

# The NCTCUG Journal

[www.nctcug.org](http://www.nctcug.org)

May 2006

Volume 29 Issue 3

## Keeping Up

By Paul Howard, NCTCUG

### Slip-Slidin' Away

Five years ago, Linda and I decided it was time to use our living room for something besides the venue for my post-prandial snoozes, i.e. Dagwood naps. We moved some furniture, bought a new TV, relocated the sound equipment, and set up a low end home theater system. We have 5.1 channel sound, and while the TV is only 27", it works for us, given the room size.

With the new TV, a VCR with hi-fi sound and S-VHS recording capability was soon to follow.

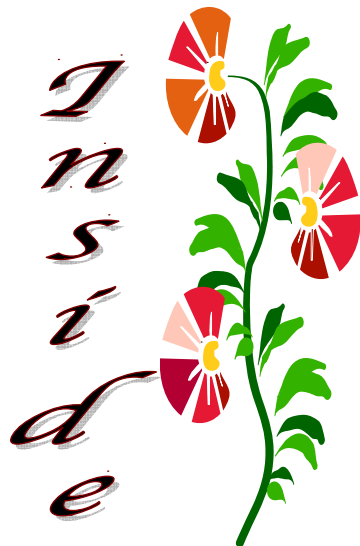
The first time I put a tape in the new VCR, a change in technology was evident. Push in the tape cartridge, and the VCR skittered across the shelf like it was on wheels. This VCR was unlike several of the older units I owned, with a big power transformer, heavy metal chassis, and lots of weighty components, where sheer mass



kept the unit virtually glued to the shelf. The S-VHS marvel weighed about four pounds, vs twenty plus for the older vintage units.

The solution was a product called Magic Cover® Grip, whose primary use is as a non-slip drawer liner, and for coasters. Then, there's office uses, such as keeping keyboards and trackballs from sliding around Formica desktops — an application I can heartily endorse. The material, a rubbery weave, comes in rolls, typically 12" wide by ten or twenty feet long. It looks like strings of flat 3/16" beads, connected horizontally by wavy threads, and with more threads at 15 degrees off each side of the vertical.

*(Continued on page 14)*




---

Why Can't I Just Copy My Programs To My New Computer? .....	page 2
Freecycle Network — Never Ending Garage Sale .....	page 4
Windows: Safe Mode .....	page 5
Wi-Fi Wireless Internet And Network Availability .....	page 7
Don't Get Caught By Phishing Schemes! .....	page 8
Anti-Spam Programs — Do They Really Work? .....	page 11
Computer Hysteria — Crash! .....	page 15
lections From The Deals Guy .....	page 12

---

## Why Can't I Just Copy My Programs To My New Computer?

By Brian K. Lewis, Ph.D., Sarasota PCUG, Florida [www.spcug.org](http://www.spcug.org)

Let's start this with a discussion of imaging software. Something that many of us use to backup our hard drives. Imaging software makes a very complete "bit-mapped" copy of your hard drive. Bit-mapping means that everything contained on the hard drive is being copied, usually to a compressed file. Generally, imaging software also backs up open files, those that are currently in use on your computer. Most, but not all, regular backup software can only make copies of files that are not in use at the time of the backup. Thus it is very easy for a standard backup to miss some files or to produce a backup of your hard drive that is incomplete, especially with regard to files currently in use by your Operating System (OS). Imaging software overcomes this problem.

So when you buy, build or upgrade to a new computer, why can't you simply use your image file to transfer all of your programs and data from one computer to another? The basic answer is related to the difference in hardware between the two computers. If you are just replacing a hard drive in your computer, you can use the image file to move everything to the new drive. Some imaging software allows you to "clone" the old hard drive to a new drive. That is, providing both drives are connected to the same computer. However, when you change to a new computer with a new motherboard, CPU, chipset, USB ports, sound and/or integrated video are different and require new drivers.

The image file contains a complete copy of the Registry that has all the settings needed to connect to your hardware. It also has all the settings for the software installed on your hard drive. These settings are references to the files on your hard drive that are absolutely essential for the proper operation of both hardware and software. On Windows versions prior to WinXP/Win2K, the registry was contained in two files: system.dat and user.dat. In Windows XP this has changed greatly. The registry is now found in files in hidden folders within the System32 folder and the Documents & Settings Folder. Presumably this is to prevent users from deleting vital files. You can examine the Registry by running "regedit".

However, it is not advisable to make changes to the Registry unless you are a very experienced user. It is quite easy to corrupt the Registry and find that your computer will not run.

The Registry has five main branches in WinXP/Win2K. In earlier versions there were six. These are identified as keys. The most important are HKEY\_CLASSES\_ROOT which has all the file types used by your software; HKEY\_LOCAL\_MACHINE which contains all the information on the hardware and software in your computer.

So if you used the image file to transfer everything from your old computer to your new computer you would overwrite the Registry settings for the hardware and pre-installed software on your new computer. This would very likely prevent it from completing a boot-up. It is really not practical to try to selectively transfer items from the Registry on the old computer. This would introduce other problems. I did a search in the registry for items related to one application. The search found 128 entries. This may not have been all of them. Considering the number of programs you might have on your hard drive, the total number of entries to be transferred is mind-boggling.

Another example, the Windows folder contains many Dynamic Link Library (DLL) files that are associated with the particular version of Windows you have been running. There are also many shared DLL's used by Windows and your application software. How do you know which ones should be transferred and which ones will create problems with your new OS or your new software. Finally, the motherboard, chipset and CPU in your new computer require driver files that are specific to them and very likely are quite different from the drivers used on your old computer.

Faced with this problem, what do you do? The most commonly used solution is to dig out all the original disks for your application software. Find the serial numbers and/or other information

needed to do a new installation on your new computer. Once you have the programs installed you can transfer the data files for each application. This gives you a clean install for your software and, if the programs are compatible with the new OS, you will have no problem running your applications.

This, however, can be a long and tedious process. Also, what happens when you can't find the original program discs? Maybe it was downloaded and you didn't keep the install file or make a copy of it. Or maybe you can't find the serial numbers you need to install some of your programs. Then you have to ask the software manufacturer for help, providing you registered the software when you first installed it. There is another option.

