The New Orleans Personal Computer Club Newsletter

Mother Board

Volume 19, Issue 10 October 3, 2001

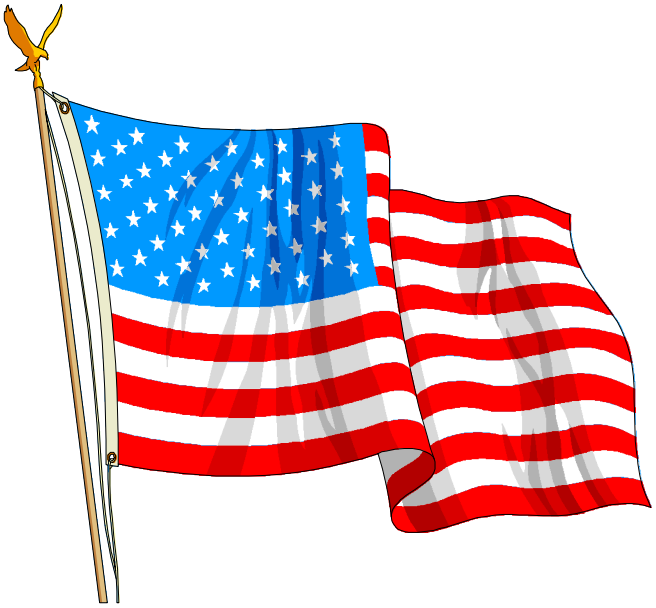
This Month at NOPCC:

Fast Access:
The Case For Cable

By

Cox Communications

Inside this issue:



"I do solemnly swear, that I will support and defend the Constitution of the United States against all enemies foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; that I will well and faithfully discharge the duties of the office on which I am about to enter; So help me God."

The "Oath of Office" each and every officer and enlisted person of our military takes upon appointment and every time he/she receives a promotion while in the service of this country.

Editor

Ramblings from the Veep

With the recent tragic events that have happened in this past month, it is difficult to compose words for the newsletter but I'll do the best I can. I think I speak for the entire NOPC board that our thoughts and prayers are with the victims and the rescue teams in both New York and Washington. They are also with our armed forces who are about to go into battle; we pray for their safe return.

Over here, let's all do our part to help our country rebuild itself. Please contribute whatever you can to the Red Cross and other legitimate charities, and donate blood wherever possible. Since I'm an avid user of eBay auctions, I'd like to mention that both eBay and PayPal are making it fairly easy to contribute to the ongoing relief efforts.

As if all this weren't enough to have to deal with, there's still the constant threat of new viruses. Most if not all anti-virus programs have automatic update functions that can grab the latest definition and program updates from the manufacture's web sites; if you have an internet connection, use these features. If you have a broadband internet connection, be sure to use some sort of firewall protection for your system.

Microsoft is also putting on the next eXtreme event and the Windows XP launch very soon. Both are free but you must register to be able to attend. I have created events for both on our electronic calendar; you can click the links in the popup boxes to go straight to the registration pages for the venues closest to the NO area.

Also coming up is the annual election of NOPC officers. Our own Virginia Kieran has been "drafted" to head up the election committee; if you are interested in running for a position on the NOPC Board of Directors, please submit your name to her sometime between now and the end of October. All candidates are invited to submit a paragraph on their skills for publication in the newsletter.

Peace be with us all, I'm out.

Ray Paternostro

Doing My Part...

From: Steve Gibson <support@grc.com>
Newsgroups: grc.news, grc.news.feedback
Followup-To: grc.news.feedback

A few days ago (9/18) "Joseph Kafka" posted a command directed at me in the feedback newsgroup under the thread topic "STEVE GIBSON ...". His command was: "Post the flag of the United States of America on your website." What ensued from this was a moderately interesting discussion about the pros and cons of the issue of my doing so. Then, yesterday (9/20), a representative of the National Security Council in the White House asked the director of the SANS Institute if he would ask ME <<gulp>> to draft the user guidelines for their forthcoming "Homeland Cyber Defense Initiative." Would I?!!!! :) Of course I would! I loved the idea of being able to contribute to this effort and in a way that I uniquely and meaningfully could ... and which would ultimately mean a lot more, and help a lot more, than one more web site with a waving flag.

