



The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 4

April 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
Inside Photoshop CS	Page 4
Apress Puzzle Contest	Page 7
Out for Review	Page 7
The Best Spyware	Page 8
Resume Writer Deluxe	Page 12
March Meeting Report	Page 15
Event Calendar	Page 16

Main Meeting Wednesday, April 27 Southwest Tennessee Community College

5983 Macon Cove, Memphis

MEETING LOCATION

Fulton Room 214

First Floor - Fulton Engineering Building

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

*Plans for the April meeting
were not complete in time
for the newsletter deadline.*

Come and expect a surprise.

Bring along a friend!





The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Hopefully we all know not to open unexpected email attachments, and we can even be reasonably sure that most computer users know a phishing exploit when it arrives in the inbox. Most everyone has heard plenty about these nasty tricks and how to recognize them. Some folks, unfortunately, learned about them the hard way when they clicked a link or attachment and got burned. Being safe has a lot to do with knowing what to watch for and avoiding anything that looks suspicious.

But how safe can we be if a threat is hidden behind something that we all trust and take for granted every day? Is a danger that is impossible to see also impossible to avoid? Robert Vamosi, a Senior Editor at CNET, reported just such a threat in February. New twists on the old networking vulnerability of "domain spoofing" may indicate a new direction in malware and identity theft. Security professionals are calling this new threat "pharming."

How serious a problem pharming may become is still a topic of speculation. Since it is based on an already well-known vulnerability, some professionals, like Richi Jennings at CircleID Security, don't believe that pharming will become a big problem. He believes phishing, viruses, worms, and spyware are all much worse threats.

On the other hand, Michelle Delio at Wired News agrees with Vamosi that pharming has the potential to become a serious threat. Delio interviewed Chris Risley, president of Nominum, an IP infrastructure provider, who stated that "phishing is to pharming as a guy with rod and reel is to a Russian trawler." Phishing traps users one at a time, while

pharming harvests many users with a single exploit.

Both phishing and pharming have the same goal and result. An unsuspecting computer user is directed to the wrong Web site, where illegal attempts are made to gather personal and financial information. Pharming is the more difficult exploit to detect. Everything looks okay from the user's screen. Even when the user enters a URL known to be correct, the computer is directed to the wrong site. That's because pharming often makes use of "domain poisoning," where the correct IP address of a site on a DNS server has been changed and no longer provides correct routing.

Phishing has been alarmingly profitable for criminal elements capable of exploiting Internet technology. Considering the steady increases in online shopping, electronic bill paying, funds transfers, and Internet banking, the opportunities for fraud and theft resulting from pharming exploits can't be calculated. Imagine that every customer entering a bank was instantly and unknowingly "transported" to a duplicate, but fraudulent location. It sounds like something out of Star Trek, but the technology to do it on the Internet already exists, and has already been used a few times.

Although the pharmer have yet to perform "DNS poisoning" that affects the address of a major bank, it was done to other sites during March by exploiting a firewall vulnerability. Taking advantage of IP addresses cached in a proxy server, pharmer redirected customers attempting to go to eBay, Google, and weather.com. The affected users weren't aware that they were at a bogus Web site, and most were unprotected when the

bogus sites installed spyware on their computers. Security professionals who investigated these redirections concluded that this was a trial test. There were only a few victims and the damages inflicted were fairly mild.

Another recent attack was more serious. It wasn't specifically pharming-related, but similar in methodology. In January, an unknown cracker found a way to enter a domain server and change the DNS address of Internet Service Provider panix.com. Since the domain network replicates address changes to other servers, both users and companies with their Web hosting on Panix were denied service until the DNS tables could be corrected. While the change was in effect, DNS look-ups indicated that the ownership of Panix had been transferred from New York to Australia. Panix customers' were redirected to servers in Great Britain, and their email went to a location in Canada.

No identity theft resulted from the Panix DNS change, but while the redirections were being done, if bogus Web pages of Panix customers had been online, lots of confidential information could have been compromised. Other hosts and providers have been similarly misdirected in the past, but not on the scale experienced by Panix. Users were lucky that the exploit was not committed with well prepared criminal intent. The outages and loss of service were annoying and expensive, but not as costly as might have been. The Panix attack proved that DNS poisoning is both possible and difficult to correct.

The one comforting fact in the Panix attack, and in most other DNS exploits recently committed, is that the security breaches exposed already known vulnerabilities. Since then, many networks have patched those vulnerabilities and incorporated other available security measures. Those who believe that pharming isn't a major threat point out that had any one of several safeguards been in place when the Panix attack occurred, the DNS change could never have been made. That's true. The attack was facilitated by human error. But are we willing to bet that there's not another server out there somewhere with a similar or equal vulnerability? Can we be sure that there isn't another hole in the DNS services that we haven't yet found?

Until we are convinced that all systems are invulnerable, we should take pharming and all other threats seriously. Maybe that's a way of saying that no matter how good our defenses seem to be, we still cannot be complacent.

MPCUG Education Services can't offer 100% protection against pharming and other security threats, but we can recommend measures that will keep your computer safe from the majority of malware exploits and cracks. Visit the Wizards' session each month before the main meeting and take home better security.

