



# The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 9

September 2005

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

## *The Bridge Staff:*

Editor  
Gil Hennon

Review Editor  
Rick Fischer

Publisher Emeritus  
Les Owen

## *In This Issue*

The School Bell	Page 2
XP Personal Trainer	Page 4
MS Front Page 2003	Page 5
Put 'em Behind Bars	Page 6
Manage Your Money	Page 10
PC Annoyances	Page 11
Out for Review	Page 12
SIG News	Page 12
The Wizard's Tips	Page 13
Event Calendar	Page 14

## Main Meeting Wednesday, Sept. 28 Southwest Tennessee Community College

5983 Macon Cove, Memphis

---

**NOTE CHANGED MEETING LOCATION**

## Thornton Room 104

First Floor - Thornton Office Building

---

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

---

## *September Meeting*

Rick Fischer asks if any members have experience with Desktop Search Utilities. Several of these relatively new tools are available. If you have tried any of these, please join in a discussion on what you liked or disliked about these tools. Bring along a friend!





# The School Bell

## News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Hardship brings out both the best and the worst in people. For the past week, we've seen extreme hardship on the Gulf Coast in TV news filled with death and destruction. Images of looters and shooters in the streets, as well as angry city officials and residents demanding aid. That was people at their worst, and what the news reporters preferred to cover. But from people still there, those doing their jobs despite unimaginable obstacles, we heard a different story. They told us about people handing food and water to passers-by from their homes, emergency shelters set up in stores and hotel lobbies, and medical aid being given in bars and drug stores. These were the people showing their best, and for every looter and whiner there were hundreds of good folks doing whatever they could for others. This is what makes us proud to be their neighbors, despite the self-serving campaign by the news media to sour the public's sympathy for the victims.

Another contingent of the worst people showed up the day after Katrina passed through. A well orchestrated spam campaign attempted to attract computer users to malicious Web sites with offers of breaking news, victim rosters, and where to get help. Instead of information and aid for the hurricane victims and those who wanted to help them, the Web sites installed back doors, malicious code, and keystroke logging software on visiting computers. There were also plenty of bogus requests for donations to non-existent hurricane relief organizations and fake sites that looked like the American Red Cross and other legitimate benevolent foundations. The speed at which these scams appeared and their sophistication indicate that a well-organized effort was behind them. Most of the pieces had to be in place before the disaster struck.

Since similar, though not as well prepared scams appeared following the Asian tsunami earlier this year, it appears very likely that the perpetrators had a system in readiness and merely waited for the next disaster to occur.

The good news is that these spam and infect operations weren't very successful. Several watchdog agencies, including the Sophos anti-virus organization, identified the malicious Web sites and luring spam very quickly, raising an alarm that resulted in many being quickly shut down. Law enforcement investigators are cooperating across international borders to find and disable these threats faster than ever before. Since many online scams are controlled remotely, with servers and Web sites in one country while the operators are in another, the only successful solution is quick police action in both locations.

In the past month, a Minnesota pharmacist who illegally sold prescription drugs and controlled substances through spam from the Dominican Republic was arrested by U. S. authorities. Christopher William Smith's Xpress Pharmacy Direct has been regarded as one of the worst spam offenders by anti-spam lobbying groups for more than a year. His income from the sale of pain-killers and other drugs is reputed to exceed \$20 million. Among the charges for which he has been indicted are wire fraud, distribution of controlled substances, and money laundering. Smith's assets and those of his family and associates were seized by the U. S. District Court in May and included his mansion and \$1.8 million worth of luxury automobiles. In another indictment, the government seized cash, gold bars, and a Hummer H2 from spammer Brad Bournival.