I got into all this because I have just built a new computer and needed to transfer all, or most, of my software to a new computer. I had used two different transfer programs in past upgrades and found them to be somewhat lacking in both accuracy and speed. Since my new computer is running Window XP Pro I also looked at the "Transfer Files & Setting" Wizard. This transfers the Internet browser and e-mail settings between the two computers, providing you are using Internet Explorer and Outlook or Outlook Express. It will also transfer the contents of your "My Documents" folder. It will not transfer any applications. For me this was useless, since I don't use IE or OE.

In my searching for possible solutions I found a program called "Move-Me" from Spearit Software. It is the first transfer program I've found that uses network connections to move programs, data files, settings, etc between your old and new computers. It can also use the USB ports or the parallel ports. These are much slower than a LAN connection. Move-Me also works with removable media that can be read by both computers. Now before you get too excited, this is not a free program. It will cost you \$39.95 for the Internet download version. You can download a trial version that has all the information and help files. It just will not do any transfer until you enter the serial number. That you get only after paying for it. The only thing that makes me nervous about the whole process is that you have to turn off your software firewall and virus checker during the serial number validation process. This validation re-

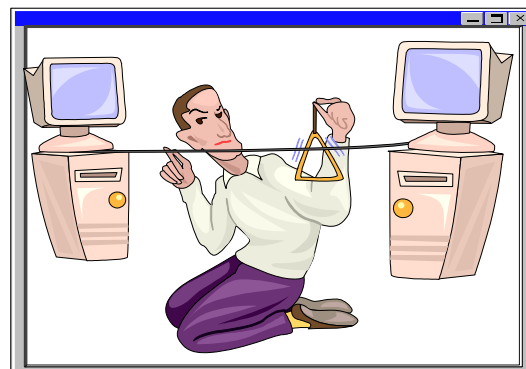
quires that you be connected to the Internet. In my case I still had a hardware firewall in my router, but that's not always sufficient protection. But I went ahead and ran the software. (You know the saying "Fools rush in.....")

Yes, it did work, but with some glitches. First let me say it transferred over 12 gigabytes of programs and data from the old to the new in just over 1.5 hours. Now that is a definite time saving. I had estimated it would take me more than a day to reinstall all my software and move the data files. Only a couple of applications and my external devices needed to be reinstalled after the move. By that I mean printers, scanner and external drive. The big exception was the Bookmarks for Firefox and the e-mail address book and mail settings for Thunderbird. Those I had to transfer manually. Once I found the instructions on the Mozilla websites, the setup went quickly.

The point of all this is, if you buy a new computer, try to get the dealer to transfer your old software as part of the deal. If you do it yourself, a file copy won't work. You need special transfer software like Move-me or Aloha Bob's PC Relocator. However, if you don't have a LAN connection between your computers, expect to spend 1 hour per gigabyte for a USB 2.0 transfer and much, much more time with a parallel port transfer.

Dr. Lewis is a former university & medical school professor. He has been working with personal computers for more than thirty years. He can be reached via e-mail: [bwsail at yahoo.com](mailto:bwsail@yahoo.com).

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.



## Freecycle Network Offers Never-Ending Garage Sale (And It's All Free!)

By Gabe Goldberg, APCUG Advisor and Columnist, AARP Computers and Technology Website

"It's not easy being green", sang Kermit the green Muppet frog. But it's getting easier, as people, corporations, non-profit organizations, and government agencies recognize benefits of conserving and recycling resources of all sorts.

There have always been opportunities such as garage sales, flea markets, and thrift shops for casual/local exchanges of goods. Most of us have likely both bought and sold: giving new life to things we've enjoyed but no longer need, cashing in gifts we can't quite imagine using, and finding economical goods courtesy of neighbors and charitable organizations.

Before we recently moved [[http://www.aarp.org/learntech/computers/life\\_online/Articles/a2005-01-05-preserving\\_tech\\_moving.html](http://www.aarp.org/learntech/computers/life_online/Articles/a2005-01-05-preserving_tech_moving.html)], my wife and I took the opportunity to get rid of anything we thought was surplus. Fortunately, we beat the year-end crush at places like Salvation Army. But in December I did see 18-wheelers being loaded with goods from people who suddenly remembered the tax deduction for making such donations to charitable organizations. And I wondered how much of the tonnage being hauled would actually be sold and reused.

As in many other areas, the Internet lends new sparkle and efficiency to an old idea: using things until they're completely worn out. It's really true that one person's junk can be another person's treasure. In fact, the worldwide Freecycle™ Network [[www.freecycle.org](http://www.freecycle.org)] offers goods at the Internet's favorite price (at least for buyers): free! Perhaps best of all, the Network offers in-person one-to-one transfers making it likely that goodies will go places where they're cherished.

The Web site notes:

The worldwide Freecycle Network is made up of many individual groups across the globe. It's a grassroots movement of people who are giving

(and getting) stuff for free in their own towns. Each local group is run by a local volunteer moderator (good people). Membership is free.

The Freecycle Network was started in May 2003 to promote waste reduction in Tucson's downtown and help save desert landscape from being taken over by landfills. The Network provides individuals and non-profits an electronic forum to "recycle" unwanted items.

Freecycling is interesting because, while it could only be done on the Internet, it has a very local focus. That is, while Web sites and discussion mailing lists draw worldwide clientele, physical transfer of free goods is constrained to relatively small areas.

So Freecycle operates as locally oriented mailing lists. For example, in the Washington, DC region, there's a huge list for the central city (one of the top ten lists with more than 6,000 people), and many suburbs have their own lists with dozens or hundreds of subscribers.

The main Freecycle Web site lists rules and etiquette, which are echoed by welcome messages to new subscribers. It's all simple and reasonable:

Goods offered must be available for pickup in the local area; stick to recycling, avoid politics, spam, and off-topic messages; begin all e-mail subject lines with one of the words OFFER/TAKEN/WANTED/RECEIVED

Rules such as "Keep it free, keep it legal, keep it safe for all ages" prohibit offering or requesting items such as guns, prescription drugs, "adult" material, alcohol, and cigarettes. Pets are OK, though. Only free and physical stuff is allowed; barter/exchanges/sales are barred, as are services offered or wanted.

