Midland Computer Club

January 2007

GENERAL CLUB MEETING 7:00 P.M.
Meets 4th Wednesday of the month at the Midland Community Center
2001 George St., Midland, MI
http://mcc.apcug.org/

This month's date: January 24th

THIS MONTH'S TOPIC: Wireless Network Safety presented by Frank Koenig

PROGRAM COORDINATORS
Contact :
Frank Koenig frankkoenig@charter.net
Co-Chairman Larry Piper larryp56@chartermi.net

What you missed!

December featured our annual Holiday party. It was a festive time with plenty of good food and fellowship.

Upcoming Activities

In **January**, we have Frank Koenig on the docket to present a program on "Wireless Network Safety." Wireless networks provide tremendous convenience, but at the same time offer the potential to open your network up to "drive by" hackers. By performing a couple of extra steps during the setup of your network, you can increase the security of your data and your system. This should be a very timely presentation, especially if you have been thinking about going wireless or have recently installed a wireless network. Hope you can make it. The program was originally scheduled for the October meeting, but due to illness, had to be postponed.

February will have Bob Miller talking about using

(Continued on page 2)

The President's Corner

With the pending appearance of Microsoft Windows Vista in the stores, the propaganda machine is in full force with the reasons that you should consider upgrading to the new version of Windows immediately. Needless to say, the hardware vendors are on the bandwagon so that they can sell new PCs. However, at the same time, you can read many "10 reason" lists on why not to upgrade to Vista right out of the gate. Most of these reasons are very good, especially if your machine is over a year old and you are satisfied with your current operating system. Most of these reasons are the standard ones to take into consideration with any new software release: hardware requirements, application incompatibilities, hardware drivers, cost of the upgrade, etc. But the one that bothers me the most is the built in DRM within Vista. I have very strong feelings about the use of pirated software. **Do not use pirated software!** But I am also one, who likes to have backups of the original CDs that come with my software or audio CDs. Virtually anything that you handle regularly runs the risk of being damaged. When you move your CDs from your car to your CD player to your computer, you handle the disks on a regular basis. Why should you have to buy a new CD when you damage it? If I damage a page in a book, I will tape it together and can still read it. However, if you scratch a CD you might as well pitch it. DRM will prevent you from using a copy of that CD on your PC and will also prevent you from making a backup copy of that copyrighted CD.

While there are plenty of reasons not to upgrade, I do expect to be running a copy of Vista in the next month or two. But it will not be on my primary machine for quite some time!

So what do you think? Let me know.

— Howard Lewis

(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)

MCC OFFICERS

POSITION		EMAIL:
President	Howard Lewis	lewis3ha@chartermi.net
Vice Pres.	Bill Tower	stressed@tir.com
Treasurer	Bob Miller	barloshelties@sbcglobal.net
Membership	Gary Ensing	gensing@juno.com
Editor	Jan Ensing	btiger6@juno.com

http://mcc.apcug.org/

Special Interest Groups:

CLUB PROGRAM COORDINATORS

Co-Chairman	Frank Koenig	frankkoenig@charter.net
Co-Chairman	Larry Piper	larryp56@chartermi.net

BOARD MEMBER

Mary Branson	molly688@chartermi.net
Robert Hughes	MIDItunez@yahoo.com

INTERNET SIG

Terry Brown	t_bbrown@yahoo.com

PUBLICITY

Kathy Bohl	kbohl30265@aol.com

Board Meeting

The next board meeting will be 7 p.m., February 13, 2007, at Chapel Lane Presbyterian Church, 5501 Jefferson Ave., Midland.

(Continued from page 1)

Quicken to do your own home accounting. Using an accounting tool like Quicken (or Microsoft Money), you can easily track your income versus expenditures. The tools included may surprise you on how you are really spending your money.

