March 2005 Volume 21 Number 3

PPCUG NEWS

A PUBLICATION OF THE PRINCETON PC USERS GROUP

Hard Drive Disaster!

Paul Kurivchack

Monday, March 14, 2005

The presentation will address backup techniques for preventing data loss and the options available to the average computer user for recovering data files when the operating system becomes corrupt from a virus or software download. Demonstrations will include the use of IBM's ThinkVantage Technologies Rapid Restore & Recovery as a tool for data backup and restore of the system to using Easy Recovery Pro from OnTrack in performing a data recovery from a non-bootable hard drive.

Paul Kurivchack has been involved in selling and technical support of high tech instrumentation and computers systems for over 30 years. Starting as a sales engineer in the process control industry and then moving into personal computer sales and technical support roles 12 years ago.

Paul is currently providing third level software support for desk side technicians throughout the USA. This includes PC configuration (primarily laptops) and software trouble shooting including Windows 2000 and XP Pro. Paul has setup a data recovery lab to perform customer data recovery from OS and virus damaged hard drives.

Paul has a BS in Electrical Engineering Technology from Trenton State College (now The College of New Jersey)

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 this issue:

Coming Events:

April 2005 —Joe Budelis on VoIP for Dummies
April 16, 17—Trenton Computer Festival (www.tcf-nj.org)
May 2005 —Vic Laurie on his Six Favorite Programs.
June 2005 —TBD
July 2005 —TBD

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:	
Joe Budelis	609-921-3867
Treasurer:	
Paul Kurivchack	908-218-0778
Members-At-Large:	
Al Axelrod	609-737-2827
Vic Laurie	609-924-1220
Kim Goldenberg	609-631-9140
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

2005 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 February Meeting

Clarke started the meeting at 7:30 PM. We started with a discussion about the TCF which will be at The College of New Jersey this year. In previous years we have run the Parcel Pickup for the Festival. Paul K. will contact the organizers to see if we can do this again. He will then send out a call for volunteers to manage the area for Saturday and Sunday.

The computer of a member's neighbor worked fine one day; the next day, as soon as it's turned on, it gives a Windows System 32 conflict screen. It was suggested to choose repair (middle choice) from the setup disk if can not start it in safe mode. You get to safe mode by holding down the F8 key during startup. If the above suggestions are unsuccessful, the HD probably has to be formatted. This problem could be caused by a virus or by an incorrect shutdown. Incidentally, Paul mentioned that, even if you have to reformat the HD, you might be able to save the data on it. Stay tuned, that is Paul's topic for the meeting next month.

Another question was whether a Jump Drive was a worthwhile investment. Yes, since most machines do not include floppy drives and, anyway, *small files* nowadays are often 3-5 Megs and thus won't fit on a floppy.

An XP Professional problem was presented. Although IE functions, Windows Explorer starts but then fails with an error message and nothing can be done with it. It was suggested that the exact error message may allow a better understanding of the problem. However, probably data should be copied off the HD and then Windows reinstalled.

An unusual network problem was presented in which IE works fine for about 8 minutes after reboot of a WIN98SE system but then no longer connects to http sites via the laptop wireless network. Meanwhile another PC on the wireless network continues to work with no problem. What is really strange is that, while IE and also Firefox stop working, AIM and AOL continue to be able to access the internet. Actually, IE does not stop completely; it continues to be able to access https pages! No one had any solutions other than a suggestion to try a different wireless card.

Picture of Joel May by Tom Carman

Joel May's presentation slides for "The Many Faces of Google" are available at http://snipurl.com/googlefaces Just when we thought we knew how to use Google, Joel comes along and, surprisingly, was able to add to practically everyone's knowledge of the Google site. The presentation slides are quite complete.

- Submitted by Joe Budelis

President's Letter

I like computers so much I had one installed in my chest. On February 10th the Doctors at Deborah Heart and Lung Center implanted an AICD (Automatic Implantable Cardio-verter-Defibrillator). It is similar to a Pacemaker but programmed differently.

