ACPCUG Newsletter

Cuyahoga Falls Public Library

June 7, 2003

Inside:

June Program:

Starts at 6:00 PM

WinZip v. 9.0 **by Art McRowe +**
Q&A +
MS (XP Pro) Media Center
By Rick Beech

June 2004

Akron-Canton PC Users Group

From The DealsGuy for July, 2004,

by Bob (The Cheapskate) Click
of Greater Orlando Computer Users Group

***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

(Continued on page 2)

(Continued from page 1)
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.

*Ain't Technology Grand?

Trade shows often have magazine stands with interesting ones to read. At the Home Electronics Expo I found ElectronicHouse [http://www.electronichouse.com] which I enjoyed, and this caught my eye. We're familiar with our bathroom vanity and have often looked in its mirror. What about one that may seem like it morphs? Royal Phillips Electronics has developed a new twist for the bathroom vanity. It is called Mirror TV and it might be looking back at you, sort of. It will turn into a TV screen that could be showing your favorite news broadcast or stock reports. How about that --- turned off, it's a mirror, or on, it's a TV! When offered, it will first appear in hotels, then to home users sometime in 2005. If the news is interesting though, how long might those BMs take? What about if your stock is dropping? Don't watch it too long or you may shut off the circulation to your legs. Can they be sued for that? Probably!

ElectronicHouse also had an article about putting your audio system on IP. Giving your speakers their own IP address properly can make amazing improvements to the sound. I was also looking through an issue of FlatPanel World that had interesting articles. It is a new publication by CE-Pro. One article offers explanations about various types of flat panel displays. I didn't see a Web site except for the parent magazine's [http://www.ce-pro.com] Author Robert Archer stresses that dealers need to know the difference between LCD (Liquid Crystal Display) and LCOS (Liquid Crystal On Silicon) as well as plasma display technologies when giving their sales pitch. He explains them all including DLP (Digital Light Processing) and explains the importance of calibration on a thin screen, which can cost upward of $300. He discusses some technologies of plasma displays. I saw several great articles

(Continued on page 3)

(Continued from page 2)
about FPDs (Flat Panel Displays) and audio techniques.

In Digital Connect Magazine's March issue [http://www.digitalconnectmag.com], I read an article concerning the licensing of low voltage integrators (installers). I'll bet many of you didn't know that in some states, integrators who work with low voltage systems, such as remote controlled lighting, audio/video or telephone systems, must be licensed. Their license presently specifies 50 volts or less. One state is considering a bill requiring home installers performing electrical work at more than 50 volts to obtain high voltage licenses. CEDA (Consumer Electronic Design and Installation Assoc.) is lobbying the state to classify high-voltage projects as starting at 100 volts, a level that would not shut out integrators with a low voltage license from working with audio, video and home telephone systems. You might think that anybody could pull in some low voltage cables and hook them up according to the color code, but an experienced integrator for that type of wiring would know the importance of wire routing to eliminate interference and other problems. From my own experience installing auto audio, wire placement is extremely important. Not just anybody is capable of always installing a successful integrated digital system without experience.

With home wiring turning toward IT more and more, appliances and controls are also changing. For example, you are all familiar with your AC/heat thermostat, which originally had only the ability to turn the system on or off. Times are changing --- new controls are capable of talking to the appliances as well as controlling it. Other appliances will become the same way in the future. New technologies pretty much lets your home think for itself. I hope mine doesn't get mad at me for neglecting it!

*Last Minute Changes

Two vendors pulled out at the last minute because their material suppliers are raising prices at a dramatic rate and they want that to stabilize, so here are some things I have kept in reserve. Also, if you forgot to take advantage of the great Executive Software Deal, I think they will still honor the deal, but act soon. [http://consumer.execsoft.com/home.asp]
Addendum: Don't forget also the MailWasher deal from last month. [http://www.firetrust.com/products/pro/].

*A Nice Tool For Teaching About Computers

This item has limited interest at best for my readers, but since we have

(Continued on page 4)

(Continued from page 3)

teachers in our user groups, I am including it. Some larger users groups also have hardware SIGs, some of which are structured and might be interested in this product, although it may be too costly for a SIG. While browsing through the "Association For Technical And Education Show" I saw many types of training stations and this one caught my eye. It is a "Personal Computer Training Station" with the motherboard, keyboard and some other components mounted on the top, easily accessible right before your eyes. Pull out a drawer and you will find the drives, which can be snapped out of their respective holders and quickly unplugged. It has a custom-built 350-watt UL power supply and supports AT/ATX/P4 motherboards. It also offers high-speed hard drive duplication capability.

