



The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 1

January 2005

For group information
please visit our Web site:
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
Microsoft Access 2003	Page 5
Hardware Hacking	Page 6
Out for Review	Page 7
The View from the Bridge	Page 8
Creating a Presentation	Page 9
Unofficial Spyware Shootout	Page 10
Microsoft Visio Pro 2003	Page 14
Nov-Dec Meeting Report	Page 17
Deck the Gulch	Page 18
Seniors' Corner	Page 22
Degunking Email	Page 22
Event Calendar	Page 24

Main Meeting Wednesday, Jan. 26 Southwest Tennessee Community College

5983 Macon Cove, Memphis

NOTE: NEW MEETING LOCATION

Parrish Room 3

First Floor - Violet Parrish Hall

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

January Meeting

Converting your 35MM slides to digital images



Somewhere in the attic or basement or a closet we all have a box (or several dozen boxes) of 35MM color slides. Carlton Smith will demonstrate converting those aging photographic images into digital images that can be emailed to friends and stored on a hard drive or burned to a CDROM. Don't drag out that projector and screen ever again. Let Carlton show you how to share your slide photos the easy way. Bring along a friend!



The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

One year ago several e-mail security vendors testified before Congress that "anonymous bulk e-mail," the kind we call "spam," constituted more than 50% of all e-mail in circulation. Our lawmakers were apparently impressed enough, or maybe being spammed enough themselves, to enact the "CAN-SPAM" Act. It required proper identification in the sender block and an effective method for the receiver to "opt-out" of future messages among several requirements defining legal bulk e-mail. Senders who do not comply with "CAN-SPAM" requirements are subject to Federal prosecution, with penalties of fines up to \$6 million, prison time up to five years, or possibly both.

Fast-forward to this year for an analysis of how the CAN-SPAM Act has helped us. The preliminary report of a year-end study of e-mail activity estimates that now all e-mail traffic contains 93% spam! Federal investigators identified and indicted three individuals for CAN-SPAM violations in 2004. One has already been acquitted on a technicality and the other two have yet to go to trial. Prosecutors are not really optimistic that they can get a conviction. The CAN-SPAM law has some serious faults, not the least being that it possibly violates the First Amendment. Some legal analysts believe that CAN-SPAM has actually aided spammers. It nullified previously enacted state laws that were usually more stringent and enforceable. Since it requires spam recipients to "opt-out" rather than "opt-in," spammers (and their lawyers) can argue that this constitutes a federal government approval on spamming. CAN-SPAM also prevents individuals and companies from suing spammers for costs associated with preventing spam or lost productivity.

Only state governments and Internet providers can file civil suits. The law puts so many roadblocks in the way of enforcement that the spammer community sees no need to take it seriously. The same year-end study cited earlier indicates that less than 6% of all bulk-email complies with the requirements of CAN-SPAM.

One factor that contributed significantly to last year's remarkable increase in spam was a proliferation of viruses and trojans that install "back doors" into vulnerable PCs, turning them into "zombie" e-mail forwarding machines. Few individuals whose PCs are being used in this manner are aware it is happening. Is the computer running a little slow these days? Surely it's not Zafi.d churning out a million spam messages a day or Email Tarantula borrowing clock cycles to hunt through the Internet and harvest e-mail addresses. All it takes to unknowingly participate in the exciting process of spamming is an unpatched PC or out-dated virus definitions.

The business of spam has also matured over the past year. With spammers raking in millions of dollars in profit, not only have the ranks swelled, but otherwise legitimate software developers are now selling highly sophisticated spamming applications openly on the Web. A Google search for "anonymous e-mail software" gets over four million hits! Typical software like *SendSafe* and *StealthMail Master* equip a neophyte spammer with all of the necessary tools to send out anonymous spam without the risk of being cut off by an Internet Service Provider. Basic utilities include "harvesting" software to collect e-mail addresses, list management tools, templates, and a direct mailing engine that does not leave

any traces through an SMTP server. Some even include a "honeypot hunter" that identifies fake addresses set up by law enforcement to trap spammers and a registered version of *SpamAssassin* to test and make sure the spam can't be blocked.

If an aspiring spammer doesn't want to do any boring work at all, *LegalMail* will lease a server in Asia with everything ready to run for \$1,300.00 per month. The server has all of the spamming software installed and is capable of churning out up to 2 million e-mail messages per day with 24/7 upkeep and technical support. These servers change their IP addresses every 10 minutes to prevent blocking and to remain completely anonymous. Tutorials are provided to learn the tricks of address harvesting, penetrating filters, bypassing firewalls, and using zombie PCs.

Some states have anti-spam laws that were not completely set aside by CAN-SPAM. Maryland, for example, based their law on consumer protection rather than e-mail regulations, and continued to indict and prosecute spammers in 2004 on the basis that consumers were being sent misleading information. However, in December, a judge in Rockville, Maryland struck down the law, ruling that it is unconstitutional because it seeks to regulate commerce outside the state's borders. A key point of the argument was that even if a resident of Maryland was the target of a spammer, the spam message itself might not be received within the state of Maryland, since the recipient might be accessing e-mail on a laptop or handheld device from someplace outside the state. Indeed, it is almost impossible to write a law these days that covers in specific detail every possible scenario to which it might apply. Our legal system is so convoluted that lawyers boast that they can always come up with some minuscule detail that the lawmakers overlooked, and use that as a wedge to negate the law in its entirety.

While U. S. anti-spam laws have problems crossing state lines, international borders are an even bigger headache. While no countries have yet attempted to prosecute spammers in other countries, a few are going after local mailers who break their laws. Netherlands courts issued three separate penalties for spamming in December. The fines ranged from \$58,000.00 down to \$27,000.00 depending upon the volume of messages sent, as the Dutch laws prescribe. Unfortunately, the law is flawed. The lowest penalty was levied against the firm whose spam did the most damage. In that instance, the spam went to mobile phones, and each phone owner was charged a \$1.49 messaging fee. The fines were also not much more than a slap on the wrist for spammers, many of whom make much more than the cost of their fine in just a few hours. Still, the three spammers vowed to appeal their fines.

continued on page 4

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.
P.O. Box 241756
Memphis, TN 38124-1756
Internet: www.mpcug.org
Information Line: 901-375-4316

One of the few anti-spam schemes that actually worked during 2004 is no longer with us. Lycos Europe, the search engine/portal organization, launched the "Make Love, Not Spam" incentive early in December. The Lycos Web site distributed a screen-saver application that "spammed the spammers" by sending a stream of requests for information to sites identified in spam e-mail. Lycos was careful to monitor these request streams, and several times they turned them off before melting down any mail servers. But otherwise, the requests tied up the servers and prevented them from sending out the normal volumes of spam. Spammers retaliated with a barrage of untruthful invective claiming that Lycos had launched targeted Denial of Service (DoS) attacks against their servers. When the spammers' smear tactics failed, they put pressure on their Internet Service Providers, and when those ISPs began blocking Lycos from customers and turning the request streams back onto Lycos' servers, Lycos was forced to shut down the anti-spam crusade.

The allegations continued long after the three day run of "Make Love, Not Spam," with tempers high on both sides of the argument. The ISPs who forced the shutdown have been severely criticized by their customers, millions of whom downloaded and used the screen saver. The ISPs defend their position saying they felt the Lycos scheme was illegal, but they don't often mention that many of them make more money providing an Internet connection for spammers than they make from the ordinary individuals who comprise 99% of their customer base. No action was ever taken against Lycos by any governmental agency, and despite the spammers' claims, Lycos probably did nothing that was illegal.

The Lycos scheme was amazingly popular. Although it was never advertised, users passed the URL to each other and the screen saver was probably downloaded and installed more often in those three days than any other software ever has been. It may be one of the most accurate measures ever taken of how frustrated the general public has become with spam. Unfortunately, in the long run, the wants and needs of the people seldom count when a small, ethically-challenged group finds a way to profit by abusing the innocent. CAN-SPAM and Lycos have proven to be no match for greed.