-0-

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

Inside Photoshop CS

Book Review

**Reviewed by
Vanessa A. Muldrow**

An excellent self-help book for the beginner to the advanced user, *Inside Photoshop CS* provides excellent demonstrations, language and information that is clear-cut and effortless.

Reading this book was refreshing. Having read several self-help, enrichment books over the past years, I found some of them to be too boring, too hard to follow, too many less than impressive jokes and gimmicks, or they lacked a sense of humor at all. *Inside Photoshop CS* is completely the contrary to this. The authors embrace every detail thoroughly with playful humor and simplicity, yet expressing every aspect effectively and efficiently. Allow me to take you "inside."

Chapter zero, yes zero, as in the number zero that means zilch, zip, nothing. Aside from its obvious idiosyncrasy, chapter zero is something the new user of *Photoshop* will find significantly useful. This chapter, "Answers to the Important Imaging Questions," answers some really important questions

that the beginner will find greatly important, such as: what is a pixel, explanation of bitmaps and vector graphics, introduction to the RGB color mode. Each section provides a clear and concise explanation as well as giving tips and notes to better the readers understanding.

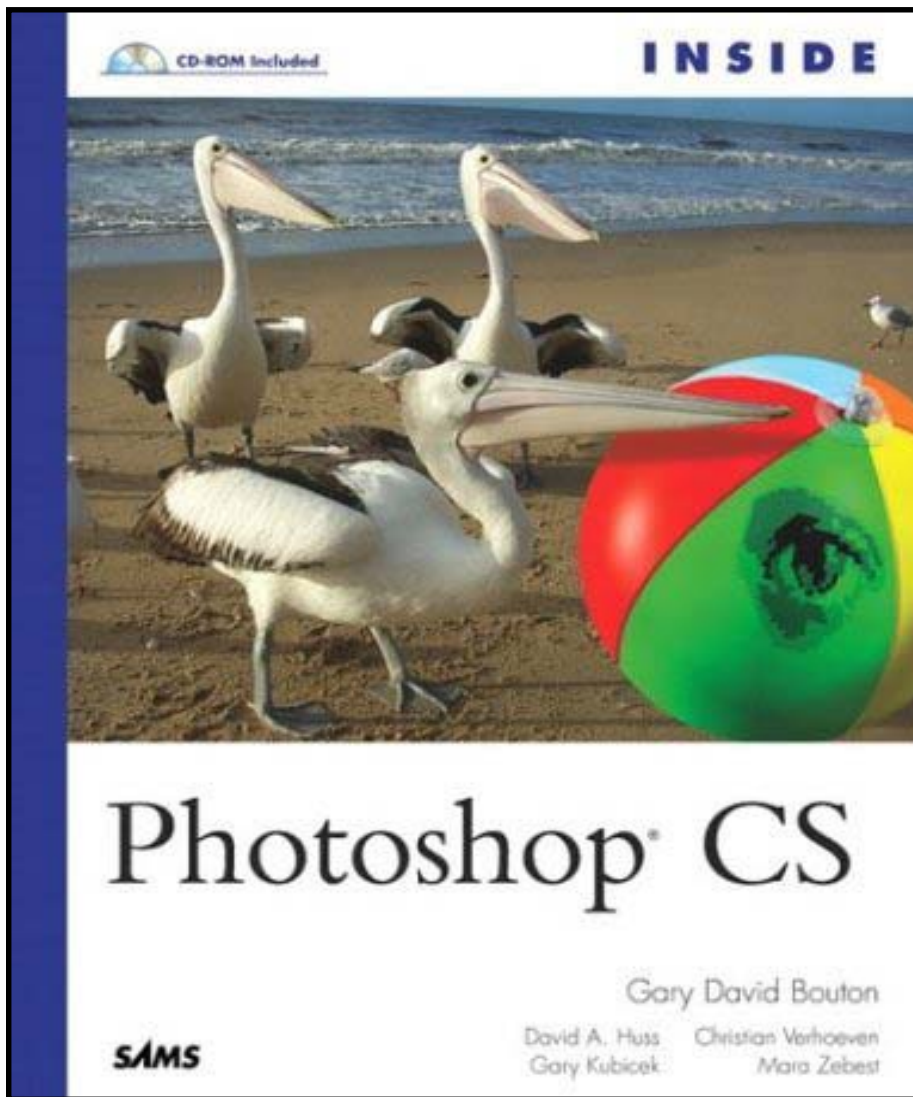
Chapter one opens the reader to *Photoshop* fonts, how to add something new to present images, editing, merging layers, adding text to images and how to save edited text inside of images. In this chapter the reader can now open the CD inserted in the back of the book, this is when it becomes useful (as with all additional chapters). Using the CD in this chapter, the author walks you through a step-by-step process that shows you how to drag a photo onto an existing one and how to flip the photo horizontally.

Chapter two is all about color. You learn how to understand and function with *Photoshop's* CMS (Color Management System) and how to set its defaults, how to create a custom profile, how to create an ICC profile for your monitor, how to use

the color settings dialog box correctly and effectively, how to decide when you need to assign or convert a profile, how to apply color management theories to your work, and give you, the reader, different practices to perform before you print your work.