This is a sort of breadbox type workstation and everything is very handy. Go to [http://www.atp-p51.com] where you can get more information and pictures of the product. The guy said he was unable to offer a deal because he depends on distributors. I am printing it just for your information, and for the many teachers belonging to user groups.

***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] 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 PC UG who wrote about this one some time ago in their newsletter.

That's it for this month. Meet me here again next month if your editor permits. 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]. 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 an-

(Continued on page 5)

(Continued from page 4)
nouncements that I received over a period of time. More will be forthcoming.

Don't Be a Victim of Health Scare Stories

By Alicia King Padgett
Alicia-apcug@comcast.net
APCUG Advisor for Region 9

Health scare artists are utilizing the Internet as a medium for terrorizing the public, and unfortunately many adults are taking the stories seriously. These tall tales are often written citing evidence and research that sounds legitimate. Frequently an e-mail is sent to you from a reliable friend who had received it from another acquaintance who had "personal knowledge or personal experience" with the alleged dangerous item. The health scare messages are always the same—whatever it is will make you sick or even cause death.

If you try to research accurate health information about the topic sent, you may literally become caught in the Web, where health hoaxes and urban medical myths run rampant. Many of these Websites appear to have valid researched data.

Before you decide to believe or, worse forward e-mail with serious health claims, do a little checking. Start on the Web with www.urbanlegends.com or www.snopes.com that catalogue the more persistent rumors. These two sites also detail persistent legends on other topics in addition to health scare stories.

Then go to reliable health sites, like:

www.mayohealth.org for general health
www.medhelp.org especially good for cardiology
www.oncolink.org for cancer
www.cancer.gov for cancer
www.navigator.tufts.edu for nutrition
www.fda.gov for latest updates on food/drugs as well as extensive archives

So keep yourself informed and don't become one of the individuals caught in a web of confusion by believing the stories and passing them on to others.

Many of us have been victim of health-related frauds, myths, and fallacies. We have to make many decisions about our health and care and want to make them will informed. This site will keep you up-to-date on the latest findings on health care frauds.

(Continued on page 7)

(Continued from page 6)

Quack Watch is an informative site that deals with such issues like growth hormone scams, coral calcium, and acupuncture. It has a section on allergies and alternative medicine. You might want to start with *Tips for Navigating our Web Sites.* In the "Quackery" section you will find the following sections: Seven Warning Signs of Bogus Science, Ten Ways to Avoid Being Quacked, Signs of a "Quacky" web site.

Always seek a second opinion, but please peruse www.quackwatch.org

Internet Annoyances

by Sherry Zorzi, Secretary, Cajun Clickers Computer Club, Baton Rogue, Louisiana, and Advisor for Region 8.

The Internet is full of creepy-crawly beasties. Spam, popups, hoaxes, cookies, spyware -- what are these critters and how do I tame them???

Spam – unsolicited, usually commercial email, also known as UCE. You can't stop it; the best you can do is try to limit it.

- Don't post your address on publicly-accessible websites (newsgroups, chat rooms, directories). Web "crawlers" harvest these addresses for spammers' mailing lists. You can obtain free, "throwaway" email addresses at sites like Yahoo (www.yahoo.com) or Hotmail (www.hotmail.com) to use in these situations.

- When you register for a legitimate website (Microsoft, Amazon, Delta Airlines, etc.), opt-out of any newsletters or mailings they offer to send you. If opting out is not offered, don't register for the site unless you want advertising email!

(Continued on page 8)

(Continued from page 7)

- Use "filters" in your email program to automatically route suspected spam to a special folder, which you can check periodically and delete. Or use special (free!) software, like MailWasher (www.mailwasher.net) or K9 Spam Killer (www.keir.net/k9.html) to automatically check incoming mail and handle suspected spam for you.

- Don't ever follow directions to "unsubscribe" or stop receiving mail, unless you know you are dealing with a reputable source. Replying to the message or clicking a link to supposedly unsubscribe is often just a ruse by the spammer to verify that your email address is valid and that you are naïve enough to open spam. You will get more, not less, spam!

- Use SpamCop (www.spamcop.net) to report spam. The service is free. They will automatically report, in your name, the true source of the spam to the appropriate ISPs.

- Send a copy of the spam, with full headers, to the Federal Trade Commission at uce@ftc.gov. They keep a database of fraudulent spammers.

- Support strong legislation at the state and federal level to stop the scourge of spam!!! Write, call or email your Senators and Representatives and urge them to support strong legislation.

Popup – advertising that "pops up" in a small window of its own. Some websites pop up an unsolicited ad in a window on top of the page you are trying to view. Others hide the popups beneath the site you're visiting, so that you see it when you finally close your main window. Some sites pop up several, or even dozens of popup ads – sometimes "freezing" the computer. The new popup scourge is controlled by one or more programs hiding on your computer, causing popups even when you are not online! They are all bad, bad, bad!