MPCUG Education Services doesn't have the answer to spam either, but we can recommend filters and tactics to ease the pain a bit. Join the Wizards each month before the main meeting. Bring all of your computer problems and supporting documentation when possible. The Wizards will help you get back on the right track.

For friends of Don Helyer . . .

Many of you remember Don from the earlier years of the Memphis PC Users Group. Don and a few other members of the disbanded River City Computer Club decided that there was still a need for a computer users' organization in Memphis and they started the MPCUG. He was President for several years and Editor of the newsletter more years than that. He named the newsletter "The Bridge," and even after he handed off his Group Staff duties, he continued to offer his talents and experience in guiding the Group. After he retired from his position in the Electrical Engineering Department at State Technical Institute at Memphis, Don and his wife, Pat relocated to be with their family, especially their grandchildren.

Pat Helyer informed us in a Christmas message that in late November Don began radiation and chemo treatments, and then experienced complications just before Christmas that put him into the hospital. Better news came the day after New Years when Don was able to return home. He still has several months of chemo therapy left, and is weak and sore, but determined to return to good health and regular activities.

We offer our prayers for Don and Pat through this difficult experience and our best wishes for his speedy and complete recovery. If any of his old friends would like his email address, please request from gil@ahls.us.

Microsoft Access 2003: Forms, Reports and Queries

Book Review

Reviewed by Rick Fischer

It seems I have more time to read *Access* books than play with *Access*. And, that may be a good thing because it gets the very strong impression that you want to get your database design correct the first time. The more you know about options, the better the product should be.

This book is about options associated with forms, reports and queries. My copy has lots of highlighting throughout.

McFedries wants to give us the knowledge to work independently of IT folks. He says this book will give you "the skills required to extract the data you need (queries), build efficient front-ends for that data (forms), and publish the results in an attractive and easy-to-read format (reports)" (p. 1).

I want to build a database to track graduate students here at the University of Memphis. I will use it in my department and will share it with other graduate coordinators throughout the University. I have defined the

fields we will need and want to make it easy for people who have little or no experience with *Access*. I also realize that some departments will want to collect information that other departments do not need. So, my finished product will not really be finished. And, it needs to be user friendly, or it won't be used.

I plan to have this book nearby when I attach this project.

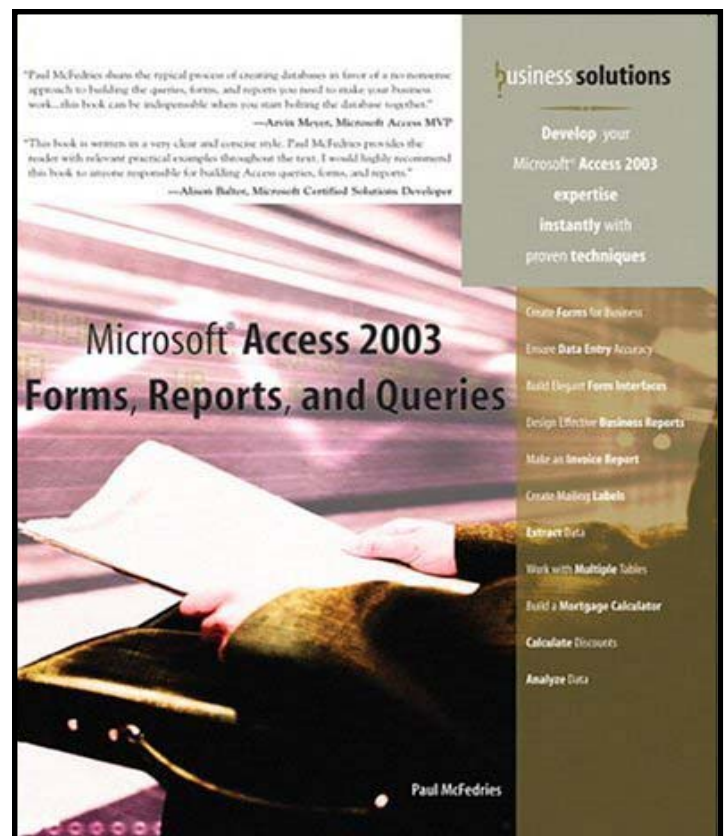
It features the step-by-step instructions I like. You get to see renderings of what the screen will look like when you actually do it. Approaches are explained and compared. Should I use a wizard? Or, should I build my

form/report/query by hand?

I may start with a wizard, but modify it by hand.

The only thing missing is a CD or supporting Web site with the examples and an opportunity for me to practice with the databases I am reading about.

Microsoft Access 2003: Forms, Reports and Queries by Paul McFedries. 2005. Que. 370 pages \$30.



Hardware Hacking Projects for Geeks

Book Review

Reviewed by Vanessa A. Muldrow

Do you know those people that have one computer, one mouse, a printer, maybe a scanner, and the only thing they know about the technical aspect of computers is how to match the keyboard cord to the matching color on the back of the machine? Well, that's me.

I can give myself *some* credit, though. I am not completely ignorant to the techno-computer world. I can plug the keyboard into the right place. But, when my sister took down her computer for added space, who was the one that put it back together? Me.

Maybe I am learning something by being associated with the Memphis PC Users Group. We all have to start somewhere.

Yes, I have some skills, but I am in no way a "hacking computer geek" which is why *Hardware Hacking Projects for Geeks* did not immediately grab my attention.

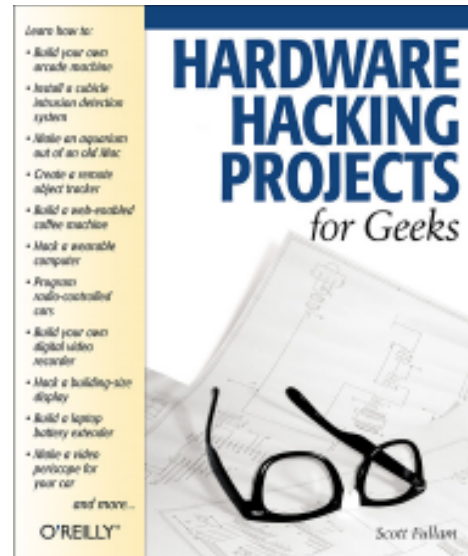
From its rather (for me) dull cover, to the inside that was a little over my head, the book was not a must read for me.

The cover: title, pieces of paper with "schematic diagrams" - I'll get to that later, and a pair of glasses with tape holding them together in the end. Boy, that says "geek" to me. Ok - I'm the wrong demographic for this book.

The cover also promises I will learn to: build my own arcade machine; install a cubicle intrusion detection system (already I am lost); create a remote object tracker, and more. My eyes were full of wonder, but not excitement. I wanted to see what the book could offer someone like me, the non-computer "geek."

As I began flipping through the book, I fell upon topic after topic on how to build things.

Part 1 begins by giving us a look at the tools needed to begin some "basic hack-



ing skills." Fullam gives us a list of tools that he uses while hacking. He suggests we have the basic soldering equipment: a small 12-watt iron for soldering surface mount parts, a larger 75-watt iron for soldering large connectors, solder, solder flux and a solder sucker or a solder wick. I learned I will need still more tools. Tools are cool. Maybe for Christmas.

As promised, Fullam shows us electrical diagrams. These diagrams are used to describe circuits. Fullam goes into detail about what these diagrams are for, how they help in the hacking process, and how to read them. Do you think I'll turn into a computer geek? Don't tell my mother.

We learn how to build a power supply for a portable laptop. We start, as we do in each chapter, with a list a list of things we are going to need in order complete each task. Fullam provides a project overview before giving us the step-by-step instructions. Through images and instructions, you learn how to perform each task. It's the same in each chapter.

What's a Mac good for?

This is cool. Many in the PC world have wondered what you do with a Mac.

Fullam lets the secret out. You build an aquarium.

Fullam gives step-by-step instructions, complete with pictures, on how to do it. I am beginning to warm up to this book.

