



# The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 11

Nov. - Dec. 2005

For group information  
please visit our Web site:  
[www.mpcug.org](http://www.mpcug.org)

## *The Bridge Staff:*

Editor  
Gil Hennon

Review Editor  
Rick Fischer

Publisher Emeritus  
Les Owen

## *In This Issue*

The School Bell	Page 2
The Art of Photoshop	Page 4
FileMaker Pro 7	Page 6
Out for Review	Page 7
October Meeting Report	Page 8
Silicon Gulch Reloaded	Page 9
OmniPage Pro 15	Page 14
The View from the Bridge	Page 16
Event Calendar	Page 18

## Main Meeting Wednesday, Dec 7 Southwest Tennessee Community College

5983 Macon Cove, Memphis

### **MEETING LOCATION**

## Thornton Room 104

First Floor - Thornton Office Building

Wizards Session 6:30 p.m.  
Main Meeting 7:30 p.m.



A Happy  
Thanksgiving  
and very  
Merry Christmas  
to everyone  
from the  
Memphis PC Users Group





# The School Bell

## News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

In October, the weather changed. Nippy mornings and evenings and a gusty breeze told us that summer was over. With winter at the door, It's time to dig out the long, red flannel underwear. But the draft you may feel blowing through the trap-door bottom on your Union Suit might not be the chill of Autumn. It might be the realization that Uncle Sam's privacy-hating bureaucrats have left you seriously exposed.

Last month two government departments took bold regulatory steps to invade your personal life and keep track of your movements and identity. Critics believe that the regulations will, at the minimum, increase the risk of identity theft for every citizen. At the worst, the regs could put our lives in danger. The agencies involved claim they will take precautions to protect citizens from these risks, but there are some serious holes in the plan. And it is very likely that the courts will be called upon to determine if the two regulations are actually legal.

The Department of Justice was first out of the gate when they notified all U. S. colleges, universities, and Internet Service Providers that their networks and online systems must be updated to facilitate law enforcement agencies collecting data. The data to be collected includes email, instant messages, and records of Web sites visited along with what was done there.

So far, the schools and ISPs have not complained that this sort of surveillance has been ruled illegal wherever it has been challenged. For many years, the FBI, CIA, DEA, and other Federal law enforcement agencies have been lobbying to get this kind of power, but Congress would not authorize it. The colleges and ISPs overlooked the legalities and concen-

trated their gripes on the costs. The Justice Department included a wishy-washy promise that abuses would be prevented "because the government would have to win court orders before undertaking surveillance." In truth, "winning" a court order requires nothing more than a request to a judge. This kind of surveillance, like a wiretap, is done in secret. The victim never gets any opportunity to argue that the court order should not be issued. There is not even a requirement that a crime be committed in order for a judge to issue a surveillance or wiretap court order. So far, though, the complaints raised from the schools and ISPs have centered around who should pay the substantial costs that the upgrades will require. They want the Feds to foot the bill, while the budget-challenged Justice Department wants the cost to be borne by the owners of the networks.

The second surprise in the same week came from the U. S. State Department. As of October, 2006, all U. S. passports must contain an electronic chip that can be queried by a remote radio signal. The chip will respond with the personal information of the passport owner, including name, nationality, sex, date of birth, place of birth, and a digital photo.

This particular regulatory proposal was announced earlier in the year with a solicitation for comments from citizens and other interested parties. Since then, 2,335 responses have been received, with 98.5 percent of them negative for various reasons. Despite this overwhelming opposition, on October 25<sup>th</sup>, the Justice Department went ahead and issued the regulation.

Presumably the passport will contain "shielding" to prevent the information

from being collected while the covers are closed, but the National Institute of Standards and Technology, where evaluation of the passport's vulnerability is in the works, so far has not certified that the shielding is effective, especially against the latest, high-powered RFID receivers capable of reading chips from about 160 feet away. The technology clearly exists to allow a distant or concealed operator to read the passports of unsuspecting citizens from a distance or from concealment. Not only does the regulation open another opportunity for identity theft, but could pinpoint citizens of the United States or other countries as ideal targets for terrorist kidnappers or killers. This is a very dangerous application of an immature technology that, as yet, has insufficient experience and safeguards.

In an almost amazing coincidence, during the same week in October the Washington Post published an expose' of abusive, clandestine surveillance of U. S. citizens from 2002 to 2004. The source was FBI documents obtained under the Freedom of Information act. Although heavily censored and apparently incomplete, the documents did contain evidence of thirteen serious incidents of illegal citizen surveillance. Agents kept one target under surveillance for five years, and for fifteen months of that time without the oversight of legal warrants. Other illegal activities against citizens included violations of bank privacy, improper physical searches, and interception of email messages after the authority to do this had expired.

FBI officials claim that the infractions were not serious and that none of the cases involved individuals suspected of serious criminal activity. They broke the rules, they admit, but that's supposed to be okay because the targets were innocent people. The Washington Post concluded that the documents show how little Congress and the public know about the abusive and illegal surveillance tactics used by the FBI and other agencies.

Considering the two new regulations that were passed in the context of the revelations of the Washington Post story, public confidence is as low as should be expected that additional data gathering and smart chip passports will be used properly by the government. And because of additional risk to the privacy and lives of U. S. citizens, it's somewhat reassuring that challenges to both regulations have already been filed in the courts. Citizen rights watchdog organizations are also bringing the issues before Congress, since the regulations grossly enlarge the powers of the agencies beyond what the law appears to allow.

At the MPCUG Wizards Session, we can't secure your passport, but we can help you secure your PC to protect your privacy and identity. Join us each month immediately before the main meeting. Keep those spybots and phishers out of your computer!

