



MOUSE TRACKS



Volume 3, No. 1 - January 2008

SHOULD I UPGRADE TO VISTA?

The first anniversary of the introduction of Microsoft's Windows Vista operating system is a logical time to ask, "Should I upgrade?" The consensus of computer professionals and writers who cover the PC scene is, **NO!**

Windows Vista upgraders continue to experience a higher probability of something going wrong than those who don't. The decision key appears to be, "if it ain't broke, don't fix it." So as long as your Windows operating system (XP, 2000, Me, or whatever!) is doing what YOU want, don't mess with success and continue to plug along with it.

This is especially important if you're running older versions of Windows programs like Quicken, etc. Many companies have still not resolved compatibility issues with older programs and so yours may not work with Vista!

On the other hand, if you're in the market for a NEW computer, Vista offers substantially more graphics and increased security - but be aware it's available in several versions, so carefully consider what you plan to use your computer for.

The 'Home Basic' version, includes, "all the safety features that make Vista a more secure platform for all of your needs, the brilliant instant search feature for tracking down your files quickly and easily." But the 'basic version' doesn't come with Windows Aero Graphics or Media Centre, so if you think you may ever want to use your computer to display photos, play music, make DVDs or play games, you'll likely be better off upgrading your new computer to run Windows Media Centre -

included in both the "Ultimate" and the "Home Premium" versions of Windows Vista.

The Microsoft Web Site has details of all five versions of Vista available to help you decide which is right for you.

(<http://tech.msn.com/microsoft/article.aspx?cp-documentid=2942738>)



ANOTHER ALTERNATIVE to "Office"

Previously we told you about Open Office (www.openoffice.org) which will have a NEW version available for free download in March. The suite "StarOffice" also supports most Microsoft Office formats (except those of Office 2007!) and, like Open Office, Star Office can export documents as PDF files.

StarOffice costs \$70, but is available FREE as part of the "Google Pack" of free software downloads.

(http://pack.google.com/intl/en/pack_installer.html?hl=en&gl=us).

It's worth noting that StarOffice has a huge installer (over 140 MB), so download it ONLY if you have a fast Internet connection!



**INSTALLING YOUR NEW
"HIGH SPEED INTERNET EXPRESS"**

Upon ordering, you will be sent a self install kit including coaxial cable, a splitter, and a modem - which remains the property of Arledge Electronics. Arledge will maintain the connection to the modem and the modem, but they do NOT charge a monthly fee for the modem!

Follow the instructions that come packed with your modem and you shouldn't have any trouble - but here are a couple to look out for:

1. First, check your computer to see if you have an "Ethernet" port. If so, do NOT install the USB software from the CD provided. Connect the Ethernet cable from the modem to the Ethernet port when the instructions tell you. Before restarting your computer, UNPLUG your dial-up phone line.

When the modem is ON, an AMBER light should be blinking to indicate there is activity between your computer and the Internet via the modem. If your home page appears, click REFRESH and if it still is visible you're good to go! (This ensures what you're seeing isn't simply retrieved from the computer's memory.)

2. IF you don't have an Ethernet port (or you can't get the Ethernet connection to work, ONLY THEN should you install the USB program from the diskette! Unplug the Ethernet cable and use the USB cable between the modem and your computer. When you restart it, your home page should appear.

If not:

Open Internet Explorer

On the TOOL BAR Go to:

TOOLS

INTERNET OPTIONS

CONNECTIONS

Make sure "Broadband Connection" is the (default connection). There should be a "check" next to NEVER DIAL A CONNECTION.

To the RIGHT of the "Broadband Connection (default)" window, click on SETTINGS. ALL selections should be BLANK!!



**Are You Problems with
(bookmarks/favorites) on your
new Broadband connection?**

Some people have reported problems with some of their "Favorites" (Bookmarks) being 'grayed out' after upgrading to the new Greenspring Broadband access. If you experience that, try the following to fix the problem.

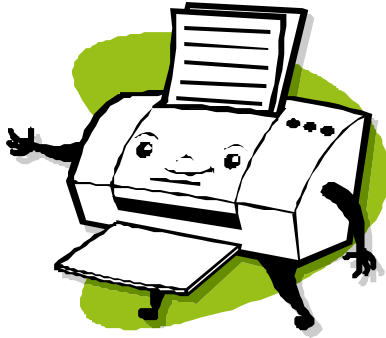
On Internet Explorer 7 (all the way to the right....>>)

Click on TOOLS (this is different than the toolbar 'tools' above)

Unclick the (check mark) next to "Work Offline". Close Explorer and then restart it (you may have to restart your computer before this takes effect.)