Although I learn something in every computer book I read, the book really is targeted to the fully certified card-carrying computer geek. *Hardware Hacking for Geeks* is for the advanced hacker. Call me a novice hacker. The language, graphics and style are all geared to someone with a great interest in hacking and/or who knows a lot about hardware in general. Without this knowledge, you will be left with turning computer cases into aquariums.

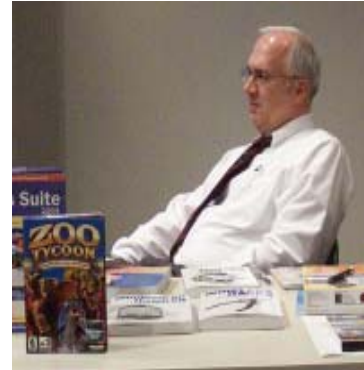
Review editor's note. Vanessa wanted to learn more about hardware, but this probably was not the book to start with. Many others in our group will understand completely what she is describing. The O'Reilly Website describes the book this way:

"From building an Internet toaster to creating a cubicle intrusion detection system, *Hardware Hacking Projects for Geeks* offers an array of inventive, customized electronics projects for the geek who can't help looking at a gadget and wondering how it might be "upgraded." Beginning with basic hacks, tools, and techniques for those who may not have a background in electronics, the book covers the tools of the hardware hacking trade and basic soldering techniques, then moves into more advanced hacking projects. Clear step-by-step instructions allow even those with no formal electronics- or hardware-engineering skills to hack real hardware in very clever ways."

Hardware Hacking Projects for Geeks by Scott Fullam. (2004). O'Reilly. 348 pages. \$29.95

O'Reilly User Group Discount: 20% on all O'Reilly books and conferences when you order direct. Include your User Group code: DSUG. Go to: <www.oreilly.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
Flash MX	Laura Cochran
Windows XP in a Snap	Vicki Dabney
Wipe Drive 3.0	John Dodson
Windows Security Handbook	Dorothy Drum
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
Inside Photoshop CS	Vanessa Muldrow
Maximum PC 2005 Buyers Guide	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
Burn, Baby, Burn	John Schuster
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas
Using FileMaker 7	Tommy Towery
Photoshop CS Down and Dirty Tricks	Jin Yang
Start Your Own Business In No Time	Jin Yang

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

The View from the Bridge

Opinion

by Gil Hennon, Editor



At the last meeting we had a brief discussion about the future direction of the Memphis PC Users Group. There were good points made about the group's current financial health even as membership has declined. The following is a summary of observations made by several members.

Problems:

- Our membership is steadily declining
- Our membership is steadily aging - few or no young members
- Our Tennessee non-profit corporation status has expired
- We have several open staff and board member positions
- We have not been able to attract speakers and programs for all meetings
- There are only a few volunteer members doing all of the work

Strengths:

- We are financially sound and have no debt
- Our Post Office box fees are paid up for another year
- Our Web hosting fees are paid up for another year
- Our meeting room will be hosted by STCC for another year
- We are delivering our monthly newsletter by email at no cost
- We still have vendors providing free software and books for review
- We have members with both business and technical talent and experience
- The current staff members are willing to continue their duties
- John Dodson volunteered to fill the Treasurer vacancy

After some discussion, no large decisions were reached. However, there was general agreement to continue the operation of the group during 2005 while we consider new plans and attempt to attract more members and presenters. The Board of Directors have not met for quite a while. The duties of the Board need to be rethought and perhaps redefined. In the meantime, the operation of the group will have to be the responsibility of the remaining membership. The group has always belonged to the members, and their wishes will direct the actions of the staff. By the same token, the staff will be looking to the membership for a commitment to the group's continued existence and for support in making the group grow. We are very close to having little to offer and almost no one to offer to. If we cannot put the group on to a new growth curve with a reasonable opportunity to improve, we are just wasting time and effort while prolonging the inevitable.

Suggestions, arguments, or comments are welcome and will be published in the next issue of The Bridge. Please send them to gil@ahls.us.

Creating a Presentation in PowerPoint

Book Review

Reviewed by Rick Fischer

Peachpit has a new series called the Visual Quickproject Guide. It has more to do with the output than the fine points of the software involved.

And in the case of *Creating a Presentation in PowerPoint*, it covers *PowerPoint* for both the *Windows* and *Mac* platforms.

I was interested in this book because it looked like it might be useful for students who needed to produce a *PowerPoint* presentation at the end of a semester when time is critical. It is and I plan to add it as a recommended text to my research and campaigns syllabi.

Negrino recommends starting with the text outline before doing anything else. He shows us how to do that in *PowerPoint* and *Word*. He presumes (correctly, I think) that most folks already know *Word*.

Once the text is fairly well set, he invites us to select images and sound files that might enhance our presentation. We see all the places we might find those files – from our *Office* suite, to the Microsoft Web site, to independent sources.

Now, we select the look of our presentation. Here we are invited to select a design template, and it is the only place in the book where we aren't told how to bring up the slide design window. I didn't

know that the Mac shipped with many more templates (110 compared with 63 for *Windows*) than did the *Windows* version of *PowerPoint*. Since our students have access to both Mac and *Windows*, it will be useful to look at both sets of templates. They work across platforms, so that is a valuable tip.

Negrino points out how the look of the presentation (fonts, bullet style, etc) is distinct from the background of the template. First we pick the presentation style, and then add in the background. It's great if you like both in the same template, but he shows us how to make adjustments when we only like one or the other.

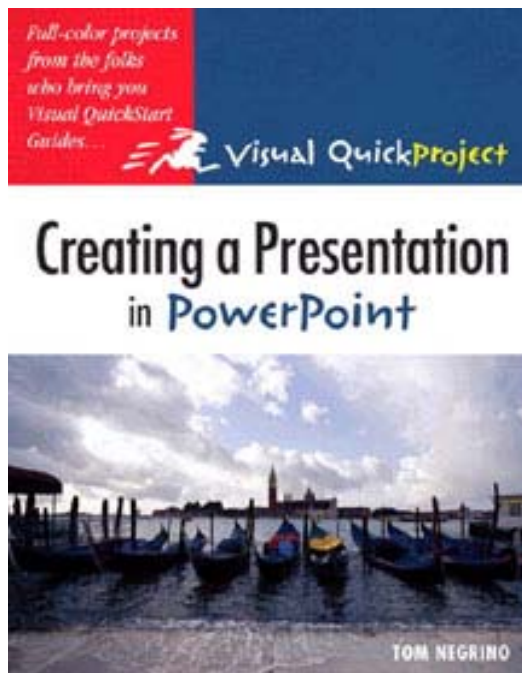
We polish our spelling, insert tables, graphs and hyperlinks. As with every book I read, I always find features that may be new or new to me, or find other ways to do tasks I have been doing for years. That was certainly true here.

We finish by sending our presentation out for comments, practicing our presentation, then saving it to a CD along with the viewer, or publishing it to the Web.

I think Negrino has captured all the steps along with the details necessary to be successful. I think the editor might help us with differences in the way the *Mac* and *Windows* text and illustrations are handled in the next version. It should be obvious that we are switching from one to another, and that transition isn't always obvious. It's just a matter of consistency.

Although my comments were written for the student who is using *PowerPoint* for the first time, they apply equally for the business presenter or person who needs to illustrate a talk at the club. You won't get bogged down in detail you don't need to produce the result. This is fast-tracking at its best.

Creating a Presentation in PowerPoint by Tom Negrino. Peachpit Press. 2005. \$13. 142 pages.



The Unofficial Spyware Shoot-out

Software Comparison

by Gil Hennon

Viruses and worms are bad. Everyone knows that, or nearly everyone. Even new computer users find out very quickly that they need anti-virus software. In fact, so many PCs are now protected by a reasonably effective anti-virus tool that only a few of the nasty things are still hanging around and causing trouble. And for most of us, our virus scanner catches and deletes them as they arrive with our email. The best thing that can happen is that they are already history before we even know they came to call.

Spyware, though, is a whole different problem. Rather than showing up when the email comes, "bots" are secretly installed when we visit Web sites, answer surveys, use search engines, or download files and programs. In other words, there are as many ways to get spyware as there are kinds of spyware.

