The New Orleans Personal Computer Club Newsletter

Mother Board

Volume 26, Issue 11

November 5, 2008

This Month
How Internet Service Provider's Work
by
John Souvestre

Inside this issue:

ELECTION TIME

At the November 5th meeting we will be electing officers and directors to lead the NOPC in 2009. The officers are President, Vice President, Treasurer and Secretary. In addition, we have three Directors at Large. These seven members constitute the Club's Board of Directors. Each member of the Board will serve from December 1, 2008 until November 30, 2009. The Board meets once a month, usually the second Wednesday, at 6:30PM.

Any current member in good standing can run for a position on the Board. If you want to know more about the duties and responsibilities of each position, please contact Virginia Kieran (kierano@bellsouth.net, 504-887-5746) or Mike York (mike@gnonug.org, 504-289-4046).

At the November 5th meeting, nominations for the Board can be made at the meeting. The member nominated must be present at the meeting to run. We will then vote for each officer and director.

The Club needs your time and talents. Please consider helping the Club by running for an officer or director at large.

Come out to the November meeting and take part in the election of your Board for 2009.

This Month at the NOPCC
How the Internet Works

John Souvestre Southern Star and Integrated Data Systems of Metairie will present an insider's view of "How Internet Service Providers [ISPs] work." He will also discuss "How ISPs handle email and spam., including The Web 1.0, Web 2.0, and Web 3.0".

John has been a long time member of the New Orleans Personal computer Club (NOPCC), providing internet service and web hosting for the club during that time. His ISP was up and running before anyone after Katrina.

In the early days when the Internet was still a mystery to most computer users, John was always available to assist one in getting "on-line" and connected.

This is a "don't miss" presentation.... It will be held at :
Ochsner Hospital
Caldwell Room
2nd floor of "Hotel Conference Center"
Questions @ 6:30 pm—Lecture @ 7:00 pm

Broadsides

by Ron Broadhurst,
a member of the Space Coast PC Users Group, Inc., Florida
www.scpcug.com
ringram728 (at) earthlink.net

*This article has been obtained from APCUG with the author's per-
mission for publication by APCUG member groups; all other uses
require the permission of the author (see e-mail address above).*

These ideas are compiled from years of accumula-
tions from various magazines, books, on-line sites,
and my own personal experience. I claim neither
originality nor ownership to any of its contents. My
only intent is to share the various "tips, "tricks", &
"hints" in hopes of helping & maybe enhancing your
computing experiences. They are all intended for
anyone who uses a PC. It is for beginners as well
as advanced users. njoy and use as you will.

Ron Broadhurst

HOW TO GET RID OF "SEND ERROR REPORT TO MICROSOFT

Right click My Computer on the desktop or in the
Start menu.
Click Properties.
Click the Advanced tab.
Click the Error Reporting button at the bottom.
Click Disable error reporting. You can select the
checkbox under it if you still want to be notified
when errors occur.
Click OK.

Note that you can disable error reporting for the op-
erating system only, or for programs only, by un-
checking the appropriate box under the Enable
error reporting option.

You can also configure error reporting only for spe-
cific programs by clicking the Choose Programs
button.

ALPHABETIZE START MENU LISTINGS

When you install a new program on your system, it
will often appear at the end of your Start menu. Re-
organizing files alphabetically in the All Programs
menu does not

affect how they appear in your start menu. In order
to alphabetize your start menu, you'll want to click
Start and select All Programs. On any file or folder
right-click and then select Sort By Name. Now all of

your Start menu programs are in alphabetical order.
You can also sort subfolders in your Start menu the
same way.

MAKE YOUR QUICK LAUNCH ICONS BIGGER

Unlock the Toolbar

Right click the QL toolbar

Select the View tab

Select large icons

PIN AN APPLICATION TO START MENU

The Windows XP Start menu includes an area
where two or more Microsoft applications, usually
Internet Explorer and Outlook Express, are perma-
nently positioned for easy access. You can add
your favorite application to this same convenient
location. Open Windows Explorer and locate the
executable file for the application. Right-click the file
and select Pin To Start Menu. The application will
now appear in the Start menu. To remove an appli-
cation, locate it, right-click it, and select Unpin From
Start Menu.

Alternatively, you can right-click the app in the Start
menu and click Unpin From Start Menu.