The best way to squash popups is with free software like Popup Stopper (www.panicware.com). Works perfectly and the price can't be beat!

(Continued on page 9)

(Continued from page 8)

Hoax – fictitious email forwarded around the Internet by your well-meaning friends. Flesh-eating bananas, large corporations controlled by Satanists, viruses that cause your computer to catch fire – all are fabricated hoaxes. Most of us have at one time been taken in by one of these, forwarding it to everyone in our address book only to be embarrassed to find out it's a fake. Any email, even if it's from your mother, that says "Please forward this to everyone in your address book" is a hoax. Any email that promises you will get something for nothing is a fake.

- Never, ever forward anything to everyone in your address book, no matter how "true" it sounds. Even if it is supposedly from IBM, Microsoft, or the government.

- Type a few keywords from the email into a search engine like Google (www.google.com) and follow several of the links that come up. You should quickly discover that the mail is a hoax.

- Before you hit "forward", check out the "story" on one of the websites that specialize in de-bunking urban legends and hoaxes:

    - Snopes (www.snopes.com)

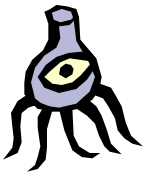
    - Urban Legends (www.urbanlegends.com)

(Continued on page 10)

(Continued from page 9)

- HoaxBusters (www.hoaxbusters.com)

Spyware – technology that aids in gathering information about a person or organization without their knowledge. Spyware usually comes "hidden" within software you voluntarily install. Along with what you wanted, you also get a small piece of software than installs itself behind the scene and sends back information on your surfing habits to an advertiser or marketing company.



You can control spyware with some free tools available on the web. The tools will either prevent spyware from getting on your machine, or remove it once it is there.

- Ad-aware (www.lavasoftusa.com)
- SpyBot Search and Destroy (http://beam.to/spybotsd)

Cookie – a small text file placed on your computer by a website you visit. Cookies can be innocent, but some operate as spyware. Spyware-controlling software like Ad-aware will control spyware cookies, too. You can also exercise some control over cookies in Internet Explorer by clicking Tools, then Internet Options. Click the "Privacy" tab to allow or disallow various kinds of cookies on your system. Be aware that some features of some sites won't work properly unless you allow cookies.

Virus, worm - a piece of programming code that causes some unexpected and usually undesirable event, such as spreading itself (in your name!) to everyone in your address book, locking up your computer, or deleting important files. They can be transmitted as attachments to an e-mail, as downloads, or be present on a diskette or CD.

- Install antivirus software and keep it up-to-date. Popular brands include McAfee Virus Scan, Norton Antivirus, and TrendMicro PC-cillin. Free antivirus software, which works well, is available at www.grisoft.com. HouseCall, a free online virus scanner, is available

(Continued on page 11)

(Continued from page 10)

from TrendMicro at http://housecall.antivirus.com/housecall/start_corp.asp.

- Don't allow "autopreview" features on your email programs. When an email message is previewed, it is really "opened," which can trigger a virus.

- Don't open emails or attachments from unknown sources. Even when mail is from a trusted source (such as your mother), don't open any attachments unless you are expecting them without checking with the source first to be sure they intended to send the attachment and are sure it's virus-free.

Trojan horse – similar to viruses and worms, Trojan horses are particularly nasty as they can open up ports on your computer, making it possible for an intruder to control your computer remotely.

Anti-virus software is not great at catching Trojan horses. You should install and periodically run a Trojan scanner, such as the free SwatIt (www.swatit.org).

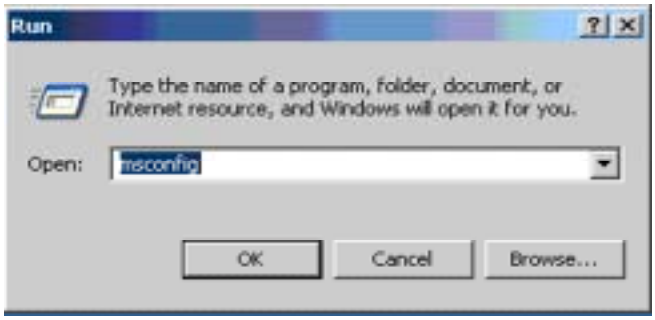
If you use the available tools, your Internet experience will be more pleasant for you, your computer, and for all your email correspondents. Don't forget the most important tool of all – **YOUR BRAIN**! Use it.