Chapter three focuses on how you can make *Photoshop* work for you. It involves customizing the software so you can perform operations smoothly, at a quicker pace and in the end you will have produced greater outcomes. This chapter is extremely thorough. The authors suggest that the reader may want to "set aside a whole afternoon with PS CS and this chapter," and I happen to agree.

Part II, *A Hands-On Reference for Creating and Editing Photoshop Images*, consists of chapters four thru seven. In chapter four, the authors guided you through layers and channels. Both are explained in detail and help you become more at ease with working with each of them and their sub-parts. In chapter five, it's all about selections. Here you



digital camera and his or her computer, how to work with picture and photo CDs, how to prepare an image for scanning, how to scan using *Photoshop*, how to scan slides and negatives, how to transfer pictures from non-camera sources and how to convert non-digital images using a scanner. Chapter nine involves the relationship between digital photography and *Photoshop*. In this chapter you will learn ways to load digital images, hear advice from the authors regarding moving from film to digital photography and information about balancing the convenience of compression and the desire of quality and learn about RAW format and about working with Adobe's Camera.

Chapter's 10 thru 13 all involve "correcting, restoring and retouching images." In chapter 10, the reader learns how to select image areas for color alteration, the basic of tweaking color, how to alter the background, how to create reflections, how to add the effects of falling snow and how to add image highlights. Chapter 11 is about Picture CDs and chapter 12 deals with curves and adjustment layers. In each chapter you will learn what each function is, what it does

will learn the basics of the selection process, be introduced to the marquee tools, the uses of the lasso tools and the magic wand, how to use a layer mask, how to make selections quickly and choose the best ones, how to combine selection methods, how to save and load selections for future use and, my favorite part from this section, how to use several selection tools to replace an overcast sky with one you develop *Photoshop*. Chapters six

and seven get you more in touch with your creative side by introducing you to the pen tools and their functions in chapter six and filters in chapter seven.

The next two chapters involve attainment of image basics. In chapter eight, you learn how to load digital images into *Photoshop CS* from scanners, digital cameras, photo CDs and much more. In this chapter the reader learns how to transfer images between a

and how you can use it. In chapter 13, "Keeping up Appearances: Techniques for Retouching Images, you will learn how to "fix" a photo or retouch it by learning how to straighten the photo, improve the color, take out unwanted elements and add new elements.

For those who are ambitious in nature or for those who believe they are ambitious at heart, Part V will be of great interest to you. In this section, the author guides you through steps of retouching, creating, balancing and replacing. In chapter 14, you learn how to retouch a group scene. In chapter 15, you learn how to create a great photo from a not so great photo by understanding what is important to keep and take out, how to correct the color and eliminate blemishes, how to get rid of red-eye and how to paint over parts of the photo. Chapter 16, a particular favorite of mine, teaches you how to "create a cover girl image from an average picture." Ok, so all the ladies now want to try it. In this chapter you learn how to edit unwanted litter from an image's background, how to get rid of shadows and blemishes, how to remove bright colors, how to lay

out a photo with text for a magazine cover. Chapter 17 involves surrealistic *Photoshop* and chapter 18 involves changing the main elements of a picture with new ones.

As you become more and more advanced with *Photoshop*, you will want to advance your skills. Part VI and VII help you do this by guiding you through the steps of dealing with historic photos, typography and page layout, output and working with the World Wide Web with *ImageReady* photographs.

As with Parts VI and VII, Part VIII is most definitely for the mid to advanced *Photoshop* user. In this section, the authors give you a list of ten *Photoshop* tricks and as well as using *Photoshop* with other software applications such as: *Quark*, *Illustrator* and others.

The authors of *Inside Photoshop CS* offer many perks to its reader. The simple format, the detailed photographs and the included CD-ROM allow the user to gain hands-on experience while following along with the book. It makes you feel as though there is an instructor sitting with you, guiding you along. Many may believe this book is more for the

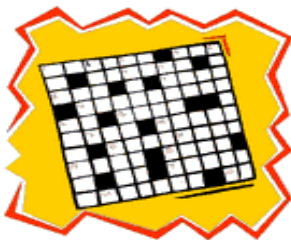
beginner, one who has never used *Photoshop* or who have only used it on special occasions, on class projects or just goofing around. I say, perhaps they are right; however, coming from a person that has used and still uses *Photoshop*, I find this book to be one of the best *Photoshop* books I have come across. This is not a book I would put on the shelf to fill space. I am 100% confident I will use this book many times as I sit down to edit a photo or if not for anything else but for reference which is why I believe this book is great for the beginner to the advanced alike. The contents of this book allow you to do things that you have never done or did not know you could do. So, whether you are a photo editing machine or if you have just heard the name *Photoshop*, *Inside Photoshop CS* will introduce you to new functions, make functions more clear and serve as an excellent reference tool to be used again and again—not to mention friends and family will be impressed to see it on your bookshelf.

