

# The NCTCUG Journal

www.nctcug.org

August/September 2004

Volume 27 Issue 5

## Keeping Up

By Paul Howard, NCTCUG

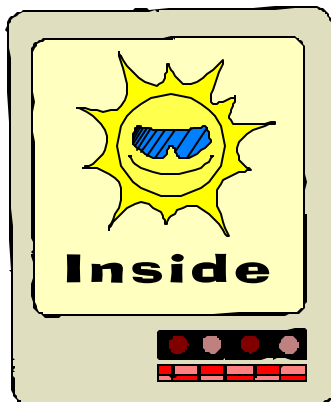
Every few years the NCTCUG gang has to do what all of us face at home — cleaning up and organizing. We had such a session in place of a board of directors meeting in June, and went through much of the group’s accumulation in the Carlin Hall attic. Over the years, our members have generously donated monitors, computer systems, reference books, VCRs, and other tech related materials.

In our collection, we had a number of items that were ready for recycling, such as monitors that no longer reliably displayed all three basic colors that make up a CRT display. We had a VCR that would no longer rewind, and several other technology artifacts we just felt were no longer likely to be useful. We disposed of a 386 system that we doubted would be of much use to anyone after stripping out several drives. We also took the opportunity to label several recently donated items as NCTCUG property.



Over the last few months, Bill Walsh and John Keys have presented programs in the APCUG “Presentation in a Box” series from microprocessor manufacturer Intel, on topics of “Digital Home Experience” and “Hyperthreading Technology.” We were pleasantly surprised to receive an email from Kathy Whittle of Webworking Services, who coordinates the distribution of the Intel programs, offering NCTCUG a motherboard and Pentium 4, 3.06 GHz processor donated by Intel.

*(Continued on page 15)*




---

Computer Rage .....	page 2
Anniversary Of Computer Virus No Cause For Celebration.....	page 4
E-Mail Is 32 Years Old .....	page 6
Virus Attacks Continue At Record Rate .....	page 8
PCI Express: Say Goodbye To AGP And PCI Slots .....	page 9
Computer Memory.....	page 11
Selections From The Deals Guy .....	page 12
<b>Election Notice .....</b>	<b>page 6</b>

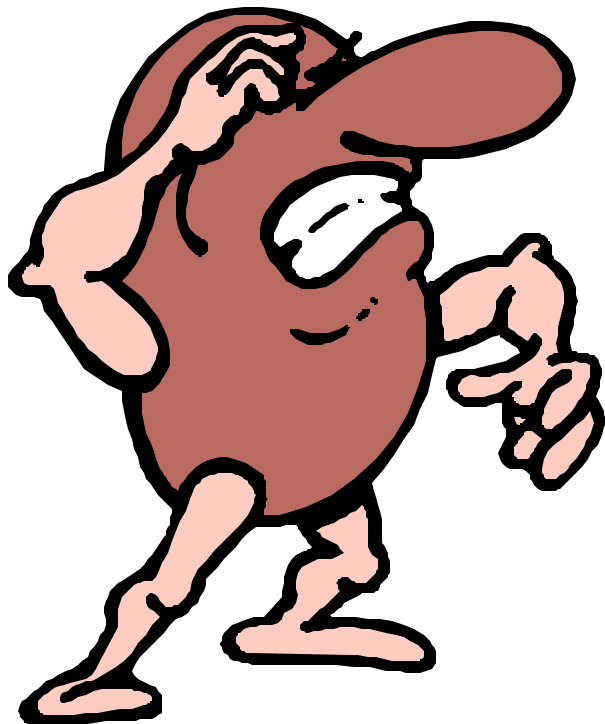
---

## Computer Rage

By Elise M. Edgell and Jim Sanders, North Orange County Computer Club, California  
[EliseME@aol.com]

I have heard about road rage for years and have even seen instances of it. For some people just putting them behind a steering wheel gives them an angry feeling toward all other drivers on the road.

I am seeing a similar reaction with some people as soon as they are in front of a computer keyboard. Suddenly they are no longer reasonable, rational people using the computer to make their life better. They react as put-upon individuals that are using a tool, which they would rather not use, can't really see the benefit in using it, would rather be doing anything else other than sitting there in front of their computer, and they do not want to learn anything about their computer other than how to use the applications that they have been forced to use because of outside pressure. They act as if it is an imposition to have to learn anything more about their computer than how to turn it on. They see no useful value in understanding any of the workings of the computer. They have much more valuable use for their time than to spend any of it learning useless (in their estimation) information.



Unfortunately, not only do we have the "Computer Rage" group that think it is chic to hide behind their rage with an "I would rather work harder, than smarter" attitude, there are others. Some groups that come to mind are the "I am too old to learn this computer stuff," the "I am too dumb to learn this computer stuff," the "I am so computer illiterate that I don't even know how to turn one on, and proud of it," and the "I would probably do something wrong and break it" group.

What could be some of the reasons for these attitudes, reactions or myths to using a computer?

One reason is that computer software and hardware companies have fostered the idea that in today's world computers are so sophisticated that they can be run without any necessity for the user to learn the basics. As an example, the Windows operating system installs with many of its defaults set to "protect" the user from much of the really useful information that is needed for intelligent operation of the computer. The problem with that is, if the information is hidden, the user may be unaware of needed information.

So why should you make the effort to learn more about your computer? Even if you are using a computer under duress (real or perceived), once a computer is an integral part of your personal or business life it is very upsetting for the computer to be unavailable to perform the tasks that you've come to depend on.

When a problem occurs with your program or with your hardware, instead of just feeling abused, put upon, frustrated, helpless, or mad, you will have some options if you learn some of the basics. You will be able to take care of some of the simple and common problems yourself. When you get the "Disk A: is write-protected" error message while trying to save a file to the floppy disk, you will know that all you have to do is take the floppy out of the drive, slide over the write-protect tab to cover the hole, and

re-insert it in the drive. The problem was solved in ten seconds, no rage, no anger, no anxiety, actually, no real problem. It was just one of those things that happen and have to be dealt with.