The most common form of spyware is the Tracking Cookie. In general, most cookies are good things. They provide "persistence" across the Internet, so search engines

know what to send us when we ask for the next page, and vendors can match us with our shopping cart contents when we are ready to check out. The small difference that makes a particular cookie "track" is that it is accessible to more than one host site, so as we visit several sites, it logs our "trail" through cyberspace, and the log can be grabbed by an unscrupulous Web site to build a profile of our online behavior.

Other forms of spyware are password grabbers, keystroke loggers, browser hijackers, adware (advertising), remote access tools, and ID theft/fraud facilitators. There are probably a few other types, but don't worry, in a few days there will be even more. And if you are getting the feeling that I believe spyware to be a much worse problem than viruses, you are definitely not the weakest link. All of these "bots" with their ads and logs and harvesting of confidential information cost individuals and businesses many millions of dollars per year for prevention and/or actual losses. They annoy me so

badly that for about a year I have been using two different anti-spyware programs to hunt down and terminate the nasty "bots." For this reason, I have been on the look-out for a single program that would eliminate all of the different types of spyware.

Every giant software download site (CNET's download.com, ZDNet.com, Tucows, etc.) has different programs they tout as the "best and most popular." At the vendors' Web sites the superlatives flow even more freely. Every product is the "most thorough," "highest rated," and "best protection available." Is it hard to choose which one to install? You bet it is! How can anyone know which one really does do the best job of eliminating spyware? I decided to download four with good references and lots of previous downloads. All four were "evaluation" versions that can be tried for free before purchasing anything. Then I ran a very informal test, comparing them against the anti-spybot software that I was already using.

I started with an aver-

age PC with an Intel Pentium III 800 MHz processor. Although not a speed burner, it has 90 Gb of hard drive and 1 Gb RAM memory, so it isn't completely a slouch. Also, it contains over 275,000 files and programs, which would give the scanners a good workout. Then I visited some Web sites known to install spyware, and also used all of the major search engines to look for CD music, the Internet's most popular product. From an examination of the cookies these sites installed, it looked like I picked up about ten spyware "bots." (That was a low guess, as I discovered when we started testing.) I had no idea how many registry keys or files had been created. First, here are raw results:

Program	Web site	Price to Register	Speed of scan	Cookies found	Registry entries or files found
Spybot S&D	security.kolla.de	Variable donation	4 min	11	2
AdAware SE	www.lavasoft.de	\$27.00	21 min *	13	none
Spy Sweeper	www.webroot.com	\$29.95	35 min	21	none
Spyware Doctor	www.pctools.com	\$39.95	16 min	12	25 **
Aluria Spyware Eliminator	www.aluriasoftware.com	\$59.95 ***	44 min	none	2
CA Pest Patrol	www.pestpatrol.com	\$39.95	253 min	17	19 ****

* AdAware found exactly the same spyware in 21 minutes on "Full Scan" as it did in 3 minutes using its "Smart Scan" setting. "Smart Scan" is obviously well targeted and very efficient.

** All 25 registry entries were "BonziBuddy" and reported as "very dangerous." I could not confirm that the entries were actually "BonziBuddy," and no other spyware scanner found "BonziBuddy" on the PC. No other authority considers "BonziBuddy" to be of more than a minor risk. It is a benign downloading help tool, although somewhat difficult to remove from a PC. I suspect this was a case of false identification.

*** Aluria is currently offering this software at a discount for \$29.95.

**** Pest Patrol identified 16 registry keys and 3 data files it believed was spyware. The 3 files were definitely false identification. One was a standard Java file and the other two were Corel Draw images. 3 of the registry key hits were confirmed to be real spyware, but 5 were perfectly safe registry keys necessary for the proper operation of installed software. I could not determine whether the other 8 registry keys identified might actually be spyware or not.

The numbers in the table need even more qualifications. Some programs count multiple cookies from the same source as a single spyware instance, while other programs count every individual cookie. The same appears to be true of registry keys. So the raw results are an “apples and oranges” comparison. Also, some of the evaluation software updated itself to the most recent spyware definitions available during installation. If it didn't, I tried to get the latest definitions manually. I never found a current definition list for Aluria Spyware Eliminator, so it may have been using an old definition file. Both of the registry keys it identified as spyware were of the Gator variety, which has been around for a couple of years, but it did not catch any of the more recent ones. Aluria's evaluation version also seems to ignore cookies.

Computer Associates' Pest Patrol home edition does not have an evaluation version. I was able to download an evaluation version of their Corporate Edition 5.0 on the assumption that all of their products are built around the same scanning engine. The Corporate Edition has a network administrator

interface that allows scanning any PC on a network, entire workgroups, or the whole network. It had extensive logging and reporting features, and was an impressive professional tool. For administrators, this would be an excellent interface, but overkill for individuals or small offices. Except for a propensity to falsely accuse perfectly good files and registry keys of being spyware, Pest Patrol was the most thorough scanner tested. Pest Patrol's Web site also had the best information on spyware of any vendor. The “pest encyclopedia” pages were very useful in verifying that an unfamiliar cookie or key was actually spyware.

General features of all of these spyware eliminator programs were nearly identical. Every one has an “automatic” operating mode that will scan new files as they are received or opened. They also have a scheduler function that will run scans during the night or at another time when the computer is not heavily in use. Every program can be run in the background, so other work can be accomplished while the scanner is running. All of them require a “definition” or “signature” file that is updated



regularly, such as every week or two weeks. All but Aluria would connect to the vendor Web site and update definitions automatically. Only Spybot Search & Destroy was a complete and fully functional application. All of the others were evaluation versions, and so they were crippled in some manner. Several would identify spyware, but not clean it off until a registered version was purchased.

Some of the products were more user configurable than others. Spybot Search & Destroy has an inconspicuous “settings” button at the bottom of its menu bar, and Pest Patrol has tabs for advanced configuration menus. AdAware hides its settings under a “gear” icon. Most users won't need to do any tweaking though. Every program came well configured for the average PC. Only if you have something unusual, like software that requires some “spyware” to allow its use (like Kazaa) might

you need to tell the scanning program that you have cookies or keys they should ignore. You can also limit scanning to only certain drives. And on the rare occasion when you actually need to restore components that the scanner eliminated, the tools for doing it are usually located in the advanced settings areas.

I expected more “overlap” among the products we tested, but each program works in its own way and uses its own definitions list. There was a lot of variation in the results of this informal test. Some scanners seem to concentrate on cookies, others on registry keys. Of the two, cookies are easier to find because they identify the owner. There were some cookies that almost every scanner found, but there were a few that only one or two identified. No scanner managed to find every one that was there, although I didn’t know some of them existed until the scanners started ferreting them out. The same is true with registry keys, but they are more cryptic and the possibility for a false identification is greater. I believe there were actually five, but no scanner correctly caught more than three.

This wasn’t a formal

test with carefully controlled conditions. The PC had both known and unknown spyware on it. To some extent, the results are inconclusive, because no single scanner emerged from the pack as being significantly better than the rest. I still like Spybot Search & Destroy from Kolla Security the best. It is simple to use and works well exactly as it is installed. It caught most of the cookies and two registry keys that I could confirm were spyware. The runner-up was Pest Patrol, which might have taken top honors except that it false identified on eight items for sure, and maybe a few more. If you are willing to examine carefully the results and not allow Pest Patrol to eliminate some of your necessary components, it does a very thorough scan and appears to recognize more threats than all of the rest.

Except for Aluria Spyware Eliminator, the remaining programs were nearly as good as the top two picks. There are more spyware elimination programs available; a search on Google turns up about thirty. So there is plenty of competition in this category of software. I tested only the products that had won some recognition and were popular downloads. I certainly

may have overlooked a less popular or unacclaimed scanner that would have blown me away.

