September 2006 Volume 22 Number 9

PPCUG NEWS

A PUBLICATION OF THE PRINCETON PC USERS GROUP

Upgrading Your Personal Computer

John Goodwin

Monday, September 11, 2006, 7:30 p.m.

John will discuss upgrading and improving the performance of your PC. This will include adding more memory, upgrading hard disk drives, adding DVD writers, etc. He will demonstrate how these are done. He will also discuss hardware upgrading for the new Windows Vista operating system. Bring your questions to the meeting. Or if you wish John to address specific topics you can send him email (Jgoodwin88@verizon.net).

John Goodwin has 25 years experience in the computer support business. He provides on-site PC hardware and Windows software support to both individuals and businesses. John is the owner of J.A.M. Computer Services, located in Hamilton NJ.

Lawrence Library Meeting Rooms 1 & 2
US Alternate Route 1 South & Darrah Lane, Lawrenceville, NJ

Meetings of an organization at any of the facilities of the Mercer County Library System in no way imply endorsement of its programs.

In this issue:

Coming Schedule

Oct. 16 ------Vic Laurie on Searching the Web for Medical Information
Nov. 13 -----Hank Kee on Remote Computing
Dec. 11 --------Member's Holiday Party
January 8, 2007 ----- TBA
February 8, 2007 --- TBA
April 27, 28, 29, 2007 ---Trenton Computer Festival at TCNJ

About PPCUG

General Meetings

Second Monday of the month at the Lawrenceville Library, Alternate Route 1 and Darrah Lane.
7:00 PM: Social Time / Tech Corner
7:30 PM: Meeting comes to Order
7:45 PM: Featured presentation

For information about upcoming meetings or joining PPCUG, see:
http://www.ppcug-nj.org
or email us at:
ppcug.nj@gmail.com
(Please include "OK" in the subject line.)

Board Meetings

Board meetings are open to all members. Notice of an upcoming meeting will be posted on the web site.

Board Members

President:	
Clarke Walker	609-883-5262
Vice-President:	
Tom Carman	732-828-6055
Secretary:	
vacant	
Treasurer:	
Judge Landis	609-737-2997
Members-At-Large:	
Al Axelrod	609-737-2827
Kim Goldenberg	609-631-9140
Paul Kurivchack	908-218-0778
Vic Laurie	609-924-1220
Sol Libes	609-520-9024

Chairpersons

Hospitality:	
Bill Hawryluk	609-655-0923
Member Records:	
Paul Kurivchack	908-218-0778
Newsletter Editor:	
Clarke Walker	609-883-5262
Program Coordinator:	
Sol Libes	609-520-9024
Web Master:	
Joe Budelis	609-921-3867

2006 Annual Dues

Dues are $40 per calendar year with a mailed newsletter or $20 per year with online access to the newsletter. New members pay $3.25 or $1.75 per month times the number of months remaining in the current year.

Minutes of the August Meeting

The meeting started at 7:30 p.m. by President Clarke Walker.

The only question was from a member who reported having difficulty reading email on the Yahoo! Server.

The feature presenter was Martin Mosho who told us how to start a "Successful eBay Business".

Martin Mosho by Judge Landis

Pictures from the August Meeting

by Judge Landis, judge@alumni.princeton.edu
Member of the Princeton PC Users Group

Help Wanted

Secretary

The group is in need of a Secretary to take minutes of the meetings. Also to read and respond to club email. Please see a Board Member for more information.

President's Message

For this issue I put out a call for articles. Thankfully Vic Laurie responded with an excellent article about protecting your computer.

You do not have to be a gifted writer to write an article for the Newsletter. The main premise of the User Group is to share information. It can be programs you are using or have tried or experiences you have encountered.

At last month's meeting Sol Libes took a poll to see what specific topic area you wanted John Goodwin to speak about. The majority are interested in upgrading their computer hardware. So John will focus on those issues.

- *Clarke Walker*

Link of the Month

Mark Russinovich and Bryce Cogswell maintain a web site of many useful Windows System Internal applications and information:

http://www.sysinternals.com/

Have you discovered a useful link? Then share it with the members of the P PC UG.

