The New Orleans Personal Computer Club Newsletter

MotherBoard

Volume 23, Issue 7 July 6, 2005

This Month At NOPC

Stump The Experts Presented By

?

Inside this issue:

July Door Prize
Synonymous Humor 2
Slipstreaming

Slipstream (cont'd)
Positive Outlook 3
What is Spyware?
Portable Blood Pressure Units

BP Units (cont'd)
Managing Bookmarks
Don't Let Thieves Steal 4
Your Good Name

Thieves (cont'd) 5

Barnacle –definition
Time to Lighten Up! 6

NOPCC Directory 7-8

Calendar of Events

Norton Internet Security 2005

Norton Internet Security 2005 is the easiest and most complete online security and privacy suite for home users and small offices. With virus protection, privacy protection. Intrusion prevention, a firewall, and spam filtering, Norton Internet Security 2005 offers users the best way to maximize protection and improve their online experience without having to worry about product integration and compatibility. Norton Internet Security 2005 offers protection from spyware, keystroke logging programs and includes new outbreak notification alerts. Enhance privacy control, and superior spam filtering.

The Norton Internet Security 2005 suite features the latest versions of Norton AntiVirus, Norton personal Firewall, Norton Privacy Control, Norton AnitSpam, and Norton Parental Control.

Key Features:

- Advanced intrusion prevention technology inspects the content of Internet traffic for online attacks such as Blaster and Sasser and then automatically blocks these attacks.
- Detects non-virus emerging threats such as spyware and keystroke logging software programs alerts users to take proper action.
- Scans and removes viruses from incoming attachments from AOL Instant Messenger, MSN Messenger, and Windows Messenger.
- Ad blocking keeps banner ads. Pop-up windows , and other Web distractions off the screen.
- Automatically filters spam in any standard POP3 email connections; integrates with Microsoft Outlook, Outlook Express, Eudora, Hotmail, and Yahoo! Mail.
- Prevents confidential information from being sent through standard POP3 email clients , Microsoft Office attachments, and MSN Messenger, Windows Messenger or AOL Instant Messenger without the users knowledge.

Stump the Experts

Our meeting on July 6th will be different from our regular meetings. Instead of a speaker, a team of your fellow members will answer (or try like heck to answer) your questions about computer hardware, software and noware. Any question is welcome from basic to advanced. This meeting is the time to ask that question and harness the power not only of our expert team but of all the NOPCC members. If you want to insure your questions are addressed, call your question into our Hotline at 887-5746 or email tomford@bellsouth.net. We will have the answers waiting for you at the meeting.

Mark your calendars with a red/green pen, create an entry in your Palm Pilot, HP or Dell pocket PC, update Outlook (all versions) and join us on Wednesday, July 6, 2005. 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.

(Continued from page 1)

- Identifies virus infections in Windows XP/2000 compressed file archives in real time, even before those files are used.
- Smart Filtering engine learns what is and isn't spam; by analyzing user's outgoing messages.
- Prevents friendly messages from being tagged as spam; identifies specific email addresses and domains as spammers.
- Network Detector enables the user to define firewall settings for different networks and the automatically switches to the proper settings for the current network.
- Automatic LiveUpdate checks for new protection updates when the user is online. Keeping the user protected without interrupting work. Automatically updates virus definitions , firewall rules, antispam software, intrusion prevention signatures to ensure users have up-to-date protection.

System Requirements:

The Norton Internet Security 2005 suite is compatible with Win98, ME, XP Home or Professional and Windows 2000. The following is required for all Windows installations:

- 60 Mb of available hard disk space (without Parental Controls feature installed)
- 116 Mb of available hard disk space (complete)
- CD-ROM
- Microsoft Internet Explorer 5.01 or alter.
- Microsoft Windows Internet support.0.