Here is the first draft of the initiative guidelines which I wrote and submitted yesterday for the use of our United States government:

The Homeland Cyber Defense Initiative

"There is a very real threat that our own personal computers could be turned against us and used to attack this nation and its people. Until now, the computer viruses and worms which have traversed the Internet at the speed of light, rapidly infecting thousands of innocent personal and corporate computers, have carried largely benign payloads. These viruses have been an inconvenience, certainly, but their authors appear to have been more interested in demonstrating what can be done, than in actually doing it. But therein lies the danger.

The terrorist attacks of September 11th have forever removed any doubt about whether there are people willing to seize any opportunity to attack this nation's people. Any of the viruses and worms that have torn across the Internet could have been far more destructive than they were. The next one could be. The only thing missing has been intent. Today, no one can doubt the intent that exists.

An infected and security-compromised computer can be used to spread the infection to other computers, to attack the computer upon which it resides, and to actively attack our nation's critical Internet infrastructure. Therefore, the vulnerabilities inherent in our personal and corporate computing systems represent a clear and present danger to this nation. These vulnerabilities could be maliciously exploited at any time. Every personal computer-using citizen of the United States can do a great deal to help prevent the malicious exploitation of our computers and of the Internet.

What can YOU do? Not only must we ALL practice MUCH safer computing, but we must also preach it to our friends, family, and coworkers ...

You should avoid and turn down all offers and solicitations for free software being offered anonymously over the Internet. Malicious hackers use postings in online chat rooms, IRC dialogs, and USENET newsgroups to lure unsuspecting users into downloading and running malicious software. When such software is run -- even once briefly -- the innocent user's computer can be permanently taken over and remotely commanded to perform the bidding of anonymous and malicious hackers located anywhere in the world. You should also take the opportunity to publicly scold anyone offering software in an anonymous forum so that others will be

(Continued on page 3)

Doing My Part… (continued)

reminded of the danger and be less likely to accept such offers.

NEVER run any software received through eMail, even from someone you know very well. Viruses often eMail themselves from the computer of someone you trust. You should also never run software received through eMail, no matter who sent it. Unless the sender wrote the program themselves, they are unable to guarantee all that the program does. You should also take the opportunity to gently suggest to someone who is eMailing programs that it is unsafe and unwise to do so.

Delete unsolicited (Spam) eMail immediately. If possible, identify Spam by its address and subject line, then delete it without ever opening or viewing it. If you do open unsolicited eMail, NEVER click on any links, and NEVER visit any web sites being advertised -- no matter how appealing and compelling their promises may be. It is also unwise to click on spam eMail "removal" links since these are often, instead, used to confirm the validity of your eMail address to someone who has already proven not to care about your rights. Since any eMailed links could have malicious behavior, it's best to delete unsolicited eMail as quickly as possible.

If you must use software obtained from the Internet, avoid passing programs around. Any software provided by someone else could be infected by an undetected virus and should be turned down. Instead, always try to download software directly from the program's original publisher. You should also gently explain to anyone offering software third-hand why this is an unsafe practice and that they should instead be providing a reference to the software's authentic publisher.

If your personal computer is shared with others, sit everyone down to gently and carefully explain the serious responsibilities of safe Internet use. Seek their agreement not to act in ways, as described above, which would endanger the computer and property of everyone with whom the machine is shared. Try to create a circle of pride and work together to safeguard the group's computing resource. Adopt the challenge and intention of "keeping the bad guys out."

Fortify your computer with the latest patches and updates, and keep posted about news of new threats: As part of your anti-hacker measures, adopt a policy of frequently checking with your computer system's software publisher for newly released updates. Clever hackers are constantly finding new ways to sneak into your computer, so you must stay ahead of them by tightening the screws as often as possible. Most computer and operating system manufactures maintain easy-to-use security and Internet update facilities that you should briefly visit no less than once per week.