Getting the AICD wasn't enough fun for me. On March 1st I had a root canal done. Again I saw some amazing technology, digital x-rays. Instead of the traditional film you hold a plate connected to a computer. Within a second the picture is displayed on the screen and can be enlarged. ("My what big teeth you have.")

I bet we can all create a hard disk disaster. If not, Paul K. will show us and most importantly tell us how to recover it at the March 14th meeting.

If you are interested in giving a presentation please let Sol Libes our Program Coordinator know.

- Clarke Walker

More on "Phishing"

by Vic Laurie, PPCUG

Since I first wrote about the Internet scam called "phishing (http:/vlaurie.com/computers2/Articles/phishing.htm), the problem has become ever more severe, Viruses and worms are bad enough but phishing is especially dangerous because your finances and your identity are at stake The criminals who are involved have become quite sophisticated in their attempts to relieve you of your bank account. Because the methods that are used can be quite devious, I am revisiting the subject to point out how to guard against some of the newest tricks.

As discussed in the previous article, emails that claim your account at some bank or other place has to be "updated" to prevent your account being cancelled are spurious. The links in these emails that purport to take you to the bank's site where you can enter the updated information are in fact links to the criminal's site where they will happily take down your personal data and passwords. I suspect that by now most PC users are on guard against this particular form of the scam and know not to click on links in these messages. In the past, it was often stated on various Internet sites that it was safe to copy the links and then paste them into the browser address bar. I have never agreed with this and recent exploits makes it even more certain that links in these emails should be absolutely ignored.

Even trickier is the fact that simply reading a message in hypertext format can be dangerous. If Internet Explorer is not up to date with security patches, miscreants can secretly download Trojan horses onto your computer as soon as their emails are opened, even in preview. Even if you have all of the Microsoft updates installed, new holes are constantly being found. Therefore, for safety, it is best to turn off any preview pane in your email client and to read messages in text format only until you are sure that the message is legitimate. Outlook Express (and other email clients) contains settings for turning off the preview pane and for reading in text only. (Instructions for Outlook Express are given at http://surfthenetsafely.com/reademailsafely.htm)

Host File Tricks

One of the latest methods of robbing your accounts involves using a Trojan horse to modify something called the *Hosts* file that is part of the Windows system files. (The Hosts file is explained in more detail at http://vlaurie.com/computers2/Articles/hosts.htm) Briefly, the Hosts file is way to store locally the translation from an URL to the numerical IP address that computers require. (For more details about IP addresses, see the article http://vlaurie.com/computers2/Articles/Name.htm) By modifying this file, a legitimate URL can be made to go to a scammer site instead. The crooks have gotten so good at faking sites that look just like the legitimate ones that most people can be fooled. If the Hosts file gets changed, entering the actual Web address of your bank into the browser address bar or using a favorite place will take you to the fake instead.

One of my favorite free programs, *Win Patrol*, allows you to lock the Hosts file and to view it if you wish. It will also warn you if something tries to modify the Hosts file. This program can be downloaded at http://www.winpatrol.com/. Some of the anti-spyware programs also allow for locking the Hosts file.

You can also check out the Hosts file yourself with no added software. The Hosts file is a text file that can be viewed and edited with any text editor. However, the filename has no extension and if you click on it, Windows may ask you what program to use. Choose Notepad. The Hosts file is located in the Windows directory in Windows 98/Me. In Windows XP, it is buried in *\Windows\system32\drivers\etc*. You may want to use the Search function to find it. Go to **Start-Run-Search** and enter "hosts" (no quotes). Note that there may be other files such as "hosts.sam" or "lmhosts". The file of interest is simply "hosts" with no extension. The file will likely contain only a few dummy entries. An example Hosts file is shown at http://vlaurie.com/computers2/Articles/hosts.htm. Some anti-virus programs such as Symantec that use proxy servers to check email may also have made a few entries. What you are looking for is to make certain that there is nothing there that refers to a bank, brokerage, or other site where personal information might be entered. Any such site can be deleted. However, the presence of entries of this type is likely to

indicate a possible infection and appropriate measures should be taken to remove any Trojan horse (http://surfthenetsafely.com/surfesafely2.htm)

More on the use of the Hosts file by malware is at http://www.pcmag.com/article2/0,1759,1649060,00.asp

Phishing at Wireless Sites

Many of us who do any traveling and carry a laptop make use of wireless connections at coffee shops, hotels, and other "hot spots". When these public areas are used, they should be regarded as insecure and care must be taken with any personal information that might be broadcast.

