



The Paper Modem

October 2004 Volume 4 Issue 9

Inside this Issue:

Page #

Stand - In Editors comment..	1
Technology...	2
Advice from Greg...	3
How is your sense of Humour...	4
Hackers Jump On Windows Flaws...	5
Back to Basics etc...	6
Safe Mode and What is on in October...	7
Some things you should know... & Anti-Spam...	8
Ant - Spam continued.. And more Back to Basics, by Greg...	9

It is a little while since I did this job and following Yvonne makes it a little more difficult as she really did us proud as editor of the Paper Modem.. Most of what you read here was supplied by Yvonne, and Greg Wilson our Chief of Research...

However please do not despair you may not have to put up with me for very long... Yvonne tells me that she rather enjoyed doing the Paper Modem every month and some of our members were very good in providing some of the info contained therein.. I hope that they will be as kind to me..

So, while I have your ear, or rather, your eye.. I thought that I would re-emphasise the theme our worthy President Wes has been dwelling on these last few meetings..

This is your Club but it does not run itself... We need some help on the Executive..

Simple things: Like being responsible for setting up or helping to set up and put away the equipment prior to a meeting. Manning the table, selling tickets and answering members or prospective members questions..

Less Simple things: Such as searching out and arranging for future demonstrations..
Or even taking over this publication sometime down the road..

Please give it a thought... "Many Hands Make Light Work" and you might just find that you quite enjoy being a little more involved...

We promise to break you in gently, not throw you in off the deep end.. The AGM is November 10th. If you are willing to run for the Exec. Please let Pres. Wes. know .. Thanks in advance..

WinZip Vulnerable To Hacks

By [TechWeb <http://www.techweb.com/>](http://www.techweb.com/)

WinZip this week warned users that its popular compression utility is vulnerable to a pair of buffer overflow-based attacks, and posted a new version to plug the holes.

The vulnerabilities could be used by hackers to compromise a WinZip-equipped PC and hijack the machine.

"WinZip was not aware that any of these vulnerabilities had been publicly described or exploited," the company said in an alert posted on its Web site. "However, WinZip recommends that all users upgrade to WinZip 9.0 SR-1 to avoid the possibility of future exploitation of these vulnerabilities."

Danish security firm Secunia rated the flaw as "highly critical," and said the vulnerabilities affected all version of WinZip as far back as v. 3.0.

The update, which can be downloaded free of charge by registered users from the [company's site, <http://www.winzip.com/upgrade.htm>](http://www.winzip.com/upgrade.htm) also takes a page from Microsoft's Windows XP Service Pack 2 (SP2), and pops up cautions when users do potentially dangerous things, such as double-clicking an .exe file compressed within a Zip.

Numerous worms, including the most recent Bagle variant, have taken to packing their payloads in .zip files as a way to slip by defenses that block executable file attachments.

"404 Error - Page Not Available" - Newbie Club

How many times have you clicked a link to visit a Website, and all that came up onto your screen was a page saying the requested page was not available. Or just simply '404 error'? Many people assume that the page does not exist. Someone's made a typo. Some fool has messed up!

Well that's not always the case.

I know you're not interested in the techie reasons for this happening, but sometimes if you click 'Refresh', the page will load for you. You'd be surprised at how often you'll be successful.

If that doesn't work, try returning later and see if it loads. And sometimes you may find that a page is taking aaaaages to load. The bar in your taskbar is crawling across at a snail's pace, and you feel your eyes beginning to grow heavy and your chin slowly drops closer to your chest.

It is NOT recommended that you squirt lubricating oil into the back of your PC. However, the burning smell *will* keep you awake whilst you're staring at a black screen.

It's better to try clicking 'Stop' and refresh the page. Sometimes the page loads almost instantaneously.

Why? Coz it's technology, that's why:-)

Back To Basics by Greg..

Create a Personal Screen Saver -

For a great way to put your digital photos to work, try creating a slide show presentation for use as a screen saver.

1. Right-click an empty spot on your desktop, and then click Properties.
2. Click the Screen Saver tab.
3. In the Screen saver list, click My Pictures Slideshow.
4. Click Settings to make any adjustments, such as how often the pictures should change, what size they should be, and whether you'll use transition effects between pictures, and then click OK.

Now your screen saver is a random display of the pictures taken from your My Pictures folder.

Changing Your Home Page -

Do you have your own website? Would you like to have it as your home page? Got a favorite website that you would like to see when you first log on? Here's how you can change your home page:

Go to 'start'--'settings'--'control panel'--click on 'internet options'.

Be sure you are on the 'General' tab.

