The PULP

Newsletter of the Hartford User Group Exchange

http://www.huge.org Volume 26 Issue 2

H.U.G.E.

Member of Association of Personal Computer User Groups APCUG

UGC™

Apple User Group

February 20th General Meeting:

How to Create a DVD

Stuart Rabinowitz will be demonstrating how to convert video from a variety of inputs to a DVD...

East Hartford Public Library
Main St. & Central Ave., East Hartford, CT.

Q&A Session: 6PM–7:15PM
Meeting starts at: 7:15PM

Huge This Month:

February 20	**General Meeting** See above; 7:15 P.M.
March 5:	Deadline for **ALL** Articles. Please upload articles to editors@huge.org, or give them to the Pulp Editor
March 20:	**General Meeting** Starts at 7:15 P.M.

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATIONS

East Hartford Public Library
Main & Central Avenue
in the Lion's Room(downstairs)

Wethersfield Public Library
500 Silas Deane Hwy.,
Wethersfield, CT

From The Editor

by Pat Teevan

Not much time to talk this month – As usual, I'm running late.

I've started hearing the initial results of the Vista rollout and the first-hand reviews are infrequent and mixed. Infrequent, because most people aren't rushing out to buy it and mixed because, everyone's experience differs somewhat.

Of course, most people will get Vista when they buy a new computer. I've got one friend who has just done that and another who is thinking about purchasing one. This route has the advantage in that, hopefully, the vendor has already made sure that Vista runs properly on their hardware. All you need then is to hope that all the software you rely on will run properly on the new OS.

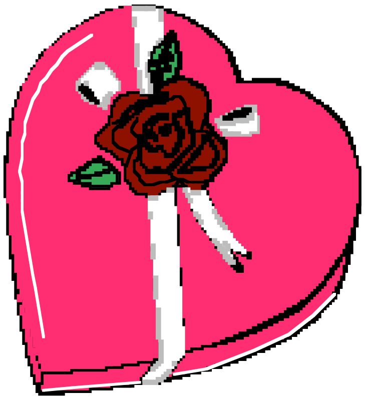
Recent reports indicate the much of Apple's software, including iTunes, Quicktime, Software Update and Bonjour does NOT run correctly on Vista.. Other vendors products are reported to also need updates to run on Vista, so if you're thinking about getting a new Vista PC, check with the vendors to make sure that your software will work or that there's an update available.

For you adventurous souls who might try to upgrade an XP machine to Vista, there are reports that it works and reports that it doesn't. I've been told that there's small print on the back of the box that says a clean install (that's format the drive). "may be required". The specific example I'm aware of is trying to upgrade an XP Pro PC to Vista Home Premium. Since XP Pro has features that are not in Vista Home Premium it's considered a "downgrade" and requires that you do a clean install. Better save your data before trying an upgrade (which is always a good idea anyway).

In case you missed it, last Wednesday, February 14th, was Valentine's Day. Of course, if you did, I'm sure you've been reminded of it by now!

'Til next month…

Happy computing!



A Little Computer Quiz

by Stuart Rabinowitz

January Quiz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

Another month of match the computer name to the picture

1 Altair

2 Apple II GS

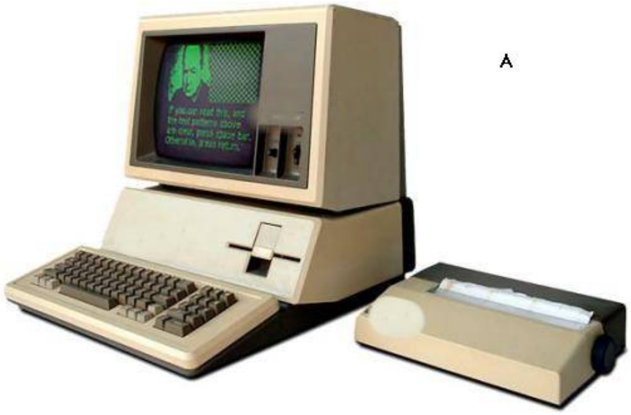
3 Apple IIc

4 Apple III

5 Coleco Adam

6 Kyotronic 85

(Images from; Vintage-Computer.com & Oldcomputers.net)



Pictures for B-F on page 4

December Quiz Answers

1 Beside the fact that they're all highly successful individuals in the computer field, what do Steve Wozniak, Bill Gates, Larry Ellison, Paul Allen, Steve Jobs, and Michael Dell. have in common?