Use Run commands for fast access to almost everything

by Linda Gonse, Editor, Orange County PC Users' Group, California

Did you know that the Run command is the Swiss Army knife of Windows' built-in apps? Using it can make your computing time move along more quickly and smoothly.
Available since Windows 3.1, the Run command is often overlooked by users except as an option for installing programs, although techies use it frequently to access various system diagnostics and information.

But, the average computer user should take a closer look at Run for its versatility to start programs and utilities, to open files and folders, to open web sites (when connected to the Internet), and as an alternative to placing shortcuts on the desktop.
To use Run, left click on the Start button. Click on Run. If you hate to take your fingers off the keyboard to access Run, you can avoid using the mouse by pressing the Windows key on your keyboard and the letter "r". Commands are typed into the open box.



For example: In the open Run box, type msconfig to give you quick access to the Startup Configuration tab. Click on the StartUp tab, and check or uncheck boxes of programs you want to run on Startup. (You will be prompted to restart your computer. If you want your custom startup to take effect immediately, click OK.) Msconfig is one of the Run commands you will probably use often.

Following are other Run commands for you to try out. (If you get hooked on Run, you can search Google for "run commands" to find others. There are lots of them! Many will include "switches," familiar to DOS users, that will allow some of the commands to be customized.)
calc (opens calculator utility)

(Continued on page 13)

(Continued from page 12)

cdplayer (opens cd player)
charmap (opens character map utility)
clipbrd (opens clipboard utility)
command (opens DOS window at command line)
defrag (opens defrag utility)
drvspace (opens drive space utility to compress drives, etc.)
dxdiag (for DirectX, sound, input devices-joysticks, etc. info)
freecell (opens freecell game)
mplayer2 (opens Windows Media Player 6.4)
msconfig (accesses programs that run on startup)
mshearts (opens hearts game)
msinfo32 (accesses system resources info)
notepad (opens program)
regedit (accesses command to edit the registry)
rsrcmtr (loads resource meter utility in system tray)
scandskw (accesses scan disk utility)
scanregw (registry scan)
sndrec32 (opens sound recorder)
sndvol32 (opens sound volume utility)
sol (opens a solitaire game)
sysedit (accesses the System Configuration Utility)
sysmon (opens system monitor utility)
win.ini (accesses file that loads some Windows components)
winipcfg (displays Internet connection/adapter info)
winver (displays the Windows verson installed on the computer)
wmplayer (opens Windows Media Player)
wordpad (opens program)
wupdmgr (connects to Windows update)

Using the Run box can also give you a jump start on addressing your email messages. Go to Run and type in mailto:<desired email address> and press OK. (Example--mailto:editor @orcopug.org.) Your e-mail application will open to display a blank new message that already has the email address you typed in the 'To:' field! You can even check websites by typing in a web address in Run. (Ex-ample-http://www. orcopug.org.) When connected to the Internet, you will be whisked to wherever you want to go.

Among the switches you can type in the Run box to customize tasks are attrib, move, and xcopy. DOS command and switches, and instructions on how to use them in conjunction with Windows Run, are at http:// www.Techiwarehouse.com/DOS/XP_DOS _Tutorial.html, and http://www. computerhope.com/msdos.htm#02

(Continued on page 14)

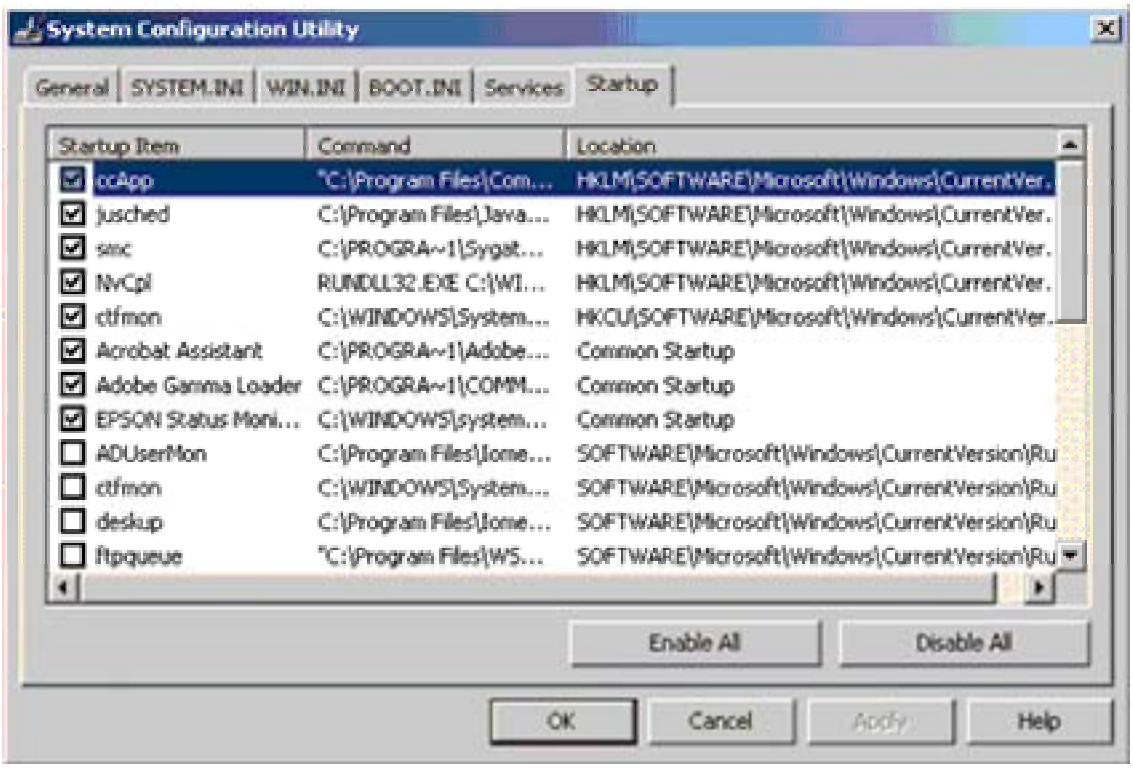
(Continued from page 13)