That should allow you to access all your Favorites/Bookmarks.





FIXING COMMON PRINTER PROBLEMS

1. Multiple Pages Feed Through the Printer

If your printer is picking up multiple sheets of paper:

- A. Remove the paper from the tray. FAN the edges, re-square it, then reload the tray.
- B. Slide the paper WIDTH guide to the right until it stops at the edge of the paper.
- C. Slide the paper LENGTH guide against the paper end of the paper.

TIPS:

Always keep MORE than 10 sheets in the tray. Ensure the paper is not loaded too far and extends past the In tray. Store paper in a dry, cool place. Humidity causes this issue more often. Do not print on paper already printed on; the dampness causes pages to stick together.

NOTE: Not all printers have rear access doors so skip THIS STEP if your printer does NOT have a rear door.

Remove the rear-access door (if applicable) and clean the internal rubber rollers with a soft lint free cloth moistened with distilled water. Wait until the rubber rollers dry and replace the rear access door.

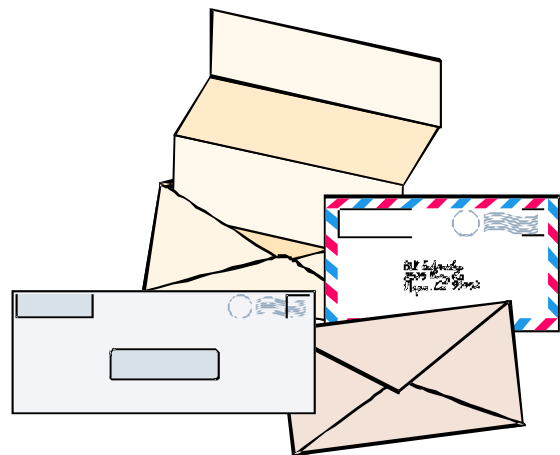
Verify that the correct media size and type is selected in the printer settings along with the appropriate quality.

If the issue persists, try a different brand, type or weight of paper.

2. Print Jobs Fail to Be Deleted from Print Spooler when canceled

In Windows XP, and earlier versions, print jobs may be caught in the **Printer Spooler** which causes pending jobs not to print.

- A. Click START then CONTROL PANEL.
- B. Click PERFORMANCE AND MAINTENANCE (on some versions you may go directly to Step C, below)
- C. Click ADMINISTRATIVE TOOLS
- D. Click SERVICES
- E. Scroll down the right side to find: PRINT SPOOLER
- F. If the service status is STOPPED, click the START tab. If START is not highlighted, click STOP to restart the Print Spooler.
- G. A progress message should appear and the Print Spooler will be clear.
- H. It should now be possible to print again.





BOT-NETS by Brian K. Lewis, Ph.D

(bwsail@yahoo.com; www.spcug.org)

From APCUG w/ author's permission for publication by
APCUG member groups.

Keeping your computer safe while connected to the Internet is becoming more and more difficult. The “attackers” are becoming more sophisticated and are sharing more ways to get their software into your computer. Business Week recently ran an article on the major security problems expected in 2008.

Unfortunately, most of them arrived long before the new year started. We have been warned for years that it was possible to recruit unprotected computers into networks that could be controlled by an external source. This recruitment network problem has gotten much worse over the past few years. It is estimated that 7% of the computers connected to the Internet have been infected with a Botnet program. So what is a “Botnet”?

A robot or “bot” software program allows a computer to be remotely controlled without the knowledge of the computer’s owner. When you have a number of “bot” controlled computers it is referred to as a “botnet”. All of the computers in the botnet carry out commands issued by the network controller. Just one example of what can be done with a botnet is the sending of spam. The controller can easily have 100,000 computers in its network. So the botmaster will contract to send out one million e-mail messages. The network can then send ten messages from each of the compromised computers. With the constant connection to the

Internet using cable or DSL the computer owner will have no idea that his/her computer has been the source for ten spam messages. Now you might say that the idea that someone can control 100,000 computers in a botnet is ridiculous. However, as of October 2007 a major Internet security service had the IP addresses of over 12 million computers that were infected with bot software.

There is also a newer threat called the Storm Worm botnet that has infected millions of computers just this year. In addition to its computer recruiting ability, it has built-in defenses that are preventing security services from analyzing it. In an E-Week article it was noted that “.. Storm worm is sending DDoS attacks to not only the researchers looking into it but to anybody on their subnet, within 5 seconds of (their) initiating efforts to fight it or examine it”.