If, despite all this, something should slip past your defenses … It is admittedly difficult to always practice safe computing, and tricky new schemes are continually being developed by those who wish to seduce you into handing your computer over to them.

Fortunately there are many groups, organizations, and companies working just as hard to track down and decode every new wrinkle and scheme the moment it appears. But none of these efforts will help you if you fail to take advantage of them. If you are not currently using a leading anti-virus system, ask your friends and coworkers what they use and recommend, then acquire the software and get serious about using it.

Next, keep it up to date: Malicious software is continually being created. To be effective your anti-virus system must be updated no less often. So just as you often check-in with your computer and operating system's vendor for their latest updates, make a point of keeping your anti-virus system current and perform scans, as recommended, to assure yourself that nothing has crawled into your system while you weren't looking. Once you have become familiar with your anti-virus system, ask around and make sure that all of your computer using friends and family are also using some sort of protection and making time to keep it up to date.

Employ a personal Internet firewall for extra fortification and notification: An extra layer of defense can be provided by the use of a personal computer Internet "firewall". An Internet firewall is free or inexpensive software that can help to prevent the exploitation of your computer by malicious software. The best firewalls completely hide your computer from the Internet, rendering it invisible and much less likely to be attacked. The most popular firewalls also allow you to grant or deny individual software programs access to the Internet. You should only allow programs you recognize and expect to be using the Internet to have access. An attempt by unknown software to use your Internet connection can be your first warning that something may have entered your machine without your knowledge or permission.

As before, ask your friends and coworkers about their knowledge, use, and recommendations of personal Internet firewalls. And once you're "in the know" and comfortable with your firewall's operation make sure your friends, family and coworkers are aware of the advantages of using a personal firewall.

Let's win this. Resistance is never futile. Personal and corporate computing can be a lot of fun. For the sake of yourself, your family, and your fellow Americans, let's all work to deny access to our computers to anyone who would use them for their own malicious purposes. Together, we can do it."

They needed this quickly because they want to make the initiative public in five days. I have no idea what will happen to it now, but I'm proud to have been able to help. :)

Steve Gibson

This article was passed along by our good friend, Carole Rike.

How Secure is Your Computer?

By Ira Wilsker ***iwilsker@ih2000.net***

According to published reports, the havoc caused by the SirCam worm/virus continues. Since warning about it last week in the Examiner, the availability of free utilities to detect and kill SirCam has increased dramatically, with virtually all of the antivirus publishers now offering these utilities. Still, SirCam continues to spread, and mutants and variants, some of which can slip by the earlier antivirus updates, are now becoming endemic. To reiterate last week's warning, it is an absolute necessity to update your antivirus software frequently, maybe even daily, to reduce the chance of infection, and never open an email attachment unless you are certain that the sender intended to send it to you. The concept of human engineering is alive and well, and helping to spread SirCam and its cousins, as the virus payload comes disguised as an attachment from a sender known to the potential victim. The new variants, not existing at the time of last week's column, now use many additional file extensions, and different message bodies. One variant, discovered on July 29, actually takes a paragraph from an existing "doc" file on the infected computer and uses it for the message body. It is not just the risk of confidential information being sent out over the net, as happened to the FBI, but the fact that over a period of time SirCam will render the files and data on the "C" drive unreadable and incapable of being executed.

It would be bad enough if SirCam was the only major contemporary cyber-concern. Unfortunately, there may be additional bad news brewing in cyberspace as the "Code Red" worm threatens to degrade or shut down the net. As I type this, trying to meet my weekly deadline, the national mass media and the technical publications are echoing a warning issued during a press conference by the FBI's National Infrastructure Protection Center (NIPC) on Monday, July 30. `There is reason for concern that mass traffic associated with the worm's propagation could degrade the overall functioning of the Internet and impact ordinary users," said NIPC Director Ronald Dick at the news conference.

