

**INSIDE THIS ISSUE:**

<i>Committee Information</i>	Page 2
<i>Ron's Ramblings</i>	
<i>OPEN News &amp; Schedules</i>	Pages 3-4
<i>Newbie Club Tutorials</i>	Page 5
<i>Contagious Computing</i>	Pages 6-9
<i>More Newbie Club Tutorials</i>	Page 10
<i>Subject: Over 40's</i>	
<i>Getting More from Adobe Reader 6</i>	Pages 11-12
<i>Oztralia</i>	Page 12
<i>His post was Toast &amp; Selective Start ups Win 96 &amp; XP</i>	Page 13
<i>Neat net Tricks Newsletter Hints</i>	Page 14
<i>Subject: AAADD</i>	Page 15
<i>Carols for Mental Health</i>	Page 16
<i>Not So Subtle Reminder re: Win 98</i>	

NEXT MEETING  
 WEDNESDAY 3RD MARCH  
 STUDIO WORKS  
 Committee 6 pm  
 Beginners 7 pm  
 Tutorials 8 pm

Newstream Articles

Deadline : 10 Days before Meeting  
 Editors Contacts:  
 Address: 8 Cadorna Street Mowbray Heights 7248 Phone 6326 5824  
 email address editor@lcg.org.au

Correspondence

Address all Correspondence to:  
 Launceston Computer Group Inc  
 PO Box 548  
 Launceston 7250

Membership

Single \$10, Family \$15 (Includes Email edition Newstream)  
 Printed & Posted Newsletter \$20 extra

**Disclaimer:** The articles in this newsletter may be reprinted as long as credit is given to the original author. Opinions expressed are those of the author & not necessarily the views of the Editor or the Group. Unless otherwise noted material is copyright 2004 for the Launceston Computer Group Inc.

# General Information

Position	Name	After Hours / Business	Email
President	Glenn Gilpin	6330 1129	president@lcg.org.au
Vice President	Ivan Turmine	6327 1825	vicepresident@lcg.org.au
Treasurer	David Gray	6343 2514	treasurer@lcg.org.au
Secretary	John Frearson	6335 4802	secretary@lcg.org.au
<b><u>General Committee</u></b>			
Library MAC	Ivan Turmine	6327 1825	maclibrary@lcg.org.au
Newstream Editor	Ron Baker	6326 5824	editor@lcg.org.au
Publicity & Promotion	Judy Hall	6394 7358	publicity@lcg.org.au
Assistant Treasurer	Iris Meek	6327 3162	Assistanttreasurer@lcg.org.au
PC Library	Judy Hall Julie Hjort	6394 7358 6344 5686	pclibrary@lcg.org.au
Public Officer	Judy Hall	6394 7358	publicofficer@lcg.org.au
Meetings Chair	Ron Baker	6326 5824	committee@lcg.org.au
OPEN Chair	June Hazzlewood	6327 2562 0414 770 864	open@lcg.org.au
Linux Chair	David Gray	6343 2514	linux@lcg.org.au
WebMaster	Chris Ralph		webmaster@lcg.org.au
Web Editor	Reinhardt Von Samorzewski	6327 1552	web@lcg.org.au

## RON'S RAMBLINGS

Following a suggestion that the Newsletter was hard to read on the net I have altered the layout this month as a trial to see if it is any improvement. The printed version may have to be changed back and 2 versions prepared.



Those members who didn't attend the December 2004 meeting missed out on a treat as Steve Scott (Pictured) demonstrated the programmes used in teaching Musical Appreciation at Riverside High School. He also showed music recording programmes and played his guitar to illustrate. We are still not getting much feedback as to what members want at general meetings. If members are content with using General Meetings to discuss their problems and seek advice on remedies, that is OK. But if Guest Speakers are preferred, we need to find out the preferences of members as to topics and/or speakers. Some have suggested getting Paul French from Tasmanian Cartridge Company back for a repeat of the talk he gave last year. It is always possible to learn something new from a repeated talk. Other possibilities are David Stallard or Geoff Daw, (He gave a very good lecture on Mobile Phones to the National Seniors Association a couple of years ago).

**Ron Baker**  
Editor

**Launceston Computer Group  
SOFTWARE LIBRARY**

**Dated 1<sup>st</sup> March 2004**

These small programs are some of the best programs currently in the shareware library.

**DISK 1000 - Your Library on Disk**

*Have you received your copy of Disk 1000? The disk holds a complete listing of programs available in our PC shareware library. This disk is free of charge to all new members.*

**DISK COPY PRICES for CLUB MEMBERS ONLY \$1.00 per disk**

**Disk Prices - Box of 25 = \$12.00** Members Only

**CD Prices - Box of 10 = \$10.00** Members Only

Judy Hall, Shareware Librarian

**AVAILABILITY OF LIBRARY**

The Shareware Library is available in-between meetings from the following people. Please telephone first to arrange a suitable time.

**The library is also available at the venue -**

**Studioworks most Wednesdays 9am to 3pm.** Email: opencomputingtas@hotmail.com

**LAUNCESTON**

Julie Hjort

Flat 2, 115 Penquite Road, Newstead Phone 6344

5686

**Email: [jhjort@intas.net.au](mailto:jhjort@intas.net.au)**

**Monthly Workshops**

**Graphics - 17<sup>th</sup> March**

Next class

**PSP7 Editing Photographs**

**Wednesday 17 March 1pm - 3.30pm**

**\$6.50 fee** - Numbers limited to 8 please register on noticeboard or call **Judy** 63947358 or 0428 947358.

**Family History Online**

Next Classes

**Wednesday 10<sup>th</sup> March 1pm-3.30pm &**

**Tuesday 23<sup>rd</sup> March 9pm - 12pm**

**\$4.00 fee** Numbers limited to 8 people

Please register on noticeboard

**Microsoft Publisher**

Next Class

**Tuesday 11<sup>th</sup> March - 1pm to 3pm**

Please register on noticeboard - Fee \$4.00

**Making Music**

Creating a digital version of your favourite music

**Wednesday 24<sup>th</sup> March - 1pm to 3pm**

Please register on noticeboard - Fee \$4.00

**Monthly Workshops**

**Animated Email Magic**

Creating animated emails for special occasions.

**Wednesday 31<sup>st</sup> March 1pm to 3pm**

Please Register on Noticeboard Fee \$4.00

**Tutors Tutorial**

How to use family history CD Roms and what is available on the Internet.

Wednesday 3<sup>rd</sup> March after meeting.

Special tuition for tutors who would like to improve their skills and provide better quality service to OPEN.