A They are all college dropouts

2 Can you name the computer company each is associated with?

A Steve Wozniak & Steve Jobs started Apple

Bill Gates & Paul Allen started Microsoft

Larry Ellison started Oracle

Michael Dell started Dell

3 Who started a company called PCs Limited?

A Michael Dell. He later changed the name to Dell.

4 What was the original name of Microsoft

A Micro-Soft

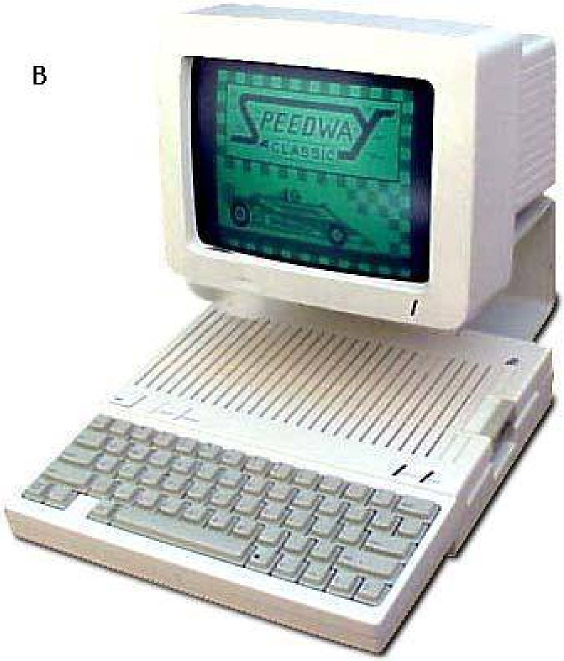
5 Steve Wozniak received a bachelor degree in electrical engineering and computer sciences from what college?

A UC Berkeley in 1986

6 In an effort to shield himself a little Woz used an alias to attend college. What was pseudonym did he use?

A Rocky (after his dog) Clark (his wife's maiden name)

B


SPEEDWAY
CLASSIC

E

C

01 Jan 1900 Sun 00:00:47 (C)Microsoft
BASIC TEXT TELCOM
Select: 29638 Bytes free
ENTER
SHIFT

F

COMPUTER

D

Should You Upgrade to Vista?

Written by Brian K. Lewis, Ph.D., a member of the Sarasota PCUG, Florida
http://www.spcug.org
bwsail at yahoo dot com

As regular readers of this column know, I have been using the beta version(s) of Vista and writing about my experience. I'll grant you that I haven't covered every aspect of the Vista experience. However, it is difficult to touch on everything in an operating system as massive as this. The best I can do is pass on comments on the parts I use frequently. As to the answer to the upgrade question – it's "maybe". I'll give you some of the pros and cons related to my experience.

In deciding whether or not to upgrade you need to determine if your hardware is adequate to run Vista. The system I am using has 768 MB of RDRAM, a 1.2 GHz Intel processor, and an NVIDIA GeForce 2 MMX video card (a correction from previous articles) and an 80 GB hard drive. Frankly, I don't think you would want anything less. A faster processor combined with 1 GB of RAM would be the minimum in most situations. You will also need a DVD drive, as Vista will be sold on DVDs only. From what I have learned it appears that Microsoft will produce only one DVD, but it will contain all the consumer versions of Vista. When you pay for the Vista Basic version and start the installation, the product key that you have to enter tells the setup program which version to install. Then if you decide you need to upgrade to a version with more bells and whistles, you get a new product key that unlocks and installs the upgrade version you paid for. I've already seen some comments on the web that the hackers will be paying for Vista Basic and then will hack the DVD to install the Ultimate version. Let's hope not!

