Mother Board

This Month At NOPC

Open Office 2.1 by Ray Paternostro

Inside this issue:

VistaVexes
The Windows Vista Pains'n'Gains Page

Written by Jan Fagerholm,
Assistant Editor, PC Community
Hayward, California
http://www.pcc.org
jan-f@pacbell.net

OK, so I've suffered through the betas and RC1 and RC2 (Release Candidate = not quite done yet), and now through two succeeding RTMs (Release To Manufacturing = the finished product) So what's the final version of Windows Vista finally like? Is it worth the pain of upgrade?

I'm not going to spend much time telling you how pretty the Aero interface is, or how cool the Flip3D task switcher is – the computer press has already given lots of space to these features. I intend to relate some experiences with hardware and software that I have encountered. I'll sometimes talk about the new features, as these are the reasons for upgrading to Vista, but I'll mainly be focusing on the stumbling blocks, as these are the reasons that you may want to wait until the problems that relate to

This Month's Presentation

Our meeting program for January will be Open Office 2.1 by our past club president and current vice president Ray Paternostro Jr. Different aspects of this free office suite will be demonstrated as well as how it stacks up to Microsoft Office.

The full installation of Open Office contains five programs: a word processor, a spreadsheet, a presentation program, a database, and a vector drawing program. It is open source software which means that it is collaborated on by many different authors and is free for anyone to download and use. For more information or to download and install it, point your web browser to http://openoffice.org.

Mark your calendars with a black/gold pen, create an entry in your Palm Pilot, HP or Dell pocket PC, update Outlook (all versions) and join us on Wednesday, January 3, 2007 for a fun and informative evening. The monthly meeting of the NOPCC starts at 6:30pm on the first Wednesday of every month. Location of the meeting is the J.D. Meisler school cafeteria at 3700 Cleary Ave. Metairie. Use the entrance through the breezeway on Pharr Street.

New Users SIG—Schedule

The New Users SIG usually meets the third Thursday of the month. Our meetings are from 6:30PM to 8:30PM. Each month, our moderators (Don Herrmann and Tom Ford) will present several tips for improving your computer skills plus general information about hardware and Windows software. The remainder of the meeting will be spent answering your questions and solving your computer problems. While some of our attendees are new users, we welcome all members who have general computer questions or problems; in fact, let us know your question or problem and we will have the answer waiting for you at the meeting.

We meet at the Old Metairie Library at 2350 Metairie Road. The meeting room is to your left as you enter the library, past the circulation desk. There is additional parking for this library at the American Legion Hall on 2431 Metairie Road. View a map.

You can reach Don at 831-1284 <donobevo@cox.net> and Tom at 985-643-3172 <tomford@bellsouth.net>.You can use 985-502-5654 on the day of the meeting.

Because of a scheduling conflict, the January and March 2007 meetings will not be on the third Thursday but on the date shown below:

Date	Day	Start	End	Date	Day	Start	End
1/11/2007	Thursday	6:30 PM	8:30 PM	7/19/2007	Thursday	6:30 PM	8:30 PM
2/15/2007	Thursday	6:30 PM	8:30 PM	8/16/2007	Thursday	6:30 PM	8:30 PM
3/8/2007	Thursday	6:30 PM	8:30 PM	9/20/2007	Thursday	6:30 PM	8:30 PM
4/19/2007	Thursday	6:30 PM	8:30 PM	10/18/2007	Thursday	6:30 PM	8:30 PM
5/17/2007	Thursday	6:30 PM	8:30 PM	11/15/2007	Thursday	6:30 PM	8:30 PM
6/21/2007	Thursday	6:30 PM	8:30 PM	12/20/2007	Thursday	6:30 PM	8:30 PM

(Continued from page 1) Vista Vexes

you are resolved. If you went through the XP changeover five years ago, you are in for a similar experience with Vista.

I've previously written bits about Vista and done Vista presentations for PCC, and now hope to provide you with some insights gained from experience with the final version of Vista. I plan to submit a "pains & gains" column on Vista to PCC News over the next few months as it makes its way into the marketplace and on to your desktop. What I can offer here is some real-world experience with hardware and software support, as well as a perspective gained from a programmer's view of the workings of Vista and how it affects you through the interface, as well as a comparison to other OSs that I regularly use, Linux and Macintosh OSX.

I am an unabashed Linux geek, so what am I doing messing with Vista? I tell myself that I need to know Vista because my Windows clients are going to ask me about it, and I need to give them a better answer than Microsoft's marketing department will give them. I participated in the beta program and even rejoined MSDN

(Microsoft Developers Network) for the carrots they offered, one of which was a downloadable .ISO image of the final RTM version when it was released to MSDN on Nov. 17th. There is some real-world pain involved with upgrading to Vista, and I'd like to relate some of these experiences, for you shall certainly share my pain if you decide to go with Vista the minute it hits the street.