I'm told that the list is best read in individual messages rather than digests (which collect dozens of messages into one e-mail) since offered items are often snatched up in just a few minutes. A reply in five minutes might be too late!

Messages are transmitted by the Yahoo! Groups Web site [groups.yahoo.com] so list archives can be searched. This allows making sure that no TAKEN or RECEIVED has been sent for the OFFER or WANTED you're about to answer.

Donors can decide which request gets the goods. First-reply-wins is a fine approach, but some decide based on why a person needs something. Businesses can use Freecycle to dispose of goods—for example computing equipment that's usable but not marketable. A company with 25 monitors might offer them to a Freecycle list—perhaps specifying minimum pickup of five. So smaller companies, recycling organizations, or community-minded individuals could collect and redistribute them where they're needed.

A very unscientific analysis of about 40 postings divided into 16 OFFERs, 12 TAKENs, 10 WANT-EDs, and two RECEIVEDs—a very respectable success rate for OFFERs and WANTEDs! As of when I'm writing this, more than 2,000 large and small communities have Freecycle groups with more than 700,000 members. And the Web site gives step-by-step instructions for starting one where there is none. Go forth and Freecycle!

This article appeared originally on AARP's Computers and Technology Web site, [www.aarp.org/computers].  
© AARP 2004/2005.

Permission is granted for reprinting and distribution by non-profit organizations with text reproduced unchanged and this paragraph included. Please e-mail the author, Gabe Goldberg, at [gabe@gabegold.com] when you print or post it.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.



## Windows: Better Safe (Mode) Than Sorry

By Gabe Goldberg, APCUG Advisor and Columnist, AARP Computers and Technology Website

Though the Windows operating system isn't usually dangerous, it includes a special "Safe Mode". This is a handy way to boot a PC to investigate and fix problems. You may have read advice about when to use this, and even how to run it. But scarce and fragmented Safe Mode information can make it sound more exotic than it is.

Windows XP books' indexes provided surprisingly few entries for "Safe Mode". I found the best coverage in two O'Reilly books [www.oreilly.com], "Windows XP Pro: The Missing Manual" and "Windows XP Home Edition: The Missing Manual". Naturally, Google found a gazillion hits. But they're mostly "just the facts" writeups targeting people who already know "what" and "why" and just need "how" information. So this article provides background for this built-in Windows facility.

Over the years, as it became more powerful and reliable, Windows grew significantly from its slender 1992-era Version 3.1 self. There's no free lunch; learning new tricks required more software. But that complexity gets in the way when problems occur. Just as doctors rarely diagnose patients through heavy winter coats, Windows needs to shed layers to expose problems' causes.

Safe Mode slims Windows down, only loading and running specific pieces needed for basic operation. So your video display looks strange in Safe Mode because Windows doesn't load the monitor's specific driver program. This lets you recover from problems caused by buggy drivers you may have just installed. There are other restrictions: you likely can't get online and may not be able to print. But Safe Mode lets you perform tests, fix problems, and install/uninstall programs.

If you think your PC may have a virus or spyware, it's worth installing the antidote in Safe Mode, since some malware prevents installing anti-virus software. If in-

*(Continued on page 6)*

(Continued from page 5)

stalled anti-virus software can't remove a virus, Safe Mode may let it succeed. (Some experts recommend always running virus/spyware scans under Windows in Safe Mode.) If defragmenting your hard drive [www.aarp.org/learntech/computers/howto/Articles/a2004-06-16-defrag.html] never finishes, Safe Mode may remove programs that keep interrupting it. And it lets you erase files that Windows normally says are in use (though only do this when you're sure what you're doing).

Windows XP defines two kinds of user accounts: "administrator" and "limited". An administrator can install/remove software, change settings, etc., while a limited user can only run programs and use facilities. Even if only one account is defined, a secret companion called Administrator is available. Booting in Safe Mode lets you access this account, handy when normal accounts won't work—for example, uninstalling software that doesn't want to leave.

Enter Safe Mode by repeatedly pressing F8 as your PC boots, just after BIOS information displays; then select Safe Mode from the options list. Leaving Safe Mode is simple—just reboot via the Start button and your usual procedure; Windows will return looking normal again, not holding a grudge for being run in diagnostic Mode.

Here's an important point: It's worth practicing booting into Safe Mode when you're relaxed and your PC is working properly. Consider running a PC in Safe Mode to be like starting your car's engine with the hood up at a service station. It's routine; there's nothing alarming about it. But just as you wouldn't want to open the hood for the first time (*Where is that latch release?*) when something is wrong with your car, you shouldn't first use Safe Mode when you're already worried about a PC problem.

And a PS: It's sometimes hard picking between a dozen competing books on a topic. A helpful technique for evaluating choices is searching for a few topics—like Safe Mode—in the books' indexes and judging them on coverage.

This article originated on AARP's Computers and Technology Web site, www.aarp.org/computers, and is copyrighted by AARP. All rights are reserved; it may be reproduced, downloaded, disseminated, or transferred, for single use, or by nonprofit organizations for educational purposes, with attribution to AARP. It should be unchanged and this paragraph included. Please e-mail Gabe Goldberg at gabe@gabegold.com when you use it, or for permission to excerpt or condense.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.



# Wi-Fi Wireless Internet And Network Availability

By Ira Wilsker, APCUG Director; Columnist, The Examiner, Beaumont TX: Radio Show Host

## Websites

<http://www.jwire.com>  
<http://intel.jwire.com>  
<http://www.wi-fihotspotlist.com>

Recently, one of my daughters called me from a major city, and asked me where she could find some free “hotspots” or wireless “Wi-Fi” locations where she could get free broadband wireless internet access. She gave me her street address, and within moments I found several nearby locations where she could access the internet for free using the wireless “802.11b” PCMCIA card she had with her notebook computer. She told me which hotspot she selected, and I gave her the “SSID”, or “Service Set Identifier”, a simple code, usually a name, that identifies a local hotspot.

I recently purchased a new notebook computer for another daughter, and this computer came with an Intel Centrino chipset, which provided integral wireless internet access, where ever available, whether at home or on the road. As she travels around town, at school, or away from home, she can likely access the internet at high speeds.