Code Red infects computers running Windows NT or 2000 also running Microsoft's Internet Information Server (IIS). It is not currently a direct threat to computers running Windows 95, 98, or ME, or MACs. While patches and fixes for the IIS have been available for several weeks, there is some documentation that this worm has the capacity to infect massive numbers of computers in a very short period of time. One study, cited by the FBI, says that on July 26, in only nine hours, about 250,000 internet servers were infected, with the potential of infecting 500,000 servers a day. Code Red spreads from server to server by sending out huge numbers of small packets of data to "IP" internet addresses looking for security holes, and then implanting the worm on the target computer, infecting it as well. ``What makes this one different from any other is how dramatically ... it has been able to propagate itself and the viciousness associated with that," Dick said at the FBI NIPC press conference.

The viciousness he is referring to is the scheduled assault on the net, which if it happens, is scheduled to start at 7pm, Central time on August 1. At that time, the infected Internet servers are expected to flood the net with mostly meaningless data intended to overburden the net, effectively shutting it down. Some variants of Code Red, which have been identified, can deface websites stored on those servers. An earlier attack, aimed at the now former IP address of the White House server, as well as other government websites, posted a message on the websites "Hacked by Chinese", as the volume of data slowed the net, and effectively shut down some sites. The contemporary risk is that if successful, a massive "denial of service" attack could effectively cripple the net by consuming bandwidth and server processing time, effectively eliminating the ability of emails to pass through the system, slowing or preventing e-commerce, restricting the ability of people and business from exchanging data, and otherwise slowing or stopping net traffic. "This spread has the potential to disrupt
business and personal use of the Internet for applications such as electronic commerce, e-mail and entertainment." said the NIPC spokesperson. This is not just a domestic problem, as huge numbers of servers throughout the world have been infected, which could conceivably cripple the net globally. Russ Cooper of TruSecure Corp. is quoted as saying that Code Red is "huge" compared to the Melissa and ILoveYou viruses. It is "enough to cause the meltdown of the Internet," Cooper told Reuters. "Whether your machine is vulnerable or not, if 300,000 machines all try and send you 8 kilobytes of data, you won't be able to use the Net in the process."

Again, as I am typing this column before the assault is scheduled to begin, there is no way of knowing whether this will be a net-crippling attack, as the FBI NIPC has warned, or it will be "much ado about nothing" as was the cyber non-event of Y2K. What is certain is that this may very well be a warning of things to come. Denial of service attacks are not new, and not at all uncommon; what is new is the size and scope of the contemporary threat. Another incontrovertible fact is the substantial recent increase in probes of servers looking for security holes. Again, according to the FBI NIPC, "This uncontrolled growth in scanning directly decreases the speed of the Internet and can cause sporadic but widespread outages among all types of systems."

While this version of Code Red is not directly a threat to the computers using the ubiquitous Windows 95, 98, or ME software, or MACs, the technology exploited by Code Red, which is not new, could very well be a real threat. This is not some future threat, but a threat that has been happening for the past few years, only not to the degree or scope presented by Code Red. Most Internet users are not aware of how vulnerable their personal computers are to attacks from outside sources. Most of us feel safe with our current and frequently updated antivirus software protecting us from cyber-harm. While necessary, antivirus software only protects

How Secure…? (continued)

us from some of the threats. What it does, antivirus software generally does well, but it by itself is not adequate to provide enhanced protection to our computers on the net. With the widespread use of DSL, and the soon to be extensive local availability of cable modems, both typically using a fixed IP address for each user, the chance of hackers finding security holes in our home and work computers increases dramatically. It was once thought that dial-up users were immune to probing attacks, as virtually all dial-up accounts used a dynamic, or changing IP address with each connection, but the improved technologies made the common dial-up accounts vulnerable.

To provide the additional protection while online, the installation of "firewall" software may have become as critical as antivirus software. Simply, a firewall is designed to allow the user access to the net to send and receive data, but restrict or prevent others on the net from illicitly accessing the user's computer. While firewalls have been the lesser-known step-cousins of antivirus software for several years, they are suddenly exploding in popularity as users realize how vulnerable their computers are to outside access. Theoretically, on a PC, there are about 65,000 "ports" or potential points of entry for data on a computer. Thousands of these ports are accessible while online, and antivirus software generally does not protect these ports; that is the function of firewalls.