Inside Photoshop CS by Gary Bouton. (2004). Sams. 1128 pages. \$ 45. www.samspublishing.com

The Apress User Group Puzzler Contest

During the month of April, Apress is sponsoring a promotion open to all Apress registered user group members in the United States and Canada. The creator of the best Apress puzzle will win a SONY PLAYSTATION PORTABLE. Here's how it works:

Contestants must be 18 years or older and create a small crossword puzzle that incorporates ten different Apress and Friends of ED author last names (no first names) as can be found at <http://www.apress.com> or <http://www.friendsofed.com>



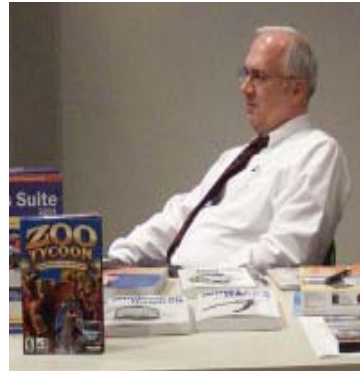
The puzzles should be "five-up/five-down" type crossword puzzles in English with clues like: "A Yale graduate and project manager for the Microsoft Excel developer team; he 'blogs' his way to fame." (Answer: Spolsky)

Submit one puzzle per participant at <http://www.apress.com/userGroups/crosswordpuzzle.html> by April 30, 2005.

Apress will judge all puzzles submitted and choose a winner who will be notified by mail on May 27, 2005. The winner must agree to allow Apress to reproduce and display the winning puzzle.

All current members of the Memphis PC Users Group are eligible to participate.

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
Windows XP in a Snap	Vicki Dabney
Wipe Drive 3.0	John Dodson
Windows Security Handbook	Dorothy Drum
PowerPoint Personal Trainer 2003	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
PC Hacks	John Schuster
PC Hardware Annoyances	John Schuster
Create Your Own Website	Jesse Strauch
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas
Using FileMaker 7	Tommy Towery
Start Your Own Business In No Time	Jin Yang
Photoshop CS	Jin Yang

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

The Best Spyware Money Can Buy

Editorial

by Gil Hennon

Last Christmas there seemed to be a good chance that Congress would pass legislation against abusive spyware. Discovery of more than sixty forms of spyware on computers used by the Energy and Commerce Committee prompted many legislators to scan their own office computers. When they discovered how many uninvited processes they were hosting, they raised a hue and cry, then introduced two different bills in the House of Representatives aimed at putting an end to these invasions.

One bill was bipartisan and took a hard line against all types of software secretly installed on a computer without the approval of the owner. It defined the act as a felony and prescribed heavy fines and prison time. The other bill wasn't as stiff, but did impose costly civil penalties. Unfortunately, both bills have lost momentum in the legislature and are now unlikely to reach the floor for a vote. What happened?

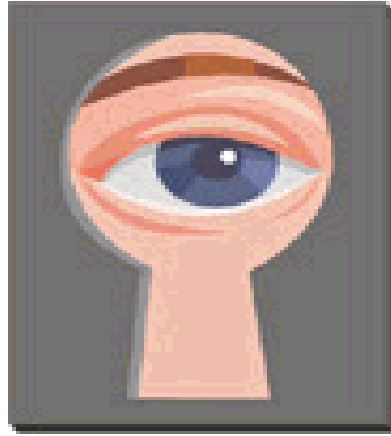
About the same time that Congress cooled down about spyware, many Internet Service Providers (ISPs) and Web site administrators were receiving "cease-and-desist" letters from the legal departments of several companies whose products were being identified as spyware. The tone of these letters ranged from conciliatory to threatening, but the message was the same: Take any references to our software being spyware off of your servers. In several instances, Web sites with no references to spyware at all were threatened with being shut down by court order. The offensive effort by the spyware companies caught many ISPs by surprise, and in a knee-jerk response meant to avoid litigation, they closed down lots of Web sites without determining whether or not the allegations were just. Some of the letters had a slightly different twist.

Rather than demanding that references be removed, they wanted the references edited and their software called something other than spyware or malware. Those two terms tended to evoke threats of slander lawsuits.

Maybe it was just coincidence that as Congress lost interest in spyware and Web sites were being threatened for talking about it, a couple of the most respected anti-spyware vendors quietly quit scanning for *WhenU*, an advertising bot. Both Computer Associates' *Pest Patrol* and Lavasoft's *AdAware* identified and removed *WhenU* in the past, but during January, both of them stopped looking for it. *WhenU* was once listed on *Pest Patrol's* "Most Prevalent Pests" list, but all references to it on *Pest Patrol's* Web site were removed. Even more curious, Aluria *Spyware Eliminator* software used to certify *WhenU* as being spyware free, but after Aluria and *WhenU* formed a partnership to produce other software, Aluria began to detect and remove *WhenU*!