Even if you can't solve the situation on your own, you will be able to communicate the problem in understandable terms. This makes it possible for you to ask for help over the telephone, or even on the Internet. You'll also need to know when you really need help and to know if the "help" you are getting is valid. Last, and far from least, most windows have a "Help" menu, and there is always the "START" button and general "HELP" option. But once again, if, for whatever reason, you have not bothered to learn some of the basic concepts and terminology, you won't be able to ask the right question, or understand the answer if you stumble across it.

I have also heard people say. "I watch TV but I don't have to learn how it works, why should I have to learn how to use my computer?" My response is that today's computers place an unbelievable amount of access to information, knowledge, and creative programs at your fingertips. For chump change (don't know what that means? — look it up on Google.com) you can buy a nice computer and access to the Internet. As soon as you buy that combination you have an almost unimaginable power sitting on your desk. Power that just a few years ago only governments and large corporations could afford. Once you are on the Internet, most of the information, a lot of the knowledge, and quite a few of the applications are free! You may have seen the TV ad showing a one man garage shop company that looks like a large company because of what the computer can do. This is a true story, not an advertiser's pipe dream. Information is power and the Internet makes information available on about any subject. Aside from the "chump change" what does all this power cost? The willingness to spend the time to learn how to use it!

I am no longer envious of people who live near a large library. I use the Internet to answer many of the questions which I think about but forget before I get to a dictionary, encyclopedia, or other paper research material. Now I can get an almost instantaneous answer and can ask to be notified by e-mail when a certain topic comes up in the news. For ex-

ample I used this recently after I read a murder mystery based on a deadly chemical named sodium azide. I had never heard of it before. I searched the Internet using Google and found many articles about it and its deadly properties. This chemical is readily available and widely used. I was concerned enough to use a feature of Google to send me an e-mail when sodium azide is in a news story.

Wouldn't you be willing to invest some of your time to be able to really use this type of power? What about really learning some of the abilities of the software that is probably sitting on your computer? Have you ever really looked at the features of WordPad in Windows XP? Have you ever clicked on help in WordPad? Did you know that the "Help Menu" in WordPad contains a "Help on how to use Help" section? Are you taking digital photos? Are you in sales? Do you have a disability? Of course you can find use for some of the more advanced features of your software. The problem is you won't ever know what these may be, unless you expend some effort to learn what is possible.

Once you decide that learning more about the potential of your computer is a benefit to you, it makes it a lot easier to find the time and energy to accomplish this.

Understanding goes a long way toward the feeling of being in control. When you feel in control of your computing experience, the irrational feelings of rage will probably go away or at least be minimized. This doesn't mean that you will no longer get mad or upset with your computer, far from it, just that you will be more likely do it for a real cause.

How do you acquire the information and skills you need to feel in control of your computer? One good way is to go to a computer users group. Unfortunately, if you are the person this article is about you are probably not getting this newsletter. My suggestion is that those of you who are getting this newsletter give a copy of this article to your friends that have 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.

## Anniversary Of Computer Virus No Cause For Celebration

Beverly Rosenbaum, Member, HAL-PC (Houston Area League of PC Users), Texas

Over several decades, viruses and worms have grown from academic exercises to online threats, wreaking havoc on millions of computers worldwide.

Not everyone agrees on their exact origin, but they date back at least 20 and maybe even 30 years. The idea of using the term “virus” to describe unwanted computer code was first published in 1970, and some accounts detail the spread of the first virus in 1975 as simply the distribution of a game on UNIVACs (Universal Automatic Calculators). The virus Elk Cloner that infected Apple IIs followed in 1982. In 1984 a professor at the University of New Haven wrote a research paper describing possible threats from self-propagating viruses and explored potential defenses against them. He wanted to further investigate antivirus countermeasures, but the National Science Foundation denied his request for funding.

The term “worm” was first used in a 1982 paper by researchers at the Xerox Palo Alto Research Center to describe the automated program they used to update an Ethernet performance-measuring application. However, a bug in the program eventually crashed all 100 of the experiment’s computers. The paper cited a 1972 science fiction novel describing a “tapeworm” program spreading around the global networks as the inspiration for the term.

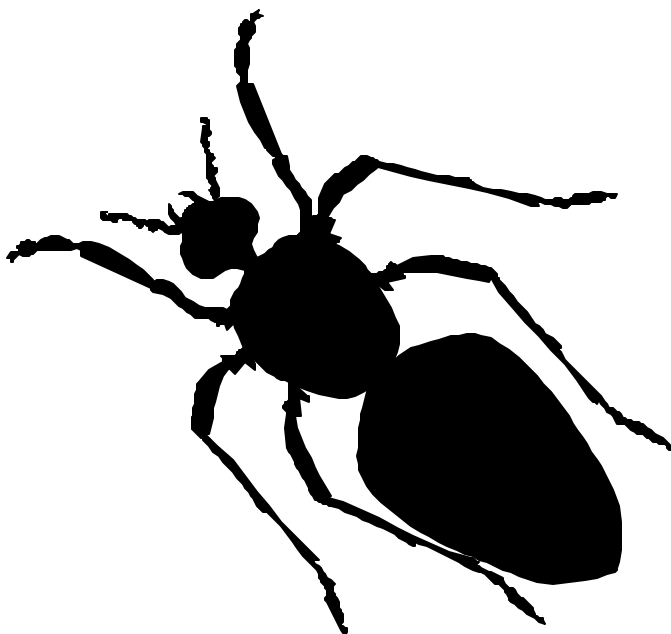
Many virus historians believe that two Pakistani brothers created the first IBM personal computer virus in 1986 as a way to advertise their company, Brain Com-

puter Services. They programmed the Brain virus to overwrite the boot instructions found at the start of system disks, displaying the message “Beware of this VIRUS.... Contact us for vaccination...”

That was only the beginning of viruses that infected floppy disks, hard disks and files. Although viruses and worms took more than a decade to emerge in significant numbers, they soared in subsequent years. By the end of 1990, about 200 viruses had been identified. Today, that number has jumped to more than 70,000.