I travel extensively, and always take my notebook computer with me, as I often find it necessary to check my email, find restaurants, or locate other information on the internet. Through experience, I have found that many hotels, restaurants, airports, and other locations offer wireless broadband internet access either for a fee, or for free. Now before I leave home, I check a website [www.jwire.com](http://www.jwire.com), or its twin sister site supported by Intel, [intel.jwire.com](http://intel.jwire.com), to determine what wireless access is available enroute, or at my destination.

Jwire.com is one of the leading interactive directories of publicly available wireless internet locations, typically using one of the industry standard 802.11 protocols. Standardization, as well as substantial downward compatibility, has ensured that almost all computers equipped with 802.11 type wireless internet hardware can effectively communicate at broad-

band speeds. As I type this, Jwire is listing almost 70,000 public access wireless hotspots around the world. The Intel companion site lists almost 30,000 wireless hotspots in the U.S., and about 40,000 international wireless hotspots. According to the Intel site, the top U.S. cities for public wireless are New York City with over 550 public access locations, followed by Chicago (434 public wireless locations), San Francisco (412), and Seattle (320). Texas is well represented in the top 10 most “unwired” cities with 309 public hotspots in Houston, 250 in Austin, and 192 in Dallas. California is listed by Intel as the state with the most public access with over 5000 locations, followed by Texas with almost 2000 hotspots, Florida with about 1800, and New York with over 1600 public hotspots. It should be emphasized that these numbers are only the wireless sites that allow public access, either for free (sometimes with some strings attached) or for a fee, and does not include the millions of sites that are private wireless networks. The listing also does not include many of the hotel chains that offer free wireless access to registered guests.

Many of the free sites listed are local restaurants, some hotels, many airport terminals, RV parks, and other locations. All it takes to access these totally free and public sites is the SSID of the wireless host and appropriate hardware; the Jwire sites list the SSID's of the public sites. When the wireless access on the notebook computer is activated, the wireless networks within range can be identified, and if accessible, the SSID can be entered, and connections established. It is important that from a personal security standpoint, these public connections are not often encrypted, and can be “sniffed” or picked up by anyone with suitable equipment; sensitive information, passwords, banking, and other critical information should never be sent on an insecure public network.

In addition to the free sites, there are many thousands of publicly accessible but commercial (fee based) hotspots, often in coffee shops, restaurants,

*(Continued on page 13)*

## Don't Get Caught By Phishing Schemes!

By Linda Gonse, Editor, Orange County IBM PC Users' Group, California,  
November 2005 editor@orcpug.org

In one week, I received three emails appearing to be from well-known companies. But, knowing that phishing scams concentrate on disguising themselves as ISPs, retail, or financial companies, I resisted clicking on any of the links which could lead to a bogus website and possible infection by a keylogger program.

Instead, I suspiciously read the text in one authentic-looking email from "PayPal," and studied the full header on the message (see header below).

Looking at the header is easy to do in Outlook Express. Just right click on the unopened email file. Then, left click on Properties. Left click on the Details tab, and click on the button Message Source. (At other times, this also allows me to peek inside an email without officially opening it and letting a virus or worm loose on my system.)

Next, I went to PayPal's site and took a look at their answers about phishing scams.

### Email header from spoofed "PayPal" message

```
Received: from main2.ezpublishing.com ([72.19.192.71])
    by rwcrmxc11.comcast.net (rwcrmxc11) with ESMTTP
    id <20051024211706r1100p6kqre>; Mon, 24 Oct 2005 21:17:06 +0000
X-Originating-IP: [72.19.192.71]
Received: from main2.ezpublishing.com (localhost [127.0.0.1])
    by main2.ezpublishing.com (8.13.1/8.13.1) with ESMTTP id
    j9OLGWBG020266
    for <my personal email address>; Mon, 24 Oct 2005 14:16:32 -0700
Received: (from root@localhost)
    by main2.ezpublishing.com (8.13.1/8.13.1/Submit) id j9OLGWWB020263
    for <my personal email address>; Mon, 24 Oct 2005 14:16:32 -0700
Received: from jamaicans.tv.propagation.net (jamaicans.tv.propagation.net
    [64.182.1.110])
    by main2.ezpublishing.com (8.13.1/8.13.1) with ESMTTP id
    j9OLGVIZ020257
    for <editor@orcpug.org>; Mon, 24 Oct 2005 14:16:32 -0700
Received: (from nobody@localhost)
    by jamaicans.tv.propagation.net (8.11.6p2/8.11.6) id j9OLH7v15310;
    Mon, 24 Oct 2005 16:17:07 -0500
Date: Mon, 24 Oct 2005 16:17:07 -0500
Message-Id:
<200510242117.j9OLH7v15310@jamaicans.tv.propagation.net>
To: editor@orcpug.org
Subject: Paypal Security Measures
From: <service@paypal.com>
Reply-To:
MIME-Version: 1.0
Content-Type: text/html
```

By then, I was sure that the emails I'd received were fake and intended to "phish" out my personal information. All the targeted companies provided email addresses to report fake emails to follow up on them, so I forwarded those I'd received and deleted them from my email program.

The top 10 companies targeted as phishing bait are: Citibank, eBay, US Bank, PayPal, Fleet Bank, Lloyds TSB, Barclays, Earthlink/AOL, Halifax, and Westpac.

According to The Washington Post, "EarthLink gets around 300 phone calls and spends just under \$5,000 per incident. Still, the nation's fourth-largest ISP encounters about 15 new phishing scams a month featuring email that purports to come from its own service.



“Phishers now focus almost exclusively on banks and online shopping sites. During the past 10 months, nearly 60 percent of their attacks targeted Citibank or US Bank, according to the Anti-Phishing Working Group, <http://www.antiphishing.org/>. Earth-Link and America Online are the targets for about 3 percent of the scams.”

**How can I tell the difference between a real PayPal email and a fake one?**

- ▶ The term spoofing and phishing have been used to describe the act of collecting personal information using a fake email in order to commit identity theft, credit card, and Internet fraud. If you click on a link included in an email you’re not sure is from PayPal, make sure the address at the top of the browser window you’re brought to reads exactly **www.paypal.com**.