As you type commands in the Run box, a list of your Most Recently Used (MRU) commands--a history of the commands you've used--accumulate. The growing list can come in handy, because you can just click on any command to activate it without retyping it.

On the other hand, you may not want to wade through a long list, or you may not want others to have access to the visible commands. In these cases, you need to clear the MRU commands. Here are two ways you can do that.

1. Right click the start button and go to properties. Click on the radio button next to Start Menu and click on the Customize... button. Then, click on the Advanced tab. Locate the Run box and check the box on the left. Then, click on clear history.

2. You can navigate to HKEY_CURRENT_ USER\ Software\Microsoft\Windows\ CurrentVersion\Explorer\ RunMRU. This is where you will find all the commands in the Run history. Delete the ones you don't want. But, backup the registry first!



Tech News

By Sue Crane, Editor

Bearly Bytes, Newsletter of the Big Bear Computer Club, California

**Windows XP Service Pack 2, scheduled for release next month, will be available as a “critical” download on the Windows Update site and will ship with new PCs. The update will introduce technologies for network protection, memory protection, secure e-mail handling, secure browsing and PC maintenance. A new Windows Security Center allows firewall monitoring, Automatic Update and third-party anti-virus software and warns customers when they need to apply patches. Microsoft will probably ship free CDs, but consumers will probably pay for shipping and handling.
**Chipmaker, Intel, and PC makers are shifting the PC to multimedia hub for the home. Intel predicts two new categories

**Entertainment PCs will imitate stereo and video components, like a VCR, and will play music and DVDs, record TV programs and even show picture slide shows.

Entertainment PCs will use your TV for display and be operated by remote control.
Lifestyle PCs, designed to inhabit bedrooms and kitchens, will look like desktop computers and will be operable via remote control or keyboard, allowing users to write an e-mail and later play a video or music. Lifestyle PCs will also come with multimedia software such as Windows XP Media Center.

The new PCs will be pricey. An entertainment PC might start at $700 - $900 and sell for $1,400. Lifestyle PCs could start at $600, but with a large flat panel display could sell for as much as $2,000. PC makers have also announced plans to offer special media adapters called the Windows Media Center Extender, which will let consumers view Media Center files on TVs. SnapStream Media has also figured out a way to get your PC in touch with TV. Firefly is a remote control that lets people manage media and entertainment on their PCs --TV tuning, DVD playback, streaming video, digital music players and photos. Firefly is compatible only with Windows XP and Windows 2000 PCs equipped with a 500MHz processor, 128MB of memory, 100MB of free hard disk space, and a CD or DVD drive. Firefly will cost $49.99.

**HP’s Media Center PC of the future has a remote control with a built-in

(Continued on page 16)

(Continued from page 15)

LCD screen for programming recordings. The PC, known as the Windows Home Concept, also supports Internet telephony, dual high-definition TV tuners, biometric security, and a built-in cable modem. For a web-based slideshow and more information about these new concept PCs, see: http://www.eweek.com/article2/0,1759,1586428,00.asp

**Internet2, the high-speed network designed to facilitate scholarly collaboration among university researchers, has spawned a new turbo-charged file-trading network dubbed i2hub. University network administrators are concerned that copyright violations are occurring and a computer support specialist at Florida State University says: "The fact is, (the network) cost a lot of money and downloading games and music should be the last priority on any campus network."