This newsletter is a monthly publication of the Memphis PC Users Group, Inc. (MPCUG) Copyright ©1998 MPCUG. Unless otherwise indicated, articles may be reprinted in other non-profit publications without express permission, subject to the following conditions. Full acknowledgement must be given to the MPCUG, The Bridge, and the author. The article must be reproduced in its entirety from magnetic media, without editorial changes, deletions or additions. Two copies of the entire publication containing the reprinted article should be sent to The Bridge within 30 days of publication. All other rights reserved. Any changes to the article require the written permission of the author. All articles are made available through the APCUG BBS and on disk to qualified non-profit organizations.

Any opinions expressed belong to the author and not the Memphis PC Users Group, Inc. Articles in this newsletter may contain trademarks of various companies. Any proprietary right those companies have in those names is hereby acknowledged.

Unless otherwise indicated, all submissions to this newsletter become the property of Memphis PC Users Group, Inc., and are subject to editing by the staff. The MPCUG reserves the right to determine the suitability for publication of all items received.

Members are encouraged to submit articles for publication. By submitting articles, the author gives permission for publication in this newsletter and for publication by other user groups. The editor cannot guarantee that all submissions will be used.

The information contained in this newsletter is believed to be correct and accurate; however, the Memphis PC Users Group, Inc., cannot and will not assume responsibility for the consequences or errors contained in articles or misapplication of any information provided. Any information used from these articles is at the user's own risk. If a review of any hardware or software contains errors or inaccuracies, upon notification of these errors or inaccuracies by the manufacturer in writing, a correction will be printed in the subsequent issue following receipt of these corrections.

The Memphis PC Users Group, Inc., makes no warranty, expressed or implied, as to the suitability of any advertised product. You must determine that yourself. The Memphis PC Users Group, Inc., also expressly declines to assume liability for any use of any published software, and your use of same constitutes your agreement to hold us blameless.

Memphis PC Users Group, Inc.  
4746 Spottswood Ave. PMB 178  
Memphis, TN 38117-4815  
[www.mpcug.org](http://www.mpcug.org)

# The Art of Photoshop, CS2 Edition

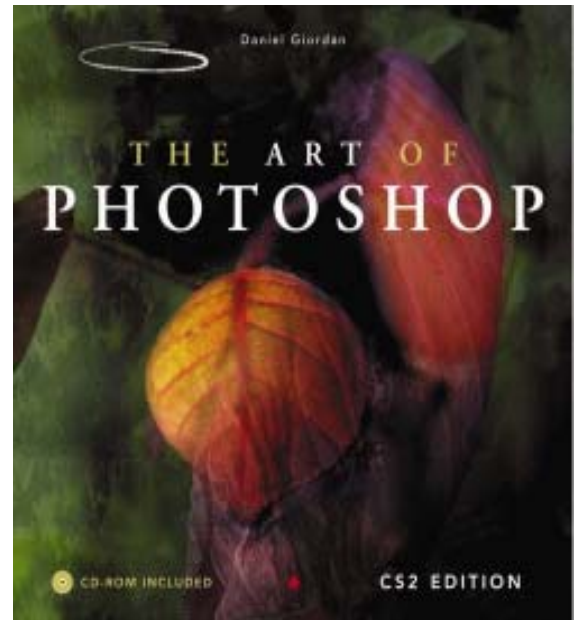
*Book Review*

**Reviewed by Rick Fischer**

It's about art. It's about *Photoshop*. It's about making art using images and *Photoshop*.

Giordan offers 19 completed and named works made from his own original images. This is the gallery – the show. Then, he takes each work and describes his vision and the tools he used to create them. That vision and description make up the balance of the book.

Written for the intermediate and advanced user, it inspires and instructs. This is for designers, for people that already have a vision. It is *not* about touching up an image. It is about taking seemingly unrelated images and making something completely new. See samples with this review.



The Art of Photoshop by Daniel Giordan (2006). Sams. \$50. 303 pp. with images on CD.

[www.artofphotoshop.com](http://www.artofphotoshop.com)

[www.samspublishing.com](http://www.samspublishing.com)





# Special Edition Using FileMaker 7

*Book Review*

Reviewed by  
Tommy Towery

Valuable, but not a  
beginner's tool

In my early computer days, *FileMaker* was always a Mac program. It was their simple version of *dBase* and I guess that my memory of those days has always kept me from ever considering it for a PC application need.

In the PC world that existed for me, *dBase* was followed by the very powerful *Access*. While *Access* was powerful, it was also frightening to many old time database users. Many switched to the simple database function of *Excel* when faced with the needs for a small database or address book manager.

There still exists a need for a small, powerful, and easy to use database program like the one that the Macintosh users had used from upgrade to upgrade – like *FileMaker*. While the program has also grown greatly in its own way, adding functions and other such things, it can still be used as a simple database if

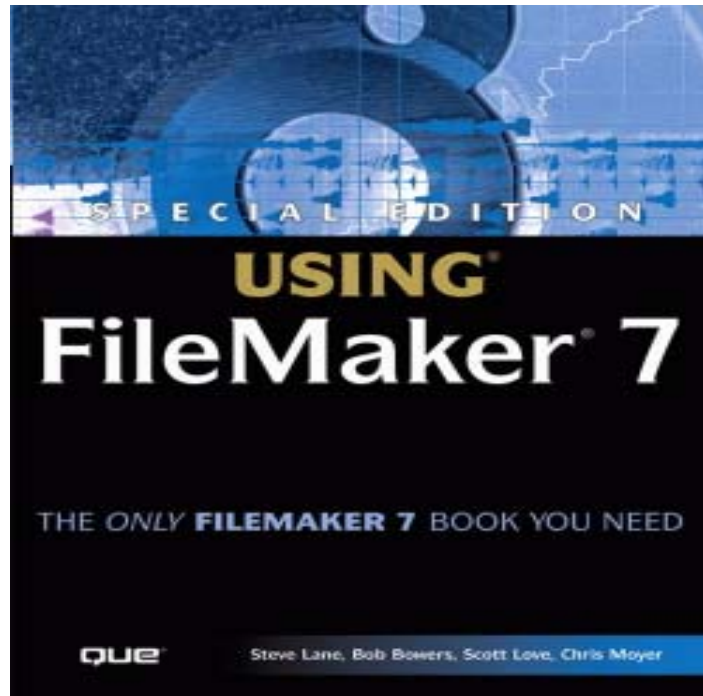
one elects to do that.