- ▶ PayPal emails will address you by first name, last name, or business name, and NOT by Dear PayPal User or Dear PayPal Member.
- ▶ If you are ever uncertain about the validity of the email or the email links, open a new web browser window and type in **www.paypal.com**.
- ▶ If you think you have received a fraudulent email, forward the entire email to **spoof@paypal.com** and then delete it from your email account.

If you receive a suspicious email from a familiar company, follow PayPal’s guidelines to help you separate fake emails from real ones. (Just substitute the name and web address of another company for PayPal’s.)

*(Continued on page 10)*

**This email is not from PayPal**  
 Clues are: no personal salutation,  
 European-style date, misspelling (“bellow”),  
 and instructions urging you to log into your account.



**PayPal Security Measures!**

We are contacting you to remind you that: on 22/10/2005 our Account Review Team identified some unusual activity in your account, one or more attempts to log in to your PayPal account from a foreign IP address.

IP Address	Time	Country
80.53.1.130	22/10/2005 15:05:08 PDT	Poland
80.53.255.174	22/10/2005 15:07:58 PDT	Poland
141.85.99.169	22/10/2005 15:13:09 PDT	Romania
141.85.99.169	22/10/2005 21:28:08 PDT	Romania
195.61.146.130	22/10/2005 21:33:43 PDT	Romania

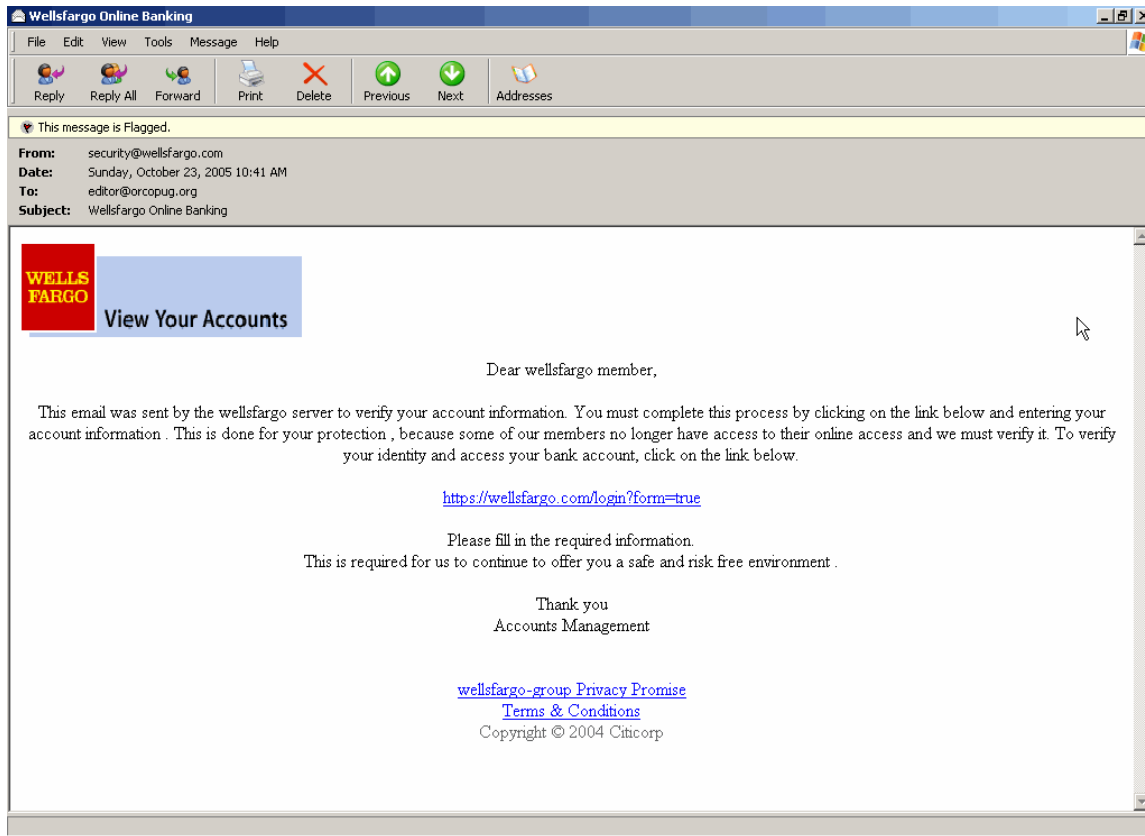
In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. To secure your account and quickly restore full access, we may require some additional information from you.

To securely confirm your PayPal information please go directly to <https://www.paypal.com/> log in to your PayPal account and perform the steps necessary to restore your account access as soon as possible or click bellow:

To continue your verification procedure [click here](#)

Thank you for using PayPal!  
 The PayPal Team

## What about this Wells Fargo email — is it real or is it a fake?



### Answer

Notice the top of the message. It has no personal information (such as your name or account number). Wells Fargo is one word and it is not capitalized.

Now, take a look at the email's header (condensed due to space limitations). It gives other indications that this email is meant to phish out your personal information. Note the originating domain and the notation "it may be forged" that was added to the header by our web host's server.

### The Wells Fargo email is fake.

Received: from web1.brainwavebb.com (216-8-70-66.brainwavebb.com [216.8.70.66] (may be forged)) by main2.ezpublishing.com Sun, 23 Oct 2005 10:40:33 -0700 Received: from nobody by web1.brainwavebb.com with local (Exim 4.52) id 1ETjqA-0006yy-11 for editor@ orcopug.org; Sun, 23 Oct 2005 12:41:02 -0500 To: editor@ orcopug.org Subject: Wellsfargo Online Banking From: Reply-To: X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse: Primary Hostname - web1.brainwavebb.com Sender Address Domain - web1.brainwavebb.com

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

## Anti-Spam Programs — Do They Really Work?

By Vinny La Bash, vlabash@home.com, Member of the Sarasota Personal Computer Users Group, Inc., Sarasota PC Monitor February 2006 [www.spcug.org](http://www.spcug.org)

Among the most effective anti-spam programs are the ones that use some kind of approval based email management system. They work by constructing a “white list” of permitted email addresses, accepting mail from anyone on the list, and rejecting everything else. The program initially sniffs through your contact list, inbox, and other email folders, organizes the email addresses it finds, asks you if you want to add or change anything, and the list is complete.