Do We Need a Paradigm Shift in Anti-Virus and Anti-Spyware Protection?

by Vic Laurie, http://vlaurie.com
Member of the Princeton PC Users Group, www.ppcug-nj.org

Thomas Kuhn, a noted historian of science and my former faculty colleague at Princeton University, coined the expression, "paradigm shift", to indicate the occurrence of a completely new and different way of looking at an area in science. Personally, I think that a paradigm shift is exactly what we need in the area of computer security. Fans of UNIX systems, especially Mac and Linux users, are going to immediately say that all that is needed is a switch to their favorite operating system. And they have a point. However, the Windows PC monopoly is not about to go away and the comments that I give here relate to the typical home computer user.

The present way of protecting computers against malware such as viruses, worms, Trojans, and spyware is basically reactive. It depends on a local database of information about known malware in order to recognize and disarm the invaders. Some attempt is made at using so-called "heuristic" techniques to recognize new malware that is not in the database but maintaining the protection still requires constant updating of the local database. Also, since the different types of malware have different behavior patterns and signatures, more than one type of protection is needed. Although software suites may combine the different kinds of protection in one package, many people end up with a hodgepodge of different applications. For example, I have an anti-virus program, a software firewall, a hardware firewall, three anti-spyware programs, an email filter, two Trojan removers, and various Internet toolbars for blocking popups, ads, phishing, JavaScript, *etc*.

Having to run all these programs and having to constantly update them is not only cumbersome but also makes a hit on system performance. For example, Symantec products were such a drag on my system that I never ran them in the background but only used them manually. (I finally chucked Symantec's Norton anti-virus in favor of AVG.) The fact is, even with con-

stant updating, systems are still vulnerable to so-called "zero-day" and undocumented exploits. The constant parade of new security problems makes it clear that something better than the current approach to safeguarding computers is needed.

There are already several possible alternative ways to go. One is the procedure used on many systems that are open to the public in places like libraries and schools. A standard system configuration is established and any changes, including malware, that occur on the system during an individual login session are erased when the user is finished. The system is simply returned to its standard configuration. This approach has been very satisfactory in our classes at SeniorNet where we use the program Deep Freeze. (http://www.faronics.com/index.asp) Students can do anything they want to the system or even get it infected by malware but when it is rebooted it returns to its original pristine state. This is very satisfactory for a setup which remains static but can be tedious where a user installs a lot of new software or frequently creates new files. Changes to the system can be incorporated into the standard configuration if desired but this is a multi-step process and not really suitable for dynamic systems where content changes frequently. However, this approach can be modified to add flexibility by having a separate unfrozen partition where data files and frequently changed programs are kept. Installations that require Registry entries will still need to be done in a multi-step process but the average home user who is an infrequent installer of new programs could certainly use this approach. Note that this procedure is much less time-consuming than restoring something like a Ghost image. Also, it is very important that the user does not have to do anything except reboot. A typical home PC user is not about to maintain up-to-date Ghost images.

A related approach that is attracting more and more attention is the use of "virtual" machines. The equivalent of several independent operating systems can be created on one computer. This is especially attractive for those who install or test a lot of software. David Berlind at ZDNet has an article on the virtues of VMWare. (http://blogs.zdnet.com/BTL/?p=2462) You can have one virtual machine that is the standard setup and another test machine that gets exposed to the Internet. If the test machine gets infected, it is deleted and the standard setup is copied. Creation of new data files on a virtual machine is no different from a regular computer. Installation of new software can be tried on the test machine first to make sure that the software is legitimate or has no undesirable effects. It is also possible to have a host machine that can access a virtual machine while the virtual machine is ignorant of the existence of the host. At the moment, one problem with virtual machines is Microsoft's draconian licensing. They demand that two virtual Windows machines on the same computer pay for two licenses. This seems short-sighted to me. Microsoft has its own virtual PC software that it bought with Connectix and this is not a way to encourage its use. (Free download is at http://tinyurl.com/eba5h). Also this licensing policy seems likely to drive people into taking a look at Linux. There are ready-made Linux virtual machines available for downloading. I can easily imagine a setup where a Linux machine with its greater security is used for Internet connections while the more versatile, easier-to-use Windows machine is used for other applications. The average home PC user may not be quite ready for the virtual machine approach but I think it is well worth considering.

Neither approach mentioned above requires a lot of defensive software with constant updates. It is not necessary to try to recognize large numbers of malware. Personally, I believe that approaches of this type combined with a good firewall are very promising. I do believe that a firewall is a must since crackers are constantly probing for machines with open ports and the time it takes before you are likely to be attacked is too short. A firewall will keep intruders out and will also warn you if something does get on the system and tries to connect to the Internet. Note that the firewall responds to what something does, not what it is. This general type of protection is behind a new approach described next.

