MotherBoard

This Month At NOPC
Amateur Photography
—
More Than You Think
by
Ashton C. Mouton, Jr.

NORTON SYSTEMWORKS 2005

Norton SystemWorks 2005 is Symantec's market leading problem solving and data protection suite. It now includes a full version of Norton GoBack 4.0, Symantec's powerful data protection tool that includes capabilities for restoring and recovering data. Norton GoBack 4.0 allows users to easily undo serious computer problems by returning a PC to a previous state when it was fully functional and its data intact.

Norton SystemWorks 2005 also includes Norton Utilities and Norton Cleanup, comprehensive solutions for maximizing PC performance. To prevent PC problems and maximize users' productivity, Norton System Works 2005 includes the enhanced One Button Checkup, as well as two new features: System Optimizer and Smith Micro Software, Inc.'s CheckIt® Diagnostics. Additionally, Norton SystemWorks 2005 features advanced anti-virus protection and expanded threat detection with the latest version of Norton AntiVirus.

Tools to Solve Problems and Maintain System Performance
Ensuring a PC runs at optimal performance levels requires frequent maintenance. Regular use of a computer can cause changes in system settings and registry files, and results in a build up of unwanted Internet clutter and temporary files. While these issues may seem trivial, if left unchecked, over time they can lead to slow system performance or more serious hard drive problems.

Norton SystemWorks 2005 includes a full range of easy-to-use tools designed to detect and resolve these types of problems. With One Button Checkup, users can quickly check their system, fix common registry problems and eliminate Internet clutter and temporary files. Users can run One Button

Amateur Photography – More Than You Think
Have you ever wondered what it would be like to take your own pictures, edit those pictures and have a wonderful memory. Well, wonder no more. Our very own Ashton Mouton has been dabbling in digital photography and will share his adventures with us from purchasing a camera, books and software to modifying his pictures. He will also show us the finished products. Ashton is a valued member of our club. He has served as Vice President and SIG leader with the NOPCC.

 Mark your calendars with a purple pen and a dog/cat photo, create an entry in your Palm Pilot, HP or Dell pocket PC, update Outlook (all versions except Express) and join us on Wednesday, August 3, 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.

Checkup on demand or schedule it to run automatically. Norton SystemWorks 2005 also includes Norton Cleanup, which provides users with a method to remove cookies, history lists, caches and temporary files that clutter disks after web browsing and other activities. Norton Cleanup can now be customized to scan and preserve favorite Web sites from future cleanups.

New features to Norton SystemWorks 2005 include System Optimizer and Checklt Diagnostics. System Optimizer allows users to control Windows XP settings from one convenient location, making it easier to manage shortcuts, customize appearances and change registry settings. Checklt Diagnostics offers a quick, thorough evaluation of a PC's hardware.

The Need for Comprehensive Data Protection
Computers have become an integral component of everyday life with increasing numbers of people using their PCs to store information that was once kept on paper and filed away in a cabinet. Essential data such as contact lists, financial information, credit card and account numbers, and photos now call a computer's hard drive "home." This valuable, and often irreplaceable, data makes problem solving and system maintenance tools even more important. A computer that is not well-maintained can easily morph into a system that won't function properly, thus compromising the data stored on the hard drive.

Norton SystemWorks 2005 enables users to protect data stored on their computer with the award-winning Norton GoBack, a powerful system rollback tool that recovers and restores data. In the event of a system crash, virus damage, failed software installation, or user error, Norton GoBack 4.0 can recover changed files or an entire system, restoring a computer to a healthy state. Norton GoBack 4.0 allows users to rescue one or several files that have been altered, damaged or accidentally deleted without having to restore the entire hard drive. Users can also test new programs with confidence by using SafeTry Mode, Norton GoBack 4.0's unique feature that creates a temporary state to run new software and gives users the option to accept or reject any changes.

Protects Against Viruses and New Hacking Tools
Norton SystemWorks 2005 includes a full version of Norton AntiVirus 2005, featuring Norton Internet Worm Protection, which protects users from Internet worm threats by blocking unsolicited, suspicious inbound traffic.

QuickScan, an additional feature of Norton AntiVirus 2005, provides a more proactive line of virus defense. QuickScan automatically scans a system as soon as it re-

ceives the latest virus definitions, and immediately removes those threats with improved removal capabilities. Norton AntiVirus 2005 also employs enhanced PreInstall Scan to detect and terminate infections already loaded in memory that try to destroy the product during and after installation.

Norton AntiVirus 2005 also continues to provide automatic removal of viruses, worms, Trojan horses and instant messaging infections; detect spyware; scan and clean incoming and outgoing e-mails and attachments; and detect virus infections in compressed files. As a result, Norton AntiVirus 2005 serves as a wide shield against an expansive range of malicious code.