CHANGE SYSTEM SOUNDS

Through the Control Panel you can change your
system's program event sounds. Click Start and
Control Panel. If you're using Category View, click
Sounds, Speech, and

Audio Devices; and Sounds and Audio Devices. If
you are using the Classic View, click Sounds and
Audio Devices. This loads the Sounds and Audio
Devices Properties dialog box. Choose the Sounds
tab. Select the sound you'd like to change in the
Program events box, and then select a new sound
from the Sounds drop-down menu. Or select a
sound you've saved to the hard drive by using the
Browse button to navigate to the sound file. Change
as many sounds as you like. Save your changes as
a sort of theme from the Sound Scheme drop-down
menu above the Program events box. (Select the
blank line and click Save As.) You can also choose
to disable program event sounds. When you're fin-
ished click OK.

(Continued from page 2)

SAVING E-MAIL MESSAGES

To save e-mail messages highlight the message you want to save, then click on File -Save As. Select where you want to save the message and then save it as a txt file.

FastStone Capture
A Review by Ron Hirsch,
a Member and Contributing Editor
of the Boca Raton Computer Society, Florida
www.brcs.org
Ronhirsch1439 (at) comcast.net

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

THE BEST SCREEN CAPTURE PROGRAM I'VE EVER USED

Since it is possible that some of you may not know what a "screen capture program" is, I'll start off by defining that program type.

WHAT IS A SCREEN CAPTURE?

When you are working on your computer, the material you are working on/looking at, is displayed on your monitor screen, as a bunch of pixels. Often, it is nice to be able to "save" the info onscreen, or parts of it, for further uses.

Windows does offer a "Print Screen" capability, to send info to the clipboard or printer, but as with many of Windows utilities, it's a pretty barren utility, with very few options. Fortunately, there are several 3rd party utilities out there, one of which I consider the best I've ever used.

MY HISTORY WITH FASTSTONE

When I started using FastStone Capture in early 2007, it was still freeware, with a request to send in a "contribution", if one liked it. I liked it so much, I sent off a contribution immediately, and received a very nice "Thank You".

Shortly after my contribution, it became a "paid for" utility. For $19.95, you get the program, and updates are free forever. There is a 30-day free trial period, during which you can use a fully functional version, to convince yourself that this is indeed a program that you want to keep using.

LINKS

FASTSTONE MAIN SITE

The link to the FastStone site is:
http://www.faststone.org/index.htm .
While here, check out the other excellent programs, all of which are free, or click on the Download button for FastStone Capture to download it.

FASTSTONE CAPTURE PAGE

The link to page for this program is:
http://www.faststone.org/FSCaptureDetail.htm
or just click on the "capture" program when you are on the first link noted above.

WAYS TO USE SCREEN CAPTURES

Below, I've included some of the ways I use this screen capture program – which, by the way, I use just about every time I'm on my computer.

Remember, this program can capture a wide variety of areas on your screen - see the listing below in one of the screen captured images.

1. Have you ever installed something where a variety of screens and dialog boxes came up, and had to be filled in with info for various options, etc.? Sometime later on - weeks, months, or even years, you need to know what info and options et al that you filled in. No problem - just save each screen and store the saved screens in a named folder. Then all that info is available at a moments notice. All you have to remember is where you stored it. And you can also print out each of the screens after saving them, and file those pages in a loose leaf notebook.

2. You have some digital photos that you'd like to send to someone in an e-mail. If you just "insert" the pix into the e-mail message as many people do, they may come out to a very large size - much larger than you wanted, or expected. There are of course a variety of ways to "resize" image files, but there is one that is pure simplicity. What I do is to display each picture file in a program such as Windows "Picture and Fax Viewer", or the free Fastone Viewer offered on their site. Then adjust the size of the displayed image on the screen, to what you'd like the

(Continued from page 3)

size to be in your e-mail. Then capture the image. When inserted into your e-mail it will be exactly the size that you captured, since it captures pixels, and monitors all have very similar pixels/inch.

3. You're on a web page, and there is something interesting that you want to save, but you don't want to print out the whole page. Just select the desired area using Fastone Capture, and save/print that area only.