This different approach is mentioned in an article at PC Magazine. (http://www.pcmag.com/article2/0,1895,1911010,00.asp) The company Sana Security has a program that monitors all running processes and examines suspicious behavior patterns. If it detects a process that it considers malicious, it quarantines files and Registry keys related to the process. According to PC Magazine, "*Because it specifically responds to what a program does rather than to what it is, it is most likely to detect malware immediately upon installation or just after a system restart.*" It remains to be seen how effective this particular software will be, but the general approach of focusing on the behavior of software and not its specifics is the type of thing that should be pursued. A free trial can be downloaded at http://www.sanasecurity.com/products/standalone.php. This approach could be the trend of the future but there are many companies with vested interests in the present way of doing things so there may be resistance from the Symantecs of the world.

A wildcard in all of this is the intentions of Microsoft. The company is moving steadily into the security software area. No one outside of Redmond (and maybe not even there) can be sure about exactly how involved they are going to be in the security field. There may be anti-trust issues involved here so it isn't clear how far Microsoft may think it can go in incorporating new features that overlap with the products of other companies. However, security measures are a natural function for an operating system.

Finally, I have to mention the weakest link of all in the security chain, the user. If people used more common sense, it would

solve a large part of the security problem. Without fertile fields of gullible suckers, spammers and phishers wouldn't find their scams worthwhile. If people thought twice about what they click on, all those worms wouldn't be propagating and my mailbox would be a lot emptier. I hope that I'm too pessimistic but I don't see a lot of hope here. I end with two quotes. The first is from MJ Ranum (http://www.ranum.com/security/computer_security/editorials/dumb/)

> There have been numerous interesting studies that indicate that a significant percentage of users will trade their password for a candy bar, and the Anna Kournikova worm showed us that nearly 1/2 of humanity will click on anything purporting to contain nude pictures of semi-famous females.

The second quote is from Neil Rubenking at PC Magazine (http://www.pcmag.com/article2/0,1895,1980522,00.asp)

> Even if there were such a thing as perfect protection against every attack, though, you're still vulnerability. As we used to say, the part of a car most likely to cause an accident is the nut behind the wheel. If you mindlessly obey e-mail messages like, "We am you bank. Fax to us you password for safeness," there's nothing any software can do to help.

Choose Your Own "Home Page"

by Ira Wilsker, iwilsker@apcug.net
APCUG Director; columnist, The Examiner, Beaumont TX;, http://www.apcug.net/

I work on a lot of different computers at a variety of locations, and one factor that consistently astounds me is that many people have blissfully ignorantly never changed their startup "home page" from its default. This is the page that first opens when the user connects to the internet. For example, many Dell computers have the Dell website set for the startup page when the user first accesses the internet, while Windows itself, unless otherwise changed, defaults to Microsoft's MSN home page, making it one of the mostly used startup pages. Many internet service providers (ISP), such as AOL, AT&T, and others changed the users' home page to the ISP's selected home page.

Startup or "home" pages are big business because they are commonly advertiser supported, and the more views (also referred to in the industry as "hits"), the more revenue generated by the host. This on-screen real estate is so valuable that a type of malware or spyware, sometimes known as homepage hijackers, will attempt to change your homepage to its client's home page, for which the miscreant receives compensation for each page such changed.

There are many different services offering home pages, and if the user finds one that he likes, it is very easy to make the selected page the new home page. The process for selecting the default home page is the same for most browsers. Using Microsoft's Internet Explorer (IE), which is still the most widely used browser in the world, the process is simple. If the user visits a website that he would like as his homepage, he simply clicks on "Tools" on the menu bar, and then that will open a window where the home page can be selected. If the open page is what is desired, then click on the "Use Current" radio button, and the current page will be displayed each time the browser is loaded. If "Use Default" is selected, the home page will revert back to the Microsoft (or other manufacturer) default start up page. On the new Internet Explorer 7 (Beta), which offers tabbed browsing, a different home or startup page can be selected for each tab. For those who do not want to connect to any page at all when loading the browser, IE7Beta offers the option of a blank page. All versions of IE also allow for the manual entering of any selected internet address for a home page. To directly go back to the home page at any time, simply click on the little house or "home" icon on the menu bar.