Even if viruses aren’t designed to be intentionally malicious or dangerous, there can be unexpected results if they get outside a controlled environment. The exponential doubling of viral code greatly magnifies minor errors and becomes the difference between a harmless prank and a devastating attack. The ability to propagate across the Internet has allowed this kind of malware to spread very quickly. Although many programs quickly fizzled out, others have far outgrown the intentions of their authors, and small modifications of the original code produced new variants that continued the attacks.

Later, worms evolved into two categories. Some camouflage themselves as interesting e-mail attachments, which execute when opened, infecting systems and mailing themselves to every name listed in the computer’s address book. Other worms need no human interaction, infecting computers that have certain security flaws and then using the new host to scan for more computers with the same flaw. These worms are modeled after the Cornell Internet Worm, which overloaded an estimated



3,000 to 4,000 servers, or about 5 percent of those connected to the early Internet, in November 1988.

The growth in popularity of computers and Internet use along with the vulnerability of the Windows platform and other Microsoft programs have allowed the rapid spread of viruses and worms. In 1995 Microsoft accidentally shipped the first macro virus that could infect Word documents. The Concept macro virus rewrote the rules for viruses and they began spreading via e-mail and the Internet. In the early days of viruses it would take months for a virus to spread into the wild. The first successful mass-mailing computer virus was Melissa, a macro virus that started spreading in March 1999, and contained a lot of code from previous viruses.

Today, a virus can spread around the world in a matter of minutes, and virus writers quickly pass techniques for creating the latest worms by posting their toolkits in the virus-exchange underground. Many worms are written in one of several scripting languages, which can be read by even semi-knowledgeable virus writers and changed to release variants in only hours after a major virus epidemic. For example, virus writers latched onto LoveLetter, which struck in May 2000, and cranked out more than 40 variants.

Boot viruses began to diminish in 1997 as macro viruses flourished until 2000, when they too declined as worms began a steady rise. Soon the worms dominated the top ten variants of malicious code. Two months after the major Code Red worm attack of July 2001, Nimda hit the financial industry hard, giving Microsoft a security wake-up call and illustrating the dangers of self-reproducing threats that used multiple vectors of attack. Nimda infected computers through the same flaw Code Red used but also infected shared hard drives, spread itself through e-mail, and created Web pages that spread the worm. Even after Microsoft issued patches for the vulnerabilities, most people were apathetic and failed to download and apply the patches.

To stave off future attacks, companies and Internet providers began filtering e-mail attachments at their gateways, the connections to the Internet. Antivirus software companies try to beat worms at their own

game by distributing new virus detection faster than the viruses can spread. However, if a new virus doesn't match any of the types contained in the filtering software's definitions, the scanner won't flag the attachment as malicious code.

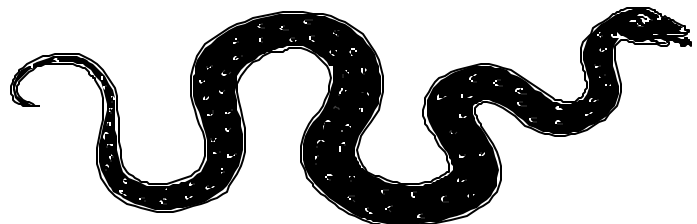
The latest Mydoom virus was effective because it initially passed the scanning software. It posed as a harmless text file containing an e-mail message that claimed to be a failed mail transaction from a colleague or friend, offering the believable explanation that the original message had to be translated into a plain-text file for delivery. Even some savvy recipients were duped to open the attached file, which was really an executable file that included a malicious virus. The innocuous subject line of the infected e-mail was "Hello," "Server Report," "hi," "Mail Delivery System," "Mail Transaction Failed," "Status," or "Error."

The SCO Group, target of the original worm's denial of service attack scheduled for February 1, 2004 (its fourth in the past 10 months), offered a \$250,000 reward for information leading to the virus author's arrest. When a variant targeted Microsoft, they offered a similar reward.

MessageLabs reported that in the first 4 days it had trapped over 5.5 million copies of infected e-mail headed for its clients. At one point, one in every 12 e-mails was laced with this worm, compared to last year's SoBig virus outbreak, which peaked at an infection rate of 1 in 17 e-mails. Other antivirus companies reported that Mydoom (also known as Novarg) generated more traffic than any e-mail worm in history.

Viruses that have multiple vectors are the worst threat because they can send e-mail, perform a distributed denial of service attack and open a back-

*(Continued on page 6)*



(Continued from page 5)

door. The most problematic viruses have been the most recent. The SQL Slammer broke all records for the speed at which it was able to spread, to the point of disabling ATM machines and bringing Internet traffic to a halt. The SoBig Project employed spammed worms to infect PCs that could be used to install spyware, steal financial credentials, act as a front for spamming operations, launch DDoS (distributed Denial of Service) attacks on anti-spam sites, and allow spammers to be virtually untraceable.

Although many worms are benign, they demonstrate serious vulnerabilities, and the sheer volume of traffic can cause effective denial-of-service attacks because of bandwidth consumption. While IBM-compatible computers are the initial target, the network downtime and cleanup costs affect computers on all platforms. Mail servers are overloaded with the sheer volume of bogus messages, and automated responses from filtering software multiply the problem.

Once the latest threat has passed, the opportunity still remains for potential control of infected machines. So everyone should remain vigilant to apply patches, maintain current virus signatures, and otherwise secure their systems. Whether the next attack comes from worms, e-mail spamming of Trojans, newsgroup postings, websites or other methods, one thing is for sure. This kind of malware has gone from being just a nuisance to a permanent menace.

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.

## Election Notice

The NCTCUG Annual Meeting will be on October 6, 2004, at 7 pm at Carlin Hall. Elections will also be held then. All officers and four director positions are up for election. Anyone interested in running, please contact any officer or board member.

*Thank you!*

## E-Mail Is 32 Years Old

**By Jim Smith, President, Business and Professional Microcomputer Users Group, Inc. (BPMUG), Connecticut**

Spring has finally arrived and the winter weather is starting to give way to warm, sunny days. March was the anniversary of Email. Yes, in March of 1972 the very first basic e-mail program was written and the "@" sign was chosen for its "at" meaning. Here it is 32 years later and email is a mainstream means of communication and an normal tool for most businesses and for personal use.