What many fail to know is that today *FileMaker Pro* is one of the easiest to use cross-platform data base applications. At the university where I work, several of our departments have implemented *FileMaker Pro* for both their Macintosh and PC needs. It allows PC based and Macintosh computer users to work and play together seamlessly.

*Special Edition Using FileMaker 7* by Que is intimidating at first glance. It weighs in at a whopping 1082 pages. This is not one of those simple yellow and black

covered book that teaches you how to use the software in a one-hour sitting. You might want to check the bookstore for one of those if you need it put in simple terms. Instead, I see it as one of those “everything you always wanted to know, but were afraid to ask” type books. Basically, it is a reference book for a developer – plain and simple. That being said, it is also a very good reference book that can be used to look up complicated challenges to using the functions of this program.

Included with the book is a CD that accompanies the text. The first few



chapters can be used to brush up on database basics, or skipped if you are already comfortable with the terms and functions of basic databases. Other chapters in the book concentrate on cross platform, report creation, and scripting. A lot of old time *dBase II* developers will already know many of the function formulas. There is a whole chapter on database security, a much needed topic in today's Internet environment. The idea of portals and relational databases gets a chapter as well.

The assertion in the executive summary that this book is the only *FileMaker 7* book you need might may be a little exaggerated if you are a beginner to the world of databases. Its value to the world is more for the developer, and might be the only reference book that class of people need. A beginner might want to find one of the yellow and black books to get started before you crack the pages on this robust publication.

Special Edition Using *FileMaker 7* by Steve Lane, Bob Bowers, Scott Love, & Chris Moyer. Que. 2005. \$45  
[www.quepublishing.com](http://www.quepublishing.com)

# Out for Review



Here is a list of software, books, or other products you can expect to see reviewed here in the coming months. These members checked out items to review for the benefit of all.

Windows Me: The Missing Manual	Greg Adams
Teach Yourself GoLive 5 in 24 Hours	Allison Banks
Teach Yourself Adobe Photoshop CS in 24 Hours	Judith Bogan
TIVO Hacks	Jacob Burke
Home Theater Hacks	Osborne Burks
Windows XP in a Snap	Vicki Dabney
Windows Security Handbook	Dorothy Drum
Smart Home Hacks	Megan Hefner
The Little Web Cam Book	Mike Heinrich
Microsoft Works 7.0	Jim Ingram
How to Use Microsoft FrontPage 2002	David Levine
The Complete Idiot's Guide to Starting A Business Online	David Levine
User Interface in C#	Jim McGee
Maximum PC 2005 Buyers Guide	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
Create Your Own Website	Jesse Strauch
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas

Thanks to all who checked out products for review. Let's keep the Group vital and provide value for membership.

# October Meeting Report

*Hard drive hard knocks, OmniPagePDF conversions, and Google's desktop search tool*

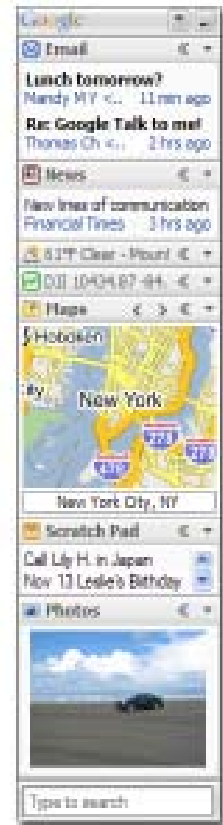
John Schuster brought two dead hard drives—one a standard 3.5 inch and the other a 2.5 inch laptop drive—to show what he learned about the G forces that the different drive types could tolerate. The published specifications indicated that the laptop drive could withstand a surprisingly greater amount of force without damage, and after opening the drives, John discovered that the big difference was in how the heads were parked when the drive is not reading or writing. A standard 3.5 inch drive parks the heads close to the spindle on an area of the disks that is not used. The 2.5 inch drive parks the heads outside the disk area, separating them on thin ramps of soft plastic. So the increased tolerance in G forces on the laptop drives is the result of the heads not being parked on hard disk surface.



Rick Fischer brought an evaluation copy of *OmniPage* character recognition software. A recently added feature, the conversion to and from the Adobe PDF file format, has been very handy for him. Rick converted a Microsoft Word file to a PDF file, and then back again. While the PDF was identical to the original document, the “rebuilt” Microsoft Word file lost some of its formatting. All of the text was still there, but some fonts had changed and words that had been in a table were no longer in table format, but inside text boxes. Rick pointed out that the PDF conversion back to an editable version will probably need some manual tweaking to make it identical to the way it was originally, but the conversion does produce a reasonable facsimile of a PDF file and saves the time of retyping text and/or redrawing illustrations.