The Norton AntiVirus 2005 component of Norton SystemWorks 2005 protects computers in the following ways:

* Automatic removal of viruses, worms and Trojan horses; functions without interrupting the user's work.
* Spyware programs that may expose the user's private data are immediately detected. The product also identifies adware, keystroke loggers and other hacking tools that have the potential to compromise system security.
* All inbound and outbound e-mail messages and attachments are scanned to prevent virus and worm infections.
* Instant messaging services have become a more frequently used conduit for the transmission of threats. Norton AntiVirus automatically detects and removes threats transmitted through services such as MSN® Messenger, Windows® Messenger, AOL® Messenger and Yahoo!® Messenger (version 5.0).
* Symantec's LiveUpdate downloads protection updates (virus definitions) automatically, keeping users' systems safe against new threats while ensuring that their PC's security tools stay up to date.
* Virus infections in compressed files are detected in real time in all files downloaded from the Internet, including those originating from instant messenger and peer-to-peer networks.
* Worm blocking technology detects worms such as Nimda in outgoing e-mail to prevent them from infecting other computers. This proactively guards against certain known and unknown threats without the need for updated virus information.

(Continued from page 2)

∗ Script blocking defends against fast-moving script-based viruses such as Loveletter and Anna Kournikova. This feature avoids risks by detecting viruses lurking in e-mail attachments before an attachment is launched or saved.

∗ When a program patch becomes available, Norton AntiVirus 2005 helps users keep their software up-to-date by automatically notifying them of the update.

∗ Users who choose to change the default settings may guard their new settings through password protection. This feature defends against special types of viruses that may attempt to disable the virus protection.

∗ The quarantine feature isolates infected files in a contained area of a hard drive until they can be repaired.

∗ Built-in links take users directly to the Symantec Security Response Web site for additional information on specific viruses just when they need it most.

∗ A direct link from Norton AntiVirus 2005 allows users to subscribe to the Symantec Security Response newsletter and be kept up-to-date with prompt information about virus threats.

∗ The Scan and Deliver wizard makes it easy to send infected files to Symantec Security Response experts for analysis.

∗ Integration with Windows Explorer lets users easily access many common Norton AntiVirus 2005 functions.

∗ The product activation process ensures authenticity, protecting users from pirated or counterfeit software.

Barlow's Hard Drive Newsletter - July 2005
Protecting your Hard Drive from Unwanted Changes
By Gene Barlow
User Group Relations
Copyrighted July 2005

Your hard drive is the heart of your computer. It contains the operating system that manages your computer's hardware. All of your application programs and settings are stored on your hard drive. Most important of all, the data files that you create using your computer are trusted to your hard drive. If anything should happen to this hard drive, your computer would no longer run. All of your financial records, family photos, genealogical databases, email correspondence, and other data files would be lost and gone forever. You must protect your hard drive from unwanted changes or you risk loosing your computer and all of your important data files. Having a good backup of your entire hard drive is the first thing you should do to protect your computer. (See the Perfect Backup Approach at http://www.ugr.com/newsletters.html) Then, if anything should happen to your computer, you will at least be able to rebuild your hard drive from your backups. However, waiting for a disaster to happen with the knowledge that you can rebuild your hard drive is not enough. You also need to set up a defense around your hard drive to prevent unwanted changes from taking place on your hard drive in the first place. Unwanted changes attack your hard drive in many ways. Three of the most common ways are Internet predators, other users of your computer, and bad software installations. We will look at each of these ways that unwanted changes can damage your hard drive and then look at ways to protect yourself against these changes.

Unwanted Changes Attack your Hard Drive
Whenever you connect to the Internet to get your email or browse web sites, unwanted items are quietly installing themselves on your hard drive. These include dangerous viruses and worms that can damage your hard drive. Recently, we have seen a great increase in Spyware and Cookies being stored on your hard drive. While less dangerous than viruses and worms, they can still choke up your computer and share your private information with others. Your hard drive also collects hacker tools and other cyber junk as you use the Internet. With a broadband connection, you are constantly connected to the Internet and your hard drive is open and vulnerable all of the time. This is a serious problem that needs your immediate attention. If your computer is ever used by others, then your hard drive is exposed to any changes these others may make on your system. Many of us have children or grandchildren who use our computers. Have you ever noticed how your computer doesn't run the same after these young people finish using it? They probably do not mean to hurt your computer, but in the process of downloading their games, they may cause serious damage to your hard drive. This is especially true in classrooms and computer labs. After a few hours of use by various students, some of the computers no longer work at all and the others have been modified by the students. You need to have your computer protected before you let others use it or you risk losing your hard drive information. Another common source of damage to a working hard drive is software installations. These can be software downloaded from the Internet, software purchase from a computer store, or upgrades to existing software. In most cases, the software has been thoroughly tested

and the installation will not cause your computer problems. However, some software will not install cleanly and may damage your hard drive during the installation. It is often difficult or impossible to remove the changes and get your computer working after a bad installation. Don't install software on your hard drive until you have it adequately protected.