Naturally with this handy mainstream concept comes those wanting to abuse it. I would hope that most of you are aware of some of the tricks and hoaxes that can be offered via email. For the others, I'd like to review some of the more common ones so you won't be tricked.

First, there are the obvious scams trying to get you to buy endless supplies of gimmicks that promise to make many of your body parts larger or somehow enhanced. Less obvious are sites that promise prescription drugs for bargain rates and ones with Hormone Growth solutions, or great mortgages on-line or credit repairs and many others. Much like the snake oil sales team of yesteryear, most of these are scams. The occasional one that is legit should also be considered suspect since anyone desperate enough to jump on the wagon with the snake oil sales team is not likely to be around for long enough to deliver anyway. Businesses that use unsolicited commercial email (spam) to sell their products should be viewed with great caution.

Then there are hoaxes that alert you to something that request that you spread it to everyone in your email address book. Any time you get an email that tells you to spread it around, think about it first! Most likely it is a hoax. The most recent one I've seen is the one that asks everyone to not buy gasoline from the big producers in order to prove a point. Searching on-line will give plenty of reasons why this is a farce but it still doesn't stop people from continuing to send it around. Of course there are plenty of hoaxes around about viruses that will eat

your computer unless you send it along to everyone else you know. There are jokes that beg to be sent to everyone and there are emailed chain letters that promise doom and gloom for breaking the cycle. Don't continue to clutter up the email system with these.

Here's something to consider—if you do what you are told and send these to everyone in your address book, and they turn around and add the addresses from their list, and it goes through that for a while, eventually it will likely land in the hands of someone that will sell all of those email addresses to junk emailers who will delight in sending a huge assortment of get-rich-quick and body enhancing scams to everyone listed. I get enough of those spams without friends adding my email address to those lists.

The other popular email hoax is the endless variation on the Nigerian widow with too much money from her late husband and looking for a trusting American with a bank account ready to enter into a business deal in exchange for a percentage. These scams have been around for longer than email has but, rather than using US Postal Service and phones to deliver the pitch, email is a much cheaper way to fish for unsuspecting victims.

Speaking of fishing, there is another hoax that is known by its variation, "Phishing". Phishing is when someone tries to get you to divulge credit card or passwords by pretending to be legit. If you get an email from PayPal asking you to "Click Here" and confirm your account info or from Citibank asking you to verify your credit card number, or from EBay

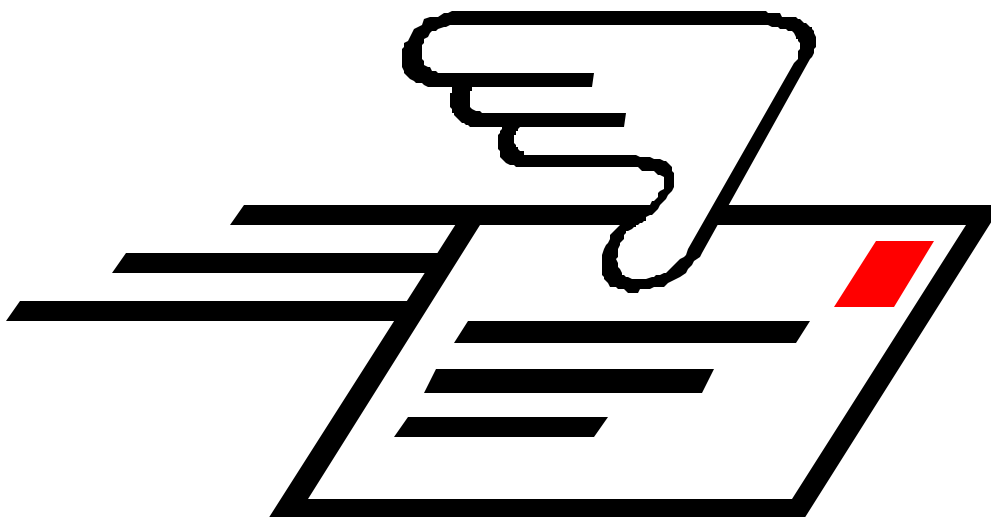
asking you to type in your password so they can keep your account active, these phishing trips are hoaxes! Do not fall for them no matter how legit they appear to be. If you are not sure of something like that, be suspicious. Assume first

that it is a phishing expedition rather than assuming it is legit. With a keen sense of skepticism, many of these hoaxes will become obvious. They prey on our not thinking too much but just doing as we are asked. Most people that fall for them are thoroughly embarrassed after it is over because they realized that if they had stopped to think about it they would have realized the absurdity of it. Don't be hooked in a phishing expedition!

So with 32 years of emailing behind us, there are many wonderful things about email and some things to watch out for. I've given you a few of them... it is up to you to stay alert to many of the other ones that are out there. BPMUG is a great resource for those wanting to find out whether something that sounds too good to be true, is true or not. Don't be taken in. Stop to ponder it first and then verify it. Then if you find an amazing deal to get rich quick that you just know will work... don't share it with me. I probably won't believe it anyway.

Now get out from behind your computers for a few minutes and have a wonderful Spring!

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.



## Virus Attacks Continue At Record Rate

By Ira Wilsker, APCUG Board of Directors

As most computer users have noticed, the number of attempted computer attacks from viruses, worms, and Trojans has increased to a record level. According to antivirus software publisher Panda Software, the average daily number of new viruses and variants appearing for the week ending April 16 was 122 a day, a rate that has been steadily increasing over the preceding few weeks. It might be of interesting historical note that on average, more new viruses and variants are now appearing on a daily basis than appeared during an average week just two years ago! For those who still follow the old, but now quite obsolete strategy of updating their antivirus software on a weekly basis, the likelihood of becoming infected by a virus is near certainty.