First, a bit of background on Vista: five years in the making, yet still rushed to finish on time. The Upgrade Install bug in the Nov. 8th RTM release, which destroyed existing XP installations, was fixed and the RTM was re-released on MSDN on Nov. 17th. This RTM version is the one that is going to computer manufacturers so they can pre-install it on the computers they sell.

After all this introduction, let's get on to some hard information. Bear in mind that I am talking about the final version of Vista, not the beta or RC versions.

Though I mentioned this previously, it's worth mentioning again because it will affect every-

(Continued from page 2)

body. Vista has a new security feature called "User Account Control" that is intended to protect the system from "unauthorized changes" that can affect the system or other user's settings, particularly from malware and spyware. It does this by popping a dialog in your face every time something tries to write to certain system or user folders. It also does this whenever you attempt to do a normal software installation even if you are logged in on an administrator account. It came up during installation of Microsoft, Adobe and Corel software. In the case of Adobe and Corel software, it also made the installation fail, even though I told it to allow the changes during installation. Installation of this software did not succeed until I turned off User Account Control. To turn off User Account Control, go to Start -> Control Panel -> User Accounts -> and click the link for "Turn User Account Control on or off". Once you have turned it off, Security Center will complain that it is off, and penalize you by reminding you it is off every time you log on to the system, but this is a small price to pay for normalizing the system.

Among the hardware that you can expect to lose with Vista is the ubiquitous Creative Sound Blaster Live! 5.1 series of sound cards. Vista has a two-channel audio driver for the card, but you lose 5.1 surround sound and the game port. Thus, I not only lose 6-channel capability of my $100 5.1 Surround speaker system, I also lose the use of my $120 Microsoft Force Feedback Pro joystick. Creative's Web site says they do not plan Vista support for the Live! 5.1 series of sound cards – I must upgrade to at least a $150 X-Fi card to get back both of these capabilities. I am NOT pleased, as I have Live! 5.1 cards in two of my computers.

Judging from manufacturers' Web sites, many scanners are going to be abandoned under Vista as well. This is similar to what happened when XP came out. (i.e. The manufacturer chose not to write an XP driver for the scanner.) My HP Scan-Jet 6300C doesn't work in Vista, and HP's Web site is depressingly silent about scanner support in Vista. Of the twenty or so different scanners of different make that I have plugged into Vista, none of them over two years old would work.

Printer support, on the other hand, is quite good. Judging from the printer database, it looks like almost everything that works under XP will also work in Vista. The Vista drivers are as rudimentary as XP's though -- you will need to get the manufacturers' drivers for high resolution printing in many cases.

Early returns are in on Vista. Many of the developer forums that I belong to are abuzz with Vista experiences, from installation (or failure thereof) to device support (or failure thereof). I intend to relate more of these in upcoming articles.

The next article should be your New Year's Resolution—Editor

Stop! Think! Click!
By Lou Torraca,
President. the MOAA Hawaii Chapter Computer User Group, Hawaii
http://www.the-tug.org
president@the-tug.org

PULL QUOTE "...most CC companies have either a $50 maximum amount which you are liable for if someone uses your # without your permission,... "

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 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 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

Where Does It End?

SCENE 1.
This is a new one. People sure stay busy trying to cheat us, don't they?
A friend went to the local gym and placed his belongings in the locker. After the workout and a shower, he came out, saw the locker open, and thought to himself, "Funny, I thought I locked

the locker. Hmm, "He dressed and just flipped the wallet to make sure all was in order. Everything looked okay - all cards were in place.

A few weeks later his credit card bill came - a whooping bill of $14,000! He called the credit card company and started yelling at them, saying that he did not make the transactions. Customer care personnel verified that there was no Mistake in the system and asked if his card had been stolen. "No," he said, but then took out his wallet, pulled out the credit card, and yep - you guessed it - a switch had been made.

An expired similar credit card from the same bank was in the wallet. The thief broke into his locker at the gym and switched cards.

Verdict:
The credit card issuer said since he did not report the card missing earlier, he would have to pay the amount owed to them.

How much did he have to pay for items he did not buy? $9,000!

Why were there no calls made to verify the amount swiped? Small a mounts rarely trigger a "warning bell" with some credit card companies. It just so happens that all the small amounts added up to big one!

SCENE 2.
A man at a local restaurant paid for his meal with his credit card. The bill for the meal came, he signed it, and the waitress folded the receipt and passed the credit card along. Usually, he would just take it and place it in his wallet or pocket. Funny enough, though, he actually took a look at the card and, lo and behold, it was the expired card of another person.

He called the waitress and she looked perplexed. She took it back, apologized, and hurried back to the counter under the watchful eye of the man.

All the waitress did while walking to the counter was wave the wrong expired card to the counter cashier, and the counter cashier immediately looked down and took out the real card.

No exchange of words --- nothing! She took it and came back to the man with an apology.

Verdict:
Make sure the credit cards in your wallet are yours. Check the name on the card every time you sign for something and/or the card is taken away for even a short period of time. Many people just take back the credit card without even looking at it, "assuming" that it has to be theirs. FOR YOUR OWN SAKE, DEVELOP THE HABIT OF CHECKING YOUR CREDIT CARD EACH TIME IT IS RETURNED TO YOU AFTER A TRANSACTION!