For additional information, click on the following link to got to the Symantec Norton Internet Security 2005 web page: http://www.symantec.com/sabu/nis/nis_pe/

July Meeting Door Prize

Thanks to the generosity of Symantec, the Door Prize for the July, 2005 NOPC General Meeting will be a copy of Norton Internet Security 2005 suite.

Remember...you have to be a member and in attendance at the meeting to have a chance to win this prize.

Synonymous Humor

Two trucks loaded with thousands of copies of Roget's Thesaurus collided as they left a New York publishing house last Thursday...

According to the newspaper, witnesses were stunned, startled, aghast, taken aback, stupefied....

Submitted by Jeanne Okamoto
Member, NOPC

Slipstreaming

Prior to Windows XP with SP2, if you had a problem with one of the applications within Windows, all one had to do was to uninstall that module and then using the Operating System CD, re-install it. If you tried with Windows XP after the installation of Service Pack 2, you were surprised to receive a warning window that the version of window installed was newer than that on your original System CD.

After much consternation, I learned that all one had to do was to install the Service Pack 2 CD (which luckily I had) and then insert the original Windows XP Operating System CD to re-install the ailing application.

This seemed to me to be a complicated and annoying way to do things. It also required that I now keep track of not one, but two, OS CD's. And then I discovered ***slipstreaming.*** Basically slipstreaming is the melding of the Windows XP Operating System with Windows XP Service Pack2 onto a bootable CD. This will require that you have the following:

- The Windows XP Operating System CD
- A copy of Windows XP Service Pack 2, either on a CD or in a distinct folder on your hard drive.
- A CD "burner" (or a DVD "burner")
- Burner software such as Nero Burning Rom 6-SE or Roxio Easy CD and DVD Creator 6.

Space on your hard drive to do this. No space requirements can be found, but since each CD can hold up to 700 Mb, I figure 2 Gb should be more than enough, and are only needed while generating the *skipstreamed* disc.

How to do this:

1. Created three folders named:

a. XP
b. XP-SP2
c. XP-BootImage
d. Copy the Windows XP CD to the XP folder. Before copying make sure the system is set up to display all hidden and system files to ensure a complete copy of all files on the CD. These settings can be found located in Windows Explorer>Tools>Folder Options>View Tab. Make sure the [Show hidden files and folders} radio button is selected and [Hide protected operating systems files] is unchecked.
e. If you have a SP2 CD, copy it to the XP-SP2 folder.

(Continued on page 3)

(Continued from page 2)

If you do not have c CD, then locate the downloaded Windows SP2 file on your hard drive and copy it to the XP-SP2 folder. If you have neither, download the file from the Microsoft web site to this folder. The file is most likely named WindowsXP-KB835935-SP2.ENU.exe.

f. Using the RUN dialogue, extract the contents of SP2 to the XP-SP2 folder.

g. Again, using the RUN dialogue, apply the extracted Service Pack to Windows XP.

h. The RUN dialogue is accessed from [Start][Run]. The command to apply the Service Pack is d:\XP-SP2\i386\Update\Update.exe –S:d\XP (where d: is the directory/drive where these folders reside.

i. Upon completion, the files in the folder XP will be updated to contain SP2.

j. That was the easy part…to complete this *slipstreaming* process, you must **extract the imaging file.** In order to make a slipstreamed CD bootable it's necessary to add an image file during the burning process. You need to extract the file Microsoft Corporation.img and save it to a folder [XP-BootImage] There are a number of ways to perform the extraction but the easiest is to use ISO Buster. This application can be downloaded from www.isobuster.com.

k. Install ISO Buster onto your hard drive.

l. With the Windows XP CD in your CD drive, open ISO Buster and. Click on Bootable CD in the left pane and then right click Microsoct Corporation.img in the right pane, finally clickin Extract Microsoft Corporation,img file.

Extract the file to the XP-Bootable folder created in step 1.c.