For home and small office users, there are several decent firewalls available, both commercial and "freeware". Some of the better selling commercial firewalls are published by the major antivirus companies as a separate, but companion product to their flagship antivirus software. This is exemplified by companies such as McAfee, and Symantec/Norton, which produce firewalls. Careful shopping can reveal bargains on firewalls. In a recent Sunday supplement, one of these products was selling for under $10 after rebate. I recently purchased a "bundle" of major name brand antivirus and firewall software for about $15, for the new computer I built for one of my daughters. There are several fine quality but reasonably priced commercial firewalls published by lesser-known companies. Many of these commercial firewall titles are available wherever software is sold.

For personal use, there are several free firewalls. While these typically have restrictions on eligibility for free use, their quality is often excellent. Arguably the most widely used personal firewall is Zone Alarm, which is free for personal use, and nominally priced for others. Available for free download at http://www.zonelabs.com, Zone Alarm is often at the top of the ratings comparing firewalls, including both commercial and free products. I have Zone Alarm on my computer at home. There are several other decent, free (for personal use) firewalls. Tiny Firewall is available at http://www.tinysoftware.com and has its band of loyal followers who sing its praises. A relative newcomer is Sygate's free Personal Firewall at http://www.sygate.com.

To either demonstrate the vulnerability to attack, or to verify the performance of a firewall, several websites offer a free online vulnerability survey. Steve Gibson's popular "Shields Up" is available at http://grc.com. Symantec has a free "Security Check" at http://www.symantec.com/securitycheck. There are several other websites offering security checks as well.

As with antivirus software, it is necessary to periodically check the firewall publishers' websites for updates, as hackers are utilizing new technologies and techniques to find ways to assault our computers.

In recent weeks, I had noticed an anomaly with my Zone Alarm reporting a significant increase in attempted probes of my computer that it stopped, while I was online with my dial-up account. Sometimes I utilize the built-in function that reverses the probe, and indicates the source of the probe. I have had several hundred recent probes from servers all over the world, with no apparent connection, until recently. Published accounts of Code Red probing the net for other computers to send its payload to can reasonably account for the probes of my computer. These probes are impersonal, typically done sequentially, possibly by the thousands every minute. Similar reports indicate that the throughput of the net has indeed slowed as Code Red seeks out additional victims. Fortunately, my computer does not meet the profile that Code Red is seeking, so even if it got through my firewall, it would not likely have infected my computer … this time. What about the new threats and variations of Code Red, SirCam, Hubris, or any trojans, viruses, or worms not even thought of yet? As I have said so many times in the past, currently updated antivirus software is a must. Now, I will have to add a firewall to the required list.

"For us to have a safe Internet the public at large has to institute appropriate security measures, of downloading appropriate fixes to various products, making sure that their anti-virus software is continually updated," said NIPC Director Ronald Dick at the July 30 news conference. Haven't you heard this before, in this column? Maybe someone is trying to tell you and I something.

Ira Wilsker is an Instructor IV of Management Development at Lamar Institute of Technology. Ira has been working with computers since 1965 when he took his first computer class at the Illinois Institute of Technology, in Chicago. A past president of the Golden Triangle PC Club, and a board member of the Association of PC Users Groups, Ira is a frequent guest on the local television news, and has lectured locally to internationally on a variety of computer topics ranging from computer and Internet basics, to CyberCrime, and Community Oriented Policing. Ira is the host of the Com-

In The News

From MS Gulf Coast Customer Service Sept. 18, 2001:

Experience Windows XP with us!

Join Microsoft and its partners for the worldwide product launch of Microsoft Windows XP! See how Windows XP sets the new standard for efficient and dependable computing while providing you and your organization the freedom to experience the best of the digital age. See it in action and discover how customers are using it today to increase productivity in the workplace while cutting operational and support costs.