The first box says, "Home Page" and has a box labeled 'address'.

Delete whatever is in this box, by hitting 'backspace', then type in your URL or the URL of your favorite site. Ex-- [<http://www.nanaimocomputerclub.com/>](http://www.nanaimocomputerclub.com/)

Click 'apply', then 'ok'. It's done!

Use Outlook Express Stationery for One Message

Use e-stationery-a colorful background, a graphic image, even colored text-to give a message that extra flair. And if you've hit upon the stationery that is just so you, you can use it for every message you send or just one message at a time.

Now and then you'll want stationery for a special occasion-for example, a holiday message.

1) Open the Outlook Express stationery collection:

If you haven't yet started a message: On the **Message** menu, point to **New Message Using**, and then click **Select Stationery**.

If you have already started a message: On the **Format** menu, point to **Apply Stationery**, and then click **More Stationery**

2) Browse through the list, and when you've found the one you want, click **OK**.

Tip: You can add stationery that you see in a message from someone else to the Outlook Express collection. Open the message, and then on the **File** menu, click **Save as Stationery**, and give it a memorable name. Alternatively, you can [download stationery <http://www.microsoft.com/windows/oe/features/stationery/stationerydl.asp>](http://www.microsoft.com/windows/oe/features/stationery/stationerydl.asp) from Microsoft. The next time you use stationery, you'll find it as a choice in the list.

[<HTTP://WWW.MICROSOFT.COM/WINDOWS/OE/FEATURES/STATIONERY/>](http://www.microsoft.com/windows/oe/features/stationery/)

How is your sense of Humor?

Dear Tech Support:

Last year I upgraded from Girlfriend 7.0 to Wife 1.0. I and soon noticed that the new program began unexpected child processing that took up a lot of space and valuable resources. In addition, Wife 1.0 installed itself into all other programs and now monitors all other system activity.

Applications such as Poker Night 10.3, Football 5.0, Hunting and Fishing 7.5, and Racing 3.6 no longer run, crashing the system whenever selected. I can't seem to keep Wife 1.0 in the background while attempting to run my favorite applications. I'm thinking about going back to Girlfriend 7.0, but the uninstall doesn't work on Wife 1.0. Please help!

Thanks,

A Troubled User.

REPLY:

Dear Troubled User:

This is a very common problem that men complain about. Many people upgrade from Girlfriend 7.0 to Wife 1.0, thinking that it is just a Utilities and Entertainment program. Wife 1.0 is an OPERATING SYSTEM and is designed by its Creator to run EVERYTHING!!! It is also impossible to delete Wife 1.0 and to return to Girlfriend 7.0. It is impossible to uninstall, or purge the program files from the system once installed.

You cannot go back to Girlfriend 7.0 because Wife 1.0 is designed to not allow this. Look in your Wife 1.0 manual under Warnings-Alimony-Child Support. I recommend that you keep Wife 1.0 and work on improving the situation. I suggest installing the background application "Yes Dear" to alleviate software augmentation.

The best course of action is to enter the command C:\APOLOGIZE because ultimately you will have to give the APOLOGIZE command before the system will return to normal anyway. Wife 1.0 is a great program, but it tends to be very high maintenance. Wife 1.0 comes with several support programs, such as Clean and Sweep 3.0, Cook It 1.5 and Do Bills 4.2. However, be very careful how you use these programs. Improper use will cause the system to launch the program Nag Nag 9.5. Once this happens, the only way to improve the performance of Wife 1.0 is to purchase additional software. I recommend Flowers 2.1 and Diamonds 5.0 !

WARNING!!! DO NOT, under any circumstances, install Secretary With Short Skirt 3.3. This application is not supported by Wife 1.0 and will cause irreversible damage to the operating system.

Best of luck,
Tech Support

Hackers Jump On Reported Windows Flaws Sept. 16, 2004

Less than a day after Microsoft detailed the latest Windows vulnerability, hackers were hunting for exploit codes.

By Gregg Keizer, TechWeb News

Hackers are drooling at the thought of exploiting Microsoft's most recent vulnerabilities, security analysts said Thursday.

Less than 24 hours after Microsoft released details of the latest vulnerability in Windows, hackers were sharing details and eager to get their hands on exploit code, says Ken Dunham, the director of malicious-code research for security-intelligence firm iDefense.

"Hackers are already actively discussing the new JPEG vulnerability and how to exploit it," Dunham says in an E-mail to TechWeb.