With the preparation out of the way it's time to actually burn the CD. There are a number of different burning or CD creation programs that can be sued to accomplish the task. Rather than go thru the step-by-step instruction for two of the better known programs (Nero Burning ROM 6-SE) (Roxio Easy CD Creator 6), I will provide links to these instructions. While the terminology and screens may vary depending on your CD burning program choice and version, the principles remain the same and can easily be adapted no matter what burning software is being used. For Nero Burning ROM 6-SE instructions, click on:

http://www.theeldergeek.com/slipstreamed_xpsp2_cd_nero.htm

For Roxio Easy CD Creator 6, click on:

http://www.theeldergeek.com/slipstreamed_xpsp2_cd_roxio.htm

Once you have completed this project, you will now have one CD to use to reinstall Windows XP applications including any modifications up to and including SP2. Now you won't get the warning that your current installed Operating System is newer than that on the CD. Also, should any additional Service Packs be provided by Microsoft, you will know how to *slipstream* your operating system to include this modification.

This article was extracted from a very helpful website named *The Elder Geek.on Windows XP* . Should you ever have any problems with Windows XP, I would recommend that you check this site out first.

Submittted by
Edward Jahncke
Editor - Motherboard

HOW TO START YOUR DAY WITH A POSITIVE OUTLOOK

1. Open a new file in your PC.
2. Name it "Housework."
3. Send it to the RECYCLE BIN
4. Empty the RECYCLE BIN
5. Your PC will ask you, "Are you sure you want to delete Housework permanently?"
6. Answer calmly, "Yes," and press the mouse button firmly....
7. Feel better?

What is Spyware

Spyware is usually defined as software that installs itself without your consent, collects indiscriminate data about you and your online habits, and sends that information somewhere without your permission. It may target you for ads, too, like adware. Adware is similar to spyware, but it generally asks you before installing itself (albeit perhaps in obscure language in the fine print of a EULA [End-User License Agreement]) and collects less personally identifiable data about you. At the same time, these can slow your computer down, cause your system to be unstable, and even open the door to hackers. Your PC can catch spyware just from visiting particular Web sites, or from installing certain freeware and shareware. Several examples can enter your computer through vulnerabilities in the IE browser and Windows, although some can also burrow in through other browsers, OSes, and applications such as instant messaging clients.

Reprinted with permission from Smart Computing

Editor—While the following is not directly computer related, it may be of interest to our club members:

Portable Blood Pressure Units

Convenience caters to the health-conscious in Pana-

(Continued on page 4)

(Continued from page 3)

sonic's new lineup of portable blood pressure and heart rate monitors (www.panasonic.com). Two of the four new models, the EW3003W ($59.99) and EW3037S ($89.99), fit neatly around your wrist. They employ Panasonic's Digital Filter Technology, which reduces or eliminates some of the movement and noise made by arm units and results in more accurate readings. In fact, the wrist units monitor a person's vital signs while inflating, which makes for a quicker read. The EW3003W stores the last 21 readings and, when placed in its compact case, is just 2-inches thick. The EW3037S retains the last 90 readings and also features a three-times-daily reminder system. Both of these models operate on two AAA batteries. Panasonic's EW3106W ($59.99) and EW3122S ($89.99) models are for use around the upper arm. The former retains 21 readings in its memory, while the latter can save up to 42 readings each for two users. The arm units run on four AA batteries. All four models will be available in June.

Reprinted with permission from Smart Computing

Managing Bookmarks

Regardless of which browser you use, the best place to begin organizing your bookmarks is the Manage Bookmarks window. (Click Manage Bookmarks in the Bookmarks menu.) From here you can organize your bookmarks into existing folders and make new folders. Bookmarks appear nested under each folder, and double-clicking a folder lets you show or hide the contents of that folder. You can organize your bookmarks by dragging and dropping them into folders. A URL (uniform resource locator, or Web address) appears beside each entry in the Location column. You can always edit an entry's name or location by right-clicking the item and selecting Properties. You can also delete a bookmark or folder by selecting the item and clicking Delete in the toolbar near the top of the window. To create a new folder, simply click New Folder in the toolbar, choose a name, and then drag and drop it where you want it. You may also wish to create separators to organize your folders into groups; click New Separator from the toolbar and drag and drop the separator into position.