The important conclusion may not be which one is best, but that more than one spyware utility is probably necessary to protect your system. I know several users who use at least two, including myself. Fortunately, most spyware is not malicious, and only wants to sell you something. But when enough of it is running on your PC, application speed and performance decreases noticeably. As the load increases, the system can become unstable. And then there are some bots that are very bad, stealing passwords and account numbers, changing the way your computer behaves, and modifying or destroying data. You certainly want to put a stop to all that!

Don’t take my informal test results as gospel. Since most of the spyware eliminators will let you try before you buy, download some that look good and give them a try. I believe you will have to find a combination of two or more to get the protection you need, but if you happen to find one that can really do it all, please let me know about it plenty pronto!

Visio Professional 2003

Software Review

Reviewed by Rick Fischer

We last reviewed Microsoft Office *Visio* in October 2002. I had planned to concentrate on the new features in this review until I sampled a small group of savvy computer users and learned that they had never heard of *Visio*.

So this is a reintroduction.

Norm Hays is working on his doctorate in education and needs to create models and flow charts for his course work. He does them in *Word*. I asked Norm whether he had

tried *Visio*. He was one of those who had never heard of it. And, it looks as though his major professors either hadn't heard of it or didn't choose to show their students a better way to draw models. Too bad.

So, I opened *Visio* and showed him some of what it can do.

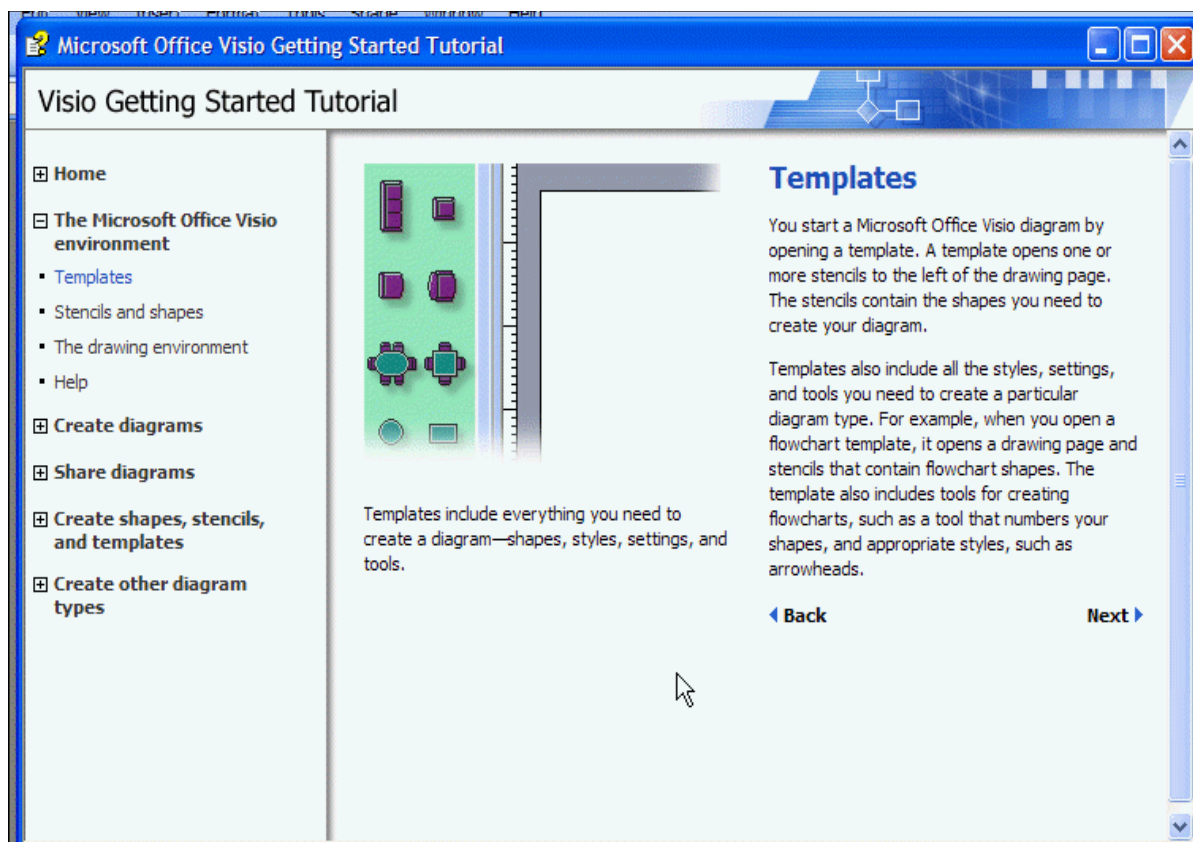
Microsoft calls *Visio* a "business and technical drawing program." *Visio* contains a collection of templates, shapes and drawing tools that you use to create a wide range of line drawings.

Big deal. *Word* and *PowerPoint* can do that!

They certainly can. But in *Visio* when you move a shape the dynamic connectors and text labels move with it. If you need to insert a shape, it easily accepts it. And, the variety of shapes!

The Standard version has more than most of us will ever need. The Professional version caters to specialties, like floor plans, electrical circuits, mechanical engineering, site plans and physical computer network diagrams.

So, I showed Norm the categories – the broad types



of templates he could select. As we clicked each category he could see the associated templates.

Norm was interested in the block diagrams and flow chart categories. We looked at one of the options and opened it. The shapes and lines were there ready to pull onto the drawing page. I know I still have graph paper in the house for when I want to create a drawing by hand. *Visio's* drawing page looks like the graph paper you already know and use.

We pulled (dragged and dropped) a couple of shapes onto the page and connected them with lines – some with arrows. We labeled the shapes and

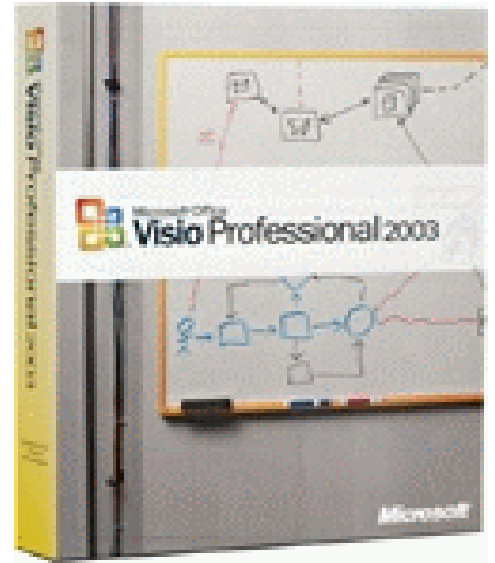
added descriptors to a few of the lines. Cool.

“Now, watch this,” I said. I dragged one of the shapes across the page and the integrity of the drawing was maintained. The lines, arrows and text moved with it!

Then I showed Norm how I could drop a new shape into my existing diagram – just hover the shape over the connecting line and it gets incorporated into the drawing.

Norm started to think about what this would mean to him and his work.

“Look,” I said. “It’s part of the Office suite. The school should be able to get a copy for you.” He works full time for the University. Now, he has



his own copy.

You can use *Visio* as a stand-alone program to produce diagrams to print. When you add the special boards and labeling objects, it looks very professional.