**Yury Gitman, a self-described "wireless and emerging-media artist" in New York, has outfitted his bicycle with an iBook laptop and Wi-Fi antennas so that everywhere he goes, a cloud of free, high-speed wireless Internet access follows. Demand for wireless Internet access in automobiles has been picking up, and plans are to offer it in airplanes soon.

**Memory designer Rambus, has begun to license designs for interfaces for DDR DRAM, or double data rate DRAM, the most common type of memory found in PCs and a technology that's often used in consumer electronics devices. The interfaces let another component retrieve data out of DDR DRAM chips. A new version, called DDR 2, will be released soon that runs at 533MHz. It will soon speed up to 800MHz.

**Last year, Congress increased the amount small businesses can write off on new equipment purchases from $25,000 to $100,000. Known as the Section 179 deduction or the SUV tax, the increase is serving as motivation for sport utility vehicle purchases, but also is an incentive to purchase technology-related equipment. It's available only through 2005, so businesses should decide quickly whether or not to spend while the spending's good.

**IBM plans Web-based desktop software. Lotus Workplace strategy, is a bundle that includes e-mail, word-processing, spreadsheet and database applications aimed at business users. The new software is designed to be distributed and accessed through a Web server, and accessible from systems running Windows, MAC, Linux, Unix and handheld devices. IBM hopes to sway customers to Lotus Workplace with ease of management, mobility and price. The new software is designed to be used offline, so mobile users on laptops or handheld devices can connect, quickly access applications and

(Continued on page 17)

(Continued from page 16)

disconnect to work offline. IBM plans to charge $2 per user per month for access to the software, plus the cost of server software to make the system work.

**The History Channel's 13-episode series on "Decisive Battles" that debuts July 17 makes use of a not-yet-released PC game to re-create the epic battles that mark ancient Rome's colorful history. "Rome: Total War" will be published by Activision this fall.

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.

(Continued on page 18)

(Continued from page 17)

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 Computer 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.

(Continued on page 19)

(Continued from page 18)

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.

(Continued on page 20)

(Continued from page 19)

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 backdoor. 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.

DIGITAL PHOTOGRAPHY AND PRINTING

by Charlotte Semple, President & Editor, Los Angeles Computer Society, California

Charles Mahan, Wi-Fi SIG Leader, Los Angeles Computer Society, California

Lee Otsubo is best known as The Digital Photo Guy. He has become a familiar figure to many user groups as he shares his knowledge and experiences in digital photography. He emphasizes two basic topics in his presentation:
1) How to get the most out of a digital camera (or how to buy one) and,
2) How to share and display great digital Photos.

Megapixels

Mega comes from Greek, meaning, great. In technological terms, it's a prefix for millions. A 3.5-inch floppy holds 1.44 mega bytes, which is 1.4 million bytes of data. A megapixel is 1 million pixels.

So, "What the heck is a pixel?" A pixel is a made up tech term for "picture element." Pixels are square.
If you look closely at a newspaper photo, using a magnifying glass, you will see hundreds of tiny dots, some dark, some light and some in between. As you move the photo away from yourself, setting aside the glass, you will not be able to discern the dots any more, instead you will see the whole photo. Digital cameras work the same way. They use millions of pixels, (mega pixels, or MP), to make a photo. i.e. a 2 MP camera uses 2 million pixels. A mega pixel is a measure of the camera's capability to capture detail, which is resolution.

You need to be aware of what kind of photography you are interesting in doing and what you are going to do with the photos in order to make the best use of the finite number of pixels you have.

CCD

The CCD (Charge Coupled Device) is the central processing unit of the digital camera. It is somewhat like the CPU in a computer, but unlike the CPU, the CCD has only one function. It takes images and munches and crunches them. The CCD of a 2 mega pixel camera contains 2 million light sensors. Each light sensor produces 1 pixel. Each pixel represents 1 of 16.7 million different colors. Each pixel has a red, green and blue component of color. Each component is a byte (of data). Each pixel has three bytes of data. A 2 MP camera produces 6 million bytes of data. Enough data to fill five 3.5-inch floppies!

(Continued on page 22)

(Continued from page 21)

Cycle Time
The time needed for the CCD to munch and crunch data and get it out of the way in time for the camera to be ready to take another photo.

Lag Time
The time a digital camera needs to look at a subject and fire enough electrical charge to be ready so that when the shutter button is pressed, the camera will capture the image of the subject.

Munching and Crunching
After the CCD captures the image it has to compress it. A 2 MP camera uses (munches) 6 million bytes of data for each picture at high resolution. This has to be compressed (crunched) down to 1 mega byte of data. Many cameras have different settings for resolution. Lee recommended that you keeps your camera on the highest setting and leave it there. If you change it for a lower resolution shot and forget to re-set it to the higher level, and you use the camera again, thinking you are taking high-resolution shots, you will be disappointed in the results. You can always throw away extraneous detail, but you cannot put it in if you didn't capture it in the first place.