A DDoS attack is a “distributed denial of service” which can bring down a computer system or network by overwhelming it with messages. A very large volume of messages are sent by the botnet in a very short period of time. It is estimated that the Storm net controls over one million computers. This would make it the most powerful supercomputer in the world, exceeding the computing power of all previous computers.

People frequently wonder why anyone would want to produce viruses, worms and other kinds of Internet attacks. Years ago it was primarily because “they could do it”. Today, it has become a real source of financial gain. Let’s take a look at one financial resource created by controllers of botnets. On many web pages you find ads of various types that are sponsored by Google. When these ads are clicked, the advertiser pays Google who, in turn, pays the owner of a web page, usually 80% of the fee. So the botmaster sets up a web page and contracts with Google to display ads. Then,

using the botnet, sends commands to the computers in its net to click on the ads. This results in payments to the botmaster. So even with a small botnet of say 5-10,000 computers, the botmaster can easily obtain \$15,000-\$20,000 per month in fraudulent payments.

When you consider that the known botnets all have more than 100,000 compromised systems, you get a better idea of the scale of the fraud involved. This type of click fraud has been estimated to make up 5-20% of the payments made by search companies.

Another use of large botnets is extortion. The botmaster can send an e-mail to a corporation warning that a DDoS will take place at a specific time unless a payment is made. As I mentioned earlier, spam e-mail contracts are also a source of revenue for botmasters. As these networks proliferate, the sale of the IP addresses of robotically controlled computers is also favored as an income source.

So far it would appear that the only persons affected by botnets would be corporations. However, if your computer is infected, everything you do can be reported to the botmaster. Bots can incorporate "keylogger" software. That will record keystrokes, especially any related to passwords, user names or other desirable information. Another function of bot software is screen capture. It can record an entire screen and transmit the data to the botmaster. A compromised computer can also be used as a base for finding other unprotected computers to be recruited into the net. Another consideration is that the largest number of computers are those in the hands of private individuals. So you may be a major part of the problem if your computer is infected by a bot. Once a computer has been compromised, the bot software is usually designed to hide and protect itself. For example it will search for and disable any other malware located on the computer or its associated network. It may also

hide itself by means of a rootkit. It may also block updates of any anti-virus or anti-spyware software. It may even fake the process so the user believes that an update has taken place. One of the most common modifications involves changes to the Windows host file or by changing the location of the host file and altering the registry.

There are also some traps on the Internet that can lead a user to download bot (Trojan) software without realizing it. Phishing e-mail can lead to web pages that have automatic download links for bot software. Web pages can be hijacked and links added to lead the viewer to web sites that contain "free" software links that are actually hidden bot programs. Bot programs are incorporating "social engineering" functions which serve to entice users to unknowingly download malware. People are the weakest link in the security chain. E-mail, web pages, instant messaging, social contact web sites are all used by bot malware as a means of collecting information and linking to compromised computers.

Many times the actions of a computer user are governed by visual clues. An attacker may take advantage of this by providing false visual clues on a web page or a pop-up. If the dialog box or pop-up is intrusive the user may click inappropriately just to get rid of the intruder. This can lead to the download of a bot.

So how do you know if you've been infected? The easiest way to tell is related to how you have been protecting your computer from infection.

Do you have all of the following?

- a. hardware firewall.
- b. software firewall that checks both incoming and outgoing messages.

(continues next page)

- c. anti-virus software that is updated at least daily.

- d. anti-spyware software that you either run weekly or that runs in RAM constantly.
- e. keep your Windows software patches up to date.

If you don't use any of these safety mechanisms, then your machine is almost 100% guaranteed to be compromised. Even if you have taken all of these precautions, you can still be infected. However, the most effective mechanism for dealing with bots is to prevent their getting into your computer. So you have to keep the software up to date and you have to use it. Ideally, your firewall hardware/software combination should keep you invisible on the Internet. Bot programs are constantly searching for unprotected computers with open ports.

You may not be aware that your computer has over 64,000 port that can be used for communication. The most common usage are the ports in the lower range, under 1,024. However, some bots use high end ports (>60,000) for transmission of commands. One place you can check your computers port and its invisibility on the Internet is www.GRC.com.

The Gibson Research site provides a free port scan and much good information on interpreting the findings as well as how to protect your system.

Ideally the anti-virus and anti-spyware software would be able to find and remove any bot software that made its way onto your computer. However, this software needs to know the "signature" of the malware in order to identify it. So the producers of the malware are always a step ahead of the good guys. The security services have to find and disassemble the new malware before they can devise the protection against it. So it is up to the user to keep the security software as current as possible to reduce the chances of infection. Like it or not, security on the Internet is a never ending battle.

Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years, developing software and assembling systems. This article has been provided to APCUG by the author solely for publication by APCUG member groups. All others require the permission of the author (see e-mail address above).



EVALUATING YOUR ANTI-SPYWARE PROGRAM

by Vinny La Bash, Member of the Sarasota
Personal Computer Users Group, Inc.

www.spcug.org (vlbash@comcast.net)

From APCUG w/ author's permission for publication by
APCUG member groups.

For many years the most acute danger to your computer was some kind of destructive virus. Today the danger has shifted from software that is programmed to destroy files, corrupt programs, and disable systems to something more insidious, and perhaps even more treacherous. This threat comes in two broad categories known as Spyware and Trojan Horses.

Spyware started out as a stealth program surreptitiously installed on your system to track your web surfing habits. The developers of spyware didn't want to damage your computer. They wanted only to sell you something. That may be annoying, but there is nothing criminal about it.

A Trojan Horse is a program that pretends to be something other than what it really is. For example, a screensaver could be designed to install a program that will take over your system to forward spam to other machines. Trojan Horses have been used to initiate denial of

service attacks, where the target such as a bank, credit card service or other high profile web site becomes so saturated with external requests that it cannot respond to legitimate traffic. When selecting an anti-spyware program, start out by selecting one with a comprehensive signatures database. The best anti-spyware programs have databases that can recognize more than 750,000 different kinds of spyware and Trojan Horse programs. Read the documentation or call the company. This is important.

The best signatures database won't do you any good if it isn't updated frequently. The bad guys never seem to rest. They release new poison daily. Don't buy any solutions that require manual updates. You have better things to do. Insist on automatic updates.

Another important capability is active monitoring of your system. Wouldn't you rather prevent a malicious program from installing rather than removing it after the damage has been done? Avoid any program that removes infections found only after conducting a manual scan. This probably means avoiding some otherwise adequate free programs. There's an old saying about getting what you pay for. The best anti-spyware programs prevent spyware and Trojan Horses from ever being installed on your system.

Go for a program that allows you to customize your scans. We don't all use our computers in the same way. Some people require more comprehensive scans than others. If you are constantly browsing the Internet, you are likely to benefit from a daily scan that checks active memory, system folders, the registry, and all hard drives. If you rarely use the Internet or find yourself visiting the same six sites over and over, a weekly scan may be all you need. You should be able to schedule unattended updates and scans. Your machine should be yours to use as you wish. Any decent anti-

spyware program should be able to run in the background unattended, and not require interrupting your activities. The program should work according to your preferences, not the other way around. Choose a program that permits unattended maintenance and administration.

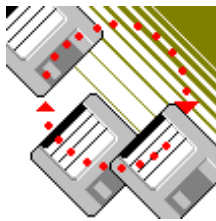
It's also important that an unattended scan can quarantine infections without requiring intervention from you. Why do some anti-spyware programs ask if you want to remove infections? Of course you do! Of all the features in anti-spyware programs, that is the dumbest. There are innumerable derivations and iterations of spyware being created. This makes it difficult for even the best anti-spyware programs to catch and destroy them. If you open the Processes tab in Windows Task Manager, you will observe the Process Manager in action.

You will see a list of objects running on your system. Some of them are applications like word processors. Others are mysterious entities that don't provide a clue as to what they do, but you can't run Windows effectively without them. Among them would be Windows Explorer, Internet Explorer, Media Center, Windows Mobile Control Center, and many others.

Beyond shutting down a process or resetting its priority, there isn't much a non-specialist can do with this feature. Clever programmers can create spyware that won't show up in the Process Manager. Any decent anti-spyware program has to have its own built-in process manager that will recognize, track down, and eliminate malevolent software that may not even be in the signatures database.

Anti-spyware programs should be able to monitor programs that load when Windows starts up. There are many very sophisticated spyware programs that do not show up in the Process Monitor or in Control Panel's

Add/Remove section. If your anti-spyware program lacks this capability, find another one. Assuming your anti-spyware program has the capabilities mentioned above, it is an excellent choice for individuals. However, businesses or organizations with multiple computers will require even more. Whoever is in charge of PCs will not have time to manually monitor or administrate individual machines. It is simply impractical in a large organization for support staff to visit every workstation, apply updates, schedule scans, and ensure that infestations are removed. If this applies to you, look for a program with a centralized administration console. This capability has the unfortunate drawback of being quite expensive, but the time saved generally justifies the cost.



LET'S CLEAN "START-UP"

by Bob Elgines, Editor, Colorado River
Computer Club, AZRCC Editor

[www.crcgaz.com/\(elginesz@\)rraz.net](http://www.crcgaz.com/(elginesz@)rraz.net)

From APCUG w/author's permission for publication by
APCUG member groups

Does your computer boot-up or run slow?
Maybe there are too many programs running in
the back ground. Let us do the following check
first.