4. You're watching a video on your TV, and there was an image of someone/something you wanted to capture. Just pause the video, and select the area you want in Fastone Capture. Your image is captured. Remember, screen captures are just pixels. The capture process doesn't care what created those pixels.

Remember, this capture method saves things as an "image" (I use the jpg choice). It will not save text in editable form. If you want to do that, you must copy and paste into a text editor, such as Notepad. But, if you have a program such as "Omnipage" which is generally included when you buy a flatbed scanner, you can use it to convert a jpg image of text to an editable page of text.

The images below are several of the screens and drop-down menus from Fastone. The choices available to the user are well thought out and very useful. Note all the various options for what can be chosen to get saved, and the hot keys for these choices.

Editor: While we try not to "sell" any particular product, over the years the program that I have used the most is a Screen Capture program from the Win 98 era. Amazingly, it still l works about 90% in Vista. For me, a screen capture is a Must Have on any computer.

Hacking 101

By Marjie Tucker,
Editor, Macon Computer User Group, North Carolina
www.mcug.org
mcug (at) dnet.net

We are being bombarded with warnings about securing our data and the entry to our computers. Do you ever wonder what the big fuss is all about? How can a hacker possibly get into your data? And, what would he be looking for? Let's spend some time answering those questions.

How Does A Hacker Get In To Your Computer?

When you give your computer access to the Internet, you need an IP (Internet Protocol) address. The IP addresses that we are currently using have 4 octets with periods between them. They will be something like 192.168.100.1. When you access the Internet, that address is read by the router, modem, whatever that links you to your Internet Service Provider. Then it is read by the routers that route all the data through the Internet. This address makes it possible for you to send data, such as e-mail or requests for web pages. And, in turn, that same address is used to direct incoming e-mail and web pages into your computer. There are several websites and programs available that will translate these IP addresses into the name of the company that purchased them. In many cases, like our resi-

dential usages, the company name will be the ISP. For commercial use, it will be the name of the company that rents the block of IP addresses. Hackers use this IP address information to find their targets much like we use a physical address to find a house or office.

Once a hacker finds out your IP address it's relatively simple to send your computer a Trojan horse program, spyware, or a virus that will open a port that you usually don't use. Once that port has been opened, he can freely enter into your operating system and browse around just like he was there in person. He would look for programs that store valuable data like social security numbers and credit card account numbers. (Do you have that information entered into your Quicken or Money program?)

He would look through your My Documents folder for password lists and search your Internet Explorer favorites for financial sites where you saved the username and password. And, before he leaves he usually plants another Trojan horse that will give him the ability to take control of your computer in the future.

Commercial Websites

The most common way to hack into a company's website through the Internet is by using a Denial of Service attack. These DoS attacks use multiple computers to overload a website with bogus requests for information. The hacker usually creates a Trojan horse program that he sends into the computers of unsuspecting people (remember that program that was left behind when your computer was invaded above?) The message that he creates usually contains a header saying that it comes from an IP address that doesn't exist. When he is ready to attack, he calls up all the computers that he infected with his Trojan horse and tells them to contact a specific IP address. Those computers follow his instructions and send his preprogrammed message to that website. Servers that control websites always check to verify that IP addresses requesting information or webpage downloads are legitimate addresses. When a server is hit by a bombardment of these false address requests, it tries to track down every one of the fake addresses. Before long the server becomes overwhelmed by the fruitless process and crashes. When it crashes, the website will vanish and the hacker will be given access to a

prompt for the server. He can then use Linux or DOS commands to request and view information on that server other servers.

How About Wireless?

Let's put this hacker into an airport where hundreds of people are sharing a wireless network. It's like leaving a child alone in a candy store. In this case the airport's wireless system usually provides the IP addresses through DHCP and he can easily look at the list of addresses that have been supplied. He can test each of the addresses for available ports and it's quick work to access the most vulnerable. The same principles apply in hotels and restaurants that provide wireless Internet access. If you have a wireless network in your home, our hacker can drive down your street using a laptop or PDA to search for wireless networks. This process is called Wardriving. If he finds one that has not been secured at all, he doesn't even have a challenge. If you have added a password, he simply has to crack the password.

What Tools Do They Use?