Reprinted with permission from Smart Computing.

Don't Let Thieves Ruin Your Good Name

Secure Sensitive Information & Thwart Identity Theft

Amy Dolinsky, a 21-year-old college student, noticed several unauthorized transactions from her checking account. She found two $50 charges from Google Answers and a charge from SaksFifthAvenue.com for over $600. When she contacted the bank, it informed her there were other transactions for thousands of dollars that did not post to her account because of insufficient funds. However, the other charges still put Dolinsky's account in the red.

Dolinsky believes this happened because of a phishing scam email she received from what she believed to be PayPal. The email asked her to verify her debit card number, which made sense because she had just received a new card the week prior. She followed the directions in the email and entered her new number. Unbeknownst to her, she gave a thief personal information.

The FTC enables consumers to request their free report from the major credit bureaus through www.annualcreditreport.com. This map from www.annualcreditreport.com shows when free reports are available.

After filing paperwork with her bank, the Federal Trade Commission, and merchants, Dolinsky was only out a $5 fee Saks Fifth Avenue assessed. "I paid five bucks to have my identity stolen," she said.

Many companies offer a security resource center. PayPal's Security Center shows users what fraudulent emails often look like.

Because she regularly evaluates her account information online, she was able to promptly spot the problem and contact the appropriate institutions, thereby minimizing her financial loss.

According to an FTC survey, more than 27 million Americans have become victims of identity theft, a crime in which a thief uses the victim's name and other sensitive information to fraudulently open bank accounts, use credit cards, and initiate financial pandemonium. Most cases involve dumpster divers and dishonest store clerks, not online hackers.

As technology changes, thieves find new means to steal information. Phishers send emails asking recipients to "verify" personal data. Their emails and Web sites display corporate logos and mimic nomenclature derived from the company they are pretending to represent. Phishing scams often target financial institutions and popular online services such as eBay.

Avoid Identity Theft

There are a number of measures that you can take to secure personal information from reaching the hands of

(Continued on page 5)

(Continued from page 4)

thieves. Many may seem superfluous, but they are vital to keeping private data just that.

Protect your Social Security number. Many organizations use Social Security numbers to identify employees, customers, patients, and members: Ask if you can substitute another number. Many businesses use phone numbers or other unique ways to identify people in databases.

Don't keep your Social Security card on you. It should be kept in a secure place inside your home. The same is true for any documents that have the number printed on them.

Don't respond to email scams. Phishers send requests for personal information via email to unsuspecting consumers. It's hard to identify these bogus emails because they often look like those companies might send—instead, the messages are intended to lure individuals into divulging private information to supposedly verify an account. These companies never ask users to verify personal data via email once their account is created. Most financial companies have an antiphishing security group you can forward the message to to determine a message's authenticity.

The FTC established the ID Theft site (www.consumer.gov/idtheft) to educate consumers about the forms of identity theft and how to thwart it.

Secure your credit card number. When ordering items over the phone, be sure no one is eavesdropping. It may seem like second nature to rattle off your credit card number, but people in other rooms or offices can sometimes hear conversations. Cordless phones often interfere with each other. Be sure to use a corded phone on a landline instead of a cordless or cell phone when reciting your personal data.

Shred sensitive information. Don't toss those unsolicited pre-approved credit offers. Dumpster divers use these to apply for credit cards in your name and have the statements sent to their address, making it difficult to catch in a timely manner. Buy a shredder to destroy those credit offers and other personal documents. If you keep a file of your financial statements, be sure it is in a secure location. The same goes for sensitive information on your computer. Most financial software lets the user set a password.