Gil Hennon downloaded Google's new Desktop Search tool and installed it during the meeting. There are several of these “desktop search engines” available for free or at a modest cost. Some privacy issues should be considered before installing one, and the Google tool allows the user to decide whether to include email and also whether to allow any information to be returned to Google. After installation, the tool spends several hours indexing the hard drives, and then updates its indexes as files are added or edited. Google says that on most PCs the overhead indexing is transparent, but individual users should determine whether their hardware is fast enough to support an additional background process or risk a decrease in system performance. An optional “sidebar” can be displayed to organize recently searched or continuously updated information. Rick Fischer also brought a handout for everyone of PC World Magazine's recent tests of six popular desktop search engines.



# Silicon Gulch Reloaded

---

by Gil Hennon

Our annual Christmas trek to Silicon Gulch came a month early this year. We hadn't forgotten the awful storm and traveling conditions that made last year's trip messy and more than a bit dangerous, so when the Old Timers suggested an earlier get-together, we were more than willing. They weren't concerned about the weather at all, since their dilapidated van, a bizarre conversion of what used to be a World War II convoy vehicle, seldom goes beyond the dirt and gravel road through the Gulch. More important to the Old Timers, and a compelling excuse for us to show up about a month earlier, was a planned high-level pow-wow among the Old Timers and their counterparts up north on Silicon Mountain, and way down south at Silicon Shores.

It takes a serious shift in malware technology to bring the camps together for a strategy session. The last we could recall had been in the early nineties, when Concept macro viruses took the computing world by surprise. The one before had been called to deal with stealth viruses. At those times, the gathering of Old Timers from their distant hide-outs had been logistical nightmares, but this year, through the magic technology of satellite video conferencing, they wouldn't have to leave their favorite rocking chairs. We were invited to hook up to their network without coming to the Gulch, but a front row seat in the middle of all the testy bickering was too good to miss.

We arrived the evening before the conference was to begin to make sure we got our share of food and grog. The Old Timers will get very serious discussing viruses, worms, spybots, and other malware, but until the moment of commencement, they are all capable of stoking away plenty of victuals. Anticipation of the pow-wow had everyone excited, and the talk around the table was cheery, mostly about the early days at the Gulch,

when the worst threats to be countered were viruses like Stoned or Lehigh or the Pakistani Brain. A few Old

Timers remembered an early Trojan Horse program or two, and Robert Morris' 1988 laboratory worm that got out of hand and disabled ArpaNet mainframes until the network was shut down and disinfected. Those old threats don't seem so bad anymore. The viruses were not so smart and the worms left trails that were relatively easy to follow. But the hardware and software tools were equally primitive back then, and every new threat was taken seriously. They told good stories, those Old Timers, about nearly twenty years in the Gulch fighting malware. We also heard some idle speculation that evening about the agenda for the following day, but it was obvious as the Old Timers began retiring early (for them, at least) that they were saving their energy for tomorrow's strategy session.

A few were already camped around the video conference equipment when we rose the next morning. They weren't into serious discussion yet, but were busy just the same while tweaking the communication equipment and testing various camera angles. We had time for a good Gulch breakfast and joined the group as each designated local spokesperson spent a few minutes of welcome and warm-up for what was to follow.

The first discussion was no surprise. Early in the year there had been plenty of expert opinions that viruses, worms, and Trojan horse programs—the traditional products of the hacking community—were losing popularity to spam, spyware, and hijacking exploits. These new threats proliferated in 2004, and in this year they became even more dangerous by creating identity theft “phishing” and “zombie”



networks. Viruses, the experts predicted, were being pushed aside, worms' days were numbered, and Trojans were obsolete. Boy, were those experts ever wrong! 2005 turned into a year of unprecedented virus and worm infections, including a record-breaking increase of 1,685 new viruses in October. Not only are viruses and worms not going away, they are being manufactured in a more professional manner and often hang around much longer than ever before.

There were no arguments among the Old Timers yet, although a few insisted that the increase in malware was only the tip of the iceberg. For several years, combinations called "blended threats" mixed the characteristics of viruses, Trojans, worms, spyware, and spam into super threats. Malware in 2005 typically contained two or more threats, making it difficult to classify, prevent, detect, and remove. The line is blurred that defines which threats anti-virus software should handle versus which ones anti-spyware ought to attack. Users are left in confusion about which kind of protection is best, or whether any single anti-threat product will really do the job. To make the whole mess even worse, the "blended threats" have turned to crime, stealing identities and, of course, money.

Even as the Old Timers agreed that hackers appear to have abandoned writing prank code in favor of raking in cash, an argument erupted over which recent examples of malware were the worse. Many of the viruses and worms from 2004 or their variants were still in circulation this year, and quite a few of those variants were tricked out and pumped up to be much worse than their ancestors. Zafi had been a major infector in 2004 and for several months infected the most computers this year. Likewise, the Netsky family stuck around into the new year and had even more destructive behavior. Sporadic infections of Bagle and MyDoom also resurfaced as new and more dangerous variants. In the past, a single hacker wrote a virus or worm and released it, and then copycats made changes to spawn the

variants. The more recent threats appear to be the work of hacker teams. Variants add significant new and more dangerous features that seem to be pre-planned. The variants are also released very quickly. Anti-virus software developers have real problems keeping up with dozens of variants released in a very short time period. The whole exploit is just too well orchestrated to be random or the work of a single hacker. After all opinions had been heard, some louder than others, the Old Timers took a vote and came to a consensus that Netsky-P was the worst malware of the year because of its dangerous payload and longevity. It beat out the Mytob family, but not by much. Even the Old Timers were unsure of how many variants have spawned from the initial Netsky infection.