In addition, Microsoft executives will share their insight on how Windows XP can change your work and home life. With new and enhanced digital media features and exciting Internet gaming and messaging capabilities, Windows XP makes sure you get the best of both worlds. Don't miss the BIGGEST product launch in Microsoft history!

All attendees will receive a commemorative Windows XP t-shirt, special offers from Microsoft and our Partners including a $50 coupon for both Windows XP and Office XP and a chance to win hardware, software or our Grand Prize - a fabulous cruise package courtesy of Travel in the Park and Expedia!

Dates and Locations:

Houston – October 25th, Reliant Arena, Event ID 101997062

San Antonio – October 30th, Marriott Rivercenter, Event ID 101997070

Austin – November 1st, Austin Convention Center, Event ID 101997079

New Orleans – November 1st, Pontchartrain Center, Event ID 101997078

**All events, registration begins at 9 a.m., event 10 a.m. - 2:30 p.m. (lunch will be provided) Register today to save your seat!

http://www.windowsxplaunch.com

or call 877-MSEVENT

Passed along by Virginia Kiernan

Virus Hoaxes

Sometimes that latest computer virus you hear about via email or listserver isn't really a virus at all. Some people don't write viruses -- they just start rumors about viruses. To find out what's what, take a trip to F-Secure Corporation's site and read the latest list of hoaxes. You'll find F-Secure Corporation here! ***http://www.datafellows.com/virus-info/***

Network Walkman Digital Music Player EMAZING.com is giving away cool Sony stuff every day!

http://click.emazing.com/ads/wss/textlink.html

Passed along by Jeannie Okamoto

New Virus Warning...Again!

WASHINGTON (AP) _ Anti-virus researchers were fighting a new Internet attacker Tuesday similar to the "Code Red" worm that infected hundreds of thousands of computers several months ago. The worm, known as "W32.Nimda," had affected "thousands, possibly tens of thousands" of targets by midday Tuesday, according to Vincent Gullotto, head virus fighter at McAfee.com, a software company.

Even when the attack isn't successful, the worm's scanning process can slow down the Internet for many users and can have the effect of knocking Web sites or entire company networks offline. The FBI is investigating the worm, said spokeswoman Debbie Weierman. The agency has not indicated whether the worm is connected to last week's terrorism attacks.

On security e-mail lists, system administrators nationwide reported unprecedented activity related to the worm, which tries to break into Microsoft's Internet Information Services software. That software was the same targeted by Code Red, and is typically found on computers running Microsoft Windows NT or 2000. Most home users, including those running Windows 95, 98 or ME, are not affected.

Ken Van Wyk, chief technology officer at ParaProtect, said the worm tries to wriggle in through 16 known vulnerabilities in Microsoft's IIS, including the security hole left in some computers by the "Code Red II" worm, which followed Code Red in August.

Code Red, by comparison, attacked through only one hole, which could be patched by downloading a program from Microsoft's Web site.

In addition to direct Internet attacks, the worm can also travel via e-mail. The e-mail message is typically blank, and contains an attachment called "README.EXE." Antivirus experts warn that users shouldn't open unexpected attachments. Efforts to isolate and track the worm were hampered by the swiftness of the attack. Gullotto said the first report came at about 9 a.m. EDT, from a site in Norway. "It's taken down entire sites," Gullotto said. "I can't even get to the Internet right now."

On Monday, the FBI's National Infrastructure Protection enter warned that a hacker group called the Dispatchers" said they would attack "communications and finance infrastructures" on or about Tuesday.

Last week, the FBI warned that there could be an increase in hacking incidents after the twin attacks in New York and Washington. They advised computer users to update their antivirus software, get all possible security updates for their other software, and be extra careful online.