Tuesday, Microsoft noted that a bug in Windows XP, Windows XP SP1, and Windows Server 2003, as well as many of the company's flagship applications, could allow attackers to grab control of PCs. Exploit code exists, Dunham adds, to launch a successful denial-of-service attack on vulnerable applications, proving it's possible to create an exploit that executes code--in other words, make a worm. "While this type of exploit code has not yet publicly emerged in the [attacker] underground, this does prove that it's more likely for hackers to develop such exploit code," Dunham says.

Another analyst, Vincent Weafer, the senior director of Symantec Corp.'s virus research team, agrees. "We fully expect that [hackers] will go into this," Weafer says. "There's enough knowledge about this [vulnerability] to easily make it exploitable."

The most likely attack avenue, both Dunham and Weafer say, is an HTML E-mail that includes or links to a hostile .jpg image, although links to malicious Web sites or even instant messages could be used as attack vectors.

Another issue that hackers will undoubtedly use to their benefit, Weafer says, is the reputation of .jpg-formatted images. "Generally, they're considered safe by most users," he says. "People send JPEG images all the time." Images, for instance, are rarely blocked by E-mail security at the gateway, unlike other file formats such as .exe or .com. That makes it "even more likely," Weafer says, that hackers will rush to roll out worms.

Difficulties patching the bug will add to the problem, Dunham and Weafer predict. It's "complicated and tough for administrators to audit," Dunham says. Because the JPEG processing flaw is widespread--not only in the operating systems but also in such popular applications as those in the Office XP and Office 2003 suites--administrators may be hard-pressed to patch before an exploit is circulating.

"If this vulnerability is exploited on a widespread basis, it may be some time before all of the vulnerable computers are identified and properly patched," Dunham says.

Worse, even patched systems can later be turned into vulnerable computers, Weafer adds, if applications with the flawed image processing .dll are later installed on made-safe PCs.

"That could 'undo' the patch," Weafer says, "and makes the 'stickiness' of the [patches] more difficult than normal." In addition, Dunham concludes, not even the massive Service Pack 2 update for Windows XP completely protects against the bug, since "other products may also need to be patched to fully protect against this vulnerability."

More Back To Basics..

Alphabetize your start menu

Don't you hate how Windows adds new programs to the end of the start menu? The fix is quick and simple, *right click* on the menu and select *sort by name*. Ah isn't that better?

XP Legitimacy.

You say you're not sure whether that computer your neighbor sold you has a legitimate copy of Windows XP properly activated. Well, if you never did trust that guy, the easiest way to find out is by going to Start|Run and enter "oobe/msoobe /a" (without the quotes and observe the space before /a".

Index Dis 'N' index.dat - Brandon Watts

Q: I was just browsing through the files on my computer and came across a file called index.dat in my Cookies, Temporary Internet Files, and History folders. What does this file do?

A: You may just assume that clearing out your History folder will cover the tracks of where you've been on the Internet, but that is definitely not the case. This index.dat file is an Internet Explorer database that keeps track of what you've done on the Web. The reason behind this is that it allows for easy retrieval of information.

The only problem is that it's easy retrieval for anyone who wants to see what you've been doing. The file can contain months of records regarding your online activity. You'll probably be surprised at the amount and type of data that is stored within it.

If you share your computer with other individuals, you may wish to eradicate the information contained in the file. [This article <http://www.exits.ro/index-dat-files.html>](http://www.exits.ro/index-dat-files.html) provides a lot more information on these index.dat spies. You're given complete instruction on what they are, what they contain, and how to remove them.

It's far better to be aware of these things than to have a false sense of security [<http://www.exits.ro/index-dat-files.html>](http://www.exits.ro/index-dat-files.html)

Safe Mode: By Diana Huggins

Safe mode is often used when troubleshooting computer issues. To access it, you have to press F8 during startup. If you're not paying attention and don't press the key at the right moment, you'll be restarting a few times. So here is a way you can save yourself having to press F8 during startup to access Safe Mode. Instead, you can add it as an option to your Windows XP Boot Menu.

Right click My Computer and click Properties.

Click the Advanced tab.

Under Start Up and Recovery, click the Settings button.

Click Edit. The boot.ini file will open in Notepad.

Copy the line that reads as follows:

```
Multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows XP Professional" /fastdetect.
```

Paste the line you just copied after the original one.

Change the second line from "Microsoft Windows XP Professional" to "Windows XP Safe Mode" or something similar.

At the end of this line add the following:

```
/safeboot:minimal /sos /bootlog.
```

Save the boot.ini file by clicking File then Save.

Restart your computer and Safe Mode should be available at the boot menu.

What is on in October...