It’s more likely that you will create a diagram

continued on page 16

Memphis PC Users Group Membership Application

Date: ___/___/___

Membership # ___

Name: (Last) _____ (First) _____
(M.I.) _____

Mailing Address: _____ Birth Date: ___/___/___

City: _____ State: _____ Zip: _____ - _____

Home Phone: (____) _____ Business Phone: (____) _____

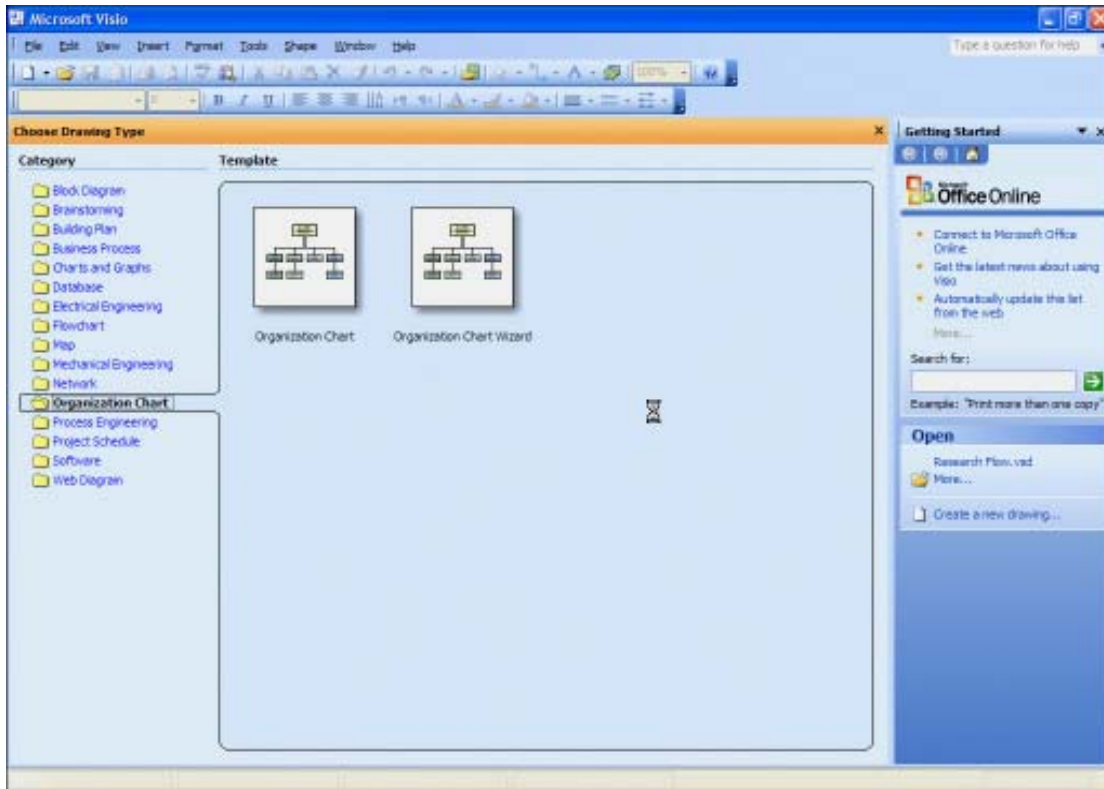
Fax Number: (____) _____ E-mail: _____

Employer: _____ Position: _____

Dues: \$35 per year

For office use only

Check#: _____ Amount: _____ Date: ___/___/___ Initials: _____



in *Visio*, then paste it into a *Word* document or *PowerPoint* presentation.

What I didn't know was that you can edit that diagram **in** *Word*. *Visio* will actually open in *Word* and you can edit your drawing right there. And, it doesn't affect the original saved *Visio* file.

New in 2003

For a full list of new features, go to office.microsoft.com and click on *Visio*. Here are some that I found interesting:

- § Easy access to clip art through the new task pane that docs on the right side of your screen.

- § Ability to mark up, add or view comments on a review copy of the file.

- § Search for shapes

within the shapes window. If you are online it will also search Microsoft's extended collection of shapes stored there.

- § Shapes can be rotated with familiar rotation handles.

- § New Business Processes category for Six Sigma and ISO reports.

- § New Brainstorming template to illustrate how ideas are linked. This is also called "mind mapping."

- § New free *Visio* viewer. View and print *Visio* documents even if you don't have a copy of *Visio*. An earlier version of the viewer did not render the file with the same fidelity as the original program. This is supposed to be an im-

provement.

The first thing I did after loading *Visio Professional 2003* was to go through the Getting Started Tutorial. The Welcome booklet that shipped with *Visio* is a nice introduction, but hardly substitutes for a manual. I found much of *Visio* is intuitive if you've used a drawing program before. But, if you use *Visio* a lot, you will want more than the tutorial or the booklet can offer. Your options are Help and/or a book written especially for *Visio* users.

Visio Standard \$199 full or \$100 for upgrade

Visio Professional \$499 full or \$249 for upgrade

November-December Meeting Report

Free and Open Source Software (FOSS)

It's not just for Linux anymore!

Warren Turkal, President of the Group Of Linux Users Memphis (GOLUM) introduced the Open Source Software concept at the November-December meeting. Warren uses Open Source software on his Debian Linux platform, and many of the applications he uses regularly are also available in Windows versions. He equated Open Source with Free Speech; users can see the source code, modify it if necessary, and redistribute it as long as they comply with the Open Source requirements. The objective of Open Source is to get more users into the FOSS community and to create more secure, cheaper, and easier to use software. Open Source means software as the user wants it to be.



Warren demonstrated the following Open Source applications that are **available both on the Windows and Linux platforms**:

- OpenOffice - an office suite comparable to Microsoft Office with word processing, spreadsheet, presentations, and more. OpenOffice reads and writes MS Office and WordPerfect office file formats.
- GAIM - instant messaging client compatible with most popular IM vendors and has plug-ins for others.
- Mozilla Firefox and Thunderbird - Internet browser and email client apps that are growing in popularity. They have features and configurability beyond what is available in Internet Explorer and Outlook.
- Celestia - A really cool astronomy display program that allows a user to choose a celestial object and the program zooms to the appropriate location.
- GCC/MingW - compilers for building Open Source applications
- Blender - a sophisticated 3D modeling tool for graphics and engineering

The following Open Source applications are **currently only available for Linux**:

- Kontact - A personal information manager/contact management program comparable to Outlook and Exchange
- Kdevelop - A source code and development documentation version control app
- Konquerer - A full-featured Internet browser

Open Source software can be downloaded from www.sourceforge.com and www.freshmeat.net

Thanks to Warren and GOLUM for a great presentation. All MPCUG members are invited to attend GOLUM meetings. Schedules and more information can be found at www.golum.org

Deck the Gulch with Worms and Spyware

Editorial

by Gil Hennon

Christmas Day down at Silicon Gulch was a mixture of the sublime and the ridiculous. Sublime fits the quiet winter day back in the remote pine forest with smells of turkey and ham around the old cabin and steaming mugs of the Old Timers' grog passed from hand to hand. What was ridiculous was the lack of grace we exhibited getting there. Three days before the annual Yuletide celebration, mother nature decided to dump several inches of icy, wet sleet on about a quarter of the entire nation. Frozen into a thick shell, it was slicker than duck butter. Driving was actually safer than walking, even though we performed a few unintentional gyrations on the twisty road. The last part of the trail had to be done on foot, to some degree, and more than once we traveled literally by the seat of our pants.

So our arrival was more an occasion for expressions of sincere relief than holiday tidings. The old cabin door opened wide, and inside we found the Old Timers already at the table, attacking loaded plates of the Christmas feast. As they passed around dishes and utensils, some were already arguing about various computer problems and the relative gravity of each. It had been a year of wildly escalating risks. More than ten thousand new viruses, worms, and Trojan horse programs reached the public in 2004. There was also a sharp increase in the frequency and foulness of spyware, and a very disturbing transition from prankishness to exploitation in all forms of malware.

Once we had plates of food and mugs of grog, we joined a conversation about viruses and worms. There were not as many arguments as farther down the

table, giving us a pause now and then for eating. The Old Timers were pretty well in agreement about which viruses were the biggest problems of 2004. NetSky.P was generally acclaimed to be the worst, and one Old Timer produced an expert's opinion to back up his position. Sophos Anti-virus (www.sophos.com) found NetSky.P to be the culprit in nearly 23% of all infections. About thirty NetSky variants were released starting in February and continuing throughout the rest of the year. As a family, they accounted for nearly half of all reported infections. Many of the Netskys exploited a flaw in Microsoft Internet Explorer that allowed them to be automatically executed and installed from an infected Web site. Other Netsky variants used more traditional mass-mailing distribution tricks or traveled the peer-to-peer messaging routes. As the year closed, Netsky was still the most likely virus that might show up in your e-mail. Being a hybrid, with the characteristics of both viruses and worms, NetSky proved to be the most prolific infector since the days of the Microsoft Word Concept viruses.