Input –The Lens
This is the first and last place where there is any real resemblance between the digital and film camera. The usual focal length of a 35mm point and shoot camera is anywhere from 35mm to 105mm zoom. Most digital cameras have 3 X zoom, which goes down to the equivalent of 35mm, for a moderate wide-angle shot, out to the equivalent of 105mm for a telephoto shot.

There are two types of Zoom: Optical, which is "real" zoom, and Digital, which is electronic trickery. When you activate the zoom function on a 35 mm point and shoot film camera, you can hear the lens moving in and out, increasing or decreasing the size of the image to be captured. This is "real" zoom. When the electronic zoom on a digital camera is activated, the zoom plays a trick on the image. The lens captures the center section of the image and stretches the pixels out to fill the frame. But one loses some resolution and the photo will not be as clear.

Using a photo imaging tool on your PC, and enlarging a photo large enough so that straight edges are no longer straight, you can see the points of individual pixels. In tech terms, this is called "Jaggies." Under the same conditions when looking at a photo of a person, you can see individual square

(Continued on page 23)

(Continued from page 22)
pixels. In tech terms, this is called “Pixulation”.

When buying a camera be aware of what component of the camera is optical zoom and what is digital zoom. Some “smart” marketers might advertise their camera as having 6X zoom capability, where they have multiplied the 3X Optical by the 2Xdigital. A 3X Optical camera is a 3X Optical camera. Another way marketers might advertise a 6X Optical camera is where they have taken a cheap 2X optical zoom and bumped up the digital zoom to 3X, calling their product 6X Zoom. You must be really careful to read the fine print. Don’t always go by the advertising printed on the box.

About Zoom

If you are taking photos at a back yard BBQ, and you are able to fill the camera frame with subjects, you probably will not need a zoom. If you are going to be taking outdoor photos with subjects 20 to 30 feet away, a 3X Optical zoom camera is probably all you would need. If you are in the “nose bleed” section of a sports arena, and your subjects seem to be 6-inches tall, you will probably need anywhere from a 6, 8, 10 to 12Xm zoom. You should be aware of the kind of photography you want to do so that the right type of zoom lens can be obtained.

Output-USB

Most modern digital cameras will have a USB (universal serial bus) port connection. If a camera does not have this don’t even consider it. A slow serial connection will drive you crazy. Simply plug the USB cord that comes with the camera into the computer and leave the camera end in a convenient place for ready use. A card reader makes an easy job of uploading the data from your camera into the computer. A universal Card Reader accommodates up to 6 different memory cards. Simply insert the memory card into the reader and it will look to a Windows machine, almost like a disk drive, and you can drag and drop photo files from the memory card.

Memory Cards

These are compact flash memory cards. The particular type of memory card that came with your camera is the type you should use. Not all memory cards are universal. The real advantage of memory cards is that they are removable and are fairly robust. Not like ordinary film. Lee recommends that you should carry at least two memory cards of a moderate range. These are all electronic devices and sooner or later you will corrupt data on a memory card. If you were gullible enough to buy only one very large range memory card, and go on vacation, and the card becomes corrupted, you are up the proverbial tree. You have two choices. Erase all the accu-

(Continued on page 24)

(Continued from page 23)
mulated data from the card and reformat the card, loosing all your photos, or not take any more photos. Neither choice is desirable. If you had two memory cards, the corrupted card can be removed and stored away safely and the second card can be inserted into the camera and you can continue taking photos. When you get home, the corrupted card can be inserted into the card reader, and a rescue software (Photo Rescue, http:// www.photorescue.com) can be fired up and most of the photos can be saved.

LCD

Instant gratification! You can see in an instant the photo just shot (but wait for the Cycle Time). It is not recommended that you waste time trying to decide which shots to keep and which shots to discard while taking the shots. Wait until the photos are transferred to your PC, and then make these decisions. Each time you turn on the LCD the power consumption increases by 2 –3 fold, and precious battery life is wasted. Also, when you buy a digital camera, make sure it has an optical viewfinder, and use it for much better shots.

Power

Most digital cameras use standard rechargeable batteries. If you use regular alkaline batteries a digital camera will just eat them up in no time. The most popular batteries are Nickel Metal Hydride (NiMH). Some people might use Proprietary Lithium Ion batteries, proprietary meaning expensive. The lithium ion batteries are very powerful and long lasting, lasting 3-4 times longer than the nickel metal hydride batteries. A warning about these batteries-be very careful how and where you store them. Don't carry them loose in a pocket with anything containing metal. You could start a fire. These batteries should be stored safely in some sort of plastic containers.