It's very easy for a potential hacker to find the tools of his trade. There are many websites that offer program tools and tutorials for using them. Here are some of the
popular:

Anonymizers and Remailers - Anonymizers are online services that eliminate the trail of information that is left behind. These sites use anonymous proxies that a hacker can use to access computers and servers without leaving his IP address on any log. Remailers strip the header off a message and replace it with a meaningless header that
can't be traced.

Command.com - When this command is typed into a server it will basically give you administrative rights. You can then see all the folders and files. It's also very easy for the hacker to create a new administrative account that he can re-use in the future.

Password Crackers - These programs try random passwords at lightening speeds. They are usually very successful.

Key Loggers - Hackers frequently install these on

computers, especially public PCs. The programs actually record every stroke that you make. Hence, when you type in a username and password, it has been captured.

Port Knocking - This is a method of externally opening ports on a firewall by mimicking the process you normally use to add a port to your firewall.

Wireshark - This popular program captures and analyzes the data on a network. It's used by hackers to find information they want and it's also used by network administrators to manage networks.

Aircrack - This program is used to crack wireless WEP and WPA passwords.

Metasploit Framework - This is a tool that can be used by hackers to search the Internet for sites that have dubious code. These are the sites that are the easiest to hack - especially when this program does the searching for you.

Networks identifying the types of data and the internal addresses of this data. It's a valuable tool for administrators, but can save a great deal of time for a hacker.

NMAP - This is a port scanner. Since a hacker knows that he needs to use a port to access your computer or network, he can use this program to see which ports you have open.

NetStumbler - This program finds any wireless networks that are in range.

Wardrivers drive through residential neighborhoods using NetStumbler to search for available wireless networks.

Kismet - This program takes NetStumbler one step farther. It searches for wireless networks that are not broadcasting their SSID.

NSLookup - If you type a domain name into this program, it will give you the company's IP address

Traceroute - This is a very valuable troubleshooting tool for technicians. It will trace a packet on its route through the Internet. It shows every IP address it visits along the way.

Snort - This is an open-source intrusion detection system. It shows traffic analysis and packet logging on networks.

TCPdump - This is the most widely used network sniffer/analyzer for UNIX networks.

Net Cat - This has been called the Swiss army program for hackers. It performs many sniffing and cracking tasks.

This was really just some of the basics. But, if we know why security is so important, we may remember to take the right precautions. Hope your web surfing stays secure.

Space Coast User Group
www.scpcug.com

The following links were obtained from the Space Coast (Fla.) User Group Website. You may find them as helpful as I did...Editor

General Security Information:

[Free Browser Checkup](#) - Series of Audits Designed to Test & Fix Your Browser's Security Vulnerabilities. Only MS Internet Explorer is Supported.

[Free Secure File/Disk Deletion Tools](#) - Destructively Delete or Wipe Data in Files/Disk. Helpful When Selling or Giving Away Your Old Computer.

[Privacy Analysis](#) - Check the Privacy of Your Internet Connection Free

[Shields UP!](#) - Free Quick Check of the SECURITY of YOUR Computer's Connection to the Internet

[Spychecker](#) - Is it Freeware or Spyware? Check with this Online Spyware Lookup Database

Virus Information:

[Panda Security](#) - Free Online Scan, ThreatWatch, and Security Info (Real-time Information & Resources to Stay Safe from Virus Attacks)

[Sophos Anti-Rootkit](#) - Free Anti-Rootkit Software, Finds & Removes any Rootkit (Malicious Object: Process, File, Registry Key, Network Port) that is Hidden on Your Computer.

[Trend Micro HouseCall](#) - Free On-Line Virus Scan

CLUB SUPPORTERS

November 2008

SUN	MON	TUE	WED	THU	FRI	SAT
						1
2	3	4	**5 NOPC Gen Mtg** **Ochsner Hospital** **Hotel Conf Center** **6:30p-8:30p**	6	7	8
9	10	11	**12 NOPC BOD** **@ TBD** **6:30p-8:30p**	13	14	15
16	17	18	19	**20 New & Inter-** **mediate User SIG** **Old Metairie Library** **6:30p-8:30p**	21	22
23	24	25	26	27	28	29
30						

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	Walt Christensen	vp@nopc.org	456-2509
Secretary	Ray Paternostro	secretary@nopc.org	737-9099
Treasurer		treasurer@nopc.org	
Director At Large	Mike York	director1@nopc.org	738-5997
Director At Large		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

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*