Second place went to Zafi.B, one of the first viruses written with a profit motive. Zafi is the result of Cracker tools being used to spread e-mail spam. It turns a PC into a "zombie" and forwards anonymous bulk e-mail. Zafi-B did its best to stuff your inbox with spam this year. Although not as widespread as NetSky, Zafi was no slouch, especially considering that it was released in June and only had half of the year to rack up one out of every five infections. A new Zafi variant, Zafi.D, appeared in mid-December masquerading as (did you guess?) a Christmas greeting. Although Zafi.D has yet to make a big stir, it spread fairly rapidly after it infected several spamming servers.

And third place goes to the Sasser

worm. It exploits a vulnerability in Microsoft Windows for which a patch has been available for many months. But too many users still don't bother to download and install critical patches. (What are they waiting for?)



Sasser accounted for 14% of all infections, according to Sophos, which is unusual for a worm that travels only across network connections. At least its infections are easy to spot. Sasser causes a Microsoft component, LSASS.EXE, to crash, and that displays an error message informing the user that the computer is about to shut down. Sasser is distinguished for another reason too; it was written by Sven Jaschen, a German teenager who also wrote the NetSky viruses. Jaschen was arrested by German police within a week of releasing the Sasser worm. He claims he wrote Sasser and NetSky to infect the spammers who released the MyDoom and Bagle virus/worms. Sven's cure was worse than the disease.

Three other virus/worm blended threats were annoying enough to get serious attention during 2004. MyDoom, a carry-over from the previous year was still circulating as an email attachment even though the trigger dates for the malicious payloads were long gone. MyDoom uses all of the PCs it infects to launch Denial of Service (DoS) attacks against Microsoft's and other servers. The virus finally dropped from the serious problem lists around the end of summer, and since then only a few infections have been reported, but for the first half of the year, the Old Timers called MyDoom the "worst ever virus."

In May, a new variant of the Bagle worm appeared. Bagle.AA opens port 2535 when it infects, allowing remote

commands to be executed. It then attempts to connect to one of about fifty different Web sites where command scripts are located. Documents, keystrokes, and other confidential information are collected by the scripts and sent back to "shar" folders on the Web sites. Although the Web sites and their command scripts have been shut down, Bagle.AA was still in circulation as an email attachment and infecting PCs at the end of the year.

A late-comer in November gave us the last serious threat of 2004. Sober.I resembled the other Sober variants that came before it, but improvements in its embedded SMTP engine and some bug fixes made it a more potent threat. It also can search networks for Domain Name Servers (DNS) where it can find plenty of email servers. During infection, Sober-I often displays an error message that "WinZip_data_module_is_missing." This virus can also be very hard to remove from a system. It runs two memory-resident processes that protect each other. Deleting either process triggers the other to completely reinstall Sober. So after normal cleaning, the virus is usually right back on the PC and continuing to infect email. Special clean-up tools from several of the anti-virus vendors are much more successful getting rid of Sober-I than the regular removal engine included with most anti-virus definitions and scanners.

Just because a mere handful of viruses and worms caused 80% of the infections last year is not an indication that this type of malware is declining. More than ten thousand new and variant strains were released on the public in 2004, and the Old Timers don't believe we will be seeing any reduction in the foreseeable future. The virus authors are smarter and much bolder than in past years. For a while, in late Spring, the crackers responsible for Netsky, Bagle, and MyDoom carried on a competition to see who could release the most variants on the public in the shortest time, and who could cause

the most infections. They even hid insulting text strings to each other in their code. But there are other forms of malware that are proliferating just as fast and pose new threats that are not as simple to eliminate as a virus or worm. We grabbed our mugs of grog and moved down the table to where other Old Timers were engaged in a heated argument over which of the various forms of spyware poses the worst threat to PCs and their owners.

Spyware was still fairly new and relatively benign when the year began. Most "spy-bots" were secretly installed when a user visited a Web site or downloaded "freebie" software. The bot then tracked the user's behavior and delivered somewhat relevant pop-up advertising. It wasn't a serious threat, although when a crowd of spy-bots collected in a PC, its performance took a nose-dive. An occasional cleaning with AdAware eliminated the annoyance for a while. None of the major anti-virus vendors took spyware seriously until this year.

As the bots became more sophisticated, they also grew more malicious. The latest versions use multiple methods of delivery to target PCs. They install secret files in many different areas of a hard drive and create multiple registry keys. All of these strategies are attempts to protect the spyware from removal utilities, or to reinstall the bots if they happened to be found and removed. Spyware also borrows successful ideas from viruses and worms, such as "social engineering" to entice a user to allow the initial installation.

One of the nastier spybots that can be encountered is PurityScan. It follows a warning that online pornography may have been secretly hidden on a user's hard drive. PurityScan offers to find the pornography, remove it, and thus protect an innocent user from undeserved legal prosecution. Many users willingly install PurityScan. Whether or not PurityScan actually removes any porn is a matter for

conjecture, but it certainly floods the PC's Web browser with pop-up advertising. It can also be difficult to remove.

CoolWebSearch (CWS) is the collective name for a whole family of bad bots. It is basically a browser hijacker, blocking users from Web sites they want to visit and steering them to commercial and search sites affiliated with CWS. More than a thousand Web sites are affiliated, and many of them are pornographic. This bot uses many different methods to protect itself, and many of its variants are immune to anti-spyware removal attempts. Too often the only way to get rid of CWS is to format the drive and completely reload the operating system and all components. Some researchers claim that CoolWeb can survive and reinstall itself after a hard drive format. The Old Timers speculate that CWS may write a copy of itself in areas that are not destroyed and rewritten during the formatting process, but they haven't seen a revival after a format with their own eyes. They do agree, however that it is among the most persistent of all malware, and extremely difficult to remove.

The Old Timers noted that plenty of spyware still merely tracks online behavior and delivers targeted advertising. Gator, KeenValue, and BargainBuddy are typical and can be found everywhere. They are annoying, but usually do no harm beyond degrading system performance. Some spyware even performs a beneficial service, like Transponder, which helps fill out online forms while it collects personal information. The worst are those that force innocent users into pornographic Web sites and "phishing" bots that log keystrokes to steal account numbers and passwords. One new malicious spyware scheme isn't widespread yet, but is still causing big problems. It secretly uses a PC's modem to dial a "900 premium service" phone number. These calls are charged by the minute, and the spyware keeps the computer connected

for hours or sometimes days. The innocent user is unaware of the connection until receiving a huge telephone bill.

The Old Timers see two new threats that just appeared in 2004 needing serious attention as we start the new year. The first is identity theft or "phishing." This can be as simple as installing a key-logger to capture account and pin numbers, or as complicated as a complete duplication of a bank or brokerage house Web site to capture users' log in and password information. "Phishing" is highly profitable for online criminals. With the right data, they can clean out a bank account or run credit card debt to its limit without the knowledge of the innocent user.

The second new threat is not quite so mature yet, but several malware exploits in the past year targeted mobile devices. Handheld PDAs that can connect and exchange data have very little security built in to them. Similarly, cellular telephones have become quite sophisticated with many new features, and offer lots of methods of intrusion. Only a few instances of viruses or spyware specifically targeting mobile devices have been identified. Most have exploited vulnerabilities in the Symbian operating system used by many cell phones. The Old Timers believe these early forays have been tests released by crackers with limited distribution. As the authors of this sort of malware learn what works and what doesn't, we will probably see a lot more of it.

Which brings us to the Old Timers' final conclusions about what they have already seen, and what is likely to come in 2005. The most serious new threats are those that don't conform to our traditional definitions. Hybrids and blended threats blur the lines between the old types. Just as viruses and worms combined a couple of years ago, so are spyware, Trojans, and "phishing" exploits being combined for better distribution and protection. Spam e-mail is being used more often to deliver malware, and malware is being used to

aid the spammers. Many of the new threats can infect and operate without the knowledge of the PC user, and if they are identified, they are extremely difficult to remove.