October 13th. 7.15pm..Beban Park

Our own Steve Wawrykow will be back to give us an Overview of his demo's on Photoshop, including, Cleaning old slides and Pictures

October 19th. 7.15pm

Angelito Herrera of Staples, Aulds Road will explain all about Web Cams, with the skilful assistance of Ben Poudrier and Yvonne Bulger...

Some Things You Should Know...

- 1. Money isn't made out of paper; it's made out of cotton.**
- 2. The 57 on Heinz ketchup bottle represents the varieties of pickle the company once had.**
- 3. Your stomach produces a new layer of mucus every two weeks - otherwise it will digest itself (eeww).**
- 4. The Declaration of Independence was written on hemp paper.**
- 5. The dot over the letter 'i' is called a "tittle".**

Anti - Spam..

By Alyce Lomax (TMFLomax) September 24, 2004

(Nasdaq: MSFT) SenderID technology may not be hitting it off with other technology companies, but the company's continuing on the anti-spam crusade that it started talking up back in January. Yesterday, Microsoft said it has filed nine new lawsuits against spam offenders, including a Web host that was allegedly a major purveyor of much-hated spam marketing.

This brings Microsoft's grand total of spam-related law suits to 100, with 70 of the suits in the U. S., according to Reuters. The Web host was National Online Sales, which supposedly offered spammers "bulletproof" services for marketing emails (the cads). According to the article, the lawsuit hopes to make it too expensive for spammers and spam-friendly operations to keep up their dastardly deeds.

Back in March, an assortment of technology heavyweights -- (NYSE: TWX) AOL, Microsoft, (Nasdaq: YHOO), and (Nasdaq: ELNK) -- joined forces in suing a bunch of high-profile spammers.

That March law suit was brought under the auspices of the CAN-SPAM Act, which, quite frankly, doesn't seem to have deterred spammers too terribly much. (I've even received, er, highly inappropriate spam messages that had the gall to claim they were being sent with the CAN-SPAM Act.)

True, recent developments surrounding Microsoft's SenderID brainchild have indicated that other technology companies, as well as the open-source movement, often distrust the giant's motives. However, when it comes to the spam war, it's a spot where Microsoft's deep pockets and clout could possibly do a lot of good.

Jaundiced anti-Microsoft folks, of course, will point out that Microsoft has a vested interest in spam control, considering spam-borne worms and other electronic vermin that tend to particularly target its products. Regardless, any company that relies on Internet users needs to eradicate unsolicited email marketing.

(Continued on Page 9)

(Anti-Spam...Continued from Page 8)

After all, more and more people are reporting an alarming amount of fatigue and distress caused by the ever-increasing onslaughts of spam in their inboxes.

To most of us, it doesn't matter too much who does it, as long as spam does get canned. (Though some have mentioned that a busy hurricane season may have put some spammers at least temporarily out of commission, seeing how many supposedly reside in Florida.)

Although it's a pleasant thought that Microsoft could make mincemeat of spam, the CAN-SPAM Act's outward signs of failure are enough to make one wonder whether the legal system and the establishment can make headway against the resilient workings of the Internet's underground. However, if Microsoft can hit them where it hurts -- the pocketbook -- we could all end up better off.

Microsoft Viruses, Hoaxes & Spam, Oh My! discussion board.

Alyce Lomax does not own shares of any of the companies mentioned.

Back To Basics (Continued)

WINCHAT.

If you're running Windows XP networked, you can use a little-known application to talk to other available users on the network. At Start|Run, enter "winchat" without the quotes. Click on Conversations and Dial, select the computer to call and click OK. This will ring the user and invite him or her to chat with you. Of course, you could step in the next room or call them on the phone, but that's so untekkie.

Tips On Spotting Fraudulent Web Sites By Parry Aftab, InformationWeek

While most Canadians do not use Citibank (one of the favorite targets of Phishers) just substitute Royal Bank or whatever name in here and be aware - it has already happened to the Royal after their major computer crash last month. Here are some tips from an Internet service provider, eBay, and Citibank on ways to avoid being phished.

Citibank Tips Citibank warns its customers to check the security certificate for any site to which they're linked.

If the name doesn't match the company owning the site, you shouldn't trust the link. It also recognizes that not all certificates are held in a name recognized by consumers accessing the site, but the bank informs its customers that all security certificates for Citibank's sites are held in its "Citibank" name.

Since not all security certificate issuers police similar-sounding "brand-related" names when issuing their certificates, knowing the exact name of the security-certificate holder is key to authenticating the page. All sites should disclose the correct security-certificate holder name at their sites.

That's All Folks... The End..