Firefox (www.mozilla.com), one of the most popular browsers behind IE, offers a simple interface to select or change the homepage. Clicking on "Tools" on the menu bar opens a window where "General" can be selected, and then "Home Page". Firefox allows the address to be manually entered, or the current page loaded can be selected. Other options allow for the home page to be selected from a previously saved bookmark (Internet Explorer calls these "Favorites"), or the option for a blank startup page can be selected. Firefox also offers the little house on the menu bar for instant access to the home page.

There are many choices for a home page, which is totally up to the user. Some users use their web mail accounts as a home page, first displaying their email when connecting to the internet, while others may choose retailers, auction sites, employer web pages, search engines (such as Google or Yahoo), newspapers (such as the Examiner at www.theexaminer.com), or any

other page of interest. While any page can be selected as a home page, the most popular home pages selected are usually news and information based pages.

My personal favorite, which I use on all of my computers, is "My Yahoo", at my.yahoo.com. I have found My Yahoo to be the most comprehensive and flexible home page. Being an information junkie, I have customized my My Yahoo page to include stock and mutual fund listings, news from dozens of sources, weather, lottery results, sports scores, my personal calendar, latest emails received, TV listings, and other information. My Yahoo, which is very easy to configure, directly offers thousands of choices. Many information resources, such as the Examiner, are now using "RSS" or "XML" feeds as a news source, and these can be added to My Yahoo often with a single mouse click. My Yahoo is also customizable with hundreds of backgrounds, color schemes, layouts, or other features to personalize it.

Microsoft is currently testing a new homepage intended to at first supplement its flagship homepage at www.msn.com, and maybe later replace it. This new homepage, currently in beta testing, is currently online at www.live.com. It will be a strong competitor to My Yahoo, offering news, sports, weather, email, and other resources in columns that are infinitely customizable.

There are countless other "My" homepages available, such as AOL's my.netscape.com, and other personalized home pages, including Google's "Personalized Home" link sitting quietly on the top right corner of the popular http://www.google.com/ig?hl=en website. All of these home pages can be easily customized to suit individual needs.

There is no need to continue to use the default startup or home page provided by your operating system or ISP. Investigate some of the alternatives, and increase your enjoyment of the web.

Editor's note: Of course all P PC UG members use http://www.ppcug-nj.org/ as their web browser start page.

"Suddenly…" OR "I didn't do anything!" Part 1 (section 1)

by Charles W. Davis, Chas@anthemwebs.com
Newsletter Editor & Webmaster of Sun City Anthem Computer Club, www.myscacc.org

Subtitle: Or — a month's log of a Sun City Anthem Computer Club "house call" doctor

In working to help Club members and others with their computer problems during the Thursday morning Computer Talk sessions, or more often when making "house calls," I often hear strange tales that usually involve acts of some gremlin like creature. However, gremlins are more closely related to mechanical problems in aircraft.

Generally the caller's comments start with "all of a sudden" or "suddenly" and end with "I didn't' do anything." I can only surmise that it was probably one of cartoonist Bill Keane's ghostly imps "Not Me." "Nobody" or even "Ida Know."

Some recent examples:
"Suddenly…"
One morning a couple of weeks ago, I received a call and the person on the other end of the phone connection was obviously very upset. She exclaimed: "Suddenly all of my desktop icons are gone! I didn't do anything! Please help me!"

This situation seemed to be serious. I had never heard of this happening. I didn't have anything on the calendar for another two hours so I hopped in my 1999 "Sapphire Blue Mica" (marketing division color name of course) Miata for the short drive up the hill to her Tall Mesa Village home. She was right, the icons were indeed missing. A simple right click on the blank desktop, hover over Arrange Icons by: and then click on Show Desktop Icons. This was definitely an act by the "little people." As I said, I hadn't heard of this situation before. Therefore, it must have been "Not Me" wishing to get off the hook by whispering in my ear how I might arrive at the solution. Since the club member was in the back room and the house girl had let me in, I quickly left the scene.

The next day the same lady called and said that her "My Computer" Icon was missing from the desktop. Realizing that it wasn't the normal desktop shortcut icon, I was puzzled. Not thinking things through, I again slid onto the seat in the Miata and shortly arrived on the scene. Sure enough most icons were visible, but the "My Computer" icon was not in its normal position. It wasn't immediately visible. I later noticed the top edge of the icon protruding just above the task bar. Once again, I moved the pointer to a blank spot on the desktop, a right click on the mouse and chose Arrange Icons by and chose Name. The My Desktop icon again assumed its prominence at the upper left. She said that she didn't drag and drop it down there. As I picked up a $20 donation to the Club, I assumed that it must have been "Nobody" and left for home.