**OPEN Computing - Session Times**

All sessions are held at the venue at Studioworks, 1 Pipeworks Rd, L'ton

**Standard Sessions** (All sessions \$4.00)

Monday every <b>Monday afternoon</b>	1 - 3	Second Step See Noticeboard
Wednesday 3 <sup>rd</sup> March	1pm on	OPEN Computer <b>Club Meeting &amp;</b> Tutors Tutorial
Wednesday 3 <sup>rd</sup> March	7pm on	<b>LCG Monthly</b> Meeting
Wednesday 10 <sup>th</sup> March	1 - 3	<b>Family History</b>
Thursday 11 <sup>th</sup> March	1 - 3	<b>MS Publisher</b>
Wednesday 17 <sup>th</sup> March	1 - 3	<b>Graphics</b>
Tuesday 23 <sup>th</sup> March	9 - 12	<b>Family History</b>
Wednesday 24 <sup>th</sup> March	1 - 3	<b>Making Music</b>
Wednesday 31 <sup>st</sup> March	1 - 3	<b>Animated Emails</b>

**TAFE eLearn Sessions** (All sessions \$4.00)

New Classes start about 22 March 2004 - Register Now

Thursday	9am - 12	TAFE eLearn
Thursday	1pm - 3pm	TAFE eLearn
Friday	9am to 12	TAFE eLearn

**Special March Sessions**

Monday	9am - 12	Beginners
Monday	1pm - 3pm	Second Step
Tuesday	9am - 12	PC & Mac
Tuesday	1pm - 3pm	Beginners
Wednesday	9am - 12	Beginners
Wednesday	2pm - 4pm	Second Step
Thursday	9am - 12	Pre eLearn
Thursday	1pm - 3pm	PC & MAC

(Continued on page 4)

(Continued from page 3)

## What's Happening at OPEN

### **OPEN Monthly Meetings**

**Next Meeting 3<sup>rd</sup> March 2004 at 1pm**

The monthly OPEN meeting will now be held on the first Wednesday of the month at the venue starting at 1pm.

### **Fee Alteration - \$2 sessions**

A decision was taken at the last meeting to assist those people attending more than one class a week. Anyone attending a second class within the same week can now pay \$4.00 for the first session and \$2 for each subsequent session.

**Please Note:** Excludes sessions where special fees apply ie Graphics.

### **Free Copy of Newsletter**

Also passed a resolution to supply everyone attending sessions with the current monthly newsletter free of charge in an effort to keep them up to date. **Don't forget to submit your email address if you wish to receive the LCG/OPEN newsletter via email.**

### **Roster Details**

Make sure you check the noticeboard regularly for changes to the current roster and special sessions registrations. You may miss out on a class if you do not register. **You can also get a copy of the roster on floppy disk.** Bring a disk in and ask.

### **eLearn Students**

The next eLearn class will start in March,

### **REGISTER NOW.**

These classes will not go ahead if we do not get enough registrations. Before you can participate in the next Tafe eLearn class you will be required to complete a short course to determine your current skills.

### **Second Step Classes**

These classes are aimed at those people who have completed the beginner's courses and would like to learn more. They will take the form of individual subject classes and will change monthly so please check the notice boards for session times for these special classes.

These classes will also incorporate the monthly meeting, the graphics class and afternoon family history class.

### **Family History Online**

New classes for family history are now available on the 2<sup>nd</sup> Wednesday afternoon and the fourth Tuesday morning of the month and will be up to three hours duration.

Rose Hodgeman & Janet Headlam have agreed to help with these new classes. Rose and Janet have a wealth of knowledge in family history and can help you draft your initial pedigree charts and information. They are also very familiar with Brother Keeper software.

### **MS Publisher Class**

Ron Baker, editor of the LCG newsletter you are now reading has agreed to hold a class once a month for those people who wish to delve deeper into MS Publisher. These classes will be held on the second Thursday of each month from 1pm and will only continue if there is

enough patronage.

### **VENUE TELEPHONE NUMBER**

A Mobile Phone Number is now available to all those wishing to contact OPEN during working hours. The number is

**0413 698 610**

### Special Monthly Meetings

### **Launceston Computer Group Inc.**

1<sup>st</sup> Wednesday of the month

**Wednesday 3<sup>rd</sup> March 2004**

**Evening 7pm – 10pm**

### **Open Computer Club**

1<sup>st</sup> Wednesday of the month

**Wednesday 3<sup>rd</sup> March 2004**

**Afternoon from 1pm**

**Tutorial immediately after**

**Using Family History CD Roms.**

### **Shareware**

**Disk# >>> 3755 <<<Category>><Com for WIN/W2000< FreeRip MP3**

FreeRip MP3 is a free application which let you extract audio tracks from compact discs and export them to Wav, Ogg Vorbis or MP3 audio files. FreeRip MP3 is a free application that can record digital audio tracks directly from compact discs, without going through your sound card (this process is known as "ripping").

**Disk# >>> 3754 <<<Category>><Gam for WIN/W98< DXBall v1.09**

DX Ball is a Windows 95/98 game which will run on 486DX2/66 as well as the latest machines. Very fast and very addictive. Requires Direct X 2 or greater.

## Newbie Club Tutorials

### Tutorial... "How To Make A Screen Capture"

Okay, you've seen screen captures. You know, those windows pictures we use so extensively in our Newbie Club Ebooks and Website tutorials.

How is this accomplished?

Ctrl + Print Screen is the key

This is where the Print Screen key on your keyboard comes in handy. It may be called PrntScn on your keyboard, or some other variant. But its purpose is to make a copy of whatever is on your screen. It copies the info to the Windows clipboard. Then you can paste into another document that will accept it, such as Word, or a graphics program.

But what if you want to capture only the active window - the actual window that you may have just brought up on your screen?

That's when you use two keys together. The Alt and the Print Screen keys. Hold down the Alt key. Press the Print Screen key. That's it! You've just made a copy of the active window, placing it on the clipboard, ready to insert wherever you want to insert it.

I use a graphics program called Paint. It comes with your computer. You can try it now. It's really cool! Or you can use some other graphics programs that are far more robust. However, nothing too fancy is required to make these screen captures.

And now you know how it works.

### Tutorial .... "What If A File Won't Open?"

Ever tried to open a file, and get that box that shouts, "You're an idiot!

You can't open that file! What program do you want me to use?"

It's called the "Open With" dialog box.

Try this. Open Notepad... (Start, Programs, Accessories, Notepad).

Type a few letters... then click File, Save As, and give it a name: "test.abc".

Save it to your Desktop for easy retrieval.