So if you have sufficient hardware then you can go to the next step. What is there about Vista that's better than XP? (Note that if you are still running Win98 or WinMe, plan on upgrading. Both Vista and XP are vastly superior to either of these older, non-supported operating systems.) One thing I found that I really like is Vista's ability to go to the Internet to find device drivers for hardware. It did this very successfully for my sound system. I also installed an external hard drive that usually requires me to dig out the manufacturer's disk to get the necessary drivers. XP frequently forgot the driver and would have to reinstall it whenever I plugged the drive into the USB port. When I plugged the drive into a USB port on my Vista computer, there wasn't even the usual found new hardware notice. So I went looking and in "Computer" I found the hard drive identified and was able to access the file on it. So I just went ahead and did a complete backup. Vista's backup software found the drive and did the complete backup in the background while I continued working. This process did not work with my Epson scanner. Vista did some searching and then said I needed to visit the manufacturer's web site to see if software was available. So you can see that this Internet process doesn't work with all hardware.

Another thing I like in Vista is the added security. I don't like that the firewall is only a one-way blocker, but the scheduled daily parasite check is valuable when you have a cable or DSL connection to the Internet. I don't find the User Account Control (UAC) system to be intrusive as some others have reported. Even when I am working in the Administrator account it is not a problem. I think having to enter a password to carry out operations that affect the system/registry is a good idea. It is one more barrier for any malware to overcome. In addition, when I am working in User mode and want to install a new application, I don't have to remember to right-click the install file and select "Run As". Instead, when I double-click the file I get a permissions window with the Administrator name and a box to enter the password. Much easier and much quicker way to get on with the installation.

I also like the change that has been made in the Start/All programs menu. It keeps you from having to search through multiple columns of programs to find the one you want. Scrolling through a single column list is something I find easier to do. For new computer users, the use of an icon in place of a “Start” button may not be intuitive. However, placing your cursor on the icon does cause the word “Start” to pop up just above the icon. One of the interesting little facets is the speed with which informative small windows pop up when you place your cursor on an icon. There is really no apparent delay, which is quite helpful.

Another change I like is that there is a search box in every directory window. You don't have to go back to the Start menu to initiate a search. Also, your searches can easily be saved. You have the options in each window to select files to burn to a CD/DVD, e-mail, or print. These selections are made using a menu across the top of the window.

When it comes to CD/DVD burning there is one aspect I don't like. That is that the default mode calls for formatting the CD or DVD so that it functions like a removable drive. Microsoft refers to this as the “Live File System”. The problem with this is that the CD/DVD may not be readable in other computers. Their warning implies that the “Live File System” can be read in computers using the Windows XP operating system. However, I found this to be inaccurate, at least as far as the beta versions were concerned. It may be different in the final release version.

You can change the formatting method to “Mastered”. This is the usual way you burn a CD/DVD by copying all the files for that disk at one time. CD/DVDs formatted for the “Live File System” can have files added by “dragging and dropping”. You can also add and erase files. However, on a non-rewriteable disk the file is still there even though it is not accessible. Frankly, there are other burner software programs that I prefer. The third party programs also work much faster than the Vista application.

In Windows XP when you have a file folder open you can move or copy a file that has been selected. When you click on the move or copy icon on the right side of the window you get a browse window which allows you to select a destination either on your local computer or a computer on your network. Vista does not have this function. To move a file or files, you must first select them to be copied. Then you have to go to the destination window and select paste from the right-click menu with your mouse. Then it's back to the original window to delete the files you have copied to the new location. If that sounds like a roundabout procedure, well it is. The XP procedure is cleaner, faster and easier.

Networking is another area where there have been some improvements made. However, if you have a network with both XP and Vista computers, there are still some bugs that have to be worked around. The Windows Help files have eliminated the references related to networking with XP computers. There are no references to the fact the new Internet protocol, IPv6, needs to be installed on XP computers for them to be networked with Vista computers. I couldn’t even find the web page reference in the Help file that give me the details on installing IPv6 on XP computers. Again, this may be changed in the final version or the current build I'm using may not need to have IPv6 installed on the XP computers. But that is something I haven’t be able to determine.