From that moment on, any incoming email that is not on the list is considered to be spam, and is automatically exiled to a quarantine folder or wherever you decided it should go during installation. The programs do work as advertised, which is both their greatest strength and their greatest weakness. Here’s what you need to know before installing one of these puppies.

**Scenario 1:** A friend you have lost contact with over the years sends you an email. That friend’s email address is not on your white list. Unless you have a quarantine folder where unapproved email is sent without automatically deleting it, you will never see this email. You have to check your quarantine folder, at least occasionally, to see if there are any false positives residing in there with all the junk. How much time will this take? Who knows? None of the programs mention this in their promotional material or specification lists.

**Scenario 2:** You install a new program or device and run into difficulties. The troubleshooting guide sends you to an email address where you can get a solution to your problem. You remember to add the email address to your white list. You wait for a reply, and wait, and wait. What happened?

Your problem was given to a technical representative who has an email address different from the general support address. You don’t see the reply unless you check the quarantine email folder, assuming that in your efforts to rid yourself of all spam you did not specify that anything not on your white list be automatically deleted.

**Scenario 3:** You order something from an online merchant and before your order is shipped the merchant emails you to ask whether you want the white one or the black one. The query has been rerouted to the quarantine folder because the person trying to contact you has an email address that is not on your white list.

**Scenario 4:** Your spouse sets up a Yahoo! Email account for the sole purpose of sending you a surprise Valentine’s Day email. For no apparent reason you are getting the silent treatment. You ask, “What’s wrong”? Your spouse replies, “Nothing”.

**Scenario 5:** Your granddaughter just got an email address of her own. She sends you a message, and can’t understand why you won’t answer. She asks her parents “Why doesn’t grandpa love me anymore”?

We could go on, but you get the general idea. 99.99% of all real spam will be banished from your sight, but the very few legitimate emails identified as spam will very likely be the ones you most want or need to see. Some anti-spam programs have a “sender confirmation feature” that automatically sends a personalized notification to anyone whose message has been quarantined. Simply replying to the challenge causes the original message to be moved to your inbox, and allows their email address to be added to the white list. Legitimate senders can respond to these challenge messages, but suppose that for whatever reason they don’t. Does a seven year old grandchild really understand why she needs a grandparent’s permission to send an email?

What you end up with is a time-consuming process of back and forth emails. Why should every email first contact have to be sent twice? What a waste of time. This might be acceptable if your email volume is very low, but who are we kidding. Simply establishing an email account anywhere will get you a boatload of spam. ISP level filters are a joke. How many essays do you want to compose explaining why someone needs “permission” to send you an

(Continued on page 14)

## Selections From The DealsGuy

**Bob Click, Greater Orlando Computer User Group**

### How Secure is Your System?

I read an article in Information Week magazine that was both amusing and interesting. It concerned a company whose CIO hired security investigators to test how good their system stood up to being infiltrated. The director of the network operations center was sure they couldn't break into the systems or facilities, but they very soon proved him wrong. Some of the weaknesses were so stupid that I had to chuckle, such as many of the passwords for work stations were written on a note taped to the machine or hidden under the keyboard. They gained access to limited access places just by calling the receptionist and telling them that some agents were coming in to do an audit and needed access, which was easily granted to the very people who made the call. Office keys were sometimes in the secretary's desk. You can find this article at <http://www.informationweek.com/management/showArticle.jhtml?articleID=177100115> and you'll find it enlightening.

### Great, The Bundle is Back

Colleen Toumayan from Executive Software sent a message letting me know that their "bundle" is back. For a limited time you can get both the award winning Diskeeper 10, Home Edition, and Undelete 5, Home Edition, products for just \$49.95 plus S&H. I have never heard anything but praise about these fine products. Mine is not the latest, but it always works well, and fast. Use this link to order: <http://purchase.diskeeper.com/checkout/addtocart.aspx?Item=1382>.

### If You Like Games —

From the creators of "Zzed" comes a new game of Wonderlines by NevoSoft. Wonderlines is a remake of a popular game. Only balls and lines remind you of its predecessor here and the rest is covered with the charm of novelty. A player will see a new bonus system, a new intricate game play structure and a fresh interface design. The music and visuals are great.

Puzzle, Action, Zen Way modes are different, yet each requires special skills. Generally, the game stayed nearly the same yet now you match several balls of one color in a line, but also blow them up over certain brown squares. The challenge of the game is to remove all brown squares in each level. 70 levels of the game are very different one from another. Another merit of the game is new bonuses: the miraculous multicolor ball, dazzling diamond and clever hammer, triple or quadruple bomb and others, which help a lot while making your way through Wonderlines.

Wonderlines runs under Windows 98/ME/XP/2000 and costs \$19.95 (USD). NevoSoft offers a 30% discount to user group members if you use this link:

[https://www.regnow.com/softsell/nph-softsell.cgi?item=8323-16&ss\\_coupon=NEVO-GPCU](https://www.regnow.com/softsell/nph-softsell.cgi?item=8323-16&ss_coupon=NEVO-GPCU).



### Washington Area Computer User Group (WAC) Meetings

WACUG Meetings will be held on May 20th, 2006, 12:30 PM to 3:30 PM. at the Fairfax County Government Center, 12000 Government Center Parkway, Fairfax, VA.

You do not need to be a member to attend. For more information on WAC meetings and events, call the WAC AnswerLine (voice) at (703) 370-7649. Also see WAC's Web Site at

<http://www.wacug.org/>

*(Continued from page 7)*

hotels, bookstores, some airport terminal areas, and other locations. These hotspots either require a subscription to a service, such as a cellular phone company or other third party, or a daily or hourly fee for access. Generally, since these pay services require some type of access code, they are slightly more secure than the free public sites, but are still usually accessible to a hacker with commonly available but illicit software. Again, it is a good practice not to type any sensitive personal information while on a publicly accessible wireless network. Some of the commercial hotspots offer "WEP", or wireless encryption protocol, which makes it more difficult for unwelcome third parties to listen in on internet communications, but the methods for cracking WEP have been widely published, and are now only considered to provide marginal security.