Strange, useful, and useless (in no particular order) Web Sites:

http://www.globe.gov/ – GLOBE (Global Learning and Observations to Benefit the Environment) is a worldwide hands-on, primary and secondary school-based education and science program aimed at students and teachers. This is a site for those who love science and learning.

http://terrapass.com/ – If you have ever thought about your impact on the earth's environment, this site will help you determine how much carbon dioxide your vehicle puts out each year. It is rather surprising to find out that a Toyota Prius puts out about 4,000 pounds of CO_2 per year whereas a GMC Yukon puts out about 24,000 pounds!

http://gocarbonzero.com/ – This is another site that helps to calculate your "carbon footprint," but this site not only figures in your vehicle, but also household utility consumption. According to this site, the average household puts out 20 tons of CO_2/year!

http://www.instructables.com/ – Instructables is a website where passionate people share what they do and how they do it, and learn from and collaborate with others. The site gives instructions on a variety of things from how to make a clock out of hard drive platters to making applesauce.

Membership Enrollment form

NAME _____ PHONE _____

ADDRESS _____ *CITY* _____

ZIP _____ *EMAIL ADDRESS* _____

Membership dues FAMILY ($20) STUDENT ($15) NEW Member ____ renewal ____

Please fill out the above form and mail it along with payment of check or money order to :

MIDLAND COMPUTER CLUB Attn: membership chairman
P.O. box 132
Midland, MI 48640-0132

you may also pay for membership at a regular club meeting

Tips, Tricks & Techniques

View Only Unread Messages in Microsoft Outlook Express

If you store your old messages in your Inbox, it is possible to hide those messages that you've already read. To hide those messages read:

Right-click the toolbar and select the *Views Bar*.
Click in the *Views* box and select *Hide Read Messages*.

Now you no longer see messages that you've already read. To show all of the messages again:

Click in the *Views* box and select *Show All Messages*.

Organize Your Messages in Microsoft Outlook Express

Rather than store all of your old mail in the Inbox, it is frequently better to create multiple folders to store important messages. To create these folders:

Right-click *Local Folders* and select *New Folder.*
Give the folder a meaningful name and press *Enter*.

Now you have a new folder into which you can move your read messages for storage. To move your messages from your Inbox to your new folder, simply click on the message in the Inbox, drag it to the new folder and release the mouse button.

Previewing Your Pictures

Windows XP makes it easy to see your graphics files in *Windows Explorer* or *My Computer*. Instead of displaying a folder full of dull windows icons, you can transform each icon into a thumbnail-sized preview of the picture. This makes it a lot easier to find that particular picture of your grandson standing on his head that you are looking for in the midst of the dozens of pictures in the folder.

To view previews:

Open the folder that contains the pictures.
Click *View* from the menu.
Choose *Thumbnails* from the drop-down menu.

Windows replaces the icons with small pictures of your photos.

++

Many things you think are safe really aren't

Written by Bob de Violini, a member of the Channel Islands PC Users Group, California
http://www.cipcug.org
rjddev(at)gmail.com

It's not too often I come across something that's a really good read, but I just have. It's an article on the Dark Reading Web site, a site that deals with computer security and is mostly aimed at those who deal with computer security and computer network security for a living. It's quite lengthy by many standards, but it's worth it. The article deals with "myth busting" or spelling out behaviors that many com-

(Continued on page 4)

(Continued from page 3)
puter end users at work believe is still "safe" (meaning that they don't think they'll hurt the computer network at work) or that they won't get caught at. Point is, someone is still watching, you just will never know when. The title of the article is "*The Ten Most Dangerous Things Users Do Online"*, and can be had at the following URL: http://www.darkreading.com/document.asp?doc_id=107771&print=true . The link will take you to a page with no ads or anything else on the page. It just has the text of the whole article, so you don't have to look at any potentially annoying ads or anything else on the page. You can even print it out and it will probably look pretty good. Some of the terms can be somewhat technical, but that's what we're here for is to answer any questions you may have and to help you have a more enjoyable computing experience, be it online or offline while working on a file or document. If you do have any questions, feel free to send me a note at the email address that appears at the beginning of this article. Bear in mind that the article spells out what users are doing mostly at work or at home with a laptop from their employer, and not from home on their own computers. How many habits that you have right now or may have had in the past are on that list?