Publicity-wise, the spyware companies have taken the battle over using the term "spyware" to journalists and magazine editors. Brian Livingston's *Windows Secrets* newsletter on February 24th recapped the arguments from both sides, coming to the conclusion that "spyware" is an imprecise term. He recommended using "adware," but didn't rule out any term that computer users like better, such as "crapware." Brian also referenced Eric Howes' excellent article on "junkware" that breaks down into categories all of the variations and catalogs nine specific behaviors typical of this sort of software. If you are into semantics and carefully splitting hairs, visit Eric at <https://netfiles.uiuc.edu/ehowes/www/junkware.htm> for the complete dissertation on nasty software.

Some of the spyware companies are taking notice of the public outcry over secretly installed software and claim they are cleaning up their act. From the other side of the fence, it looks like they have only examined the



complaints and found some loopholes to exploit. One very obvious new twist is spyware that comes with a software licensing agreement, sometimes called a EULA, that is displayed at the time the spyware is being installed. Some of these EULAs have the standard button for the user to click if he or she agrees to the terms of the license. Clicking "No. I do not agree," does not always stop the installation however. *Grokster*, for example, informs each prospective downloader that along with the music sharing application, fourteen or more spybot and pop-up ad bots will be installed. If the user decides to back out at that point, tough luck. *Grokster* will still install as many of its bots as it can before the user can get away.

Reading some of the spyware EULA agreements (if anyone ever does that) can also be a frightening experience. The one that comes with *Claria* (formerly known as *Gator*) requires over 100 page-down clicks to see the entire document. Ben Edelman's spyware newsletter notes that the *Claria* license is 43% longer than the U. S. Constitution! Maybe it takes that many words to nail a user to the wall. If you decide to read a spyware EULA, you will find lots there that is not in your best interests. All of them that we have seen require the user to agree NOT to uninstall the application. Some require that anti-spyware software be removed from the computer. Most require that the user allow the application to install any other software it wants to at any time, or even allow third-parties to

install software. The *Claria* license is typical, and used by other spyware installers, such as *Kazaa* and *GAIN*. *Grokster* displays a license for every additional bot it installs, requiring multiple "I accept" from the user. These scroll by in a small, pop-up text box that does not allow the content to be printed.

Most of us don't like spyware, whether it goes by that label or not. We aren't really impressed by long-winded EULAs, licenses, notices, or agreements either. But, to be fair, if not complimentary, there are a few vendors who make what we call spyware who are up front and honest with the user about what their software is going to do. They are rare and hard to find, but if you are looking for a music downloader, a file sharing utility, or a toolbar to make Internet browsing a little easier, I hope you will compare and choose one of the vendors making an effort to respect your time and your investment in your computer system. Unfortunately, most will not, and if you read their licenses, Web sites, and correspondence with other users, you'll find that they believe you provided your computer for their use and profit. This is marketing in its lowest and most abusive form.

One of the most confusing aspects of spyware is finding a definition that is broad enough to identify the many variations while being specific enough to not include honest and worthwhile advertising. It takes Eric Howes several pages in his document mentioned earlier in this article to describe all of his different kinds of junkware. We need a better, more concise definition. Supreme Court Justice Potter Stewart declined to try to define pornography in 1964, but he said, "I know it when I see it." Spyware is similarly difficult to define, but when your screen is full of pop-ups, your computer barely operates, and your browser will only go to three Web sites, you definitely know you've been screwed by spyware.

Without getting into an "any of the above" or "all of the above" argument,

there seems to be a few characteristics that everyone agrees are abuses typical of spyware. The most obvious is that it is either installed without the permission of the user or permission was obtained using deception. Often the user receives no notice that spyware is being installed, as in the case of "drive-by" downloads that occur only because a Web site was browsed. If any notice is given, the user may be misled into expecting something other than what is installed. The *HotSearch Toolbar*, a product of iDownloads, one of the companies sending out those notorious "cease and desist" letters, is installed from a dialog box that says "Required: Media Player Version 9 Browser Update." The toolbar has nothing at all to do with Media Player, and many unsuspecting users are tricked into downloading and installing the toolbar, which is really a variant of the *Pugi* browser hijacker. Even when notification is truthful about what will be installed, declining to continue may not completely stop the downloads and installations. If a user decides not to accept *Grokster* after reading the license agreement, then *Grokster* will not be installed. However, more than a dozen spyware programs that come as baggage along with *Grokster* will be installed anyway. If this were a non-technical issue, the methods used to distribute spyware would probably be considered an invasion of private property and also illegal. Courts haven't come to any conclusions about spyware though, just as they are not sure how to rule on the electronic impact on copyrights, surveillance, and privacy. The police and FBI must get a warrant to install key logging software on your home computer. Spyware vendors do it every day with impunity and without any warrants. This is wrong.