SCENE 3:
Yesterday I went into a pizza restaurant to pick up an order that I had called in. I paid by using my Visa Check Card which, of course, is linked directly to my checking account. The young man behind the counter took my card, swiped it, then laid it on the counter as he waited for the approval, which is pretty standard procedure.

While he waited, he picked up his cell phone and started dialing. I noticed the phone because it is the same model I have, but nothing seemed out of the ordinary. Then I heard a click that sounded like my phone sounds when I take a picture.. He then gave me back my card but kept the phone in his hand as if he was still pressing buttons.

Meanwhile, I'm thinking: I wonder what he is taking a picture of, oblivious to what was really going on. It then dawned on me: the only thing there was my credit card, so now I'm paying close attention to what he is doing. He set his phone on the counter, leaving it open. About five seconds later, I heard the chime that tells you that the picture has been saved. Now I'm standing there struggling with the fact that this boy just took a picture of my credit card.

Yes, he played it off well, because had we not had the same kind of phone, I probably would never have known what happened. Needless to say, I immediately canceled that card as I was walking out of the pizza parlor.

(Continued from page 6)

All I am saying is, be aware of your surroundings at all times. Whenever you are using your credit card take caution and don't be careless. Notice who is standing near you and what they are doing when you use your card. Be aware of phones, because many have a camera phone these days.

When you are in a restaurant and the waiter/waitress brings your card and receipt for you to sign, make sure you scratch the number off. Some restaurants are using only the last four digits, but a lot of them are still putting the whole thing on there.

I have already been a victim of credit card fraud and, believe me, it is not fun. The truth is that they can get you even when you are careful, but don't make it easy for them.

<div align="center">

JUST BE AWARE
Submitted by an anonymous NOPCC member

</div>

EDITOR– While the source and veracity of this last article has not been determined, the point of the article is worth considering in any case. We all are lax in our use of our credit cards.

CLUB SUPPORTERS

January 2007

SUN	MON	TUE	WED	THU	FRI	SAT
	1 *Happy New Year*	2	3 **NOPC Gen Mtg** J.D. Meisler School 6:30p-8:30p	4	5	6 **Living with Home Electronics** WIST 690AM 10a-11a
7	8	9	10 **NOPC BOD** @ McCann's 6:30p-8:30p	11 **New User SIG** Old Metairie Library 6:30p-8:30p	12	13 **Living with Home Electronics** WIST 690AM 10a-11a
14	15	16 **Genealogy SIG** 7:00 pm Call 887.5746 for meeting location	17	18	19	20 **Living with Home Electronics** WIST 690AM 10a-11a
21	22	23	24	25	26	27 **Living with Home Electronics** WIST 690AM 10a-11a
28	29	30	31			

The New Orleans Personal Computer Club (NOPCC) is a private non-profit organization chartered under the State of Louisiana. Its purpose is to provide an open forum for discussion and education of the membership in the use and application of PCs, peripheral equipment and software. The opinions expressed in this newsletter are those of the author (s) and do not necessarily reflect those of the NOPCC , its members or its officers. The club does not verify for accuracy the articles in this newsletter and leaves verification of accuracy to its readers. Articles in this newsletter may be duplicated as long as credit is given to the author (s) and the NOPCC. Annual Dues Schedule: Regular Member, $40/yr.; Family Membership, $60/yr.;

NOPCC Directory

Elected Officers

President	Tom Ford	president@nopc.org	985-643-3172
Vice President	Ray Paternostro	vp@nopc.org	737-9099
Secretary	Mary Prinz	secretary@nopc.org	455-1412
Treasurer	Don Herrmann	treasurer@nopc.org	831-1284
Director At Large	Mike York	director1@nopc.org	738-5997
Director At Large	Scott Minvielle	director2@nopc.org	
Director At Large	Jeanne Okamoto	director3@nopc.org	455-0977

Standing Committees

Newsletter Editor	Edward Jahncke	editor@nopc.org	985-892-4797
Public Relations	Jeanne Okamoto	pr@nopc.org	455-0977
Publicity	Jeanne Okamoto	pr@nopc.org	455-0977
Webmaster	Sherrie Henne	webmaster@nopc.org	504-913-5638

Special Interest Groups

Computer Programming	Elliot Mike York	mike@gnonug.org	738-5997
Digital Media	Ray Paternostro	dm@nopc.org	737-9099
Genealogy	Vincent Haupt	hauptv@aol.com	985-785-6288
Internet	Ray Paternostro	internet-m@nopc.org	737-9099
New Users	Tom Ford	new-user@nopc.org	985-643-3172
Web Lab	Edward Jahncke	editor@nopc.org	985-892-4797

Other Important Numbers / Addresses

Club Hotline	Recorded messages. Meeting Information. Open 24 Hours	887-5746
NOPCC Web Site	On the World Wide Web. Our own home page and club information.	*www.nopc.org*