Now, go to your Desktop and you'll see a new icon that looks like a little Microsoft Window Logo flying on a white box.

Try double clicking that icon. No the file won't open, but you will open the "Open With" dialog box.

Here's why. Windows didn't recognize the ".abc" file extension and didn't know which program to use to open the file. So it asks you. Like you're some kind of guru, right?

If you had saved that file you created in Notepad and given it a ".txt" extension, it would have opened up in Notepad when you double clicked the icon. Because Windows knows that Notepad will read any file with the .txt extension.

So... what do you do when trying to open a file that's real, but you don't have the necessary program? The "Open With" dialog box will do you no good.

You must install the program needed.

For example, you receive a file by email attachment that's a Microsoft Word document. You don't have Word installed on your computer, but do have Microsoft Works.

You can't open a Word document with Works. Sorry. You'll have to install MS Word. If you receive a file with a ".ppt" extension, you need Power Point in order to open that file.

Where you can find a list of file extensions, and the programs needed to open those files? Easy. Just jump over to <http://www.google.com> and type "file extensions" into the search box.

And you can also use Atomica to look up anything about everything <http://www.atomica.com>

The web is crammed full of resources. And you only need a couple of tools to find links to all the other tools you need to build your home on the web.

File extensions are the key. Once you understand how they work, you've de-mystified another corner of your computer

*From Newbie Club Newsletter 15/2/2004*

**Contagious computing** The threat of digital disease has reached epidemic proportions. Davey Winder examines the growing impact of the computer virus. Anyone who has been around computers for a fair few years will recall that 20 years or so ago, viruses were a by-product of the pirated games scene. Boot sector infections moved from floppy to floppy with ease, but at the same time, antivirus software stopped infections with similar ease. Relatively little damage was done, and relatively little sympathy was extended to those infected, as it was often thought that they deserved it for using pirated software in the first place. That was then, this is now. Welcome to the grown-up world of the computer virus epidemic, where thanks to the Internet and advances in network connectivity, millions of machines can be infected in minutes. Just as we've seen an alarming rise in difficult to contain biological viruses in the past few years, we're also on the verge of an epidemic within the computer world. If you don't believe me, just sit back and absorb some of the following shocking truths. Sophos ([www.sophos.com](http://www.sophos.com)) is one of the world's biggest providers of antivirus solutions in the corporate space. In its report on the first six months of activity in 2003, they concluded that eight of the top 10 viruses can spread by the multiple methods of email, IRC (Internet Relay Chat), network shares and P2P (Point-to-Point) file sharing platforms. Virus writers are no longer relying solely on email to spread their malicious code. As a result, computer users are advised to deploy desktop antivirus protection, which can detect malicious code regardless of its method of propagation.

January's Slammer worm was the biggest Internet worm of the period, targeting a six-month-old vulnerability in order to spread. Sections of the Internet slowed substantially, and users got a sharp reminder to install patches from software vendors as soon as they're issued. Another of the big antivirus service providers, MessageLabs ([www.messagelabs.com](http://www.messagelabs.com)), reported that August 2003 went down in virus history as the worst on record. With SoBig.F leading the way, MessageLabs calculated that at its peak, it accounted for one in every 17 email messages sent, and at one point, was responsible for 75 per cent of all email traffic, crashing networks the world over through sheer volume. MessageLabs stopped more than a million copies of it in the first day alone. It spread to 134 countries, generating millions of email messages within just 96 hours. Yet perhaps the most frightening aspect of the virus threat is the sheer volume of new strains that don't make the news, the ones that are caught before they can do any damage, that don't get released into the wild, but are sent straight to antivirus labs to prove how clever

the developer is.

Take the figures for August 2003, (the latest available as I write), Sophos reports that while there are 5 new entries in their top 10 of live viruses chart, that leaves 5 old ones, including Klez-H which has spent a staggering 19 months in the chart! In the same month, of the 84,277 virus strains that Sophos has identified and can offer protection against, an incredible 778 new strains were analysed. **View from the labs** So you know it's a growing problem, but what is being done to tackle it? Although the precise details regarding antivirus research is kept a closely guarded secret in order to prevent the virus writers from getting too far ahead of the game, the basics of antivirus research are well known. There's a great deal of teamwork involved, both within the antivirus lab where people with different skills can pool together, but also between different companies. It's probably the worst kept secret of the industry that virus code is exchanged between labs, despite their individual products being proprietary. Yet not only do other antivirus companies provide live code, so do customers, and surprisingly enough, many virus writers do too. The fact that virus writers supply code is often a shock to the layman, but you have to understand that for many it's the proof of concept that's enough. They don't need to actually release it into the wild and cause any damage to feel rewarded. However, while the lab rats have as long as it takes to identify a new virus and produce the vaccination, the end user doesn't have the same luxury. This is why antivirus labs are also working hard on ways to speed up all phases of the process; from identification, to update methodology, and ultimately through to the scanning and disinfection of systems. One of the most talked about technologies to combat the emerging virus threat is that of heuristics. Contrary to popular belief, heuristic scanning is nothing new. The first heuristic engines were developed in 1989 to help detect DOS-based viruses! However, it's only in the last couple of years that the technique has gained both popularity and notoriety. Whereas traditional antivirus scanning is signature or string-based, (looking for specified code strings to identify a virus), the heuristic approach looks for commands within a program that aren't typically associated with those applications. Because it looks for things that appear dodgy within an executable rather than pre-defined virus signatures, the technique means that unknown viruses can be detected – theoretically at least. In practice, heuristics has a fairly good success rate of around 85 to 90 per cent, which is why it's most commonly combined with signature scanning to provide a solid foundation for an antivirus solution. These days, you'd be hard pressed to find a