Once spyware takes up residence in a system, the computer's owner/user loses a significant amount of ownership rights. In some cases, the user may be willing to give up some portion of his/her rights to obtain another benefit. There are legiti-

mate products available for free or at very low cost because they are bundled with advertising and data collection software. They spell out exactly how the deal works up-front without deception. This is "ad ware," not spyware, and rarely does it noticeably degrade the computer's performance. If the user decides the product is worth a bit of inconvenience, then everyone wins. Spyware provides benefits to the vendor, and very seldom benefits the user. The noticeable effect is degraded computer performance as significant amounts of processor and communication time are used by the spyware for its own purposes. The spyware may also open "back doors" into the computer to allow remote users access and control of the system. Sometimes "key loggers" are installed that capture account numbers and passwords, then send these off to a remote collection point. An unsuspecting user can be damaged in many ways by spyware, up to and including outright identity theft. While spyware may promise benefits when trying to get a user to agree to installation, the truth is that the user may only be inviting a thief into the home. Even when spyware is not intended to cause damage, it still manipulates system configurations, corrupts files and registry settings, degrades performance, and facilitates the introduction of more spyware onto the computer. The problems can get so bad that the computer crashes often and hardly any productive work can be done on it. One spyware victim lamented that, "this crap turned my Pentium M into a 286." The spyware vendors say this is a good thing. It shows the owner that an upgrade to a better machine is needed. That would be good for them too, giving them the opportunity to load on more spyware.

Once a user discovers that spyware has been secretly installed, or figures out that the spyware he/she allowed to be installed isn't what was promised, it will probably be very hard to get rid of it. Spyware uses lots of tricks to keep it from

being removed. Usually, no “uninstall” button or program can be found. The exception was a family of browser hijackers that came with a detailed “readme” file on how to get rid of it. This included downloading an “uninstall” utility from a Web site. When it was run, the “uninstall” program actually loaded the computer with a lot more spyware. You won’t find the spyware that infects you listed in the “Add or Remove Programs” Control Panel applet either. If the spyware came with a “host” program, like *Grokster*, it won’t be removed if *Grokster* is uninstalled. Some spyware even disables Windows uninstall functions, so you will be unable to remove any software at all in the future. It probably corrupted or disabled other critical system functions too, so anti-spyware and anti-virus software will no longer work properly. And some really sophisticated spyware runs two copies of itself in memory, constantly monitoring each other, so that if one is removed, it is immediately reinstalled by the other one. There is spyware for which there is no reliable method of removal short of a complete hard drive wipe and reload. Formatting the hard drive won’t wipe out the spyware. There are sectors that a format does not touch, and the spyware knows which ones they are. Only a utility that overwrites every bit on the drive will nuke the spyware.

If you are getting the idea that spyware is really bad news, written by highly talented programmers, and distributed by a very well organized and well-funded group of vendors, congratulations! You win the prize. Spyware products are quickly becoming the worst threats that a PC can encounter. Viruses, worms, and Trojans were kid stuff, done as pranks. Spyware is big business bringing in big profits. There is enough money in it to attract the very best programmers away from legitimate coding. There is plenty of money to unleash cadres of lawyers against detractors and anti-spyware companies. There are profits to

fund the wining and dining of Congressmen and journalists. With the combination of technology, public relations, legal threats, and political lobbying, the spyware vendors have, in just a couple of months, effectively defused all of the public opinion that rose up against their abusive tactics. The potential for profit from spyware is almost impossible to measure, and the big dogs of finance have bought into the game.

Once again, Ben Edelman seems to have found the key. When Ben became curious about spyware while doing some consulting on another matter, he did some eye-opening research into the funding behind the larger spyware vendors. Ben tracked more than \$150 million from established venture capital firms to four large spyware operations. *Claria/Gator*, the largest of the group and possibly the largest spyware house in the United States, is particularly well funded, with a half-dozen venture capital firms financing its expansion.

I haven’t got any great revelation that will make spyware go away. It is the most despicable form of advertising and consumer abuse ever foisted upon an honest public. It invades your privacy, steals your personal information, limits your freedom to surf the Internet where you please, degrades your computer’s performance, wastes your time, and steals your money. If the same things are done to your automobile or another appliance by a vendor, you have a number of public and private agencies and bureaus to whom you can turn for help and recourse. Not so when it comes to your computer and spyware. There are powerful entities at work here with a lot more clout than any of us will ever muster. There are profits to be made with spyware that can’t be interfered with by inconsequentials like governments, populations, and integrity. Money talks, and it certainly talks loudest. Spyware will be with us for a long time. So get used to it.

-0-

IMSI Resume Writer Deluxe 2.0

Software Review

Reviewed by Megan Redmond with Rick Fischer

I just graduated from college. I needed a resume in a hurry. I didn't think I had time to read a bunch of books on the subject, so I tried IMSI's *Resume Writer*.

Is it possible to create the ideal resume from a CD in just a few hours? Here's what I discovered.

Resume Writer is a very useful learning tool for those who are just beginning the hunt for his or her first job. It is not, in my opinion, a good idea to use this program or any of its formats when trying to land an interview with a seasoned professional.

But, the program could serve as a starting point for those who are learning to write a resume.

Three-step process

Resume Writer is organized around three steps. First you input your career information into the *Resume Writer* database. See the dialog box for imputing basic information (Figure 1). There are nine steps in all where data are collected. At the end it will display what it has collected from you. To edit any of this you will need to return to the database dialog.

Figure 1: Step number 2 in creating the database.

Wizard ~ Step 2 of 9

Name... Rick Fischer

Address...