Many of the other former "truisms" about virus infections are also no longer true, such as "you have to click on an attachment to catch the virus". Virus authors have become more sophisticated and improved their programming and infection techniques. Although Microsoft released a series of patches over two years ago to close an Outlook and Outlook Express vulnerability, there are still millions of computers that remain unpatched and vulnerable. Several of the very common Netsky variants, some released as recently as last week, take advantage of this opportunity, and can infect a computer by simply having the email message appear in the preview pane of any unpatched version of Outlook. As is now common with many of the current crop of viruses and worms, once infected, any antivirus and firewall software installed on the computer is effectively killed, and ports are opened on the computer allowing continued access to the infected computer from persons unknown. Just because an icon for your antivirus and firewall software appears next to your clock, and it may also appear to update periodically, does not mean that your antivirus software and firewall are functioning. It is good security practice to periodically check all computers for virus infection and open ports by running one of the many free and reliable online virus scans and fire-

wall checks. Personally I use Housecall ([housecall.antivirus.com](http://housecall.antivirus.com)) for a free online virus scan to verify that my computer is indeed clean, and Shields Up ([www.grc.com](http://www.grc.com)) to verify that my firewall is fully functional.

Our personal computers are being infected at a massive rate, estimated to be in the hundreds of thousands to millions, by innocuous files loaded onto our computers without our knowledge. Many of these new crop of viruses are designed to slip through our antivirus and firewall defenses. One method that unfortunately has been successful has been to rapidly create and disseminate many variants of the same virus payload, and quickly flood the net, primarily by email, with the variants. By spacing each variant by a few minutes or hours over a day, it becomes extremely likely that we will encounter several virus bearing emails before our antivirus software is updated. The belief that updating antivirus software daily is an adequate defense is no longer sufficient to provide protection, considering the lag time between the discovery of a new virus, and the release of updated data files by the antivirus companies. The former holy grail of antivirus software publisher, "continuous updates" which many publishers commendably have now reached, is no longer adequate, as a new virus found right now may massively spread unchecked for several hours before updates are available. This lulls us into a false sense of security, believing that our frequent updates will protect us, while in reality dozens of new viruses will spread and infect countless computers before the next update can be released. It only takes one virus to slip through our protection, and we may be left defenseless from further attacks.

The other method of infection that has been around for years, but now becoming even more common is an attack by a virus or worm through our network or internet connections. All computers have "ports" or pathways into the computer. A good firewall should close all open internet or network ports except those being actively and intentionally used, and protect the open ports from unauthorized access. Many of the current worms and viruses try to impersonate legitimate data to penetrate firewalls, or will probe almost any connected computer looking for vulnerabilities. It is not at all uncommon for a home computer to be probed for open ports over 100 times per hour,



which is the explicit justification for a firewall to be installed on all personal computers. Home computers, especially those using dial-up internet access, which had been in the past somewhat ignored by hackers, have now become prime targets for hackers and worm generated probes looking for vulnerabilities.

This has already created a very real security threat at all levels from our own computers to the national infrastructure. Many of these new viruses flooding our email boxes, or attacking us through our internet or other network connections, contain a “zombie”, a small program either scheduled to launch a cyberattack at a predetermined time, or to silently wait for some external signal which will launch a cyberattack. It is not just possible, but now considered a near certainty that sometime in the near future we will be subjected to massive attacks on our critical infrastructures by millions of zombie infected computers, almost all of which will have antivirus and firewall software installed, but possibly neutralized. This is not just science fiction or some possibility, but a very real threat, as demonstrated in the past by the infamous CodeRed and Blaster attacks, among others.

It is absolutely imperative that we all have antivirus software and a firewall that is updated as frequently as possible, and verified to offer us protection.

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.



## PCI Express: Say Goodbye To AGP And PCI Slots

By Timothy Everingham, TUGNET [teveringham@acm.org](mailto:teveringham@acm.org)

Those of you who have been around personal computers for a while might remember plug in cards slots referred to as ISA, EISA, Microchannel, and VESA Local Bus. ISA, EISA, and Microchannel were replaced by PCI. VESA Local bus was primarily for video cards, which was replaced by PCI, then AGP slots. It was a fun time during these card slot transitions because many times you could not use the plug in cards from your old machine in your new computer or motherboard or if you did it could slow down the entire system. Well guess what, its time to do it all over again. Intel has come up with a new slot standard PCI Express, which will start to show up in computers/motherboards this spring.

PCI came out in 1992. Today these slots and its data bus technology are used for things not envisioned when it was under development over 12 years ago. PCI has its limitations and the PCI pro slots never became popular. The limitations are coming to the forefront in delivering multimedia content and Gigabit Ethernet. Of course getting higher frame rates at higher resolution and quality for video games also is an issue. PCI has been evolving over time increasing its speed to five times the original, but it has reached its limits of development. Many say that stretching out the AGP to 8x speed might be pushing at its limit too.

First let us look at the current PCI architecture you will find on most motherboards. The CPU/Microprocessor communicates with the first of two data bridges, normally referred to as the Memory Bridge or Northbridge. The Northbridge not only communicates with the CPU; but also communicates to the AGP port, which is where your main graphics card is (usually the only graphics card). It also communicates with your RAM. The fourth thing it communicates with is the second data bridge, known as the Input/Output (I/O) Bridge or Southbridge. The Southbridge also communicates to your plug in slots/

*(Continued on page 10)*

(Continued from page 9)

cards, drive controllers, and USB, Fireware/1394, parallel, serial, game, keyboard and mouse ports. The theoretical speed limit of the Southbridge communication to I/O including the PCI slots is 133 MB/second. All of the communications in the system are parallel with none of the data having any priority over any other. Blocks of data have to be sent one at a time and cannot be done concurrently. Therefore the data is transferred from one section of the motherboard to the next section based on the order received, not the importance or whether a piece of data arriving by a certain time to its destination is critical.

PCI Express, instead of using a parallel bus architecture, uses serial networking typology with only two wires for each direction. At higher speeds, it allows concurrent transfer of data while having a similar look and the same type of Northbridge/Southbridge architecture as currently in desktops and laptops.

However, in servers the Southbridge is eliminated producing greater data throughput. The PCI slots initially have a 250 MB/second throughput, but the scalable width technology (increasing the number of wire pairs) enables slots and cards to communicate at 32 times that speed in later implementations using longer slots. But the typology can also use network switching type technology, giving data priority and quality of service functions. Hot plug/swap of components is a native part of the architecture.