*(Continued from page 6)*

commercial antivirus solution that doesn't have a heuristic element within it, even if they don't all advertise the fact. As well as employing a proven antivirus software product or service provider, you can do plenty to lessen the chances of getting infected, purely by using some modern day computing common sense. If you use Outlook or Outlook Express, ensure that you apply all security patches as they become available. The same applies to operating system patches. Microsoft may get more than their fair share of the blame for security holes, but if you don't fill them in when they provide the cement, then it's on your shoulders if the walls crumble around you. Remember, Microsoft never sends security patches by email, but rather alerts to their existence if you've subscribed to the alert service. Worms such as the Swen mass mailer look like they've come from Microsoft and claim to contain a security patch, which is in reality, an infected executable. Never open email attachments you're not expecting, and certainly never open anything with a PIF, SHS or VBS extension. These are hardly ever used in conjunction with a genuine attachment, but commonly used by worms and viruses alike. The same goes for double extensions used to hide the real content, so never open things with an extension of VBS.TXT or DOC.EXE for example. If you receive a suspicious attachment from a friend or colleague, don't feel embarrassed to ask them if they sent it, what it is and why they have forwarded it to you. They can then either set your mind at rest, or you can tip them off to an infection using their contacts book to distribute itself. If the option is available to you, use it to render all email in plain text. Mature clients such as the latest Outlook 2003 upgrade will allow you to view HTML messages without any external links shown. They will also enable images from those external servers to be downloaded and displayed if you trust the source. Trusted sources can then be added to a whitelist so that they render correctly in future. Trendspotting Slammer, the worm that spread with such incredible speed during January 2003, could be the start of a trend towards anarchic viruses whose payload is the disruption caused by the act of distribution rather than anything more complex. The fastest worm so far, Slammer, would have taken just a few minutes to hit its maximum scan rate of 55 million scans per second, and only 10 minutes to infect an estimated 90 per cent of vulnerable hosts on the Internet. The only reason it took so long was the simple fact that network saturation at specific bottlenecks slowed it down, suffocating the bandwidth required to accelerate growth even further. Although not pleasant to imagine, if it had targeted specific companies or

services, or carried a particularly malicious payload as well, the damage could have been unthinkable. Indeed, such was the severity of the disruption caused, coupled with a relatively harmless payload, that some commentators have theorised that this and other high profile viruses could be part of a cyber-weapon testing exercise. Of course, there's no proof to back this up, but one thing's for sure, the people responsible for releasing these worms continue to gain skill and refine their techniques so that the threat to PCs escalates rapidly. If Slammer had been coded to scan for just 10 or 15 minutes and then stop, it could have remained unnoticed on tens of thousands of machines that hadn't patched against that particular vulnerability. The implication of this situation is that it would then take exponentially much longer to identify that any attack had taken place, and the code would be sitting there undetected, just waiting for an opportunity to strike at a later date. Extrapolate this to cover multiple worms, each targeting specific but separate server and OS vulnerabilities, each stopping once a target figure of machines were infected, all laying dormant until a specific judgement day. It doesn't take a genius to realise that the unthinkable could happen, the Internet could be brought to its knees within minutes. SoBig.F is widely believed to have been the work of 'radical' spammers – for want of a better description. Whereas both legislative and technological advances have started to effect the casual spammer, those at the commercial end of the business, who care little about legislation, but lots about Bayesian spam traps and server side filtering services – such as MessageLabs – are fighting back in the only way they know how. Aggressively. It should come as little surprise that a guerrilla warfare approach is attractive. The weapon of choice is viral distribution through resource hijacking. The evidence is already there, with 50 per cent of all corporate email being spam, and half of all that being sent via innocent third parties (assuming you see those with inadequate antivirus protection as innocent of course). Replication via email addresses found on an infected machine is old hat in the grand scheme of things, but SoBig.F has a secondary surprise up its sleeve. Instructions were encrypted to force infected machines to visit, download and install cracked copies of the WinGate proxy server. This would present the spammer with an open relay to use as a distribution centre for spamming, and a backdoor Trojan adds full control over the host PC to ensure smooth delivery of the dirty deed. Luckily, in the case of SoBig.F, the spam threat was thwarted after encrypted instructions publicly detailed the 20 download sites – themselves on

*(Continued on page 8)*

*(Continued from page 7)*

infected and ‘innocent’ computers. Action could then be taken to close them down. In the blender Blended attacks are already a reality. Just take the Nimda worm. This strain of virus-exploited email targets, unpatched IIS servers and network shares, and compromised websites to spread the infection. As well as going multi-directional like this, virus writers are getting increasingly sophisticated in their efforts to keep one step ahead of the virus police. A good example is worm design, where for some time the tried and tested method of distribution has involved using vulnerable email clients such as Outlook Express to mail itself onwards to everyone in the contacts book. Now, not only are they more likely to scan your web browser cache for addresses as well as your contacts databases, they even come with their own SMTP mail server built in. This is exactly how BugBear managed to outwit the AV scanners and get such a big distribution footprint. Others are simply removing email from the distribution equation altogether. For example, successful infections such as Lovegate.F and FunLove which struck in July 2003, did so by being network aware. These use network connections, shared devices, and mapped drives to quickly saturate a LAN and infiltrate the Internet. We can also expect to see a greater use of the semantic attack as part of an overall infection strategy employed by the virus writer. Klez, for example, made good use of semantics, including a variety of convincing message titles and body texts to dupe the unwitting reader into opening the attachment and executing the payload. By varying the subject line and body text, victims are more likely to be taken in at some point when a raw psychological nerve is touched that demands a response. In the same way, memes ideas are distributed using broadly viral techniques, and virus hoaxes are spread because we want to believe the tragic, exciting, rewarding or whatever message is being aimed at us. Their success depends on the fact that we not only want the messages to be true, but we want to share them with friends and colleagues. Weapons of mass protection? As viruses become ever more technologically advanced, particularly with regard to their distribution methodologies (as evidenced by the recent worms that infected millions of computers within minutes of being released), so ever more extreme antivirus tactics are put forward. There is one such tactic that’s causing much debate in the antivirus industry – that of the antivirus virus. Perhaps the most infamous example was back in 2001 when the CodeRed worm was causing chaos, and a CodeBlue worm was released that scanned the Internet for infected computers and cleansed them.

At the time, many received this with praise, but not so with the more recent release of Welchia. This antivirus worm detects and deletes the Microsoft Blaster infection, but has brought a flood of warnings from the established antivirus industry, who see the harmful potential it could cause. Certainly the legitimacy of such an application is questionable. After all, it’s guilty of breaking the law under the Computer Misuse Act by entering your computer without permission and altering the data stored upon it using the same IIS vulnerability as exploited by Microsoft Blaster itself. It downloads a carrier file, registers as DLLHOST.EXE and creates an automatic WINS client service. After ending, MSBLAST.exe processes it, scans the registry looking for installed patches, and downloads/installs the required RPC vulnerability patch if not found. It then reboots your PC to complete its disinfection routine. Frightening stuff! All this is happening without your permission, and isn’t under your control. Who’s to say that the usual practice of producing virus variants won’t happen with the antivirus virus, thus turning it into a malicious application itself? So if not an antivirus virus, what should we look to as our saviour? The most likely answer is behavioural blocking. Integrating with the host operating system, programs are monitored in real time for malicious actions. Because of the tight integration, the code can be isolated before any harm can be done. For example, it can spot attempts to open or modify files, write macros, change system critical settings, and scripting of email clients and so on. Instead of relying upon signature detection or odd code logic, which we all know can lead to missed detection, the behavioural approach dictates that for a virus to release a payload or attempt to replicate, it must first make a request of the operating system. So, by close monitoring at a low level, these requests can be intercepted and dealt with. No matter how good the code encryption or the obfuscation used, the virus will always be spotted when it reveals itself – as it surely must. Of course, the weakness of behavioural blocking is also revealed in that the virus can do some damage before it can be blocked, even allowing for the real time monitoring. So the real answer to our earlier question is that the future of antivirus has to be holistic, it has to incorporate all aspects of detection: signature scanning, heuristics and behaviour blocks. Indeed, the holistic approach goes even further by using all resources at your disposal – firewalls, email blocks, switches and routers, gateway filters and antivirus scanners all working together. Conclusion Antivirus software is just a small part of a system security strategy. Users also need to be educated on how to safely