Phone

Email rfischer@memphis.edu

Website

Job search situation

- I am looking for my first job.
- My experience is consistent but short.
- My work experience is erratic, with jobs in many different and non related fields.
- I have time gaps in my employment history.
- My past work history does not match the job I truly want.
- I am near or over 50.
- I have an extensive and consistent work history that includes job titles and salaries similar to the job and salary I currently want.

Help << Previous Next >> Stop

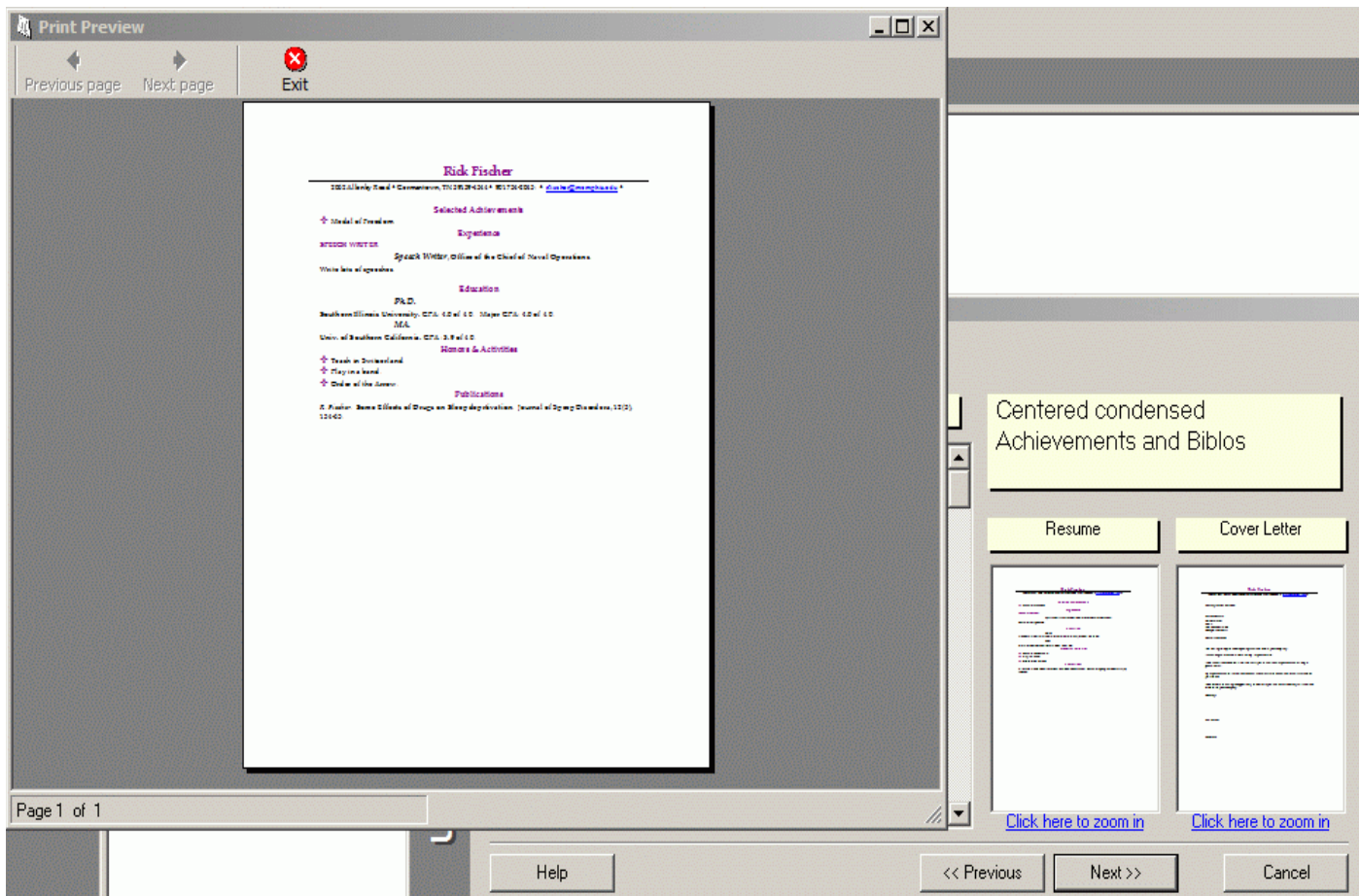


Figure 2: Resume thumbnails and enlarged view.

Once the data are loaded and you are satisfied with the spelling and such, you begin to work on your “presentation package.” You will choose “respond to an ad” or “direct solicitation” to a company. Now, on with another database to create the cover letter and select the format for your resume. You also have the option to print Avery labels. At the end of this step you will have a cover letter and resume. You can have as many presentation packages as you like.

The third step will get you out searching for jobs (on the Web). *Resume Writer* will help you link to Monster.com, Job.com, and hotjobs.com. Yes, you could have done that on your own.

Form and content

Resume Writer has an easy-to-use interface that takes you step-by-step through the process to build what the program designer’s hope will be a perfect resume. It also drafts your cover letter to go with the resume. One sentence in the cover letter for Rick Fischer read: I have a long and successful work history in speech writer.” Obviously, you should proof read what it creates for you. In another presentation package I said that the job title I was interested in was “software tester.” The cover and resume positioned me as a speech writer; no mention of testing software.