To quote Monty Python, "And now, for something completely different…" and I do mean different. There's a Trojan horse type of malware circulating out there that takes the strange step of scanning your system for other malware by installing an anti virus engine. Then, once your system's been cleaned, it then infects your machine with its own code! The Trojan uses an illegal copy of an antivirus application from Kasperky Labs to the scrubbing before it infects your system. The illegal scanner checks your system and deletes anything found after you reboot your system. That's when you get infected with this new Trojan, which goes by the name of SpamThru Trojan. Although there have been other pieces of malware that have blocked the execution of certain competing pieces of malware, this new procedure changes the whole picture. While I'd normally think of a free scan of my system to remove malware or viruses, this is the kind of favor that nobody needs. By now, most of the anti-malware scanners have had their signatures updated to catch this little bug, of go out and update your anti-malware product's definitions, or signatures, if you haven't done so in the last week. This Trojan also uses more sophisticated ways of keeping itself updated and running than others have, but the techniques are beyond the scope of this column.

Now, from the "What's New is Old" department, we have reports of Internet Explorer 7, which was just released on the 19th of October, having a new vulnerability that's actually a holdover from the first early days of IE6. There has been banter back and forth within the computer security community about whether or not it's new and whether or not Microsoft will even fix it. Apparently, Microsoft's been saying that the flaw isn't with the browser, but with it's companion piece of software, Outlook Express. The vulnerability remains unpatched to this day. There's also another bug with IE7 that was also present in IE6 when it was first released in June 2004. At that time, Microsoft said to disable the "Navigate sub frames across different domains" setting in the browser, which would avoid the vulnerability. However IE7 comes with that setting disabled and it is still vulnerable to the bug. At this writing, IE7 is available on the Windows Update site as a High Priority download, and will also be available via the Automatic Updates feature in Windows XP and Windows 2000. Because of the uproar over this vulnerability, I'd suggest avoiding the new browser for a while until Microsoft patches the vulnerability or they release a workaround that actually works. You can set the Automatic Updates feature to just notify you of the updates that are available but not download them, or you can set it to tell you about the downloads and download them for you but not install them. Either of these options will work for avoiding the installation of IE7 for now.

Now for some news from the SANS Institute about some scams and other bugs that have been making the rounds, especially one that infected iPods in Japan. If they were infected in Japan, there's no telling when it will happen on this side of the Pacific. Apple has taken steps to eradicate the bug, but it's still worth noting. Ok, here we go:

QQpass spyware (Trojan variant)
As many as 100,000 Flash MP3 players, given away as prizes by McDonald's in Japan, were found to be

(Continued on page 5)

(Continued from page 4)
infected with a variant of the QQpass spyware Trojan horse program. The players were preloaded with ten songs and the malware. McDonald's Japan has apologized, established a helpline to facilitate the recall of the infected MP3 players, and posted directions for cleaning infected PCs. More information can be had at the following link:
http://www.theregister.co.uk/2006/10/16/mcd_spyware_mp3_recall/print.html

Here is a scam that can potentially snag a lot of folks out of the "fear factor" it implements:
FBI Imprimatur Added to Phishing Scams
Fraudulent phishing e-mails claiming to be from Richard Mueller III, FBI Director, and Donna M. Uzzell, FBI Compact Council Chairman, offer recipients big bucks and threaten big penalties if you don cooperate.
More information:
http://www.emergencyemail.org/newsemergency/anmviewer.asp?a=155&z=1

This next bit was just too good to not pass along in the *The Outer Edge* (CIPCUG award-winning newsletter). It explains a term that's being used more and more these days with regards to computer security and the vulnerabilities that are being discovered:

Security Question of the Month: What is a Zero-Day Exploit?
A zero-day exploit (attack) is one that takes advantage of a security vulnerability before or on the day that the existence of the vulnerability becomes widely known. Three or four years ago, hackers needed 7-14 days to figure out how to use a newly discovered vulnerability in order to launch an exploit. That lead time allowed hardware manufacturers and software developers to notify their customers, recommend ways to cope with it, and distribute software patches and anti-virus updates.

But there are more hackers, and they're getting better at what they do. So, how do you defend your computer when you have 0 days to prepare? You can. But if you keep your computer security software up-to-date, you'll help decrease your overall risk and increase the chances that a patch or update will reach your computer ahead of an exploit.