Stop getting pre-approved offers. Opt out of receiving unsolicited credit offers through postal mail. Visit www.optoutprescreen.com to tell creditors not to send you anymore offers. It may take some time before they stop coming because many institutions already have your information on file, but when they update and you aren't on the new list, the offers should stop.

Reclaim Your Identity

If you suspect that someone is wreaking havoc with your name, there are a number of steps you can take to get things back on track.

Alert financial institutions. One of the first steps to take is to inform your bank and close any accounts the thief tampered with or fraudulently opened.

Place a fraud alert on your credit report. Contact the three major credit bureaus: Experian (www.experian.com), Equifax (www.equifax.com), and TransUnion (www.transunion.com). The fraud alert tells creditors they must contact you before authorizing any changes to accounts associated with your name. The bureaus may keep the alert on a report for up to seven years.

The Identity Theft Resource Center (www.idtheftcenter.org) gives victims tools to minimize financial loss and get started rebuilding their lives.

Obtain a police report. Many credit organizations require proof of identity theft in the form of a police report. Without this, creditors might think that you are simply irresponsible with your finances and looking for an easy way out. Contact the authorities in the community where the crook actually took fraudulent actions. This is often hard to tell with online fraud, so contacting your local law enforcement can be a good starting point.

Notarize an ID Theft Affidavit. The FTC offers a form that that creditors widely accept as proof of innocence in an identity theft case. Download the form and get other support materials from www.consumer.gov/idtheft.

When communicating with so many organizations about accounts, remembering every conversation can become difficult. Keep a log of each phone call with the date and time, person's name, phone number, company, department, and resolution or synopsis of the call. Keeping a record of communication is helpful in keeping a checklist of what institutions you need to contact.

Obtain a free copy of your credit report. The FTC recently mandated that each credit bureau provide consumers with a free report each year. The bureaus don't offer the free report directly to the consumer; you must order

(Continued on page 6)

(Continued from page 5)

your report via the FTC's page at www.annualcreditreport.com. The beginning availability of these reports varies by geographical location. All U.S. residents will have access by Sept. 1, 2005. Go to www.annualcreditreport.com to see when your region will be eligible.

When you get your report, scrutinize every entry to make sure you were the initiator. If there are any discrepancies, report them to the credit bureau from which you received the report and the institution claiming to have an account with you.

Regularly review your credit report. With three bureaus, it's sensible to space your reports out and order one from a different bureau every four months.

Safety First

Take extra precautions, including reviewing financial statements and securing private data, to ensure you don't become a victim.

by Brian Weed

Reprinted with permission from Smart Computing

Visit http://www.smartcomputing.com to learn what Smart Computing can do for you

barnacle

In a computer, a barnacle is unwanted programming, such as adware or spyware, that is downloaded and installed along with a user-requested program. Barnacles usually fall under the category of potentially unwanted programs (PUPs), a euphemistic term coined by McAfee to refer to programs that a user installs unintentionally, perhaps having unknowingly consented to their download. The term derives from the name of a crustacean that attaches itself to whales and boats, among other things. Like its marine counterpart, the computer barnacle can be difficult to eradicate. According to PC Mechanic, barnacles often use confusing uninstall wizards. Another tactic that a barnacle may use is to require the user to fill out an online form to uninstall. Because the host system is quite likely to be clogged with spyware, there may not be sufficient resources available to allow them to do so. Computer barnacles, like other spyware, can seriously affect computer performance. Unlike most spyware, however, they may also cause damage. Some barnacles interfere with the Winsock code that handles input/output requests for Internet applications in Windows operating systems. Winsock runs between a program (such as a browser) and the program that uses TCP/IP. Removal of this type of barnacle may corrupt Internet protocols and degrade network performance, in which case the user must reinstall the TCP/IP stack. The term barnacle is closely related to drive-by download, which is programming downloaded without user consent and often without the user's knowledge that any download has occurred.