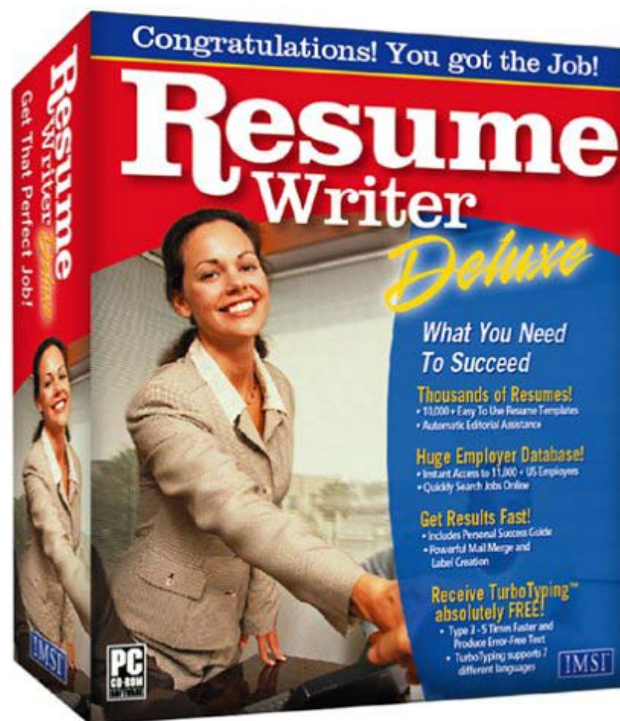
Though the program boasts having over 10,000 different resume formats, who really has the time to go through all of them to find the perfect one? And, yes, you can enlarge the small

thumbnail, but it is tedious (Figure 2).

And, that's a problem. If format is the issue, there's nothing wrong with using the templates that ship with Microsoft *Word* or those available on Microsoft's template Web page. *Resume Writer* can help with content.

But I also have to learn to write in resume style. I felt mechanical as I used *Resume Writer*. Perhaps, that's because I make my living as a writer. We have pull-down menus and lots of wording choices. Are they the right words? Is it really me I am talking about?

When the potential employer reads the resume will he or she think that it is my creation, or the by-product of a pull-menu-program that makes every user/applicant sound the same.



Send me a copy quick!

The program saves your files as a rich text format (.rtf) file. I was hoping to save and send a native Microsoft *Word* document. Note: Under File you have the option to "Save Document as MSWord." It will still be .rtf. Ok, it imports directly into *Word*.

Resume Writer will handle sending your resume and cover letter. It even creates the text in the body of the e-mail that says: "Please see my attachment and cover letter. Thank you."

When the attachment is opened by the recipient, unless, you change it, it's still .rtf and lacks some of the design elements we've come to expect in a *Word* document. That may put you at a disadvantage for the job. That's certainly not what you want.

Overall, I (Megan) thought the *Resume Writer* program was a waste of time. It is just as helpful and simple to use Microsoft *Word's* Resume Wizard for a beginner. I would not recommend that you send the resume directly from this program. Save it. Then import it into *Word*, tweak and edit it, then save it as a .doc file.

Resume Writer Deluxe 2.0 - \$ 15.00 www.imsisoft.com

Editor's note. Rick created the graphics and clarified some of the functions in this review. We wish Megan good luck finding a job in Atlanta.

*So much of what we call management consists in
making it difficult for people to work
- Peter Drucker*

March Meeting Report

Inside **Microsoft**® with Donnie Wilemon

Everyone attending the March meeting took home a Microsoft USB “thumb” drive! Donnie gave out other “door prizes” too, including a copy of HALO 2 for the X-Box. That was only the beginning of a great roundtable session about what is going on at Microsoft and some of what is in store for the future.

All of the members had plenty of questions about XP Service Pack 2, Microsoft’s new AntiSpyware software, and the Trusted Computing initiative that has become Microsoft’s top priority. Donnie described the work being done at Microsoft to make the systems and products more secure and protect users from the many threats of viruses, worms, spyware, and phishing exploits. Trusted Computing is driving all of Microsoft’s development, and will probably cause some popular products, like Internet Explorer, to be upgraded sooner than was originally scheduled.

Another part of Donnie’s roundtable session that everyone enjoyed was when he showed us his favorite “toys,” including his tablet PC, MP3 player, and PocketPC enabled cell phone. Everyone agreed that this was a great meeting. A rousing MPCUG “THANKS MUCHO” to Donnie for a great presentation. We hope he will be able to give us another “Microsoft Update” whenever he has news to share!



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
APR 2005	4	5	6	7	8	9 WEB WRITERS MS OFFICE
APR 2005	11	12	13	14	15	16
APR 2005	18	19	20	21	22	23 INVESTMENT 
APR 2005	25 CLIPPER	26	27 MAIN MEETING	28	29	30
MAY 2005	2	3	4	5	6	7 INTERNET HARDWARE
MAY 2005 	9	10	11	12	13	14 WEB WRITERS MS OFFICE