The above pieces were taken from the November issue of *OUCH!* a computer end user newsletter put out by the SANS Institute via email. More information and previous editions, as well as this month's can be had at the following link:
https://www.sans.org/newsletters/#ouch

Well, that's all for this month. Stay safe out on the Web, and remember to keep your anti virus and anti malware programs fully updated at all times to help prevent future infections from affecting you.

++++++++++++++++++++++++++++++++++

If you have any questions or need help with ANY computer issue, e-mail the board members at any time or write down your question and bring it to the meeting. Chances are that someone else has had the same issue and can help. Encourage your friends and neighbors to come to a meeting to learn to use their computers more effectively !

The Windows XP Services Manager

Written by Dick Maybach, a member of the Brookdale Computer User Group, New Jersey
http://www.bcug.com/
N2nd(at)att.net

Windows, like any multi-tasking operating system, is complex, with dozens of processes running, even when your PC appears to be idle. Some of these are independent, but many rely on other processes. In simpler times, our computers did only one thing at a time, but few of us want to return to the days when, for example, everything stopped during printing. Fortunately, XP provides some tools to help you understand what is going on behind your back, and one of the more helpful of these is its Services Manager. First, a caveat – this will help you figure out what only the benign processes are doing; it is not effective in identifying viruses and spyware, which often hide from you.

To start the manager, right-click on My Computer and then left-click on Manage. When the Computer Management Window opens, click on Services and Applications, double-click on Services, and click on the Extended tab at the bottom of the window. (You will want to enlarge the Window to see all the information.) You can now see a list of all the services available on your machine. My laptop has about 100 services, about 60 of which are running as I write this article. If you single-click on a service, you can see its status and description. For example, on my laptop the ClipBook service has the following description, “Enables ClipBook Viewer to store information and share it with remote computers. If the service is stopped, ClipBook Viewer will not be able to share information with remote computers. If this service is disabled, any services that explicitly depend on it will fail to start.” The Manager also shows that this service is disabled on my laptop. You can learn more by double-clicking on the item. Again for ClipBook, the executable file is C:\Windows\system32\clipsrv.exe. Clicking on the Dependencies tab shows that this service depends on the Network DDE and Network DDE DSDM services and that no other service depends on it. You can learn more about these dependent services by clicking on their names in the window.

The companies that provide the software supply the descriptions. Microsoft’s descriptions are helpful, but others can be less so. For example, Symantec SPBBCSvc is described as, “Symantec SPBBC.” In such cases, you can try a Web search for the name, although I ran out of patience before I found out what SPBBC does.

As is common for Windows programs, you can sort the services list by clicking on a column heading. For example, clicking on Status, lists the started service last; clicking on it a second time shows them first.

If you suspect that a service is causing problems, you can turn it off by double-clicking on its name and then clicking on the Stop button. This stops the service only for the current session; it will start again when you restart Windows. Thus, this is a safe way to trouble-shoot process problems. You permanently stop a process by double-clicking on its name and changing the Startup type from Automatic to Manual or Disabled. A disabled service never runs; and a manual one can be started by clicking the Start button. If you do this, keep a record so you can reverse anything that causes problem.

While you have the Computer Management window open, look at its left pane. In particular, click on Disk Management (under Storage) to see a text and a graphical description of all the hard and removable disks on your system. This shows the partition sizes and types, what file system they contain, how full they are, and their health. If you right-click on a partition in the graphical display, you can explore it, change its drive letter, or (be careful) format or delete it.

Protecting Your Outlook Express Email
Written by Ron Farren, a member of the Keowee Computer Club of Oconee County, SC
Ronfarren(at)mindspring.com
http://kkeyword.tripod.com/

There are, as usual, several ways to protect yourself from a drive failure and loss of your email. This tip is for users of OE only.

Your email is all stored in a single folder and, if you can find that folder, you will find that it contains a large number of files. Most of these files will have the extension of ".dbx" if you are configured to show the extension. Microsoft uses a proprietary format, which makes these files quite difficult to view except with OE. In addition, the individual files are not useful without the index, which is stored in a separate file within this folder. If you want to backup your email, it is possible to save the entire folder someplace. It is
relatively easy to copy the entire folder to an external drive or to a second drive. Should you experience a problem that causes the loss of your email, you can merely copy the folder back to its original location. Sounds simple enough.