The PCI Express Graphics Port, replacing the AGP Port, will have a 4GB/second transfer rate in its initial configuration, double that of the current 8x AGP ports. For laptops units there will be a new plug-in card to replace PCMCIA called ExpressCard. It will come in two forms, one that more looks like a PCMCIA card referred to at the 34 module form factor (34 x 75 x 5 mm) and a more oversized L looking card called the 54 module form factor (54 x 75 x 5 mm). This new architecture is compatible with existing operating systems. Also the new PCI Express slot is capable of being placed alongside current type PCI slots so a choice can be made which type of card can be used in a motherboard just like was done with ISA slots and current PCI slots. The standard PCI Express slots being put in motherboards this spring (1x) will be a lot shorter than the standard PCI slots.

All of this will mean that a lot of issues having to do with multimedia on desktop and laptop computers will have been solved. It also opens wider use of Gigabit Ethernet on local area networks. It also enables the prospects of new motherboard form factors and computer case designs. As the transition from ISA to PCI was an interesting transition with computer buyers having to do more research and planning on their purchases, the move from PCI to PCI Express will do the same. However, as was with the previous transition, the performance and capability increases of computers will be profound. Further information on PCI Express can be found at [www.express-lane.org](http://www.express-lane.org).

Timothy Everingham is CEO of Timothy Everingham Consulting in Azusa, California. He is also Vice Chair of the Los Angeles Chapter of ACM SIGGRAPH and is also on the Management Information Systems Program Advisory Board of California State University, Fullerton. In addition he is the Vice President of the Windows Media Users' Group of Los Angeles. He is also part-time press in the areas of high technology, computers, video, audio, and entertainment/media and has had articles published throughout the United States and Canada plus Australia, England, & Japan. Further information can be found at <http://home.earthlink.net/~teveringham>

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 Memory

by **Brian K. Lewis, Ph.D., Sarasota Personal Computer Users Group, Inc., Florida**

Occasionally the question arises as to how much memory can be put in a computer. The answer is "it depends". It depends on just what you mean by memory (RAM or hard disk), what operating system you are using and the capabilities of your computer's motherboard and its chipset. When I talk about memory I am not referring to the permanent storage of programs and data on the hard disk. Rather, I refer to the random-access memory or RAM. This is the memory provided by memory chips seated in slots on the motherboard of today's computers. Anything stored in RAM disappears when the power is turned off, so it is referred to as volatile, or temporary, memory.

If you want to upgrade the memory in your computer you have to be able to determine the memory type as well as the size, pins and speed, the number of slots available on your motherboard and the maximum amount of memory that your system can address. In general, this varies with the age of your computer. So let's look at these components in a little more detail. (Please note that although my remarks refer to Intel's Pentium series central processors, they also generally apply to the equivalent AMD processors.)

### Memory Chips

Early Pentium based computers had a CPU bus speed of 66 MHz (megahertz) and a PCI I/O bus speed of 33 MHz. These values relate to the speed of data movement within the central processor and transmission to and from peripherals such as the memory bank. In some cases transfer to and from memory was at 50 MHz. Pentium computers generally had four slots which were arranged as two banks. This meant that memory had to be installed in units of two. The memory chips were 72 pin DRAM (dynamic RAM) or SIMM (single in-line memory modules) modules. Many of these computers could support four DRAM modules of 32 MB (megabytes) for a maximum of 128 MB of RAM. There were some motherboards built for Pentium 5 systems that had 2 or 3-168 bit DIMM slots in addition to the 72 pin slots. However, you

could not use both the 72 pin and 168 pin slots, only one or the other. These systems would support either 128 or 256 MB of memory. However, at the time, many Pentium/Pentium II computers were sold with only 16 MB of RAM and Windows 95. Later, with Windows 98 the basic memory was 32 MB. In both cases, this is a less than optimum amount of memory for these operating systems. The first Pentium computers had a 32 bit address space which was theoretically capable of addressing 4 GB (gigabytes) of memory. However, none of the motherboards manufactured for these computers carried any such memory capacity.

The next generation of computers carried faster CPUs and chipsets along with faster bus speeds. For example the Intel 440 series chipsets were capable of working with CPUs with speed of 233 - 333 MHz at a bus speed of 66 MHz or with 350-450 MHz processors at a bus speed of 100 MHz. These motherboards generally had 3- 168 pin slots and would support a maximum of 384 MB of RAM. As the address space of the CPU was increased to 36 bit, the maximum addressable memory was 64 GB. However, in practice some computers running Win98 would not recognize more than 256 or 384 MB of RAM. This problem has been ascribed to the chipset design and problem with the L-2 cache. So some caution is recommended if you intend to upgrade the memory in a Pentium II or older system.

With some of the Pentium III class computers there was an additional increment in bus speed to 133 MHz. The motherboards had 2 to 4 168-pin memory slots. The maximum usable memory of such systems ranges from 512 MB to 1 GB. These motherboards for this CPU class are generally able to use 100 - 133 MHz DIMMs. The 133 MHz DIMMS are capable of working at the 100 MHz speed.

The Pentium 4 motherboards came with a whole new array of chipsets and memory chip types and speeds. The maximum memory now ranges up to 4 GB. Intel's initial Pentium 4 motherboards required the use of RDRAM or Rambus DRAM memory chips. RDRAM is a serial memory technology that

*(Continued on page 14)*

## Selections From The DealsGuy

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

### We All Like Freebies

Sally Springette, Editor for The Rochester Computer Society Monitor [ <http://www.rcsi.org> ], sent me this URL that I found interesting and felt you might like it also. If you don't like rebates, then skip this and keep going. This URL [<http://www.freeafterrebate.info/index.php?topic=Hardware>] offers leads to purchasing products that will be free after the rebates. Be aware that third-party vendors offer these products and you should do your own homework diligently before you decide to order. It might even be an older or discontinued product and you will probably pay a shipping charge. With that caveat in mind, check it out and I imagine that it will change quite often.