The biggest drawback I see to Vista is the pricing. The $99.95 upgrade for the Home version is the same as with XP Home. Except, this lowest cost upgrade gives you only Vista Home Basic. This version has fewer capabilities than does XP Home. The version of Vista that comes closest to matching XP Home is Vista Home Premium and it carries a premium price; $150.00 to upgrade. Vista Home Basic lacks the Windows Media

Center, DVD video software, and wireless networking provisioning. This latter capability, if available, would provide automatic configuration of laptops in WiFi hotspots. Vista Home Basic does not allow for scheduled backups and does not include backup to a network device. Neither Basic nor Premium allow for image-based backups. They also do not support motherboards with two processor sockets. How this will play out with the Intel Core 2 Duo processors, I really don't know. Vista Home Basic also does not have the new Aero graphic interface. That is found only in the Home Premium, Business and Ultimate versions. Unfortunately I can't tell you about the Aero interface as my computer doesn't support it.

Vista Business is the next higher priced version. It is $199.99 for the upgrade. Although it has the image-based backup capability and wireless networking provisioning, it lacks Media Center capability and as well as the Movie Maker and Video production capabilities. You would have to obtain third party software for these functions if you have a need for them.

Vista appears to be an improvement over XP, but for the average user, it is not a "great leap forward".

So if your only interest in using a computer is for e-mail, web surfing, word processing, then you might be satisfied with Vista Basic. However, you would be just as well off to stick with XP Home for the time being. If you are running a small business from your home you would probably be quite satisfied with Vista Home Premium. So who would need Vista Business or Ultimate? The business version might be useful in a small business with a wired or wireless LAN or where employees require laptops with wireless functions. It also has integrated Fax & Scan software. However, if you needed the Movie Maker, Media Center, or video production capability, then you would have to move up to Ultimate. That has an upgrade price of $259.00.

If you are concerned about the security of Windows XP and the frequent security patches Microsoft has to release, then you can consider that Vista is more secure. That doesn't mean it will never need security patching. Quite the contrary. Any OS, especially one as complex as Vista will have hackers attempting to find its weak points and that will result in the need for security patches.

My concluding thoughts on this are that you will eventually have to move to Vista, unless you want to try an alternate OS such as a Linux version or a Macintosh OS. There are emulator programs for both Linux and Macintosh that permit you to run most Windows software. If you aren't one that always needs the "latest and greatest", then you might consider waiting until you purchase a new computer with Vista pre-installed. I certainly wouldn't recommend that anyone rush out and upgrade as soon as Vista hits the market. Wait a while, possibly until the first patches are available or further reviews of the final market version are available. There also may be some "street pricing" that will lower your cost of upgrading. Vista appears to be an improvement over XP, but for the average user, it is not a "great leap forward".

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:.

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.

Stop! Think! Click!

by Lou Torraca, President. the MOAA Hawaii Chapter Computer User Group, Hawaii
http://www.the-tug.org
president(at)the-tug.org

The world has changed. Today we can work, check bank balances, book travel, research medical questions, talk to friends and family members, order books and music, bid on auction items, and even buy a car without leaving home. Thanks to the Internet, we have access to entertainment, shopping, email and other information, 24 hours a day. This access to information is greater than most folks in my generation could have ever imagined. However, the Internet is not without hazards. The Internet and the anonymity it affords can give online scammers, hackers, and identify thieves access to your computer, personal information, finances and more.