First, you have to find the folder. That is done via Tools/Options/Maintenance. There you can click on "Store Folder" and it will have the address of the folder you are looking for. You may notice that it is really buried deep into the system. Now that you know where it is, you can copy that address for future reference and periodically save the folder as backup. If you are not satisfied with trying to remember the default location of the messages, it is simple enough to move the folder somewhere else. For example, you could place the folder directly on the C: drive which would make it easier to find next time. That can be done by clicking "Change" and following the instructions. An even better solution is to place the email folder on a separate partition, which prevents it
from being destroyed if you're C: drive should be corrupted by some foreign invader.
Changing the location of the email folder will automatically move all your email to the new location.

So now you know how to save and restore your email. However, there is another step you may wish to take. Suppose you decide to backup you email once a week or every seven days. Should you have to restore the backup, you will only lose seven days worth of emails. Would you like to know how to recapture them, also? The answer lies within the options available in OE. The following will work with most ISPs although there may be some that do not allow this feature.

Open Tools/Accounts, select the account you are concerned with and select Properties/Advanced. Place a checkmark by "Leave a copy of messages on server". Now place a checkmark by "Remove the messages after" and set it to 8 or 9 days. Now place a checkmark by "Remove from server when deleted from Deleted Items". Now your email server will retain messages for 8 or 9 days. You don't have to worry about OE retrieving the messages each time you connect to the Internet since OE maintains an index of downloaded messages and will not download the same message a second time. However, if you have to restore from a backup, that index will not be up-to-date and the messages will be downloaded again. By telling the server to delete messages when you have deleted them, that should reduce the number of messages saved on the server - only the ones you intended to keep anyway.

One additional thought. If you decide to move the email folder, why not move it into My Documents? If you have already made sure you keep all of your critical information in My Documents, wouldn't it make sense to put your email there also? Now you can merely copy My Documents to that external drive once a week and you should be pretty well protected from major disasters.

It really pays to learn how to maintain and protect yourself. Once you have set up a procedure like this, it becomes something you can easily do once a week and feel more secure.

Computing should be FUN!!!

Fun with Freeware

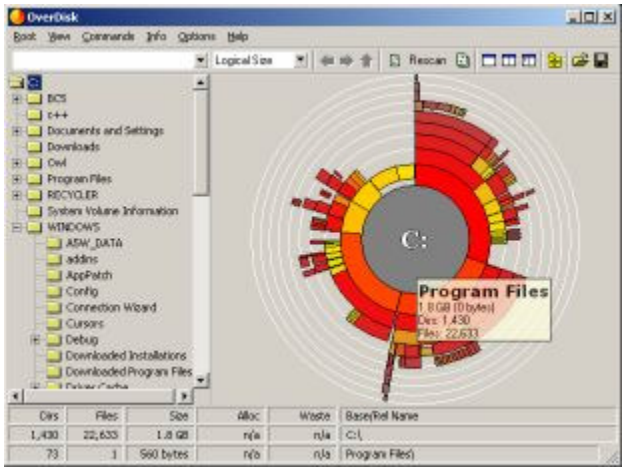
Written by Cary Quinn, a member of the Pikes Peak Computer Application Society, CO
http://ppcompas.apcug.org/
cary.quinn@gmail.com

Here are a couple of utilities I have been using lately to correct a couple of bumps in the road to a positive Windows experience.

OverDisk (v0.11 beta) (freeware)

http://users.forthnet.gr/pat/efotinis/programs/overdisk.html

Elias Fotinis, a programmer from Greece, is one of those programmers you often find on the net who in their spare time writes little apps and utilities to solve some personal issue they might have getting the operating system, or some other program, to work the way they want it to.



One of the programs he has written is a disk space monitor called Overdisk. It basically scans a drive or folders of your choice and tells you how much space is being taken up by the files therein. One special difference with Overdisk though, is the way it graphs that data to your screen.

Instead of representing the files as a pie chart, or bar graph, Overdisk shows a breakdown of folders and files as a series of concentric rings, as if you were looking down onto the disk itself and seeing the files laid out below. But it's even better than that.