*(Continued on page 9)*

*(Continued from page 8)*

handle email, as well as how important scheduled updating is. People also need to understand the nature of the threat better. Hands up if you think that surfing the web is safe, and safe because you're viewing remotely? The reality, of course, is that the browser client pulls down what it needs and this is then viewed locally. Web browsers, emails and instant messaging all expose you and your internal network to self-executing code, which leaves your company vulnerable to a wide variety of attacks using mobile techniques. The damage from viruses to the SME and SOHO market can be even more significant than attacks on larger enterprises, as these organisations often lack the internal resources to deal with infection quickly and efficiently, and lack back-up procedures. The human factor – it has to be said – is the weakest link in any antivirus strategy. This is something that's unlikely to change in the foreseeable future, unless employers, computer manufacturers, software developers and magazines like PC Plus all make a concerted effort to educate users in safe practice. We're doing our bit, isn't it time the others mentioned here started doing theirs? Davey Winder

If disaster strikes The worst has already happened, and you've been infected. Our 10 simple steps will prevent a drama from being a crisis

1. If your computers are networked, isolate the infected machine(s) to prevent further local infection.
2. If your computers are connected to the Internet, disable that connection immediately.
3. If you have antivirus protection (albeit not properly updated or incorrectly used), contact the vendor for further information. The big names will operate 24-hour telephone support lines, web and email-based support services. If yours doesn't, it's another good reason to change vendor. Some vendors, such as Sophos, will talk you through disinfection procedures, even if you aren't a customer.
4. Follow antivirus vendor disinfection instructions to the letter. Don't be tempted to take shortcuts no matter how much of an IT know-it-all you are! After all, you knew too little to prevent getting infected in the first place.
5. Update antivirus software and install all operating system security patches.
6. Scan all machines on the network, disinfecting where necessary.
7. Change all passwords if the infection involved a RAT (Remote Access Trojan) to prevent data loss or the financial implications of the use of misappropriated passwords.
8. Scan all machines again to be sure, before reconnecting your network.
9. Replace lost data, documents and so on by using your most recent back up files (you do back up your data, don't you?) but ensure that these are virus free first.
10. Investigate what went wrong with your antivirus strategy to allow infection to take place in the first place. Rectify as a priority.

On the move For many years

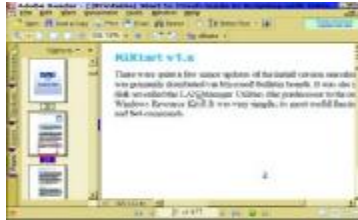
the whole idea of a virus threat to users of PDAs or mobile phones was pretty much scoffed at. However, that was until the technology of both these devices and the virus writers caught up. Now it's universally agreed that any security strategy that doesn't include the mobile devices you own is fatally flawed. It's not so much the threat of infection on the PDA itself, but more on that in a moment. It's rather the ability of your mobile device to infect your PC or network. The take up of networking in the home as well as business, advances in wireless networking, and now Personal Area Networks (PANs) have opened up a whole new avenue of viral distribution for the writers to explore. Whilst it's relatively easy for a company to prevent misuse of computers on the corporate LAN, and even control what data gets uploaded from laptops, things are very different when it comes to PDAs and smartphones. As these devices have got smarter, their developers have got dumber by not giving enough thought to matters of gateway security. When the whole point of going 'smart' is to increase productivity through collaboration and connectivity, it almost beggars belief that the virus threat was not on the development agenda. Viruses and Trojans written specifically with mobile devices in mind are a real world threat, and it's only a matter of time before they become a real world infection. Symantec have launched a product called AntiVirus for Handhelds to protect PalmOS and PocketPC devices, which constantly scans files and emails for malicious code. Importantly, it also performs a scan whenever a desktop synchronisation is performed or a storage card inserted. Mobile phones, especially the smartphone variety, aren't safe either, especially as 2.5G and 3G networks become ever more popular. Antivirus developer McAfee has predicted that within a couple of years a malicious attack on a smartphone could potentially infect a third of mobile users within three days. Thankfully, according to Sophos, only PalmOS has seen a real virus developed in the form of something called Phage, and that was never released into the wild to infect devices.

This article first appeared in PC Plus Issue 212 - February 2004 Please note that the information contained within this article is correct at the time of creation. Information may have changed since the appearance of this article in the magazine or website. Copyright Future Publishing Ltd Future Publishing Ltd, 30 Monmouth Street, Bath, BA1 2BW, England. Tel: (+44) 01225 442244 Reproduction in whole or in part without written permission from Future Publishing is prohibited. This material is for personal use only.



## Getting more from Adobe Reader 6

There are a wealth of exciting new treasures in the latest free offering from Adobe, the replacement for the Acrobat Reader



On the surface, Adobe Reader 6 appears to be the latest giveaway, necessary only because you sometimes have to deal with documents with a PDF extension. Adobe Acrobat has been particularly useful in the publishing industry, but as its advantages have become more widely known, its applications have spilled over into other arenas. The odds are that when you install a new program suite on your Windows system, there's a PDF version of its manual on the same CD. In its new incarnation, it's apparent that Adobe has pulled out all the stops and recreated their free PDF reader so that it's now a desirable tool and a great addition to your library of utilities.

### A new document reader for a new day

Adobe has recently upgraded their free support tool, the 'Acrobat Reader', so that it's now far more than a necessary adjunct for reading PDF files. In this article I will elaborate upon some of its lesser-known applications.

PDF is the format of choice for many text authoring firms today. Along with Postscript, it's the software/hardware 'language' that's transportable between greatly differing printers. PDF is compressible, and is already widely used both in Mac and PC applications.

There are plenty of reasons why you should familiarise yourself with PDF files and get used to handling them. Here are just a few of them.