Mytob was a new 2005 worm. Like Netsky, the Mytob factory churned out



dozens of variants, and the source code was published in many places on the Web to attract plenty of copycats. About 60% of the 1,685 new viruses and worms reported in October were

from the Mytob or very similar Zotob families. The Mytob worm may have been the first that completely abandoned any "prankish" payload. It and the others that followed try very hard to run transparently and leave systems relatively intact. It's not that they are less dangerous; their plan is to remain resident for a long time while they install back doors and secret remote control software. An infected PC becomes a member of a "zombie network." It may participate with thousands of other zombies in Denial of Service (DoS) attacks on business or government servers. It may become a spam forwarding station. Or it may log keystrokes, steal identities, and ferret out confidential data to return to its remote control host. A

zombie network presents innumerable opportunities for mischief. These worms won't format your hard drive, but they may read your email or clean out your bank account. The creators of today's malware use professional methodology. Their code is tight and well debugged before release. Criminals have discovered that viruses and worms are practically anonymous and very profitable. They can afford talented authors who code like well organized commercial software development companies.

Fortunately, the computing community has been dealing with viruses and worms for many years. Experienced users have learned, sometimes the hard way, the value of anti-virus utilities. New users are getting better education and advice. They take steps to protect their systems even if they don't understand why. The majority of viruses and worms released in 2005 did not infect many systems in spite of being very cleverly written and distributed. Although most weren't serious infectors, they had some notable characteristics.

- Blended threats increased significantly with multiple methods of infection, camouflage, and purpose.

- Many of the new viruses and worms targeted instant messaging users and infected cell phones as well as PCs.

- Zombie network participation became a popular payload. A few zombie networks had over one thousand PCs under control.

- New and creative ways to steal data emerged, including novel ways to capture keystrokes and complete account/password strings.

- Many communication methods were used to send data from an infected PC back to a host including instant messaging and chatroom utilities.

- Spammers created zombie networked "spam factories" of infected PCs.

Some of the really oddball threats failed because they were too specific, targeting only computers containing a particular application, open port, or vulnerability. Most often the users whose

machines were infected were those too forgetful or lazy to keep their critical security patches or anti-virus definitions up to date. The Old Timers don't have much sympathy for anyone who neglects patches and updates. Their sloppy habits put themselves and others in needless peril.

As the zombie network exploits caught on and became a staple item in late 2005, the purposes to which the remotely controlled PCs could be used became more varied. than Denial of Service attacks and spam forwarding. A clever variant of the old MyDoom worm used Google, Yahoo, and other search engines to harvest email addresses and then send infected messages. It got off to a good start and could have been among the worst infectors of the year, had it not generated so much suspicious search engine traffic and drawn attention to itself. Once identified, the anti-virus software community kicked into high gear and contained the new threat quickly. No doubt another variant of similar architecture will be along one day with more moderate behavior and a better chance of sticking around longer.

2005 saw plenty of new and unique tricks and experiments, but the most bothersome new trait was a shift toward criminal intentions in the way malware code was being written and used. Viruses and worms were not unique in this regard. The Old Timers consider illegal spyware, spam, and hijacking exploits to be the bigger threat. They tend to call these exploits "crimeware" or "stealware," and put forward their noisy, but definite opinions on how bad each type could be. When all of the rants and arguments were done, the new threats were somewhat ranked in this order:

First and most dangerous are the identity theft and phishing exploits. Usually these arrive in spam mail and direct a user to a Web site to "confirm" account numbers, passwords, and other confidential information. These sites are often so carefully crafted and plausible that an innocent user can't tell the difference between a legitimate bank or finan-

cial institution's Web site and the phony phishing site. A lot of time and effort goes into making the phony site as real as possible, and it is likely that these sites are prepared well in advance of when they are used. A phony Red Cross site showed up wanting credit card donations just a day or so after Hurricane Katrina slammed the Gulf Coast. The site was so realistic that many generous contributors were bilked. It would have been extremely difficult to create this site overnight. It was prepared and ready for use when the right disaster struck. Identity theft is big business and highly profitable for criminals. The Federal Trade Commission estimates that ten million Americans will be victims of identity theft this year, and over 10,000 unique phishing exploits are launched each month.

Nearly as dangerous as phishing are zombie networks that attempt to break into banking systems and steal financial data. Kudos to the institutions with industrial grade security that turn away these attacks, but with great persistence on the part of the criminals, some have been breached. This will become more of a problem as more and larger zombie networks are constructed. For the moment, old-style crime such as check forgery still accounts for more bank losses than online theft.

Another criminal activity related to phishing hasn't yet become a wide-spread threat, but pharming certainly has that potential. Phishing targets individuals, but pharming victimizes entire customer populations. It corrupts the routing abilities of DNS servers and redirects all traffic bound for a specific Web site to a different, phony address. For example, anyone who attempts to log onto a Bank's Web site can be diverted to a look-alike site operated by criminals. In this situation, there is almost nothing to alert the user of the deception. Web tricks can even make the correct URL appear in the address bar. This kind of attack is complicated and depends upon vulnerabilities in the Internet's DNS servers, and so far has been rarely attempted.

All of the above threats are illegal, and a few culprits have already been caught and prosecuted. There remains a great, gray area of probably legal, though hardly ethical behavior that puts innocent computer users at risk. Advertising software, usually called adware, hijacking exploits, and rootkits are being used by both hackers and the biggest multi-national corporations. In most cases, the intent is to know more about a customer in order to improve legitimate sales or increase traffic to a Web site. A few exploits, like the Sony CD rootkit scandal, were launched to protect copyright ownership. Regardless of whether the intentions were good or not, using spybots, hijackers, or rootkits still constitutes a threat to the targeted system. These tools open secret doors into users' PCs, affect performance, and interfere with normal operations.