Now, what do you do with all these great photos? Print them! In order to get the best quality prints, there are 4 components that impact the quality of the prints:

1. The printer

Use a good quality photo ink-jet printer. Epson, Hewlett Packard, and Canon are the most well known and written up in most photo magazines. They also do have a range of good quality inexpensive printers.

2. Paper

Use good quality paper. This might be somewhat of a surprise, but Epson produces the best quality prints on expensive Epson paper (about $1.00 per an 8.5 X 11 sheet). The same goes for Hewlett Packard and Cannon. Keep in mind that there are certain combinations of paper and printer that will

(Continued on page 25)

(Continued from page 24)
never work. It is not advisable to use Epson paper with a Hewlett Packard printer, or HP paper with a Canon printer. etc. . If you only print about 20 to 30 photos per month, live a little and buy the expensive paper. If you print hundreds of photos per month, look around for deals, but try a few sheets of the paper first before buying a ream or you might be stuck with a ream of unusable cheap paper.

3. Image

As Lee mentioned before, keep your cameras set at the highest resolution and you will get high quality prints. There are two exceptions: a) the use of "raw" or "tiff" mode is mostly for when one needs the highest quality possible. e. g., taking wedding photos where everything is set up, people are standing quietly, the lighting is just right, and the camera is on a tripod. Raw, or Tiff, captures every single pixel and does not compress, creating huge files. b) Taking photos for the Internet, such as for eBay. Use a low resolution that does not require compression and reduces the time between taking the shots and uploading them to eBay. If you keep your cameras at the highest resolution you will have the least compression.

4. Software

The software is the most critically important component in producing good prints. Remember when Lee talked about those square pixels where just 1pixel represented 1 of 16.7 million different colors in a RGB color scheme? Well, printers print round dots, each with a color spectrum of between 5 to 10 thousand different colors in a CMYK (Cyan, Magenta, Yellow and Black) color scheme. For a printer to make the transition from square pixels to round dots, it needs the support of good high quality software that is specifically written to do that job. (Someone actually figured out how to insert a square peg into a round hole!)

CDs

The most important reason for copying digital photos onto CDs is, digital photos have no negatives. If you transfer you photo to your computer, and if you computer fails (and it will by Murphy's law) and you have not copied them to CDs, you are out there up the proverbial creek. Your photos are history. The CD is you "negative".

The format used by digital cameras for compression is JPEG (Joint Photographic Experts Group), a powerful technology and an excellent compression log rhythm. There is, however, an insidious idiosyncrasy you must be aware of with JPEG images. After you have downloaded your photos into you PC. and you pick out a photo to examine and admire, do something with it and save it, it is re-compressed. If you open it again and save it, it is re-compressed again. Each time you open a photo and save it after viewing

(Continued on page 26)

(Continued from page 25)

it, it is re-compressed. Each time it loses a little more detail, eventually becoming one ugly photo. When this happens, and you have a pristine copy of the photo on a CD, re-copy it to the PC and you will have a fresh photo to work on. The best advice is not to save it each time you look at it. You can work with a photo, changing its composition and print it without saving the changes. CDs, when used regularly, also degrade. So make 2 CDs of your photos, keeping one in a safe place.

ACPCUG Club News

June Meeting at Cuyahoga Falls Public Library on June 7th!
Starting time is the usual 6:00 PM, sharp. This is the same ol' place formerly known as Taylor Memorial Library.

Feel free to e-mail **Q&A** questions to your officers (addresses below). If you have several, fine. But don't expect all of a series of questions will be entertained at one time. Your officers have decided to mix them up with the questions from others to more fairly give everyone a chance.

Upcoming Computer Shows:

Peter Trapp at Tadmor Temple, Sunday, **July 18**, 2004
3000 Krebs Drive, Akron, OH.
Exit 120 off I-77 (Arlington Rd.)
Right on Jarvis. Right on Krebs to top of hill. 10am-3pm

Club Officers area code 330, unless noted otherwise			
President	Murray Davis (2003)	440-248-0021	murray5050@yahoo.com
Club Outreach	Rick Lubinski (2002)	928-7179	lubinski@bright.net
Secretary	Walt Ruthenburg (2003)	283-7867	wruthenburg@usa.net
Vice President and Program Director	Frank Ramsey (2001)	699-4711	aframsey@yahoo.com
Treasurer	Jim Albright (2004)	923-8686	jra823a@netscape.net
Newsletter Editor	Art McRowe	666-3189	acpcugnews@yahoo.com
Software Evaluation			