When you mouse-over a particular section of the chart, a tooltip window will appear to give you more information about that particular folder (size, number of subdirectories, and the number of files); and if you click on a specific point of the chart you can drill down to get the same information for individual files. Clicking on the center of the chart takes you back up the directory path, or you can click on the tree view on the side of the screen to better select a particular folder to view.

I find this utility most useful when trying to identify what parts of a drive need to have a cleanup, or which folders I need to prioritize for backups.

Taskbar Shuffle (free, but accepting donations)
http://www.freewebs.com/nerdcave/taskbarshuffle.htm

From the home of the nerd cave, comes a pretty nifty little tool that answers a minor nit I have had with the Windows Taskbar for a while—why you cannot drag and drop the programs listed on the taskbar to better arrange your programs to your preference. With Taskbar Shuffle, you can. That seems pretty simple, and it appears to work quite seamlessly within the OS.

The utility leaves an icon running on your system tray that you can use to turn it on or off, or close it down completely. I've been using it for a few months, and haven't noticed any conflicts with other windows or programs that have caused me to want to shut it off.

XP or Vista?

By Elaine Drain, President, Senior Surfers Computer Club, Delaware
www.nscseniorsurfers.com

From talking with our members, it seems that quite a number of you with older computers running Win98 or ME are in a quandary as to whether to go ahead and buy a new computer now with XP or try to hold out until Vista arrives on the scene. As Jim and I tell our members when asking for buying advice, it's a personal choice you have to make depending on your needs and your budget. We can, however, provide some general information to help you choose, so read on.

XP certainly is superior to Windows 98 or ME, especially now that 98 and ME are no longer supported. Microsoft will probably continue to support XP for 4 or 5 more years (but no one can say for certain on that one). XP, even with its vulnerabilities, is a very stable operating system. Jim and I are both running XP Pro and have been satisfied with its performance overall. I have been doing a lot of reading on Vista and, from the information available, feel that it will be superior to XP, but not everyone will require all of the features that will be included in the full version of Vista.

So given that information, here are some choices:

Current Computer with 98 or ME: If you are currently running Windows 98 or ME and don't want to spend a lot of money next year for a new computer with Vista, you may want to go ahead and buy a new computer with XP soon. The Back-To-School prices for computers right now are very enticing. Certainly, the newer computers next year running Vista will cost substantially more because of the increased hardware requirements.

If you would like to upgrade to a new computer with XP now and have minimum needs only using your computer for email and surfing the Internet, and do not plan to upgrade to the Vista operating system down the road, a budget-priced computer with a Celeron or Sempron processor may suit your needs, even though you would have fewer upgrade options in the future.

If you would like to upgrade to a new computer with XP now and may wish to upgrade to Vista later on and also have higher needs such as working with digital photos and editing programs, spreadsheets, databases, powershows. etc., you should consider spending a little more to get a Pentium or Athlon processor. I would recommend a bare minimum of 512Mb of memory (RAM) if you are working with multimedia (photos/music/movies/radio) for now but you should plan to add another 512Mb of memory when you upgrade to Vista.

If you are wondering about the minimum requirements for upgrading your current computer to Vista, the following information was taken from the Microsoft website:
Windows Vista Minimum Supported System Requirements

PCs that meet the minimum supported system requirements will be able to
run the core features of Windows Vista with the basic user experience.

Processor	800 MHz 32-bit (x86) or 64-bit (x64) processor
System Memory	512 MB
GPU	SVGA (800x600) (GPU means Graphics Processing Unit, or in other words, Monitor)
Graphics Memory	(not stated, although I have heard a minimum of 128Mb)
HDD	20 GB (Hard Drive)
HDD Free Space	15 GB
Optical Drive	CD-ROM drive

(Continued on page 10)

(Continued from page 9)

Keep in mind that the above specs are for running the BASIC version of Vista and not the fully functional version which has a multitude of new features. Although Microsoft is currently stating that Vista will run with 512Mb of RAM at a minimum, I would make certain the computer could be upgraded to 1GB of RAM. Minimum requirements are just that – bare bones minimum – and I would recommend that your computer exceed these minimums. Vista is currently in the Beta2 stage and is nearing (so they say) finalization before debut, but that does not mean that the system requirements stated here won't change by the time the system is ready to sell, so stay tuned on that.