"Suddenly…"
Monday morning is usually the time for the phone calls to begin. On a recent Monday, the caller sheepishly states that "suddenly I can't access the Internet." I recognized that the person speaking to me is the same one whose 18 year old granddaughter had placed hundreds of malware programs on his laptop two weeks before. At that time I had suggested a router/firewall so that she could plug her laptop directly to the router with Internet access. He had immediately gone out and purchased and installed one. Oh yes, the granddaughter had been there over the weekend and had brought her own laptop computer.

The blue Miata once again headed up the hill (from our home in the Valley View Village all destinations seem to be "up the hill.") to their home in Arroyo Vista Village. In just a few minutes, I found that the dear child didn't plug the cable into the router as instructed, but had used grandpa's computer. Since she was an AOL user, she attempted to change Gramps' Accounts from Cox Cable to AOL dialup and failed. It would have been so easy for her to have just gone to AOL using Internet Explorer. She left for school Sunday evening and didn't mention a thing to Gramps. That way, she didn't have to tell on either "Ida Know" or "Not Me." I picked up the $20 donation to the club and was soon on my way.

An admonition: Set up a Guest Account without Administrative rights. Place a User name and password on the Administrative (your's) account.

"All of a Sudden…"
"All of a sudden" turns up many times a month and in some unusual situations. Last week, I received a call from a member that was using Microsoft Office Outlook. It seems that she had been entering information into a new contact when "all of a sudden" she couldn't enter information. She explained that she had been using Outlook and contacts for years and had never had this problem. Since this didn't seem (to me) that this required immediate attention, I arranged an appointment for the next morning. My Miata and I arrived at her Golf Mesa Village home just as the Grandfather clock guarding the entry was announcing that it was 10:00. Grandfather clocks that I am aware of don't announce "a.m." or "p.m."

She met me at the door and we proceeded to the office and she took her place in front of her computer to show me what was happening. She began keying in the house number, using the numeric key pad and just as she had said, nothing worked as expected. I immediately saw why this had happened so "suddenly." Apparently "Nobody" had pressed the Num Lock key thereby turning it off. So as she would enter a house number, things went wild as the 2,4, 6, and 8 keys acted as direction keys, 7 & 9 were Home and Page Up respectively and 1 & 3 were End and Page down. I asked her to press the Num Lock key and "all of a sudden" the problem was resolved. I collected the $20 donation check to the club and was homeward bound — downhill of course.

"Suddenly…"
On another Monday, I received a call from a member stating that she had recently upgraded to MS Office 2003 and a short time later, suddenly she could no longer access MS Publisher files. This was the result of someone else messing with functions that they should have stayed away from. Support teams at Norton will vow "Not me." But when the lady was directed to an article titled "How to use Office programs with the Norton Anti-Virus Office plug-in" she was able to resolve the problem as I watched. This article can help you extricate yourself and may be found at: http://support.microsoft.com/kb/329820/en-us

It is maddening to think that one, nay thousands upon thousands, must jump through hoops because a bunch of programmers at Symantec (Norton) can't get it right.

I have never understood their automatic plug-in installation. At least they should tell the user, including a list of possible problems and their resolution, and let them make a decision as to whether to install the plug in. Who needs viruses when "reputable" software manufacturers can do things like this to you?

A long time ago, in computer time, but actually just over a year ago, I stopped paying the extortion money for antivirus

software and have used the free AVG antivirus, which is available from http://free.grisoft.com/doc/1

"Suddenly..."
"Suddenly" you can't open Word or most other Microsoft Office products. This happened because you owned a Hewlett Packard multi-function printer with a flash memory card reader. It seems that a security update messed with the logic for these systems and caused much havoc around the world. A follow-on update was released to affected computers during the 4th week in April. If you are still having the problem, go to Start then Windows Update, download and install all Critical updates. It seems that "Ida Know" visited Microsoft's Redmond campus…

This article was originally published in Bits, PCs & Macs. Bits PCs & Macs is the newsletter of the Sun City Anthem Computer Club. All copies are available online at: http://www.myscacc.org/newsletters.htm

Temporary Help Wanted

Hospitality

While Bill is recovering from back surgery we need some one to maintain the User Name Board. Please see a Board Member for more information.

Princeton PC Users Group
PO Box 291
Rocky Hill, NJ 08553