Many commercial printers encourage use of PDF as input to them, and allow generous discounts. The freeware Adobe Reader is universally available.

PDF files are admissible documents under law (because they cannot be modified without leaving evidence of change).

PDF files are compatible across several computer systems. This makes them ideal for sharing over networks. PDF files are highly compressible. On average, you can expect a massive 75 per cent reduction in size from plain text.

PDF files feature varying fonts, colour illustrations, hyperlinking, indexing and searchability.

PDF has been an established standard format and has proved itself to be sufficiently feature-packed to stand the test of time.

PDF stands for 'Portable Document Format'. This is an extremely apt description because PDF is used even in the transfer of data between central computers and palm processors. Documents can be linked together, and with the in-built hyperlink facility available within PDF, you can also model the interactions of a web site.

One of the perceived difficulties with documents is that each is a unity, and a flat search must be performed to navigate around a document. This isn't a limitation recognised within PDF: books and longer documents can be divided into chapters, and elective bookmarks are supported, as well as hyperlink jumps for data connected beforehand. Adobe has repackaged much of its software, and has withdrawn the familiar 'Adobe Acrobat Reader' free program to replace it with its new multi-function 'Adobe Reader' which does much more, including several services that will be of interest to almost every PC user.

One of the new services on the Internet is the phenomenon of ebooks: you can now find, sample, purchase and download the text of what would, in a previous age have been a physical book bound with quality paper, pages and ink. Virtually all the features of a book are available through a PDF, and the form of these electronic books is almost always that of PDF. Already many of the computer manuals that can be helpful for you are PDF documents. Adobe Reader provides some effective tools to enhance your experience. The Reader allows you to personalise your choices and create your own virtual bookshelf. Personal library

Your own copy of Acrobat Reader becomes more than just a tool with which you read PDF documents. Used skilfully, it can become your own personalised librarian. Purchased books of your choice and manuals, can all be categorised. This can be a great advantage even without the ability to produce PDF documents from your own utilities.

### Manual centre

Once you have the Adobe Reader, it's easy work to locate copies of the full reference manuals for suites you have already installed on your system. You can then add these to your library, categorising them differently for ease of referencing. In all probability you'll find you already have several PDF documents you know are ultimately necessary and useful, but which you have seldom referenced, and would promptly lose if you printed them. Yet when you have spare time for further familiarisation with a product, or a dire need when something has gone wrong, you should no longer expect to have to search for information, as it will be classified there for you already.

You can select a part of any PDF document – or the full document – to read or print, and depending on the printer you use, you may find it useful to reverse the order of pages as they're printed. You can vary the direction in which images are printed (useful when you need large margins for notes). The real advantages of PDF come with plug-in developments that have been associated with it: Real, Macromedia Flash, and Windows Media formats can be incorporated, so that a full PDF may entail a whole presentation, or even

*(Continued on page 12)*

(Continued from page 11)

an automated slideshow. All these elements are supported within Adobe Reader, even though text and static graphics are more usually associated with the use of PDF.

A document need not be a two-dimensional record made up of words. A document can be constructed with multiple layers, including perhaps straplines, expansions, chapter heads and summaries, footnotes, tables, diagrams, bibliography and index. All these layers are preserved within a PDF document, and can also be viewed (and printed) independently by layer.

In recent years, there has been a lot of concern about certification – software that enables you to ‘sign’ a document in a way that your authorship can be established beyond doubt. Adobe Reader has all the hooks (as it were) ready, and can guarantee documents and authors, reciprocally providing a way for you to apply your digital signature to documents. There are low cost extensions that will extend Reader so that it actively deals with certification issues.

A final application, which users of Adobe Photoshop will no doubt already be aware of, is that you can use Adobe Reader to extract photos from Photoshop slide shows and prepare them for online Adobe photo services. Wilf Hey

This article first appeared in PC Plus Issue 212 - February 2004

Copyright Future Publishing Ltd

## A call for action

Look to see which version of the Reader you have on your system: Start|Settings|ControlPanel|Add |Remove Programs. Look down the list of installed suites to see if ‘Adobe Acrobat Reader’ appears. If so, this is ‘not’ the latest reader, and you should uninstall it once you have located a version of the Adobe Reader 6. If you have not seen it on recent cover disks or on recent installation CDs, you can download it from [www.adobe.com/products/acrobat](http://www.adobe.com/products/acrobat). You now have the opportunity to establish effective document handling. Find significant PDF files already on your system, and especially note those within the Program Files folder, which will often be the reference manuals for suites installed on your system.

Classify PDF files within your own personal bookcase, categorising them appropriately. Remember that these can include personal documents and ebooks you’ve purchased. Investigate the means you may already have within software to export PDF files. If you’re able, you may wish to change your favourite manual or reference file into a PDF.

Remember that there are tools that can convert HTML (as the construction of a website) and other kinds of documents to PDF, and consider whether there would be an advantage in doing this, knowing that the Reader is available to you. Establish the different modes of reading available to you (Edit|Preferences|View). Look through existing PDFs associated with software and establish whether there are diagrams or charts that it would be useful to print. Join the ebook revolution; ebooks are readable as books, and can be made physical by printing. But there’s so much more flexibility and possibility for interaction.

## Oztraylia

I love a sun screened country  
Its ranks of unemployed  
Its eyesores built by Seidler  
Its art by Arthur Boyd.

Our kids are all drug addicts  
Our businessmen are crooks  
Our pollies are a bunch of clowns  
Who couldn't raffle chooks.

But that is our tradition  
We're rugged and we're tough  
And because we live in paradise  
We couldn't give a stuff.

When we first came from England  
We stole it from the blacks  
And now we won't apologise  
In case they want it back.

But we have a great vision  
A great Australian Dream  
For every bloke a barbie  
Two cars, a football team

A fenced off yard with dogs in  
Or else a harbour view.  
A school to put the sprogs in  
And after, a dole queue.

And how I love the mateship  
What Australia's all about  
And NO it's not Corruption  
We just help each other out.

For we're battlers and we're bludgers  
We'll fight for a fair go  
We're drinkers and we're drivers  
And we always will be so.

And pity help the bastard  
Who runs the country down  
For like the tallest poppy  
They'll soon be brought to ground.

So forget your constitution  
Forget your plebiscite  
Don't fret about the future  
We're Aussies - 'She'll be right!'  
Sent by Cousin Don  
(Where does he find them)



off the mark by Mark Parisi  
[www.offthemark.com](http://www.offthemark.com)



## His POST Was Toast

Almost all PCs go through some kind of audible Power-On Self-Test or "POST" process when you first turn them on. If nothing's wrong, the PC usually emits one beep, meaning "All is well!" But if something's not OK, the PC emits two or more beeps in a specific pattern. If you make note of the beep pattern, you can look it up in a suitable reference to see what the POST is trying to tell you.