- A. Hold your CTRL & ALT buttons and press the DELETE button.
- B. Click on the PERFORMANCE tab, is your CPU Usage running more than 10% or is your Physical Memory being in total use?
- C. Go to **START** then RUN, type in "**msconfig**" which stands for Microsoft System Configuration. In Windows VISTA you can find

RUN in the ACCESSORY folder under PROGRAMS.

The System Configuration Utility windows will come up.

First, go to the upper right tab labeled **STARTUP**, here you will see the list of items that load during startup. Of course some you want, some you don't. In the first column labeled STARTUP ITEM gives a very rough idea to what it is referenced too, but the second column labeled COMMAND, is much more useful. To read it better, widen the column out by holding your mouse symbol over the vertical line located before the next column label. A double arrow will appear, then hold down left mouse button and move it to the right. This information tells you where it is located and in some cases which program is using it. Uncheck those in question, you can put them back in later if you need too. Do not uncheck you Antivirus or Spyware programs.

Next, go to the tab on top labeled **SERVICES**, this show all of the programs running now. You do not want to uncheck those labeled Microsoft under the MANUFACTURER column, so to start off, lets put a check mark in the box below labeled "Hide all Microsoft Services".

Now while you are reviewing the other programs running in the background note the forth column labeled STATUS. If it says STOPPED, then don't worry about it. We just want to stop the strange ones that are RUNNING. You can uncheck those that you are not familiar with, here again you may bring them back in later.

After un-checking all those items under tabs STARTUP & SERVICES, then click on APPLY and CLOSE.

The System Configuration Utility will now ask you to RESTART (or Boot) your computer.

After restarting a window will come up stating System Configuration Utility has been changed, be sure to put a check mark in the bottom left (labeled "Don't show this message or launch ...") before clicking OK.

If you improved your operation of your computer, you can put back in the items one at a time until you find the program that was slowing you down.



So You Have A New Digital Camera

by Robert M. Mayo, (bobmayo1@cox.net)

Cajun Clickers Computer Club, LA

www.clickers.org

From APCUG w/ author's permission for publication by APCUG member groups.

If you were lucky enough to get a new camera for Christmas, congratulations! However, along with this jewel, I'm sure you also got a complicated user's manual. I hate 'em! But cheer up; all the mystery will soon go out of that book.

When I bought my first digital camera, I felt lost. I had never worked from menus before, and they seemed so overly complicated. However, after a couple of dozen shots of my refrigerator, washing machine, and the cats, I began to feel comfortable with my new toy. And now, it seems intuitive; I can make changes in the settings without mental effort. In fact, I don't know how I ever got along without the wonderful features this camera has! So the point is: play with it; check out all of the menu options in the privacy of your home so you

won't have technical problems later. Following directions in the manual, you're not going to hurt it!

Between photo sessions, it's best not to leave your rechargeable batteries on the charger. Many chargers provide a trickle that's excessive over a period of time, and this will degrade the cells.

In what we laughingly call "the good ol' days," we had a choice of films to use in our cameras. That was wonderful! There were so many films for color pictures available, as well as the still popular black-and-white shots. And within those two groups, there were fast (ISO 400) Kodak Tri-X films for B&W news (action and nighttime) pictures, as well as slower (ISO 25) Kodachrome film for beautiful, fine-grained slides. If you were happy with black-and-white prints, there was very fine grained Panatomic-X (ISO 32) that could produce great enlargements. There was a film for everything!

But what if you had the Panatomic-X in your camera, and six frames hadn't been used yet; and you wanted to shoot a night baseball game under floodlights? You could remove the unfinished film from the camera, or you could bang away at the kids in order to finish the roll. Cheez! What a waste! Plus, you had to obtain a roll of the faster film, too. But with your digital camera, you have all of those "films" in the camera at the same time -- color or B&W-- with a choice of ISO values to be selected as you need them, regardless of the number of shots you've already made. If only they had done this years ago!

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

MOUSE TRACKS is published by the Greenspring Computer Club, Springfield VA. It

is emailed to members with e-mail accounts and is also available on the Computer Club web site:

<http://www.gs-cc.net/>

Click on MOUSE TRACKS then choose the issue you want to read. The Mouse Tracks link is near the middle of the page.

Questions, articles, suggestions, compliments or complaints may be sent to the staff thru, Jim Coulter, OH-124 or emailed to him at:

jimcoulter@hotmail.com