Anti-spyware vendors turned out dozens of new products in 2005, but none, so far, markets a tool that can recognize and remove more than about 85% of the spyware threats in circulation. Unlike anti-virus software, the anti-spyware developers deal with everything from a simple browser toolbar to a complicated conglomeration of registry entries. They also must craft their products with caution. When they do their job too well, spyware company lawyers haul them into court. Since some spyware is installed with the computer user's consent, great care must be taken in choosing what to remove. Spyware is profitable and often owned by completely legitimate companies with deep pockets and plenty of lawyers. The installation process may show a End User License Agreement (EULA), just like purchased commercial software. Although hardly anyone ever reads EULAs, they can contain clauses that prohibit the removal of the spyware software after it is installed or other limitations on what can be done to the computer. While abusive EULAs may be difficult to enforce, they can still be intimidating and threatening to the user. Also, some of the anti-spyware vendors are big software companies. It is not at all to their

advantage, or even their liking, to do anything that might bring the contract-like EULA language into question. So if a spyware installation displays a EULA of any sort, some anti-spyware programs won't touch it.

Browser and desktop hijackers are a toe closer to the illegal line than spyware. They use many dirty tricks to keep a user from getting full value from a computer investment. Most of them redirect the computer to the hijacker's Web site whenever a search is initiated. The very worst overwrite the computer's HOSTS file, limiting the available Web sites to only those the hijacker allows. Rootkits have been around for a while, but are complicated and often difficult to install secretly. They become part of the operating system and completely invisible to the user. Recently a rootkit targeted AOL subscribers, and

Sony Corporation sold at least eighteen music CDs that installed Digital Rights Management (DRM) software containing a rootkit on any PC that played one of the CDs. The company provided no notification that a rootkit was included in the installation messages. Although Sony claimed that the rootkit was benign and did no damage, when hackers learned of the rootkit's existence, they figured out how to take advantage of it. The Stinx-E Trojan uses a file hiding routine in Sony's rootkit and another hack uses the rootkit to allow cheating in online gaming. Security experts call the rootkit spyware and a threat. The Old Timers call it awfully shabby customer treatment. Sony probably never intended for their copy protection scheme to be a hacker windfall, but a lack of forethought has resulted in great embarrassment for the company.

The rootkit also came with no "uninstall" method, and manual attempts to remove it often rendered the PC unus-



able. Sony has since offered a patch that makes hidden files visible to the user, but to get instructions on how to remove the entire rootkit requires filling out a customer service registration form. Street sources say to avoid the patch. It is flawed and causes system crashes. A better solution would be one of the tools specifically made to find and disable rootkits. The Old Timers don't like having to add another tool to everyone's required security arsenal, but pretty soon your anti-virus, anti-spyware, and firewall products will need the company of an anti-rootkit utility.

Very few law enforcement agencies consider spybots, browser hijackers, or rootkits to be illegal. Only a few communities have laws on the books that define these exploits as a crime, and usually some sort of misleading or secret installation has to be involved. A few vocal citizen and consumer protection groups are pumping up public awareness of the threats and generating some bad publicity for companies using these quasi-legal hacker tools. As long as malware, even when being used in a benign manner, can be installed and operated on a computer without the user's permission or knowledge, the security of every single system remains in doubt. At the same time, the producers and owners of these questionably ethical products are lobbying diligently to prevent consumer protection legislation. In this confrontation, there's more money and legal muscle on the side of malware.

As the pow-wow wound down there were plenty of worried, sober faces around the room and on the video monitors. One of the Old Timers brought up a Web site on his laptop. It was the Home page of an online investigation firm. The largest, brightest font on the page proclaimed, "Find out anything about anybody for \$29.95!" What a low value we place on our personal privacy! But then, it's probably more than a vendor who secretly installs spybots and rootkits on your PC would be willing to pay.

-0-

# OmniPage Pro 15

*Software Review*

Reviewed by Rick Fischer

The 15 update is supposed to appeal to busy office workers who need to digitize or archive lots of paper. But, I was drawn to the included PDF conversion utility. More on the goodies for business applications later.

## PDF to something editable

Those who attended the October meeting got a chance to see *OmniPage Pro 15* conversion utilities *PDF Create* and *PDF Converter* demonstrated. Take a PDF file and convert it to *Word*, *WordPerfect*, RTF or *Excel*. It also can go the other way (from *Word* or *Excel* to PDF).

Like a little kid, I wanted to take it apart to see how it worked. I wanted to know whether ScanSoft was merely stripping away the PDF formatting, or processing the document in a way that created new formatting.

I downloaded the Microsoft template for *Word* called "white paper." You can find it at the Microsoft templates site (URL at end of article). On the cover page it has text in a box. The logo is inserted in the header. There also is normal text on the cover page. There is enough variety in the document to test the question.

Page two has two columns and the text flows using the *Word* "column" function. I converted the *Word* file to PDF using *PDF Create* and the conversion button *OmniPage/ScanSoft* places on the tool bar in *Word* and *Excel*. Then I converted it back to *Word* using ScanSoft's *PDF Converter*. It did *not* just remove the PDF formatting. The final document had different formatting from the original.

I tried the same thing using *Print2PDF* - a Software 602 conversion program - instead of *PDF Create*. The final document looked exactly like the one I just obtained. Again, the PDF was *not* just stripped away. A new format was produced. You can buy *PDF Converter* alone for \$50.

It was interesting to see how the file size changed from the original to the final reconstructed file.

	Original Size of whitepaper.doc	Size after PDF conversion	Final doc size after conversion back to <i>Word</i>
Scansoft Create	69 KB	10 KB	35 KB
Print2pdf Conversion	69 KB	62KB	35 KB

## Scanning

Besides new features, the main reason we think about upgrading our scanning software is to increase OCR accuracy. Normally, when I scan and OCR documents, I take raw OCR output and do all my editing/proofing in *Word*. I know *OmniPage* has an OCR proofreader, but I formed that habit long ago. The more accurate the OCR conversion, the less I have to edit. We also know that sharp clear documents convert more accurately than light, fuzzy documents. So, I tried a sharp clear document. I took one of the drafts of this review as printed from my laser printer.