Excellent cooperation and swift work

by Microsoft, the FBI, and the law enforcement agencies of Morocco and Turkey put two of the MYTOB/ZOTOB worm creators behind bars late in August. Microsoft investigators dissected nearly 100 variants of the worm and pieced together clues to its origin. This information was sent by the FBI to the two countries, where Farid Essebar, an 18 year old Moroccan and Atilla Ekici, 21, of Turkey were taken into custody. Essebar went by the screen name "Diablo" and Ekici was known as "Coder," and respectively they financed the exploit and wrote the code for the MYTOB and ZOTOB variants. During August, MYTOB and its variants were responsible for infecting PCs and servers of multi-national companies such as ABC, CNN, and Daimler Chrysler. Final charges against the pair are still pending while investigators follow up on connections with organized crime and a credit card fraud ring. The FBI has identified at least sixteen additional suspects and believe that the crime organization may have been responsible for twenty-one other worms and viruses that have been released onto the Internet. Turkish officials have indicted twelve individuals in the credit card fraud ring that had dealings with Ekici.

Without crossing any international borders, the U. S. Department of Justice identified and indicted a California software developer for violating U. S. Federal Computer privacy laws as well as local statutes. Carlos Enrique Perez-Melara manufactured, advertised, and sold "Loverspy" software to individuals who wanted to secretly spy on another computer user's passwords, email, chat sessions, Web site visits, and instant messages. The software could also alter or delete files, plant incriminating evidence, and control a Web camera attached to the victim's computer. A targeted computer user received an email to visit a Web site to view a greeting card. While watching the animated greeting card, the "Loverspy" software was secretly installed on the victim's PC. More than one thousand people bought "Loverspy" from Perez-Melara, including divorce lawyers and jealous spouses. The phony greeting card site installed the software on more than two thousand PCs. Specific charges brought against Perez-Melara include unlawfully intercepting electronic communications and obtaining unauthorized access to protected computers for financial gain. The charges carry a maximum of five years in prison and \$250,000 fine for each of thirty-five counts. Four accomplices have been arrested and charged on two counts each, but Perez-Melara disappeared from San Diego in 2003 and has yet to be apprehended. He may also be indicted in six other states.

The law is finally coming down hard on spammers and scammers. If you have problems with spam, viruses, or worms, visit the Wizard session before the main meeting each month. You don't have to fight the bad guys alone. And remember that there are a lot more good guys than bad guys too, in spite of what TV news reporters might tell you!

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

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

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

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

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

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

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

# Windows XP Personal Trainer

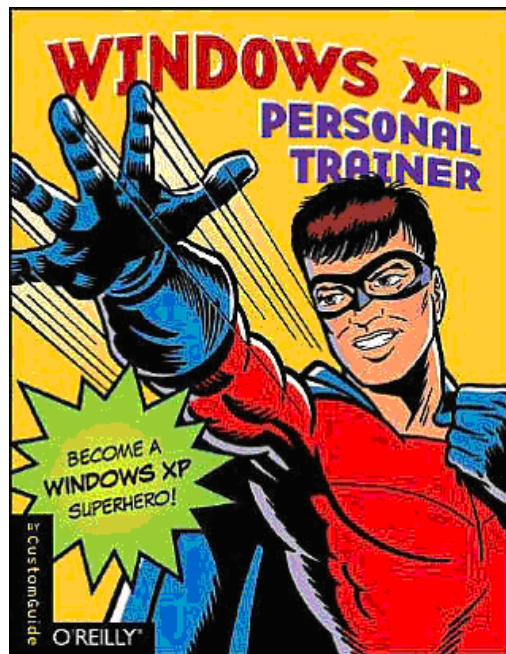
Book Review

Reviewed by  
Vanessa A. Muldrow

So, you are new to *Windows XP*, uh? Well, there is no need to worry because with *Windows XP Personal Trainer* you can “become a *Windows XP* Superhero,” at least so says its fully animated cover that bleeds cheesy and juvenile. Despite its caricature of a modern-day Superman, *Windows XP Personal Trainer* is a fully-interactive book with understandable language, quick references, quizzes and easy-to-follow steps geared to the novice, but it does not lack stimulating topics for the skilled.

From the beginning, the authors of *Windows XP Personal Trainer* guide the new user through the beginning stages of how to use *Windows XP*. In lesson one, *The Fundamentals*, the authors introduce you to the new components of *XP* including the *Windows XP* screen and the *Windows* interface. You’ll learn how to log on to *XP*, use the mouse to point, click-double-click and right-click-drag and drop, use the keyboard and exit *Windows* and turn your computer off.