Submitted by Tom Watkins
NOPC– Member

Pun In Poland

A steam locomotive passing through Poland one night was running low on coal. The engineer says to his fireman, "We're coming to a town, let's stop and send the porter out to get more coal. It's pretty dark but can you see the name of the town on the depot sign?"
The fireman replies, "Ah...it appears to be Danzig in the dark."
And the engineer shouts, "Buy coal, Porter!"

Words That Don't Exist...But Should...

Aquadextrous (akwa deks' trus) adj. Possessing the ability to turn the bathtub faucet on and off with your toes.

Elbonics (el bon' iks) n. The actions of two people maneuvering for one armrest in a movie theater.

Peppier (pehp ee ay') n. The waiter at a fancy restaurant whose sole purpose seems to be walking around asking diners if they want ground pepper.

Pupkus (pup' kus) n. The moist residue left on a window after a dog presses its nose to it.

Thanks, Jeanne Okamoto
NOPC Club Member

NOPCC Directory

Elected Officers

President	Ray Paternostro	president@nopc.org	737-9099
Vice President	Clarke Kissel .	vp@nopc.org	828-5678
Secretary	Carl Henderson	secretary@nopc.org	466-3954
Treasurer	Don Herrmann	treasurer@nopc.org	831-1284
Director At Large	Albert Fox	director1@nopc.org	269-5786
Director At Large	Mary Prinz	director2@nopc.org	455-1412
Director At Large	Tom Ford	director3@nopc.org	985-643-3172

Standing Committees

BBS SysOp	Lanny Goldfinch	sysop@nopc.org	482-5066
Newsletter Editor	Edward Jahncke	editor@nopc.org	897-1205
Public Relations	Jeannie Okamoto	pr@nopc.org	455-0977
Publicity	Tom Ford	publicity@nopc.org	985-643-3172
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	897-1205

Other Important Numbers / Addresses

Club Hotline	Recorded messages. Meeting Information. Open 24 Hours	887-5746
NOPCC BBS	Bulletin Board System for members. The original way to PC communicate.	486-7249
NOPCC Web Site	On the World Wide Web. Our own home page and club information.	***www.nopc.org***

July 2005

SUN	MON	TUE	WED	THU	FRI	SAT
					1	2 **Living with Home Electronics** WTIX 690AM 10-11a
3 **Computer Solutions** WSMB 1350AM 11a-12p	4 **Computer Programming** @ McCann's 6:30p-8:30p	5	6 **NOPC Gen Mtg** **J.D. Meisler School** **6:30p-8:30p**	7	8	9 **Living with Home Electronics** WTIX 690AM 10-11a
10 **Computer Solutions** WSMB 1350AM 11a-12p	11 **Computer Programming** @ McCann's 6:30p-8:30p	12	13 **NOPC BOD** **@ McCann's** **6:30p-8:30p**	14 **WebLab SIG** **@ McCann's** **6:30p-8:30p**	15	16 **Living with Home Electronics** WTIX 690AM 10-11a
17 **Computer Solutions** WSMB 1350AM 11a-12p	18 **Computer Programming** @ McCann's 6:30p-8:30p	19 **Genealogy SIG** @ McCann's 6:30p-830p	20	21 **New User SIG** @McCann's 7:00p-9:00p	22	23 **Living with Home Electronics** WTIX 690AM 10-11a
24 **Computer Solutions** WSMB 1350AM 11a-12p	25 **Computer Programming** @ McCann's 6:30p-8:30p	26	27 **Digital Media SIG** @McCann's 7:00p-9:00p	28 **Internet SIG** @McCann's 7:00p-9:00p	29	30 **Living with Home Electronics** WTIX 690AM 10-11a
31 **Computer Solutions** WSMB 1350AM 11a-12p						

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.; and Students (under 21) , $20/yr. Meetings are held at 6:30 on the 1st Wednesday of each month at J.D. Meisler Jr. High School on Cleary Avenue in Metairie, Louisiana.

New Orleans Personal Computer Club
P. O. Box 8364
Metairie, Louisiana 70011