A form of phishing, sometimes called an "evil twin attack," is to set up a fraudulent access point at a public place with enough broadcast power to override the signal from a legitimate source. Thus, you might think you were logging in to a wireless point provided by Starbucks when actually you are using an access point provided by someone who is monitoring all your input.

More on this subject is at http://reviews-zdnet.com.com/4520-7297_16-5630241.html.

.

[Editors's note: Hopefully no one is planning to move away, like Don Arrowsmith has.]

If Moving Can't Be Fun, At Least Make It Painless

By Gabe Goldberg
APCUG Advisor and Columnist
AARP Computers and technology Website

It's said that "two moves equals one fire" in terms of inconvenience and turmoil. Fire victims might disagree, but there's no doubt that moves range from disruptive to agonizing. Having just moved -- and, in the process, reengineered my family's computing and Internet setup -- I'll share tips for recreating or transforming technology when moving.

Some aspects of moving are the same whether the trip is cross-country or down the street: packing boxes, dealing with new quarters, etc. But moving locally allows shuttling between old and new sites, avoiding the long-distance "D-Day" moment when everything must be in transit.

I'll focus on technology: computers, Internet issues (ISP/cable/DSL), system backup, telephone (local, long distance, cellular), and electricity. (Just ensure that someone attends to non-tech services such as gas and newspaper delivery!) And remember, just as insurance needs differ, no single move strategy fits everyone. Decide what to do based on your technical skills and how you'll be affected by problems.

It shouldn't be hard to identify what you've got -- computers, accessories, network connections, etc. But listing local dependencies may be challenging. What do you depend on locally? Just as you know your doctor and plumber -- what's your technology support structure? If you use a local ISP (Internet service provider), will it be available after you move? If you rely on neighbors or local user group for technical assistance, who will replace them? Remember that AARP's technical community at http://community.aarp.org/rp-computers/start is always as near as your Web browser!

Make and update to-do lists; take notes on conversations with vendors to track progress and follow up when (all too often) necessary.

First, inventory your technology and set goals. Balance recreating your current setup against improving it. The first choice reduces change and perhaps stress; the second can offer better computing.

Next, identify what you need. If you generally keep a list -- mental or written -- of technology problems (slow computer, fuzzy monitor, pokey Internet connection), moving may be the time to solve them.

Finally -- and most fun -- think about what you want. If you're moving when retiring, you may take up new hobbies. Dealing with music, digital photography, and movies all require more computer power: CPU speed, RAM, and hard drive space. And losing access to the office computer and network can suddenly make an upgrade essential.

Plan your new place's technology; decide where to place your computer(s). Custom space and furniture are nice but not essential. Make sure there are enough electrical outlets and that circuits can handle the load. Locate other connections you'll need such as telephone and cable (TV/Internet). Draw a floorplan and experiment with placing furniture and equipment -- it's much easier to redraw lines than move heavy objects.

When your move is set, deal with utilities at both ends. You may not care when service is terminated, but there's sometimes a wait to establish telephone and cable service. For local moves I've had good results from visiting utility offices rather than making changes by phone: I could look at current products/services literature, discuss options, and read contracts. Consider new service plans -- for cable TV, ISP, cell phone, long-distance calling. Your post-move needs may be different and plans have likely evolved since you last evaluated them.

My wife thinks -- likely correctly -- that my first priority after moving is getting online. Even if you've arranged

broadband service, there may be problems: wiring or account setup may not be done; your PC configuration may not match the new service; etc. If access is essential, establish and test backup dial-access service before moving -- even if it requires a long-distance phone call.

Keep essential materials such as manuals and software install disks handy. Locate a user group where you're going, perhaps join before moving and introduce yourself to group leaders so you have a welcoming committee ready. Solicit recommendations for consultants or service shops, just in case.