I have written about it before, and so have many others, but with Christmas almost here and many of you already shopping on the Internet, I wanted to provide an update on that Internet bugaboo: SECURITY!!! First of all, for those of you who are concerned about using your credit cards for Internet purchases, a couple of things to consider: first, most CC companies have either a $50 maximum amount which you are liable for if someone uses your # without your permission. In fact, many have a $0 liability policy, sometimes tied to a requirement that you report the use within a certain time-frame. So, step one should be to check with your CC customer service and find out what the policy is. Also, it is possible, with many CCs to get a one-time use # which might be a new account number, or just the 3 digit # on the reverse side of your card. Check with the CC company or the issuing bank. Obviously, you will want to check your CC account regularly to see if any bogus charges have been added and this is pretty easy if you setup an online account. Even easier if your issuing bank or CC company has an alert setup that will notify you if an unusual charge appears. Remember that all the other security measures that affect your computer, e.g. anti virus, anti spy/malware, firewall, updating your operating system, etc. further insure your safety. A good reference is: www.microsoft.com/athome/security/viruses.

The Washington State AARP folks gave an excellent presentation on this topic at the national AARP convention and graciously gave me their permission to use any parts I wanted to for this column. Here are a few of the pretty extensive notes I took.

Protect your privacy and personal information online; if you are asked for personal information such as your name, email, address, telephone number, account numbers, or Social Security number, find out how the information is going to be used before you share it. Find out how the requester protects your personal information. Remember, it is your information.

Whether you are shopping, banking, or conducting other business online, do not provide your personal or financial information through a company's website until you have checked for indicators that the site is secure. Look for "https" in the Web address (the "s" stands for secure). Look for a padlock or an unbroken key in the lower right corner of the status bar. Double-click the padlock or key to ensure that the "issued by" name on the security certificate matches the name in the address bar.

If you get an email or pop-up message asking for personal information, do not reply or click on the link in the message. If you think there may be a need to provide information to the requester (you have an account with the company or have placed

Continues on next page...

an order) con- tact the company directly by telephone. Do not send your personal information via email; it is not a secure transmission method.

Here is an excellent place to review the topic of phishing: www.microsoft.com/athome/security

Anyone can set up shop online. It is a good practice to know whom you are dealing with and what you are getting into. Proceed with caution in your online activities. If you shop online, check out the seller before you buy. A legitimate business or individual seller should give you a physical address and a working telephone number you can call in case you have problems. Call the telephone number before you buy. Never send cash, personal checks or money orders for online purchases. Check out the terms of the deal, like refund policies and delivery dates. The law requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised.

Delete junk email without opening the message. If you open the email, it can alert the spammer that the address is good. Never reply to spam. This includes responding to an option to "Remove me from your list." Do not buy anything or give to any charity marketing through spam. Spammers may swap or sell email addresses of their customers. If you make a purchase as the result of a spam email, it may result in more spam. Do not forward chain email messages. You lose control over who sees your email address. You might also be forwarding a hoax aiding in the delivery of a virus.

Passwords are the key to unlocking your computer and online accounts. A strong password provides better security against hackers and thieves. Strong passwords should be over eight characters in length, combine letters, numbers, and symbols, and should avoid using common words. Do not use your name, your spouse's name, your birthday or location.

Change your passwords regularly or at least every 90 days.

Do not use the same password for each online account you use. Keep your passwords secret. Do not give passwords out to family or friends or send your passwords over email. Do not enable the "Save Password Option" if you receive a dialog box asking you if you would like the computer to remember your password. Do not store written passwords on or near your computer.

Record passwords and store in a safe, secure place. One way to create a strong and memorable password is to think of a "pass phrase." Think of a phrase that is easy to remember like "I save my pennies for a rainy day." Use the first letter of each word as your password, converting some letters into numbers that resemble letters; for example "Ism¢4ard." Notice the combination of upper and lower case letters, numbers and symbols.

Pay attention to what kids do and whom they meet online. Consider a rule that no child reveals personal information, including photos, without permission. Warn kids never to meet Internet "friends" in person. Parental controls are provided by most Internet Service Providers, or sold as separate software. No software can substitute for parental supervision. Talk to your kids and/or grandkids about safe computing as well as things they are seeing and doing online.

Stop and think before you click; before you provide information, open files or attachments, or download files from unknown senders, take a minute to stop and think before you click.

Free downloads can contain spyware. To avoid it, resist the urge to install any software unless you know exactly what it is. You can install anti-spyware software and then use it regularly to scan for and delete spyware programs that may sneak onto your computer.