Result? Not perfect, but close. Instead of 12 point type, it was rendered as 11 point. The

## ClickBook 9 for Windows

ClickBook 9 for Windows, the booklet printing software, is now available. We reviewed version 8 in the July issue. ClickBook automatically reduces, rotates and realigns computer files into convenient, portable books.

ClickBook 9.0 for Windows New features:

- \* Convert booklets to PDFs. Blue Squirrel integrated a PDF generator, making it possible for users to publish booklets as virus-free PDF files.

- \* Magnified zoom. Users can zoom in and view ClickBook pages up to 800% larger!

- \* Rearrange print order. Break up print jobs and rearrange them on a page-by-page basis. For example, a user can take a spreadsheet made with Microsoft Excel and put it after the first page of a 5-page Microsoft Word document.

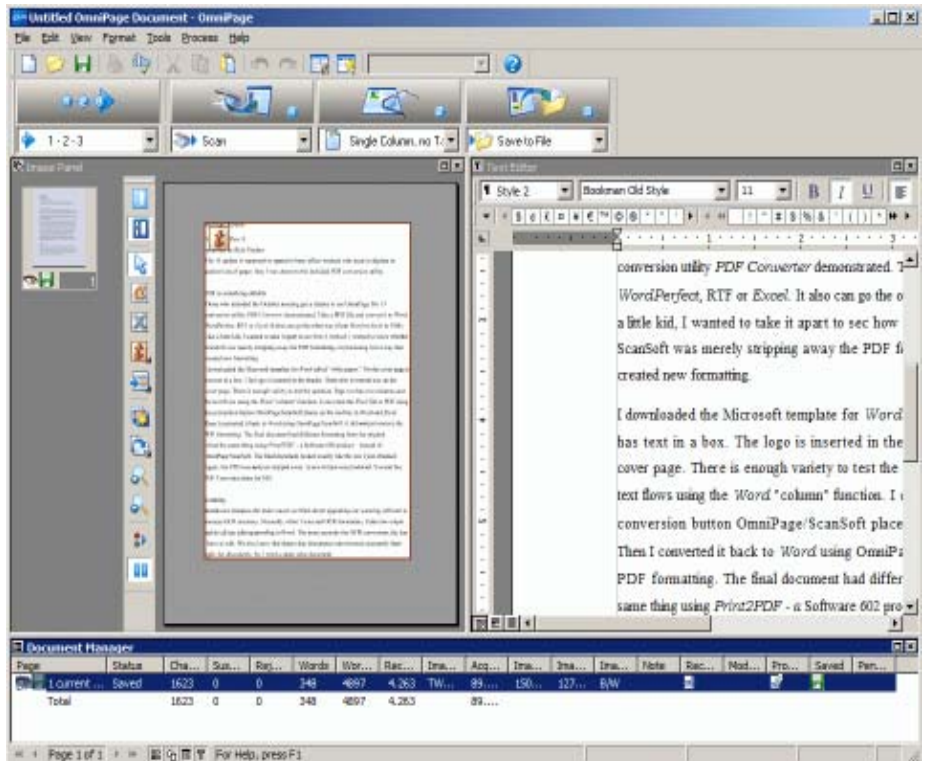
- \* Improved headers, footers and watermarks. More easily insert Headers, Footers, and Watermarks. Users can also choose to place watermarks on top of text.

- \* Access special printer properties. Access unique features of a printer from within ClickBook, i.e., turn on the stapler; change from black-and-white to color printing.

- \* Support for 48 new printers.

A 15-day trial version of ClickBook 9.0 can be downloaded free-of-charge from the Blue Squirrel Web site, <http://www.bluesquirrel.com>. A single user license carries a list price of \$49.95, and current owners of ClickBook can purchase the upgrade for \$24.95 by visiting Blue Squirrel's online store, or calling 800-403-0925, or 801-352-1551.

Special offer. Through December 31st, customers can purchase ClickBook 9.0 at the discounted price of \$29.97, and \$14.97 respectively. Free USPS shipping is available to customers entering a Coupon Code: FREESHIP. An additional \$6.95 savings. [www.bluesquirrel.com](http://www.bluesquirrel.com)



"t" in two became an I. An I became a 1. And the em dashes became hyphens. I am used to seeing " rendered as ". I wondered if OCR accuracy was dependent on the kind of output I selected: plain text, formatted text, true page, or flowing page. The first output was "flowing page."

I rescanned the page and selected "formatted page." A different I became a 1. The em dashes were, perhaps, wider than the originals. No change in the " to " substitution. This also sensed 11 point type. After consulting the manual, the selection of output type should make no difference in OCR accuracy of letters. Looks like normal variation to me.

Then I tried a faxed document. Faxes are typically fuzzier than laser printing. The page was a formal letter on letterhead paper and included small type. Some words were underlined and that created some problems. I count five errors and all were caught by the proofreader in *OmniPage*. I can make the changes there or later in *Word*.

### Languages

I wanted to try a document written in Spanish. Would it pick up the tilde over the n? The accent marks? It boasts an ability to read more than 110 languages. To save room at installation, I didn't load the language feature. If you need that feature you will want to load support for this option.