If movers will handle your equipment or you're shipping it, make sure it's adequately insured.

If staying in touch is essential, warn people that you're moving and that you'll be offline and explain how you can be reached (cell phone, new address, etc.). Auto-responders (sending a canned message to people who e-mail you) can be helpful but should be used with caution so they don't respond inappropriately (e.g., to mailing lists to which you're subscribed).

If you're moving locally, set aside fragile equipment or anything you want to keep in sight, such as financial or medical records, and shuttle it to your new place.

For longer moves, allow extra time to pack electronics carefully in original boxes. (Now you know why you keep boxes!) Consider carrying or shipping boxes containing irreplaceable material (one data backup, software CDs, etc.)

Label cables when you disassemble your PC and network and record where they connect. If you're nervous about disassembling your equipment, a local consultant can likely prepare it for shipping. That's better than having movers do it! For extra protection, remove your hard drive and pack it in soft clothing you'll take with you. That will doubly protect you: from damage if the computer is dropped or banged, from losing data if the computer is lost or stolen.

Carry a tested backup (software and data) separate from your PC. If you have desktop and laptop computers, you may be able to back the desktop system up on the laptop hard drive.

Once you arrive, even if you're in a hurry, don't neglect power protection -- using at least a surge protector, preferably a UPS (uninterruptible power supply).

Update anything displaying your address such as Web pages and email signature files. Tell tech-involved organizations such as your ISPs and domain name registrars that you've moved so you receive bills and notices. Now kick back and relax; enjoy your well-organized technology.

This article appeared originally on AARP's Computers and Technology Web site, <www.aarp.org/computers>. (c) AARP 2005. Permission is granted for reprinting and distribution by non-profit organizations with text reproduced unchanged and this paragraph included.

Link of the Month

You can learn more about the wondrous technology of ACID at www.deborah.org/consumer/clubs/zapper/icd.html or www.virginiamason.org/dbCardiology/sec378.htm.

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

Hackers are NOT Crackers

By Barry F. Phillips
Member of the Computer Club of Oklahoma City
www.ccokc.org

The media loves to publish stories about so-called hackers breaking into computer systems and causing destruction. It is time to set the record straight, based on historical truth.

The hacker culture actually started in the 1950s when computers were huge to say the least, and programming then meant connecting wires to electrodes. While they did not call themselves hackers then, that for the most part explains what a hacker is. A hacker may be defined as a person who enjoys exploring the details of programming systems and how to stretch their capabilities as opposed to most computer users who prefer to learn only the minimum necessary.

Hacker as a term was first adopted as badge in the 1960s by the hacker culture surrounding the Tech Model Railroad Club (TMRC) and the MIT AI Lab. All computer systems that we use today are based on early hacker research. Much of this research was done out of love for the subject and the fame within the hacker community. One must be recognized as a hacker by the hacker community, which is a certain ego satisfaction. Several famous hackers from the first computer club, the Home Brew Club, were instrumental in founding major computer companies.

Around 1980, a new breed of computer-fed kids evolved, due to easy access to the Internet in the United States and Europe. They soon learned that they could break into other people's systems. Unfortunately, the media called them hackers and the name sort of stuck, when in fact hackers do not consider such illegal security breakers to be hackers, but crackers. Hackers build things; crackers break them!

Much of the freeware on the Internet comes from hackers. It would seem that hackers have been given unjustly a bad name by the media and deserve an apology at the least. While crackers should be prosecuted to the full extent of the law for their illegal actions.

While it is true that many hackers possess the skills for cracking, they outgrew any desire to do so except for immediate, benign, practical reasons. Contrary to non-hacker belief, there is no thin line between being a hacker and being a cracker.

Hackers built the Internet, maintain Usenet, work in IT computer security, and all Internet related businesses owe their origin to hackers. We can demonstrate our respect for their considerable IT achievements by making sure we do not use the term, hacker, when we mean cracker, who is involved in illegal cybercrime.

My thanks to Philip Tellis who did considerable research that was the basis for this article to correctly inform the public.

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