In chapter two, the authors guide you through the steps of starting a program, learning specific parts of a window



and window options, including: how to minimize, maximize, restore, move, close, resize and alternate between windows.

In the following chapter, the authors introduce us to working with a specific program. You learn how to open a menu, use a toolbar and fill out a dialog box. You’ll enter text into *WordPad*, as well as edit, save, open and print it, along with other common formatting commands. One important topic covered within this chapter is “Getting Help with Contents.” This section introduces us to the *Help* feature, in case problems arise.

Chapter four consists of information about files and folders – from opening a folder to creating and using a compressed

folder, everything a new user would want to know about this topic the authors cover.

The next two chapters are about customizing. In chapter five, the author touches on using the *Windows* classic Start menu and classic appearance. Chapter five also discusses how to move, resize and hide the taskbar. In chapter six, the topic turns a bit fancier. We learn how to customize *Windows XP*. This includes learning how to change the date and time, adjust the volume controls, change the color scheme and appearance, add wallpaper to your desktop background, add a screen saver and more.

Do you like free? Well, if you do, chapter seven’s topic will feed your empty pockets. In this chapter, the authors introduce “The Free Programs within *Windows XP*.” The authors help us understand what the “free programs” are and how they work. You’ll cover: the calculator, sound recorder, paint feature, games and character map.

Chapters eight through 13 are for the skilled user. Topics covered in the final chapters are: working with pictures and multimedia, optimizing and maintaining your computer, exploring the Internet, work-

ing with passwords, logons and user accounts, networking with *Windows XP*, setting up networks. Although these last chapters may not be of interest to the new user right away, with the knowledge gained from previous chapters and the simplified examples and discussions you will learn these techniques in no time.

*Windows XP Personal Trainer* is a must-have for

anyone new to the *Windows XP* operating system. With its captivating, well-written content chapter after chapter and section after section, it left me feeling confident that I could do this – and, all without undecipherable examples and complicated computer-techno language. Today's software books should follow *XP's* lead. It is one of the best computer training

software books written today!

O'Reilly Media. \$29.95

O'Reilly User Group Discount: 20% on all O'Reilly, No Starch, Paraglyph, Pragmatic Bookshelf, SitePoint, and Syngress books and conferences when you order direct. Include your User Group code: DSUG. Go to: [www.oreilly.com](http://www.oreilly.com)

---

# Microsoft FrontPage 2003

---

*Software Review*

Reviewed by Chad Kitchens

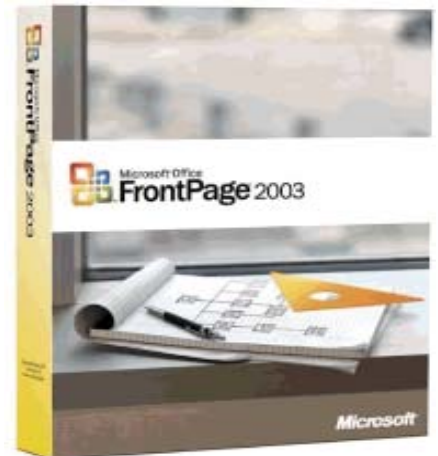
Microsoft has released *FrontPage 2003* as the newest version of its popular Web development and publishing software. This new release brings with it changes to this familiar office product.

It looks like Microsoft has concentrated on adding improvements that would aid only those who are already familiar with Web developing in this version – as opposed to the other versions of *FrontPage*, where those non-computer-savvy types out there were the main focus. One of these improvements is the **quick-tag** feature. I especially like this feature. It keeps people like me from needing a degree in computer science to understand the basic concepts of creating a decent home on the Web. Along with the use of **intelli-sense** tag completion, it makes adding simple tags idiot-proof. Intelli-sense also reveals other options to you as you type, giving you more ideas for use in your site.