Email attachments and links sent over email will not damage your computer without your participation. You have to open an email or

Concludes on next page...

attachment that includes a virus or follow a link to a site that is programmed to infect your computer. Hackers use a variety of enticing file names such as “Per your request!” or “Fwd: FUNNY” to get you to open the email attachment or click on the link. Do not open an email attachment unless you expect it and know what it contains. You can help others trust your attachments by including a message in your text that explains what you are attaching.

“Instant messaging” is a form of online communication like email. You can type messages to someone and they can see the messages almost immediately. Files attached to instant messages can also contain viruses. In most cases, viruses spread when you open an infected file attached to an instant message appearing to come from someone you know.

Finally, two things, share your knowledge with others so that they will be more vigilant on the “net and report abuses, including spam, via the Federal Trade Commission http://www.ftc.gov, your Internet Service Provider and your bank or credit union. Most have addresses to use that may begin with phishing, abuse or spoof. Check their web pages for the correct one.

That’s it for now, until next time, have fun with all those computer and electronic goodies, but remember to be careful out there on the ‘net!

Aloha, Lou

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.

Many things you think are safe really aren't

Written by Bob de Violini, a member of the Channel Islands PC Users Group, California
http://www.cipcug.org
rjddev(at)gmail.com

It's not too often I come across something that's a really good read, but I just have. It's an article on the Dark Reading Web site, a site that deals with computer security and is mostly aimed at those who deal with computer security and computer network security for a living. It's quite lengthy by many standards, but it's worth it. The article deals with "myth busting" or spelling out behaviors that many computer end users at work believe is still "safe" (meaning that they don't think they'll hurt the computer network at work) or that they won't get caught at. Point is, someone is still watching, you just will never know when. The title of the article is "The Ten Most Dangerous Things Users Do Online", and can be had at the following URL: http://www.darkreading.com/document.asp?doc_id=107771&print=true . The link will take you to a page with no ads or anything else on the page. It just has the text of the whole article, so you don't have to look at any potentially annoying ads or anything else on the page. You can even print it out and it will probably look pretty good. Some of the terms can be somewhat technical, but that's what we're here for is to answer any questions you may have and to help you have a more enjoyable computing experience, be it online or offline while working on a file or document. If you do have any questions, feel free to send me a note at the email address that appears at the beginning of this article. Bear in mind that the article spells out what users are doing mostly at work or at home with a laptop from their employer, and not from home on their own computers. How many habits that you have right now or may have had in the past are on that list?

To quote Monty Python, "And now, for something completely different…" and I do mean different. There's a Trojan horse type of malware circulating out there that takes the strange step of scanning your system for other malware by installing an anti virus engine. Then, once your system's been cleaned, it then infects your machine with its own code! The Trojan uses an illegal copy of an antivirus application from Kasperky Labs to the scrubbing before it infects your system. The illegal scanner checks your system and deletes anything found after you reboot your system. That's when you get infected with this new Trojan, which goes by the name of SpamThru Trojan. Although there have been other pieces of malware that have blocked the execution of certain competing pieces of malware, this new procedure changes the whole picture. While I'd normally think of a free scan of my system to remove malware or viruses, this is the kind of favor that nobody needs. By now, most of the anti-malware scanners have had their signatures updated to catch this little bug, of go out and update your anti-malware product's definitions, or signatures, if you haven't done so in the last week. This Trojan also uses more sophisticated ways of keeping itself updated and running than others have, but the techniques are beyond the scope of this column.