Personally, if your current computer came with Windows 98 or ME, I would not recommend attempting to upgrade your old computer to Vista unless you originally purchased a high end computer with a Pentium processor with the capability of 1GB of RAM. Even then, it may not be worth the time, effort and money to upgrade. The cost to purchase the Vista operating system, plus any installation charges, plus the cost of
the memory upgrade, not to mention the graphics card requirements, would add up to a tidy sum and in the end you would still have a very old computer (that may or may not work well with Vista).

Current Computer Came With XP: If your current computer came with XP already installed, you may want to hold out and wait to see what Vista offers and how it operates before you take the plunge.

Excellent Comparison – Vista vs XP: If you would like to take a peek and see how Vista compares with XP side by side, follow this link:
http://www.bentuser.com/article.aspx?ID=332&page=1

If you're wondering how the Apple operating system, Tiger, compares with Vista, this article may be of interest to you:
http://www.eweek.com/article2/0,1895,1842175,00.asp

++

Are You Concerned About Loss of Personal Data?

By Carlisle Barnes, Newsletter Editor, Bowling Green Area Microcomputer User Group, KY
Newcarlislebarnes(at)insightbb.com
http://www.bgamug.org/

The advanced state of Information Technology is one of the great blessings of modern times. Today it is built into our economy, and it would be hard for both individuals and corporate America to do without it. However, along with the blessings to us have come curses. These curses are going to get considerably worse unless some dramatic changes are made in the way stored information is handled by the majority of organizations.

Computer spam, pfisheng/phishing schemes and other e-mail con games, as well as a multitude of ever changing computer viruses are obvious curses to everyone using a computer on-line. Great effort is being expended to get these curses under control. Very good and still improving anti-virus programs are available. Bill Gates said recently that spam will be completely under control within two years. (It will be interesting to see if Bill is right about that.) The point is that something positive is being done to correct those Internet curses.

However, one of the worst of current IT curses is identity theft, and very few positive things are being done to stop it. Identity theft is not associated with the Internet as are many other IT curses, but it has become very much associated with computers because of the casual way in which CD's, laptop computers, and portable hard drives are often handled. People who would never ever consider leaving a collection of gold coins laying in the back seat of a car, or leaving a thousand dollar bill on a table while going to get another cup of coffee, seem to have developed

(Continued on page 11)

(Continued from page 10)
very little concern about leaving a portable computer, a container of CD's, or even a portable hard drive in all sorts of places where they can be easily stolen. (Home?)

Unlike sensitive data handled by military or military contractor organizations, the personal data stored in files of civilian Government organizations, major universities, insurance companies, credit card companies, and etc. are often treated as casually as advertising material. A recent extreme example is shocking and deserves examination. Not long ago, a Veteran's Administration senior analyst took home electronic data from the office to do after-hours work on his personal computer. He had done this numerous times before. The data included names, Social Security numbers, and dates of birth on 26.5 million veterans. These data list essentially all military personal who have served following the Second World War. The analyst's laptop and a Government owned external hard drive (along with all the data under discussion on it of course,) were stolen in a May 3 burglary of his home. He reported the theft within an hour of discovering it. VA Secretary of Veterans Affairs Jim Nicholson made a public announcement of the theft on May 22.

Jim Nicholson appeared before the House Committee on Veterans Affairs to explain the situation. While accepting a certain amount of personal responsibility for the data breach, Nicholson expressed anger toward the analyst who took the data home "without permission." Further, he said "As a veteran myself, I have to tell you I'm outraged. Frankly, I'm mad as hell." Afterward, he fired the analyst involved. For what appear to be justifiable reasons, the analyst is now suing to be reinstated.

What Nicholson did not report, and later insisted that he did not know, was that the analyst had been taking data home as part of his regular work routine since 2003. (Is the VA a good place to work?) Furthermore, existing documents dated September 5, 2002 show that the analyst -- lead programmer within the Policy Analysis Service -- was officially permitted to take the external hard drive home for "work-related projects." Specifically, he had a property pass allowing the laptop and accessories to be removed from the building and also a permit allowing him to access any Social Security numbers on the hard drive. It later turned out that there was yet a third document allowing him to remove various materials from the VA building.