One warning about wireless internet access; it is illegal to access a wireless network without the consent of the owner, despite the fact that studies have indicated that about 80% of all private wireless networks, both workplace and home based, are not adequately protected, and can easily be picked up and accessed by anyone who wants access. A popular hacker method of gaining "free" broadband internet access

is driving around town with a notebook computer with 802.11 hardware, and logging the wireless networks found, with those same networks often broadcasting the SSID necessary for access. This practice is called "wardriving". In major cities, marks are drawn on sidewalks and the outside walls of buildings in a similar escapade, "warchalking" where SSID's and other relevant information is written for all to see, and access. Locally, in a security demonstration, a security consultant drove around the business district of town, and logged hundreds of wireless networks, 80% of which were easily accessible, as they were not properly secured. These included such sensitive locations as banks, law offices, retail stores, medical facilities, and other choice locations for hackers to penetrate.

Use the Jwire sites to find wireless access, as I do, but be totally aware of the risk and security implications of broadcasting critical information. There are a variety of hardware and software utilities that can be utilized to harden wireless access, and some of those will be discussed in a future column.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

*(Continued from page 12)*

Registered customers are entitled to the unlocked game play and lifetime technical support. An evaluation version of the game, that offers 60 minutes of game play, is available as a free download at [http://www.nevosoft.com/wonderlines/wonderlines\\_demo.exe](http://www.nevosoft.com/wonderlines/wonderlines_demo.exe).

Be aware that this vendor has no privacy statement on their Web site about protecting your information.

For more information, visit us at <http://www.nevosoft.com>  
Product page link: <http://www.nevosoft.com/downloadable-game/en/games/wonderlines.html>

This column is written to make user group members aware of special offers or freebies I have found or arranged, and my comments should not be interpreted to encourage, or discourage, the purchase of any products, no matter how enthused I might sound. Bob (The Cheap skate) Click <[bobclick@mindspring.com](mailto:bobclick@mindspring.com)>. Visit my Web site at <<http://www.dealsguy.com>>.



*(Continued from page 1)*

With scissors, I cut a piece of the Grip material to a hair larger than the horizontal and vertical outside dimensions between VCR's feet, and placed it under the unit. Now it feels like the shelf would topple before the VCR would move — no skidding at all. I've used the Grip material under my CD-R / DVD player — that was so light pushing any of the buttons slid it around the top of the audio cassette deck it sits on. I've used it under my speakers, to keep them from walking around their shelves, and on top of the TV, under the center channel speaker.

As you'd expect, Grip works great for lining tool boxes, keeping the contents from rattling around, and, in light colors, lets you spot the item you're looking for. At seven bucks for a twenty foot roll at Linens and Things, it's a bargain, IMHO. I've purchased the material in "natural" color — which looks like "computer beige" — but there are lots of choices, at least on the manufacturer's web site:

[http://www.kittrich.com/MC/Grip/mc\\_non\\_adhesive.htm](http://www.kittrich.com/MC/Grip/mc_non_adhesive.htm)

### **Gotta Maintain That Protection Software**

Virtually everyone that uses a computer today is connecting to the Internet. Using the 'Net has become the "killer application" for current computer users, much as the VisiCalc and Lotus 1-2-3 spreadsheets were the apps that got personal computers through the door of corporations in the early eighties. With the Net has come viruses, adware, spyware, and other forms of malware. While awareness of these risks, and basics of combating them are generally known, a fair number of users fail to go beyond the first step — acquiring software to help prevent the bad guys from disabling your computer.

Let's consider an anti-virus product, such as Symantec's Norton Anti-virus. Most such products come with their protection turned on, automatically checking the manufacturer's web site for updates to the AV definitions, which are then automatically downloaded and installed. Also, such programs are generally also set up to scan your computer at a specific time each week, to find and remove any viruses found. But — do you know these things are true? Have you checked the program options for the default settings? For example, if the default scan takes place at 8 PM

Friday evening, and your computer isn't turned on then — quite simply, you won't necessarily catch any viruses that have crept in to your machine. Does your software have a "status" page that reports when the latest scan took place, and reports the date of the AV definition files being used?

So, you know your machine is automatically getting the updated AV definitions, and they're being installed, thanks to a pop-up window when it occurs. However, what about updates to the software itself? Symantec's products generally include a "live update" feature. Invoking this connects to the appropriate update web site, and information is exchanged with your computer to determine what updates are needed, not only "AV definition files" but patches to the programs that make up the AV software package. These need to be downloaded and installed. Are you following this approach with your software?



*(Continued from page 11)*

email? I don't respond to challenge email. Why should anyone respond to mine?

You can check your quarantine folder regularly, but with the huge quantity of genuine spam generated and thrust upon us daily, it's too easy to overlook a legitimate message. When you finally delete the spam, there is a good chance that among the junk a valuable note is lost forever.

After using one of these programs for several months, I decided that I would much rather delete spam manually, rather than run the risk of missing an important legitimate email. No computer program, no matter how expertly crafted or trained, can ultimately determine what emails I do or don't want to read. Even after being married for 38 years, my wife still can't read my mind. How do I expect a dumb computer to do it?

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

# Computer Hysteria — Crash!

By **Berry F. Phillips**, Member of the Computer Club of Oklahoma City and a regular writer for the **CCOKC** website and the eMonitor [bfpdata@gbronline.com](mailto:bfpdata@gbronline.com)

Crash! Crash! That was the sound of Stephen King's sledgehammer bashing the car that hit him while jogging. Perhaps he thought Christine from his earlier horror novel had come back to haunt him!

Crash also strikes terror in the hearts of computer users. According to the Pew Internet and American Life Project approximately two thirds of Americans use the Internet and about 87% of them through connections in their homes. While there is no research data on the number of computer users that cannot master their computers, there is evidence of anger and frustration with computers that could escalate into what one psychologist calls "computer rage."