Protecting your Hard Drive from Changes

There are many ways that have been tried to protect your hard drive from unwanted changes. Unfortunately, many of these approaches may not be very effective. Utilities that protect your hard drive from Internet predators often use the "Hide and Seek" approach. They do a poor job of preventing bad stuff from getting on your hard drive, so they must do frequent scans to try to seek out the changes and remove them. Those of you with other users on your computer rely on doing lengthy restores of your hard drive backups. Protection against bad software installations is left to system undo utilities like GoBack or the System Recovery Facility in Windows XP. None of these approaches do a great job in all of these situations. There has to be a better way! Leave it to a small software company, ShadowStor, to come up with an innovative solution to unwanted changes to your hard drive. Rather than try to undo the damage after the hard drive has been changed, ShadowStor decided to prevent the changes from ever reaching your hard drive in the first place. They developed an excellent product called ShadowUser Pro that safely prevents unwanted changes to your hard drive, but lets wanted changes be made quickly and easily.ShadowUser Pro gives you the ability to place your computer in a special ShadowMode state, when your hard drive is locked off from all changes. The changes are safely stored in a temporary area on your hard drive where they won't cause you any harm. While in Shadow-Mode, your computer will run as a virtual computer, as if all of the changes were actually made to your hard drive. This lets you test out changes that you wanted to make to your hard drive, without actually making them. Later in the day, you can return your computer to its normal operating mode and at that time, you can easily select just the changes that you want to be permanently made to your hard drive and all other changes can be discarded. Preventing all of the serious damage of Internet predators is perhaps the greatest ability of ShadowUser Pro. Before you connect to the Internet, you would put your computer into ShadowMode to keep viruses, worms, spyware, and other cyber junk from ever reaching your hard drive. Surf the net without regard, since all of the traces of your use of the Internet will never reach your hard drive. When you disconnect from the Internet, you can discard all of these bad items as you return your com-

puter to normal operating mode. For those of you with continuous broadband connection, you would leave your system in ShadowMode most of the day and only go into normal mode briefly as you shut down your computer for the evening. ShadowUser Pro gives you excellent security from Internet predators. When you let others use your computer, place it in ShadowMode before they start to use the system. Then, when they are done, you can simply switch back to normal operating mode and any changes that they made are gone. In a classroom or lab environment, simply reboot the computer back into normal mode after each student and all changes made by the prior student are discarded and never reach the hard drive. This saves a lengthy restore of the hard drive from a backup file after each class or user. ShadowUser Pro is also great protection from a bad software installation. Install the software while in ShadowMode and you can test out the software to see if it works and if you like it. If the installation causes your computer problems or you find that you don't like the software, you can simply discard the installation as you return to normal mode. Nothing was changed on your hard drive, even though you could run your computer in virtual mode and test the software as if it were installed on your hard drive. If the software installation goes just fine, then you can commit that installation to your hard drive and continue to use it.

How to Obtain ShadowUser Pro

ShadowUser Pro runs on WinNT, Win2000, and WinXP systems and is licensed for one computer and will only install on one computer. User group members and their guests may purchase this excellent product at the user group discount price of just $47. To purchase this product, go to www.usergroupstore.com and look for the product in the Security section of the web site. To order it, click on the appropriate "buy now" button next to the product and you will be able to place your order. Include the name of your user group and the special product code of **UGNL0605**. If you have questions about this article or ShadowUser Pro, please email them to gene@ugr.com and I will try to answer them for you. You'll love using this exciting product.

Gene Barlow is the president of User Group Relations, a consulting firm specializing in promoting computer products to the user group community. He has over 40 years of experience with computer systems. He worked for IBM for 34 years and managed IBM's user group support organization for 14 years. He helped hundreds of user groups get started and is sometimes called the Father of User Groups for his involvement. When he left IBM, he set up his own consulting firm and has represented many software vendors to the user group community the past 9 years. He is an outstanding speaker, writer, and helper of end users and loves working with user groups. You may contact him at gene@ugr.com.

Submitted by Jeanne Okamoto
NOPCC Member

Credit Card Scam Warning

By understanding how the VISA & MasterCard Telephone Credit Card Scam works, you'll be better prepared to protect yourself.

Person calling says, "This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460 your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for $497.99 from a Marketing company based in Arizona?" When you say "No", the caller continues with, "Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?"