For example, see <http://www.pchell.com/hardware/beepcodes.shtml> or <http://www.geocities.com/techcentralstation/BeepCodes.htm>

This reader ran into a POST problem, but managed to fix it without having to look up anything:

Turned on machine yesterday and got "peep peep" like the battery-backup when AC goes down, nothing on monitor. Check everything: power, supply and all cables inside to no avail. With flash lite in hand checked mother board, found a heavy dust build-up on the CPU and the cooling fan that's blowing right on the chip. Removed the dust with an anti-static soft brush and grounding strap. Problem solved. Maybe this will help someone else trouble-shooting a computer. ---Howard

Different machines use different beep codes, so I don't know exactly what your PC was trying to tell you. Perhaps it was a direct thermal problem due to the dust acting as insulation; or perhaps the fan had stopped spinning (some PCs won't start up if the fan is blocked, to prevent the cpu from cooking itself to death...). Or it could have been something else

But in any case, all PCs get grungy inside after a while; and the dustier the environment, the faster the buildup. It's smart to pop the case a couple times a year and get the fuzzies out of your system! Click to email this item to a friend <http://langa.com/sendit.htm>

4) Cleanliness Is Next To Godliness...

... but in PCs, it's next to impossible. For example, there's not only the kind of dust problem mentioned in the previous item, but there also can be problems with your input devices, like this:

Fred, Just something to pass on re: my slow-to-figure-out a very simple problem.

I have been griping (to myself) about how my mouse pointer seems to hang up on the screen sporadically. I have taken the ball out several times to be sure it was clean (it was). It acted like the mouse pad had grease on it-changed to different mouse pad on two occasions-to no avail.

Also have been searching the internet off and on for weeks now trying to find solution to scroll bars which keep on vertically scrolling after I moved the mouse pointer away from the scroll arrows. Sometimes scrolling would continue for more than one page-very aggravating.

Ah-Ha. The light dawns on me-take the bloody mouse completely apart (only two screws), and what do I find but a big furball (lint) completely wrapped around one of the plastic wheels; in this case, the one which senses the horizontal mouse movement.

You guessed it-complete

cleanup fixed both problems. I can't believe I never connected the dots before now. Feels like a totally different mouse too. Never read anywhere any hint re: mouse cleaning other than to clean the ball, which is usually in fine shape.

Hope this will help some other mouseketeer. ---Alan

Thanks, Alan. It's not hard to clean a mouse by hand, and you usually don't have to disassemble the whole thing: After removing the mouse ball, the rollers are usually accessible for cleaning with a soft tool like a cotton-tipped swab. In an emergency, you can even use a fingernail (gently) to scrape the rollers clean.

But there is a tool that makes it even easier: It's called a "mousewand." It has a rubber grip that makes it easy to pop out even badly-stuck mouse ball covers; and a velcro insert that's exactly the diameter of a mouse ball. You pop out the mouse ball, place the velcro insert inside the mouse, and move it around. The velcro fabric scrubs the mouse rollers clean in seconds.

Unfortunately, mousewands are almost impossible to find as separate, "quantity: one" items. They're usually sold in bulk by imprinting companies that want to slap a company's logo on the mousewands, for the company to use as a giveaway, promotional item. That's how I got mine: Some company sent me one, so their logo would be on my desk.

But mousewands would be a great item for a club or user group to buy in bulk for their members. That way, the unit cost would be very low. See <http://froogle.google.com/froogle?q=mousewand>

### Selective Starts in Win98 and XP

Fred, Long time plus subscriber. Now XP Pro user. Have a problem during boot with a loud speaker noise. Is there a way to do step by step confirmation boot up as in previous Win 9x? --LD Bartel

Sure!

In Win98, you'd hit the F8 key as the system starts, and when you get the startup menu, you'd choose "Step by step confirmation" which let you answer Yes or No to every startup item. That way, you could selectively bypass items in the Config.Sys, Autoexec.bat, and Win.ini that might be causing trouble.

It's not quite as simple in XP because XP itself isn't quite as simple as was Win98. You have to use the MSCONFIG software built into XP. To run MSCONFIG, go to Start/Run, type MSCONFIG and hit enter. By selecting either the large-scale options on the General tab, or by stepping through item by item on the other tabs, you can choose exactly what will run at the next boot, and in some cases, even change the order in which different items load.

For more, including Win2K and NT info, see <http://www.techtv.com/screensavers/windowstips/story/0,24330,3386471,00.html>

1. **FILE SUMMARY.** Windows XP has a neat feature that will jog your memory whenever you save a file to your hard drive. Simply fill out the file's Summary page for future reference. To get there, right click on the file in Windows Explorer and select Properties, then the Summary tab. This is especially handy if you need to search for lost files later on, because the Summary page can maintain category, key words, and comments.
2. **RESTORING UNDERLINED MENU ITEMS.** You may have noticed in Windows XP that the underlined letters in menus are missing. That was a convenient feature of older Windows versions. You could press the Alt key and the underlined letter to activate a menu item. If you've grown accustomed to that shortcut, you can restore the feature in XP by right clicking the desktop, choose Properties and the Appearance tab. Click on Effects and uncheck "Hide Underlined Letters for Keyboard Navigation Until I Press The Alt Key."
3. **PICVIEWER** is a shareware download at <http://www.anixsoft.com/download.html> and supports Windows 95/98/ME/NT/2K/XP. It opens to three displayed sections: folders, thumbnails of images in the selected folder, and a large thumbnail view of the selected image. You can manipulate the image by stretching, animating, autosizing, or copying it.; or, create a slide show.
4. **PRIVATE CHARACTER EDITOR.** Windows XP has a feature that allows you to customize a logo or other item for use in any document. The Private Character Editor is accessed at Start|Run and enter "Eudcedit" without the quotes. After you have constructed and saved the design of your choosing, you can access it from the Character Map by selecting Start|All Programs|Accessories|Choose All Fonts (Private Characters), then click on the character you have created, copying and pasting it into any document
5. **PLACE MARKER.** In Microsoft Word, if you've lost the place where you last made an edit change, Shift+F5 returns you to that point. Subsequent Shift+F5 key combinations will toggle through