### Help For Your E-mail

I have a couple of friends who use MailWasher and say it works pretty well to eliminate spam, although it stopped a few legitimate e-mails at times. I questioned Hewie Poplock, a good friend whose opinion

I value, who has used MailWasher for a two years and he is completely sold. He says if you set it up right, it won't filter out good messages, but if you get too fussy, it could happen. Sounds logical, but I have not had enough experience as yet. It incorporates learning by Bayesian statistics and uses FirstAlert!, a real-time global spam database. Something else I like is that you can check your e-mail right on the server instead of on your own computer, if you prefer.

Mathew Miller, Product Development Manager for MailWasher, made a special offer available for user group people and I asked him to extend the deadline so I could include it in my June column. He agreed so you get the price advantage. Mathew is offering us MailWasher Pro and a one-year subscription to FirstAlert for just \$29.95, a saving of

*(Continued from page 14)*

Windows Setup. Once you have the system monitor you can ADD memory information by clicking on Edit, then add item. Select Memory Manager. The individual items that will be the most helpful are: allocated memory, unused physical memory, page files in/ out, swapfile in use or swappable memory. The kernel reading tells you how much of your CPU capacity is being used. Generally, Win98/WinME will do very well with 256 MB - 384 MB of RAM. You just have to be certain that your motherboard and chipset can support this much RAM.

Most of the home computers I have worked on really don't have enough RAM for the most efficient operation. Does Yours?

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 at [bwsail@yahoo.com](mailto:bwsail@yahoo.com) or voice mail at 941/925-3047. :

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.



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

WAC Meetings will be held on June 19 and July 10 (NOTE: 2nd Saturday!), 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/>

\$7.00. You will need the promotional code of QTU-GAD to order. This offer is good until July 31, 2004. Get more info on this tool for all that disgusting spam and download at [<http://www.firetrust.com/products/pro/> ].

### Some Rebates Aren't So Bad

We've all heard horror stories about rebates and I seldom purchase anything with a rebate unless it's a good deal even without the rebate. I recently purchased an 80-gig external Western Digital hard drive for \$110 that had two rebates, one for \$30 and another for \$20. After mailing them, I noticed I had mailed the wrong barcode. A month later I received a postcard telling me I had not included the UPC barcode and offering the opportunity to resubmit it, which I did for the \$30 rebate. Several days later, I received the same notice for the \$20 rebate, but misplaced that card. Since I had only seven days to resubmit it, I thought all was lost when I finally found it too late.

I gave up on that rebate, but was filing another for a free telephone and was confused about something. I called the 800 number they provided for questions, and got my answer. Before she hung-up, she asked if she could be of any further help and I laughingly told her about the one I had misplaced and the time had expired. She said it was no problem and after giving her my information, she fixed it and got it back in the process. It was an OfficeMax rebate, which I have since received.



Since then, I called the OfficeMax rebate center about another one I hadn't received after almost a year. I was told the Seattle rebate center it was mailed to was closed, but he would fix it. I received the acknowledgement by e-mail the next day, and the check a week later. Fortunately, I have not lost any rebates so far.

### Reminder On A Great Software Deals

If you forgot to take advantage of the great Executive Software Deal, I think they will still honor it — Diskeeper Professional Edition 8.0 bundled with Undelete Home Edition for just \$49.95 — but act soon [<http://consumer.execsoft.com/home.asp> ]. We all know what great products Executive Software produces.

### Opt Out Of Spyware

According to Kim Komando, the Network Advertising Initiative, [<http://www.networkadvertising.org> ] helps you drop both DoubleClick and Avenue A Inc., known for spyware. I haven't tried it yet.

### Accidentally Deleted Those Pictures?

Don't worry, if you were using your digital camera and, with a slip of the finger, you deleted something from your Smart Media or Compact Flash Card that you later want, here is the answer. Just go to [[http://www.z-a-recovery.com/digital\\_image\\_recovery.htm](http://www.z-a-recovery.com/digital_image_recovery.htm) ] and download Zero Assumption Digital Image Recovery at no cost to you. Even though it says no image is there, if it used to be there, this program will recover it. Thank God for freebies, and for Bob Schuchman of San Diego PCUG who wrote about this one some time ago in their newsletter.

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 Cheapskate) Click [[bobclick@mindspring.com](mailto:bobclick@mindspring.com) ]. Visit my Web site at [<http://www.dealsguy.com> ] for interesting articles from user group newsletters. I also posted some interesting NEW Web site pages for your viewing. They contain new product announcements that I received over a period of time. More will be forthcoming.

*(Continued from page 11)*

arrived in three speeds, PC600, PC700, and PC800. RDRAM designs with multiple channels, such as those in Pentium 4 motherboards, are currently the fastest in memory throughput, especially when paired with the newer PC1066 RDRAM memory. A Rambus channel is 2-bytes wide, so we get a maximum 1.6GB/s transfer rate for a single RDRAM channel using PC800 RDRAM or 2.1GB/s for PC1066. The other form of memory chip is the double data rate DRAM. Intel and other manufacturers now have motherboards and chipsets that can utilize these memory modules. They are less expensive than the RDRAM. DDR memory modules are named after their peak bandwidth - the maximum amount of data they can deliver per second - rather than their clock rates. This is calculated by multiplying the amount of data a module can send at once (called the data path or bandwidth) by the speed of the front side bus (FSB). The bandwidth is measured in bits, and the FSB in MHz. Note that the RDRAM bandwidth is in bytes. One byte is equal to 8 bits.

A PC1600 DDR memory module can deliver bandwidth of 1600Mbps. PC2100 (the DDR version of PC133 SDRAM) has a bandwidth of 2100Mbps. PC2700 modules use DDR333 chips to deliver 2700Mbps of bandwidth and PC3200 — the fastest widely used form in late 2003 uses DDR400 chips to deliver 3200Mbps (3.2 Gbps) of bandwidth. You may see the term “dual channel” applied to memory. When properly used, the term refers to a DDR motherboard’s chipset that’s designed with two memory channels instead of one. The two channels handle memory-processing more efficiently by utilizing the theoretical bandwidth of the two modules, thus reducing system latencies, the timing delays that inherently occur with one memory module. For example, one controller reads and writes data while the second controller prepares for the next access, hence, eliminating the reset and setup delays that occur before one memory module can begin the read/write process all over again.