The software vulnerabilities that malware exploits are being constantly found and patched. A year ago, when a vulnerability was discovered, a patch usually was available before a virus could take advantage of it. In the past year, we saw the Bofra worm exploit a vulnerability discovered only four days previously. The Old Timers will not be surprised if 2005 finally produces a "zero day" exploit that begins infecting on the same day a vulnerability is discovered.

The malware is getting smarter too. Hybrid spyware can infect like a virus, travel like a worm, open ports like a Trojan, and "phone home" with built-in communication. In December, virus researchers identified the Santy worm. It doesn't infect randomly, as all previous worms and viruses did. Instead, Santy searches Google to find text strings on a Web site that indicate that site is vulnerable, then Santy finds its way to that Web site and infects it. The newer malware is also profit-motivated. Worms and viruses and spyware participate in identity theft, "phishing," and spamming. They build "zombie" networks that provide processor time and locations to aid in criminal activities. The pranksters have grown up.

Unfortunately, our protection against blended and hybrid threat malware hasn't matured to keep pace with the bad guys. We still need anti-virus scanners, spyware removers, software firewalls, and for broadband access, a secure router. The Old Timers recommend that we get the best of each that we can. We also need to keep up with software security patches and the latest virus/spyware definition files. It takes some work to stay ahead of the malware authors and criminal crackers. 2005 will definitely be an interesting year.

Seniors' Corner

by Jim Ingram

Southwest Tennessee Community College programs for SENIOR CITIZENS and/or STUDENTS with Disabilities

(1) The Sixty Plus Program

A Tennessee resident sixty years or older, or a permanently disabled resident, may audit courses without paying any maintenance fees. However, The student will be subject to a \$5.00 application fee (if not already paid) and a \$10.00 campus access fee, which includes a parking sticker.

(2) The Sixty-Five Plus Program

A Tennessee resident sixty-five years or older, or a permanently disabled resident, may take classes for credit at a reduced rate of one half the Semester hourly rate up to a maximum of \$75 plus a \$5.00 application fee (if not previously paid) and a \$10.00 campus access fee, which includes a parking sticker.

Enrollment without payment of the full registration fee will be subject to the availability of space in the class being requested. Registration for these programs will be processed during LATE REGISTRATIONS only. In other words, a senior citizen cannot displace a fee-paying student.

The above fees are for Southwest Tennessee Community College only, and they can be found in the catalog under FEES AND CHARGES. Since the University of Memphis has a higher credit hour charge, the fees for similar programs will be somewhat higher.

Degunking Your Email, Spam, and Viruses

Book Review

Reviewed by Hyun Cho

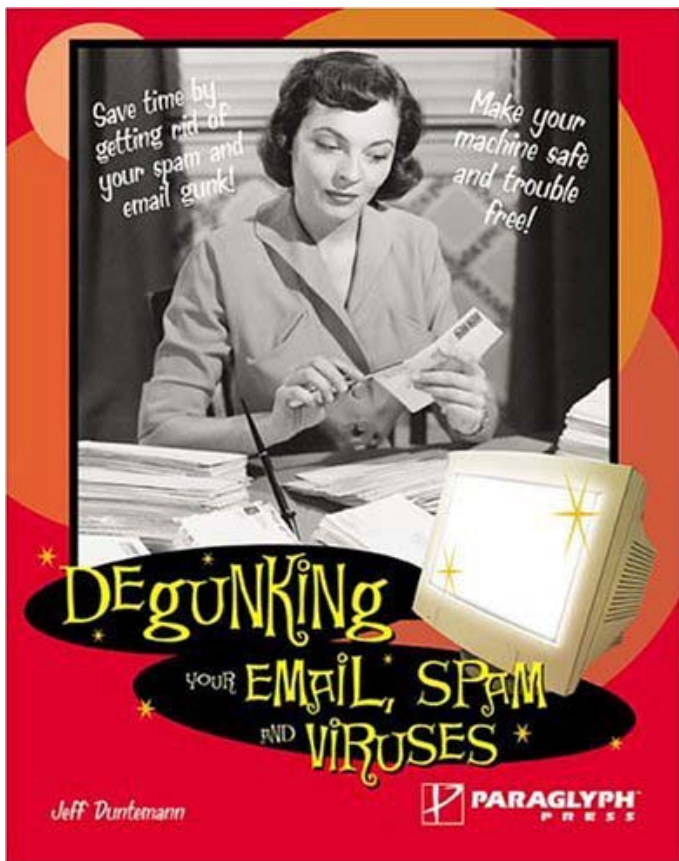
When it comes to "fixing" a computer problem, I'm not the person to ask. I may be software savvy but most of that is by accident or what people call "trial-and-error." So when I agreed to review *Degunking Your Email, Spam, and Viruses* I was a little intimidated. For Pete's sake, I use Hotmail as my primary account and though I shouldn't, I rely on Hotmail service to keep the gunk, spam and viruses out. I also use Microsoft Outlook at work. Our tech guy, Sean, even had to set it up. And when that goes berserk, I just sit and wait for him to fix it.

But I was reassured that this book was going to be easy to read and understand, and it is. But some topics can be overwhelming to non-technical folks (like me). There was a lot of information to take in about emails, viruses, etc., more than I will ever need or want to know. Therefore instead of trying to review the entire book, I found some highlighted points that I thought might interest readers on how to "degunk" their email.

E-mail

Because I am a neat-freak, I enjoyed chapter six on cleaning and organizing the mailbase and am glad to know that all my organizing pays off. Maybe some of you know how to do this, but I suspect, not many.

Some tips include how to build a hierarchy of folders. According to the book, you want to create folders by topics/task and *not* by sender because once the task is over you can delete the folder. Another helpful hint is making subfolders. Duntemann suggests that unless the subfolders are used daily do *not* create subfolders because they will clutter up the email account.



Spam

Let's move on to the pesky Spam that everyone hates. Duntemann covers Spam in four chapters – from choosing an address that can help avoid spam to avoiding software and downloads that don't work. The two most useful chapters (to me) are nine, "Deep-Clean Your Spam Using Bayesian Spam Filtering" and chapter ten, "Avoid Spam Control Methods That Don't Work."

It's obvious that most of us don't invite Spam into our computer, it just happens. And when we try to get rid of it ourselves, it seems to increase not decrease. There-

fore, knowing how to avoid the Spam control that doesn't work and using the ones that do was an eye-open experience for me.

In chapter nine, Duntemann suggest using Bayesian filtering. He explains what it does, how to download it and how to use it. He also explains what a POPFile is and what he likes about it. In addition, he gets into all the nooks-and-corners of how to configure your email client to POPFile, shows you how to use it, and how to back up POPFile's Corpus Data.

The last half of the book discusses the other annoyances on our computers – viruses, worms, trojans, adware, and spyware. I personally found the adware and spyware chapters to be most helpful because it's something most people, including me, don't know and understand. And when people don't understand, they make the mistakes of installing adware and spyware blockers that are destructive. So read this section carefully before installing a pop-up ad that guarantees a solution that sounds too good to be true.

One last word of advice: buy this book to keep handy for solutions on emails, viruses, spam, and other elements that can infiltrate your computer. But don't expect to take it in in one reading (unless you are the reviews editor). It's easy and interesting reading, just not something I'd take with me on a road trip.



Degunking Your Email, Spam, and Viruses by Jeff Duntemann, 2005. Paraglyph Press, pages 352. \$25.

*One machine can do the work
of fifty ordinary men, but no machine can do
the work of one extraordinary man.*

- Elbert Hubbard

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
JAN 2005	3	4	5	6	7	8 WEB WRITERS MS OFFICE 
JAN 2005	10	11	12	13 VISUAL STUDIO	14	15
JAN 2005	17 WORDPERFECT	18	19	20	21	22 INVESTMENT
JAN 2005	24 CLIPPER	25	26 MAIN MEETING	27	28	29
FEB 2005	31	1	2	3	4	5 INTERNET HARDWARE
FEB 2005	7	8	9 	10 VISUAL STUDIO	11	12 WEB WRITERS MS OFFICE