Here's the IMPORTANT part on how the scam works, the caller then says, "I need to verify you are in possession of your card". He'll ask you to "turn your card over and look for some numbers". There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers' that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, "That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?" After you say No, the caller then thanks you and states, "Don't hesitate to call back if you do", and hangs up.

You actually say very little, and they never ask for or tell you the Card number. But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of $497.99 was charged to our card.

What the scammers want is the 3-digit PIN number on the back of the card. Don't give it to them. Instead, tell them you'll call VISA or Master card directly for verification of their conversation. The real VISA told us that they will never ask for anything on the card as they already know the information since they issued the card! If you give the scammers your 3 Digit PIN Number, you think you're receiving a credit. However, by the time you get your statement you'll see charges for purchases you didn't make, and by then it's almost to late and/or more difficult to actually file a fraud report.

New Orleans Metropolitan Association
of REALTORS®, Inc.
Weekly News Update
July 22, 2005
Submitted by Edward Jahncke

ICE

In **C**ase of **E**mergency

This is from the UK Ambulance Service...

"Following the disaster in London, the Ambulance Service have launched a national "In Case of Emergency (ICE)" campaign with the support of Falklands war hero Simon Weston.

The idea is that you store the word " ICE " in your mobile phone address book, and against it enter the number of the person you would want to be contacted "In Case of Emergency". In an emergency situation ambulance and hospital staff will then be able to quickly find out who your next of kin are and be able to contact them. It's so simple that everyone can do it.

For more than one contact name ICE1, ICE2, ICE3 etc.

===

While driving in Pennsylvania, a family caught up to an Amish carriage. The owner of the carriage obviously had a sense of humor, because attached to the back of the carriage was a hand printed sign......
"Energy efficient vehicle: Runs on oats and grass. Caution: Do not step in exhaust."

===

First Phishing, Now Pharming

By John Pearce,
Pikes Peak Computer Application Society,
Colorado Springs, CO

First, there was phishing trying to collect personal information. A newer attack called pharming is trying to do the same thing in a more technologically sophisticated way. You need to be on guard but neither phishing nor pharming should keep you away from the Internet. Let's take a quick overview of both.

Phishing starts with an e-mail, typically from a financial institution, with a message that some dire consequences will happen if you don't immediately verify your account information. A web site link is conveniently provided for you in the e-mail. The provided link is to a web page that looks like the real web site but is actually a web site controlled by the bad guys. The fraudulent web page asks you to enter credit card and billing information or possibly user name and password information. You can imagine what the bad guys are going to do with the information they collect.

Pharming is a way for the bad guys to redirect your web browsing to a site which they control. Pharming is also known as DNS (Domain Name System) cache poisoning. DNS is what converts human friendly names like web-

(Continued from page 5)

board.apcug.org to numerical addresses like 192.160.122.122. The bad guys want to impact the largest number of Internet users possible so ISP's and large corporations are the most likely targets of pharming attacks. One goal is to download spyware or adware to your PC.

Protecting yourself from phishing attacks is as simple as ignoring the e-mail. All but one of the dozen or so phishing e-mails I have received have been from banks where I don't have an account. In that case, delete the e-mail and go on with your life. If you have an account with the financial institution and are concerned, use the telephone and ask to speak with their Internet security department. If you go to the web site to login, type the web site URL into the browser – do not use the link provided in the e-mail.

Protecting yourself from pharming attacks takes a little effort. Start by keeping your browser updated with all the security patches. Next, you should be sure the padlock icon is displayed on any page where you enter personal information such as username, account number, or password. The padlock icon indicates you are connected to the legitimate owner of the URL and the data you enter is protected by SSL encryption during transmission. The bad guys would have to know the private key of the site in order to make the padlock appear. You can view the security information by double clicking the padlock icon on your browser. You can also use a tool like SpoofStick to confirm the URL of the web page you're viewing.

Two other exploits are worth a quick mention. The first is an instant messaging worm that changes the content of the hosts file on your PC. This is effectively the same as DNS cache poisoning. The other exploit is domain hijacking which is done by manipulating the domain name registrars. Domain hijacking is what happened to Panix, a New York ISP, in January.

Being aware of phishing and pharming along with a little care and caution will keep your web browsing safe from the bad guys.

Distributed by APCUG

A father was approached by his small son who told him proudly, "I know what the Bible means!"

His father smiled and replied, "What do you mean, you 'know' what the Bible means?"

The son replied, "I do know!"

"Okay," said his father. "What does the Bible mean?"

"That's easy, Daddy." the young boy replied excitedly, "It stands for "**B**asic **I**nformation **B**efore **L**eaving **E**arth."

For Ladies Only

Sally???

Natasha???

©1999, Michigan Live Inc. All rights reserved.

That uncomfortable moment when Cyberdaters finally meet face to face.

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

August 2005

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