Passed along by John Souvestre

NOPCC Directory

Elected Officers

President	Zeke Zimmerman	president@nopc.org	456-2991
Vice President	Ray Paternostro	vp@nopc.org	737-9099
Secretary	Curtis Duhe'	secretary@nopc.org	
Treasurer	Don Herrmann	treasurer@nopc.org	831-1284
Director At Large	Ed Jatho	director1@nopc.org	834-4386
Director At Large	Bob Gordon	director2@nopc.org	469-4686
Director At Large	Ashton C. Mouton, Jr.	director3@nopc.org	241-2172

Standing Committees

BBS SysOp	Lanny Goldfinch	sysop@nopc.org	482-5066
Newsletter Editor	Ed Jatho	editor@nopc.org	834-4386
Public Relations	Jeannie Okamoto	pr@nopc.org	455-0977
Publicity	Jackie Elliott	publicity@nopc.org	455-6203
Webmaster	Manuel Dennis III	webmaster@nopc.org	835-7656

Special Interest Groups

Genealogy	Bob Gordon	gene-m@nopc.org	469-4686
Internet	Ray Paternostro	internet-m@nopc.org	737-9099
N O C K	Albert Fox	albertnm@bellsouth.net	861-1630
New Users	Zeke Zimmerman	new-user-m@nopc.org	456-2991
Suites 2000	Ashton C. Mouton, Jr.	suites2000@nopc.org	246-7759
VBLG	Manuel Dennis III	vblg-owner@listbot.com	835-7656
WADSIG	Manuel Dennis III	wadsig-owner@listbot.com	835-7656

Other Important Numbers / Addresses

Club Hotline	Recorded messages. Meeting Information. Open 24 Hours	454-6166
NOPCC BBS	Bulletin Board System for members. The original way to PC communicate.	486-7269
NOPCC Web Site	On the World Wide Web. Our own home page and club information.	***www.nopc.org***

Suites 2000 SIG

The Suites 2000 SIG did not meet last month--nobody showed up. I am sorry if the meeting info did not reach those who normally attend. We have only three meetings to end the year and December's meeting will end the word processing part of the SIG. We will decide in December what part of the suites we will cover starting in 2002.

For the new members who may not know we are covering all aspects of the different suites. We started with word processing and will soon end its coverage. We will in the future cover calendars and how to used them, presentation applications and how best to use them. Later we will cover spreadsheets and databases.

This SIG is a little different from the other SIG's because it is setup and run similar to a classroom setting. Some hands-on work is done but mostly lectures and step-by-step information is given on how to do various functions within a given application program are show and discussed. Questions are answered and examples given to better explain the concepts covered.

If you have any questions on how to use your word processor now is the best time to attend this SIG because we will be changing our topic for the next year. If you come now we can better prepare for your question and mostly have the answer for you at the meeting.

The e-mail for this SIG will be suites2000@nopc.org. Any communications outside of SIG meeting time is accomplish by e-mail or though phone calls (Ashton C. Mouton, Jr. at 246-7759). There will be samples of work, problem solving, and a question and answer session at each meeting. Hope to see you there.

Ashton C. Mouton, Jr.

October 2001

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1 Visual Basic Learner's Group @ McCann's 6:30PM	2	3 General Meeting J.D. Meisler 6:30pm	4	5	6 Living With Home Electronics 690 AM 10:00AM-11:00AM
7	8 Visual Basic Learner's Group @ McCann's 6:30PM	9 Genealogy SIG @ McCann's 7:00PM	10 Board Of Directors Mtg. @ McCann's 6:30PM	11	12	13Living With Home Electronics 690 AM 10:00AM-11:00AM
14	15 Visual Basic Learner's Group @ McCann's 6:30PM	16	17 Office Suites SIG McCann;s 6:00PM	18 New User's SIG @ McCann's 7:00PM	19	20Living With Home Electronics 690 AM 10:00AM-11:00AM
21	22 Visual Basic Learner's Group @ McCann's 6:30PM	23	24 Digital Imaging SIG @ McCann's 7:00PM	25 Lick & Stick @ McCann's 6:30PM Internet SIG aft.	26	27Living With Home Electronics 690 AM 10:00AM-11:00AM
28	29 Visual Basic Learner's Group @ McCann's 6:30PM	30	31	November 1: Windows XP Launch		

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