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

University of Maryland Professor Kent Norman says, "Men and women are taking out their frustrations on the computer and unfortunately, sometimes misdirecting it to other people." Norman, who directs the Laboratory of Automation Psychology and Decision Processes at the University, conducted an online survey where twenty percent of the respondents admitted they dropped a computer on the floor out of anger. They described smashing, microwaving, and cursing their computers. One claimed he threw his laptop in a fryer and several claimed to have shot hardware. The study further suggested computer users were most annoyed by: e-mail snafus including spam, waiting while a computer completed a simple task, having to redo something because of a glitch and having to upgrade obsolete programs. Microsoft ranked high on the list of objects of ire. With the increased popularity of wireless networks, DVD players, and game systems, the possibilities of irritations are almost endless.

*(Continued on page 16)*

## NCTCUG Information

NCTCUG, Post Office Box 949, Arlington VA 22216

Club Information call: 301-577-7899

Web Site: [www.nctcug.org](http://www.nctcug.org)

### Officers and Directors

All officer terms expire 2006

President	Jim Rhodes	703-931-7854
1st VP	Ron Schmidt	301-577-7899
2nd VP	Roger Fujii	703-426-5917
Treasurer	Paul Howard	703-860-9246
Secretary	Roger Arnold	301-946-7770

Director: term expires

Bill Walsh	2006	703-241-8141
Charles Throneburg	2006	703-476-6283
John Keys	2006	703-451-0896
Nick Wenri	2006	703-759-3938
Fred Cook	2007	703-815-1423
JJ Davies	2007	703-379-9222
Sy Fishbein	2007	703-536-5894
Dean Mires	2007	301-931-2400

### Article Submissions

Articles, helpful hints, and other items of interest to readers of the NCTCUG Journal are always welcome and will be published as soon as possible after submission. Priority is given to members' contributions. Items may be submitted via modem to the BBS or on diskette. Submissions to the BBS should be uploaded to the Newsletter Conference and a message left for the Editor. Files should be straight ASCII, unformatted, with C/R only at end of paragraphs; no indents for paragraphs should be used. Preferred format for diskettes is MS-DOS 3 1/2 720k or 1.44Mb. Diskettes in other formats may be submitted but there will be a considerable delay in processing. If absolutely necessary, items may be submitted in hardcopy only but these will also meet with delay.

### Membership Policy

The National Capital Tandy Computer Users Group, Inc. is a non-profit [501(c)(3)] organization founded in 1978 to educate users of all Tandy computers and MS-DOS compatible computers. Membership dues are \$25.00 (U.S. Funds) per year, with a \$5 surcharge for international mail. Membership in NCTCUG includes membership in all SIGs, access to the BBS and software libraries, and subscription to the Journal published 8 times per year. Applications may be obtained at any club meeting, by downloading from the BBS, by calling one of the officers or board members, or by writing to the club. A sample newsletter, membership application and related information may be obtained by enclosing \$1 and mailing your request to Jim Rhodes, 201 S. Kensington Street, Arlington VA 22204.

### Advertisement Policy

Members' advertisements: Ads are accepted from members for non-commercial purposes at no charge. Copy should be sent to the Editor in the same format as article submissions. Commercial Advertisements: Ads are accepted from commercial advertisers at the rate of \$60 per full page, per appearance, with discounts for multiple insertions. Smaller ads are priced accordingly. Payment for ads must be made in advance of appearance. Advertisers must supply a permanent address and telephone number to the editor.

### Reprint Policy

Permission to reprint articles from the NCTCUG Journal is given to school, personal computer club, and nonprofit organization publications, provided that: (a) NCTCUG Inc. receives a copy of the publication; (b) credit is given to the NCTCUG Journal as the source; (c) the original author is given full credit; and (d) the article author has not expressly copyrighted the article. Recognition is one means of compensating our valued contributors

### Newsletter Staff

Editor  
Blair Jones 202-362-7344  
[bjones44@bellatlantic.net](mailto:bjones44@bellatlantic.net)  
Exchange Newsletter Editor  
Ron Schmidt 301-577-7899

### COMPUCENTER BBS

Is no longer in operation. It has been replaced by the 'compucenter' mailing list at <http://groups.yahoo.com/>

<http://groups.yahoo.com/group/compucenter/>

### If you are moving

Please send your change of address to the club PO box as soon as possible to avoid missing issues.

(Continued from page 15)

You can lower your cyber blood pressure by taking some preventative medicine. Increase your knowledge to make yourself a more-informed user. Join the Computer Club of Oklahoma City and network with other computer users and learn from their experiences (misery loves company!). Do NOT go on the Internet without a regularly updated and weekly-maintained complete computer security system including antivirus, anti-spyware and firewall software. (Not having the money for commercial applications is no excuse as there are several excellent freeware security software programs available online. Often forgotten is a good registry and unnecessary-file cleaner that has automatic backups, which can substantially reduce your crashes. Defrag weekly if needed and scandisk at least once a month. Do not forget to make an emergency boot disk.

Finally, in case of a crash, do not panic. Write down what you did immediately prior to the crash, and any instructions you receive from your computer. Make sure you have been taking fruit to lay at the feet of your computer guru or lay money on your friendly computer tech. The life you save may be your own computer. SOS stands for Save Our System!

May 2006

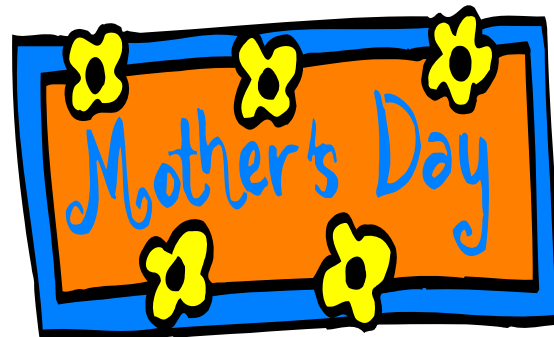
1st Wed. (5/3)  
7 p.m. General Meeting

4th Wed (5/24)  
7 p.m. Internet SIG

3rd Monday (5/15)  
7 p.m. Board of Directors



All meetings are at **Carlin Hall**, 5711 S. 4th St., Arlington VA: East off of Carlin Springs Rd, just south of Arlington Blvd/Route 50.



NCTCUG, Inc.  
P.O. Box 949  
Arlington VA 22216

**First Class**