Consider a model in which data is filled into a container (memory), which then directs the data to the CPU. Singlechannel memory would feed the data to the processor via a single pathway at a maximum rate of 64 bits at a time. Dualchannel memory, on

the other hand, utilizes two pathways, thereby having the capability to deliver data twice as fast or up to 128 bits at a time. The process works the same way when data is transferred from the processor by reversing the flow of data. A “memory controller” chip is responsible for handling all data transfers involving the memory modules and the processor. This controls the flow of data through the pathways, preventing them from being over-filled with data. Now that you are totally confused by all this memory type and speed terminology, let’s look at the next question.

### **How Much Memory?**

How much memory should you have in your computer? The answer is: probably as much as your motherboard and chipset can handle. For the newest motherboards, that may be excessive unless you are involved in digital video editing or graphic design. For most home users running WinXP or Win2K I would recommend 512MB up to 1GB. So why those figures? I have found that WinXP uses over 200 MB of RAM for its own files, if that much is available. So on a 256 MB system that leaves very little for other applications and data. The net result is a lot of swapping with the virtual memory space on the hard drive. That slows everything down. In WinXP the Windows Task Manager (bring up by pressing CTRL+ALT+DEL) shows your current performance and the amount of memory available in real time. With 512 MB and several programs running, I have over 300 MB of real RAM available. That greatly increases the responsiveness (speed) of the system as moving data to and from RAM is many times faster than using a hard disk. The Page File window shows you the virtual memory swapping your system is doing. At the moment, mine is zero.

You can do similar analyses on Win98/WinMe systems. The System Monitor application that comes with Windows can supply this information.

However, you may need to modify it to get the memory info you want. Go to Start-Programs-Accessories-System Tools and select System Monitor. If this selection is not available on your menu, then you need to install the program from your original Windows disk or from \WindowsOptions\Cabs file. You do that from the Control Panel (Add/ Remove Software) and

*(Continued on page 12)*

(Continued from page 1)

The group's board of directors established a committee several months ago to suggest what approach we should use in acquiring a new demonstration computer — buy an assembled system, from a national manufacturer or screwdriver shop, or assemble a system from parts ourselves. Intel's timely offer made the decision for us.

The new system incorporates Hyperthreading Technology, and will be available for members to borrow between meetings to become acquainted with this technology. This will also allow us to install a current operating system. Members may recall that our previous demonstration system couldn't be persuaded to load Windows XP — we spent four meetings trying but never got past "19 minutes remaining." The basic assembly of the new Intel-based system has been completed. We hope to spend the next meeting loading software, and putting the finishing touches on the system, such as wiring the front panel USB and

audio ports. Pictures of the new system and assembly process are available on the NCTCUG web site.

**Are You Using Protection?**

The continuing profusion of virus attacks makes the use of anti-virus software absolutely essential for anyone using the internet and/or email. Virus definitions need to be regularly updated — most major programs now perform that chore automatically when the user goes on-line, if you're using a current version. Don't leave this to chance — if you're not sure you have what you need, or how to configure or operate your AV program, get in touch with a NCTCUG officer and ask for help. In the same vein, anti-spyware and firewall programs are a worthwhile investment in computer security. There are commercial and freeware products available in all these categories — don't go unprotected !! We'll try to place a web page with links to resources for computer protection on the NCTCUG web site over the next several weeks.

(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 2003

President	Jim Rhodes	703-931-7854
1st VP	Ron Schmidt	301-577-7899
2nd VP	Roger Fujii	703-280-1243
Treasurer	Paul Howard	703-860-9246
Secretary	Roger Arnold	301-946-7770

Director: term expires

Bill Walsh	2004	703-241-8141
Blair Jones	2004	202-362-7344
John Keys	2004	703-451-0896
Nick Wenri	2004	703-759-3938
Fred Cook	2005	703-921-1749
JJ Davies	2005	703-379-9222
Sy Fishbein	2005	703-536-5894
Dean Mires	2005	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 CR only at end of paragraphs; no indents for paragraphs should be used. Preferred format for diskettes is MS-DOS 3½ 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 1977 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 10 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 and  
Articles 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/>

**If you are moving**  
Please send your change of address to the club PO box as soon as possible to avoid missing issues.

*Thank You!*

(Continued from page 15)

### Worthwhile Laptop Accessory

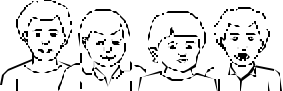
As laptops become more popular and affordable for many users, the new purchaser often discovers that their new pride and joy is missing something that they'd find useful. Frequently left out are 3.5" drives. These old standbys are becoming less needed with the advent of solid state "keychain drives"—also known as "thumb" "jump" "flash" or "mobile" drives, depending on the manufacturer. However, as we've discovered at a number of recent user group meetings, although many computers have USB ports, lots of older systems utilizing Win 95/98 don't have the necessary software drivers installed, and the keychain drives won't work. Being able to exchange files with 3.5" drives still comes in handy. Iomega is offering a great solution for new laptop owners - a combination 3.5" drive and a multislot 7-in-1 flash memory card reader with a USB interface.

**August/September 2004**

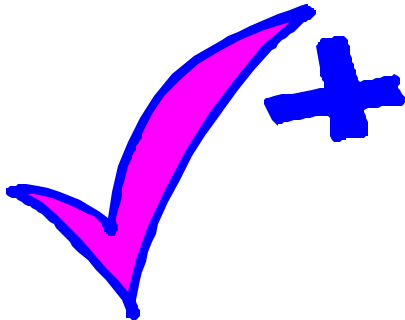
1st Wed. (8/4, 9/1) **7 p.m.**  
Virginia General Meeting

4th Wed (8/25, 9/22) **7 p.m.** Internet SIG

3rd Monday (9/6, no meeting in August)  
**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.



First Class

---

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