### Batch this

In an office environment you may have lots of documents to scan and more than likely will have an industrial-

continued on page 16 col. 3

# The View from the Bridge

by Gil Hennon, Editor

This is my last issue as Editor of *The Bridge*. Nearly five years ago, without much experience, I accepted the blue pencil from Bob Manchik. But I did have lots of enthusiasm tempered by the realization that the previous editors—Don Helyer, Steve Callahan, Noell Moseley, and also Bob—had left me a hard act to follow. Starting in January, my new and as yet unidentified successor will be steering *The Bridge*.

I want to thank Rick Fischer, our Reviews Editor, who has been responsible for most of the published content each month. He rounded-up folks to review books and software, nagged them until they got their reviews done, and whenever he had products left over, he reviewed them himself. Without Rick and the reviews, *The Bridge* would have been a whole lot thinner and much less interesting.

And although we haven't printed and mailed the issues for several years, I am still indebted to Les Owen for putting up with my learning experience on *Adobe Pagemaker*. Regardless of how much of a mess I made of those early issues, Les could figure out what I intended to do and made it come out right. Thanks, Les!

Thanks also to everyone who contributed SIG news, relevant information, and feedback. Yes, even though we never had a "letters to the editor" section, I occasionally received additional information about an article, kind words, and even a gripe or two. I appreciate every one of them. They let me know someone was reading *The Bridge*, even if it was only to overcome insomnia.

*"Twenty years from now you will be more disappointed by the things that you didn't do than by the ones you did do. So throw off the bowlines. Sail away from the safe harbor. Catch the trade winds in your sails. Explore. Dream. Discover."*

— Mark Twain

I wish the best of luck to the incoming editor, whoever you may be. I hope you have as much fun doing the job as I did.



continued from page 15

strength scanner with an automatic document feeder. Using the included Job Wizard you can automate the jobs to run in very precise ways and unattended. There are lots of options here, so see the Nuance Web site (below) to see whether this is something you might use. Also, you'll find a complete listing of features for version 15.

Along with *OmniPage Pro 15* you get the voice recognition software: ScanSoft ASR-1600. If you install this option you will get the ability to recognize seven languages. This stuff has really come a long way!

*OmniPage Pro 15* has the ability to load previously stored files and OCR them and/or save them as a different file type. I had a PC world article stored as a jpg picture. I opened it in *OmniPage Pro 15* and saved it as a TIFF. I then tried to OCR the text in the jpg file. It worked fine. There's a lot of flexibility here.

## Direct digital-to-digital doc conversion

A new feature in version 15 is document-to-document conversion which will 'transform your existing documents into your favorite formats. You can turn your *Quark* document in to *Word*, your *PageMaker* document in to *WordPerfect*, etc. Open the document and select 'save as.' I think I read more into this than I should have.

You have to be able to open the document first. From the documentation I understand that I can't do that unless I have the native application installed on my PC. I have a *Quark* file and a *PageMaker* file, but I don't have *Quark* and *PageMaker* installed on this computer. So, I was unable to test the really tough one: *Quark* and *PageMaker* to *Word*. Note: It doesn't claim to turn *PageMaker* into *Quark*, and vice versa.

### Installing and setting up

I have an HP ScanJet 3300C - a color scanner that is now a few years old. I was concerned that it wouldn't be supported. No problem. It was on *OmniPage Pro 15's* list.

As part of the install, I was asked to install MSXML 4.0. It didn't appear to be on the CD, so I went out on the Web to see what this was all about. I found it on the Microsoft site in the XML Development Center. The rest went fine.

When these surprises happen I ask myself, would my mother know what to do if she were confronted with this alert. In this case, no. There was nothing in the manual and no help on screen. This was my only fuss with the installation process.

### ScanSoft is now Nuance

In mid October ScanSoft rebranded into Nuance. You will still see ScanSoft on some its products, but the Web page will automatically take you to [www.nuance.com](http://www.nuance.com).

Requires: Pentium III or faster. Windows 98 SE, 2000 with service pack 4 or higher, Me, XP or Server 2003. Internet Explorer 5.5 or higher. 256 MB RAM recommended. 200 MB free on your hard drive. CD-ROM.

\$199 upgrade. \$ 499. new. [www.nuance.com](http://www.nuance.com)  
 Microsoft templates are at: [office.microsoft.com/en-us/templates/default.aspx](http://office.microsoft.com/en-us/templates/default.aspx)



## Memphis PC Users Group Membership Application

Date: \_\_\_/\_\_\_/\_\_\_ Membership # \_\_\_

Name: (Last) \_\_\_\_\_ (First) \_\_\_\_\_  
 (M.I.) \_\_\_\_\_

Mailing Address: \_\_\_\_\_ Birth Date: \_\_\_/\_\_\_/\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_ - \_\_\_\_\_

Home Phone: (\_\_\_\_) \_\_\_\_\_ Business Phone: (\_\_\_\_) \_\_\_\_\_

Fax Number: (\_\_\_\_) \_\_\_\_\_ E-mail: \_\_\_\_\_

Employer: \_\_\_\_\_ Position: \_\_\_\_\_




Dues: \$35 per year

For office use only

Check#: \_\_\_\_\_ Amount: \_\_\_\_\_ Date: \_\_\_/\_\_\_/\_\_\_ Initials: \_\_\_\_\_

For up to the minute information and special updates  
be sure to check our Web site at:

***www.mpcug.org***

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
Nov 2005	21	22	23	24 	25	26 INVESTMENT
Nov - DEC 2005	28 CLIPPER	29	30	1	2	3 INTERNET HARDWARE
DEC 2005	5	6	7 MAIN MEETING	8	9	10 WEB WRITERS MS OFFICE
DEC 2005	12	13	14	15	16	17
DEC 2005	19	20	22	22	23	24 INVESTMENT
DEC 2005 	26 CLIPPER 	27	28	29	30	31