A certain amount of security could have been provided for these "take home" documents, by encrypting them. However, a reasonable up-front cost for the systems, services, processes, and procedures to encrypt 100,000 or more customer records is estimated to be about $500,000. VA working personnel probably couldn't justify that sort of expense to their budget group.

Once files have been stolen, it is difficult to determine if the data have been used illegally. The computer and VA hard disk have now been returned, apparently without data loss, but if it is eventually considered necessary to contact all affected veterans and to provide them with credit-checking services, then there will be an estimated taxpayer cost of at least $100 million.

The fiasco was not quite finished when Nicholson appeared at the congressional hearing. It was revealed at that hearing that Pedeo Cadenas, the VA's chief information security officer, had resigned by e-mail 30 minutes before the proceedings began. Nicholson said he was completely unaware of Cadenas' intentions. Evidently, Nicholson has learned many things rather late.

On June 28th, not quite two months after they were stolen, the computer and external hard drive were turned in to the FBI Office in Baltimore, Maryland. A tipster, in response to the $50,000 reward being offered, had let a US Park official know that the equipment might be recovered. Quickly then, the stolen items were turned in to the FBI. The tipster was not identified, nor was it clear if either he or anyone else would receive the $50,000 reward. Furthermore, no one has been arrested for stealing the equipment, unless that particular information is being held secret for some reason.

Inspection of the hard drive by the FBI does not indicate access to the data during the time that the drive was in the

(Continued on page 12)

(Continued from page 11)
possession of the thief. Superficially then, no data were compromised and there is perhaps nothing to worry about.

Unfortunately, if the thief was a computer expert, knew what he had, and wanted to make illicit use of the data, then he could have transferred everything on the external hard drive to another hard drive without leaving a record. While that is possible, it seems improbable and it seems unlikely that there is reason for continued concern. However, can we be absolutely sure?

Those of us who served in the military, or worked for military contractors are quite well aware of the way in which sensitive intellectual material is handled by these organizations. While current practices are unknown to the author, not very many years ago, there were at least five security levels. Restricted meant that the information was not to be given to unauthorized people, was certainly not to be made available to newspapers or to other media, and was not to be left anywhere where it might be stolen. The only people allowed to see the material were those with a need to know about it. Confidential material classification, one step up from Restricted meant that the material was not to be made available to anyone not having appropriate clearance i.e., clearance by appropriate investigators. Except when being used in a cleared area by cleared personal, the material was to be locked in a desk or file cabinet with a safety bar and a combination lock. All desks and cabinets were to be regularly checked by guards. Secret material was to be handled in somewhat the same way, but clearance was more difficult to obtain, storage was in a secure safe, not in cabinets or desks, and material was to be guarded twenty four hours a day, and seven days a week. Top secret material was of course even more closely guarded, and investigations for personal clearance were carried out by FBI personnel; in general all security was substantially tightened. . Then there was “Special Clearance” which need not be discussed here, but which was very tight indeed.

It is absolutely shocking to note that as serious as identity theft can be, hardly anyone handling social security numbers, driver’s license numbers, medical history facts, educational information, and etc., etc. is required to treat personal information in their possession with a level as high as military Restricted. As this article was being written, yet another security breach occurred at Ohio University, Athens, Ohio. There were several resignations from the school staff as a result, but it is one more case of “locking the barn door after the horse is gone.”

If current sloppy handling of private data continues, then it is only a matter of time until identity theft becomes a disaster.

This article by your newsletter editor is as close as you will get to a BGA-Bytes editorial. However, your editor considers the matter to be a lot more serious than it is being treated by many people and particularly by most public officials.

If you would like to encourage your congressmen or other public officials to put some teeth into privacy laws and into laws concerning the handling of private information, then may I encourage you to write and let them know how you feel.

To help you get started in sending letters, here are three addresses of interest. There are numerous others on the Internet.

U. S. Senator Mitch McConnell, 361A Russell Senate Office Building, Washington D. C . 20510
U. S. Senator Jim Bunning, 316 Hart Senate Office Building, Washington D. C. 20510 U. S. Representative Ron Lewis, 2418 Rayburn House Office Building, Washington D. C. 20515