- the last three edit locations.
6. **REFRESH FORCE**, a free download at <http://www.pagehosting.co.uk/rf/>, reduces flickering and resulting eyestrain by adjusting your Windows 2K/XP monitor's refresh rate. It's said to work with any variation of graphics cards, monitors, or drivers
7. **XP READINESS TEST.** Evaluate your PC's RAM, memory, BIOS, hard drive, and graphics card by running the free test at <http://www.pcpitstop.com/xpready/about.asp>. While you're at this site, take a look at "The Big Picture" for reasons why you should upgrade to XP if you're still using Windows 98/ME.
8. **THUMBSPLUS** is a customisable image database/thumbnails/graphics editor application for cataloguing, locating, maintaining, and modifying your graphics and multimedia files. Our Software Review Panel gave it a thorough test and reports about this software at the NNT Web site, <http://www.NeatNetTricks.com> (click on Software Reviews).
9. **GRAB AND SEND** captures screen images, customizes the screenshot with the user's own comments using text and arrow tools, then sends the message and files to selected recipients using its own mail handler. Our Software Review Panel tested this product and reports its findings at the NNT Web site, <http://www.NeatNetTricks.com> (click on Software Reviews).
10. **TOTAL NET SHIELD** is a complete privacy suite that shields all your Web communications from even the most sophisticated methods of online spying and snooping. Check it out at <http://www.qksrv.net/click-1434278-9940309>.

*From Neat Net Tricks  
15/2/2004*

*Standard Edition 167*



Subject: A.A.A.D.D.

Ever have one of those days where you feel like you haven't accomplished a thing? Well, I think I found out why I do.

Recently, I was diagnosed with A.A.A.D.D. - Age Activated Attention Deficit Disorder, which effects most over 40's. As most of you are over 40, I thought I just would let you know some of the symptoms and how I realise that I was suffering from this devastating condition.

This is how it manifests itself: I decided to wash my NEW car. As I start toward to the garage, I notice that there is mail on the hall table. I decide to go through the mail before I wash the car.

I lay my car keys down on the table, put the junk mail in the bin under the table, and notice that the bin is full. So, I decide to put the bills back on the table and take out the rubbish first but then I think, since I'm going to be near the post-box when I take out the rubbish anyway, I may as well pay the bills first. I take my chequebook off the table, and see that there is only one cheque left.

My extra cheques are in my desk in the study, so I go to my desk where I find the can of Coke that I had been drinking. I'm going to look for my cheques, but first I need to push the Coke aside so that I don't accidentally knock it over.

I see that the Coke is getting warm, and I decide I should put it in the fridge to keep it cold. As I head toward the kitchen with the Coke a dying houseplant on the window ledge catches my eye - it needs to be watered.

I set the Coke down on the window ledge, and I discover my sunglasses that I've been searching for all morning. I decide I better put them back on my desk, but first I'm going to water

the plant.

I put the sunglasses back down on the window ledge, fill the watering can with water and suddenly I spot the remote. Someone left it on the kitchen table. I realise that tonight when I go to watch TV, I will be looking for the remote, but nobody will remember that it's on the kitchen table. So I decide to put it back in the lounge where it belongs, but first I'll water the plant.

I splash some water on the plant, but most of it spills on the floor. So, I put the remote back down on the table, get some towels and wipe up the spill. Then I head down the hall trying to remember what I was planning to do.

At the end of the day; the car isn't washed, the bills aren't paid, there is a warm can of Coke sitting on the window ledge, the houseplant isn't watered, there is still only one cheque in my chequebook, I can't find the remote, I can't find my sunglasses, and I don't remember what I did with the car keys.

Then when I try to work out why nothing got done today, I'm really baffled because I know I was busy all day long, and I'm really tired.

I realise this is a serious problem, and I'll try to get some help for it on-line, but first I'll check my e-mail... Do me a favour, will you? Forward this message to close friends you know, because I don't remember to whom it has been sent. Don't laugh - if this isn't you yet, your day is coming! And if I have sent this to you before....well, now you know why you're getting it again.



## Carols for mental health

Schizophrenia --- Do You Hear What I Hear?

Multiple Personality Disorder -- We Three Queens  
Disoriented Are

Dementia --- I Think I'll be Home for Christmas

Narcissistic --- Hark the Herald Angels Sing About Me

Manic --- Deck the Halls and Walls and House and Lawn  
and Streets and Stores and Office and Town and Cars and  
Busses and Trucks and trees and Fire Hydrants and.....

Paranoid --- Santa Claus is Coming to Get me

Borderline Personality Disorder --- Thoughts of Roasting  
on an Open Fire

Personality Disorder --- You Better Watch Out, I'm Gonna  
Cry, I'm Gonna Pout, Maybe I'll tell You Why

Obsessive Compulsive Disorder ---Jingle Bells, jingle Bells,  
Jingle Bells, Jingle Bells, Jingle Bells, Jingle Bells, Jingle  
Bells, Jingle Bells, Jingle Bells...  
From Cousin Don again

## **Not-So Subtle Reminder Re:Win98**

Microsoft has twice granted stays of execution to Win98/98SE, but this time, it looks like the end is truly near. Microsoft now bluntly says "After January 16, 2004, [Windows 98] will be obsolete..."

I have an entire feature-length article in the works for you that will go over recommended end-of-the year update/cleanup/tune-ups for ALL versions of Windows, but if you're one of the millions of users still running Win98, you might want to get a jump on things by grabbing \*and storing\* copies of all relevant Windows Update items so you'll have them on hand even when Win98 support dries up.

It's easy, and the basic process--- for any Windows version (not just Win98) was discussed in "How To Save Your Win98 (And Other) Updates Offline" in <http://langa.com/sendit.htm/newsletters/2003/2003-03-20.htm#2> .

You can use Windows Update to see what's already installed on your system ("View Installation History"); and then use the info from the link above to grab a fresh, stand-alone copy of the update item(s) that you want to save locally, so you can reinstall them any time you want, right from your own hard drive. (Or CD, or whatever.)

That process works for ANY version of Windows, by the way: You really never have to download any patch or update more than once. By grabbing it once, by the above method, you can install it any number of times from your local copy without ever having to download the same code again. (The re-download of tens or hundreds of megs of patches and updates may not be a big deal if you're on a very fast connection, but it's a huge deal with dialup, ISDN, and slower forms of cable and DSL.)

Lots more info is coming soon in that aforementioned article that will help you get your PC--- any PC--- in perfect shape for the new year. That article also will include a special section for Win98 users that will show you how to perfect and preserve your system so it will run great even after Microsoft pulls the plug!

*From LangaList 15/12/2003*

*Note since this LangaList, it has been reported that Microsoft has AGAIN extended the lifee*