Now, from the "What's New is Old" department, we have reports of Internet Explorer 7, which was just released on the 19th of October, having a new vulnerability that's actually a holdover from the first early days of IE6. There has been banter back and forth within the computer security community about whether or not it's new and whether or not Microsoft will even fix it. Apparently, Microsoft's been saying that the flaw isn't with the browser, but with it's companion piece of software, Outlook Express. The vulnerability remains unpatched to this day. There's also another bug with IE7 that was also present in IE6 when it was first released in June 2004. At that time, Microsoft said to disable the "Navigate sub frames across different domains" setting in the browser, which would avoid the vulnerability. However IE7 comes with that setting disabled and it is still vulnerable to the bug. At this writing, IE7 is available on the Windows Update site as a High Priority download, and will also be available via the Automatic Updates feature in Windows XP and Windows 2000. Because of the uproar over this vulnerability, I'd suggest avoiding the new browser for a while until Microsoft patches the vulnerability or they release a workaround that actually works. You can set the Automatic Updates feature to just notify you of the updates that are available but not download them, or you can set it to tell you about the downloads and download them for you but not install them. Either of these options will work for avoiding the installation of IE7 for now.

Now for some news from the SANS Institute about some scams and other bugs that have been making the rounds, especially one that infected iPods in Japan. If they were infected in Japan, there's no telling when it will happen on this side of the Pacific. Apple has taken steps to eradicate the bug, but it's still worth noting. Ok, here we go:

QQpass spyware (Trojan variant)

As many as 100,000 Flash MP3 players, given away as prizes by McDonald's in Japan, were found to be infected with a variant of the QQpass spyware Trojan horse program. The players were preloaded with ten songs and the malware. McDonald's Japan has apologized, established a helpline to facilitate the recall of the infected MP3 players, and posted directions for cleaning infected PCs. More information can be had at the following link:
http://www.theregister.co.uk/2006/10/16/mcd_spyware_mp3_recall/print.html

Here is a scam that can potentially snag a lot of folks out of the "fear factor" it implements:

FBI Imprimatur Added to Phishing Scams

Fraudulent phishing e-mails claiming to be from Richard Mueller III, FBI Director, and Donna M. Uzzell, FBI Compact Council Chairman, offer recipients big bucks and threaten big penalties if you don't cooperate.

More information:
http://www.emergencyemail.org/newsemergency/anmviewer.asp?a=155&z=1

This next bit was just too good to not pass along in the The Outer Edge (CIPCUG award-winning newsletter). It explains a term that's being used more and more these days with regards to computer security and the vulnerabilities that are being discovered:

Security Question of the Month: What is a Zero-Day Exploit?

A zero-day exploit (attack) is one that takes advantage of a security vulnerability before or on the day that the existence of the vulnerability becomes widely known. Three or four years ago, hackers needed 7-14 days to figure out how to use a newly discovered vulnerability in order to launch an exploit. That lead time allowed hardware manufacturers and software developers to notify their customers, recommend ways to cope with it, and distribute software patches and anti-virus updates.

But there are more hackers, and they're getting better at what they do. So, how do you defend your computer when you have 0 days to prepare? You can. But if you keep your computer security software up-to-date, you'll help decrease your overall risk and increase the chances that a patch or update will reach your computer ahead of an exploit.

The above pieces were taken from the November issue of OUCH! a computer end user newsletter put out by the SANS Institute via email. More information and previous editions, as well as this month's can be had at the following link:
https://www.sans.org/newsletters/#ouch

Well, that's all for this month. Stay safe out on the Web, and remember to keep your anti virus and anti malware programs fully updated at all times to help prevent future infections from affecting you.

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.

PULP Staff

Interim Editor	Pat Teevan
Distribution	George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries and BBS. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President: __________	George Carbonell	568–0492	george.carbonell@comcast.net
Vice President______	Stuart Rabinowitz	633–9038	s.e.rabinowitz@worldnet.att.net
Secretary: __________	Ted Bade	643–0430	tbade@cox.net
Treasurer: __________	Charles Gagliardi	233–0370	epencil@att.net
Director at Large: __	Richard Sztaba		richer1@aol.com
Web Manager: _____	Bob Bonato		
Membership: _______	Richard Sztaba		richer1@aol.com
Integrated SIG: ____	Stuart Rabinowitz	633–9038	s.e.rabinowitz@worldnet.att.net

February 2007

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1	2	3
4	5	6	7	8	9	10
11	12	13	14 ♥ **Valentines Day**	15	16	17
18	19	20 **General Meeting**	21	22	23	24
25	26	27	28			