My favorite feature of Microsoft *FrontPage 2003* has existed in all of its versions, but is improved upon in the newest 2003 release – the what you see is what you get (WYSIWYG) interface. You see immediately how your site will look from the preview panel without having to constantly publish, edit, and then re-publish your files. When altering the page straight from the design view becomes less than adequate, in *FrontPage 2003*, you can split your screen and view the preview pane along with a pane devoted to displaying and editing straight HTML code. By viewing both, it ensures that code is entered correctly because you can see the actions of your changes to the HTML right there on the same screen in the preview pane. You can also split your view into other combinations including design and preview panes.

The new version helps to make the addition of java-script actions easier, like the **mouse-over** and **on-click** features. The downside is that unless you know about it, you probably won't find it. Microsoft has buried this feature in a "behaviors" link.

Microsoft FrontPage 2003. \$199. [www.microsoft.com](http://www.microsoft.com)



# Put 'em Behind Bars

*Editorial*

by Gil Hennon

According to an old saying, there's more than one way to skin a cat. These days, it seems there are more ways to get skinned than there are cats! Right at this moment, your computer may be working harder for someone else than it is for you. It could be sending your confidential information, such as bank account numbers, passwords, credit card PIN numbers, and the contents of your email messages to remote servers. It might be logging every key you press and sending the log files to a "master control" location. Even if it is not doing something illegal, it could still be keeping track of what you do, where you go online, and what products you bought or examined and giving that information to a server that sells marketing data.

How would you know if your computer is leading a double life? You can't ask it—there is nothing it would put on the screen to tell you what it is doing in its spare time. But if you have failed to install critical system patches, forgotten to update your virus and worm definition files, or neglected to clean off spyware, then there is a very good chance that your computer now serves more than one master. It has become part of a "botnet" or "zombie network" controlled by one or more people for the purpose of gathering information about you.

A typical infection scenario begins with a user ignoring or forgetting to keep critical security components up to date, leaving a path into the system that a malicious program can find and exploit. In the past, most evil software arrived with eMail, and the computer user had to open an attachment before being at risk. Malicious eMail attachments are now just about a thing of the past. Infectious soft-

ware has become highly sophisticated. Currently successful infections usually contain many different files rather than one single virus or worm, and these require an installation process very similar to legitimate software. Attracting a user to a malicious Web site provides a big advantage over eMail attachments:

First, the computer can be examined on arrival. Since every machine is unique in one or more ways, the infecting entity gets a chance to find out what kind of operating system is in use, if any useful applications have been installed, and what kind of hardware peripherals are attached. Certain combinations of software and hardware may determine whether the computer would be most useful for forwarding spam, gathering user data, or participating in a coordinated attack on other botnets or Web sites. At the same time, the computer is probed for vulnerabilities that allow the system to be controlled remotely.

Second, if the malicious site has been well engineered, it will be attractive and interesting enough that the user will loiter there long enough for a combination of nasty tools to be installed. These might even include backup software that can be activated if the primary infections are discovered and removed. The tools can also be tailored to fit the configuration that was identified during the first step. When the user decides to leave the Web site and go elsewhere, either the software to turn the computer into a bot or zombie has been completely installed, or stub loaders are in place that will download and install everything later, when the computer is idle, but still running and connected to the Internet.

Another infection method that is proving to be very popular is Instant Messag-



ing. Many individuals and businesses have found IM to be very useful, in spite of the fact that it travels on an almost completely unprotected channel between computers. The peer-to-peer (P2P) networks that carry most instant messages use open, unencrypted public standards. Botnets that operate over P2P networks are very difficult to find and shut down. Instant Messaging provides an easy route into a computer to install worms or Trojan Horse software that collect data, then the Instant Messaging communication channel can be used again to send the information to the controlling server. Stealing credit card and banking information by Instant Messaging has become a subsidiary industry. With the right connections, you can purchase access to the database servers and browse through thousands of accounts and choose the ones you would like to exploit. Other servers keep track of business conversations and sell the content to industrial spies. Some of the information brokers who operate these servers are bold enough to advertise their products in Usenet newsgroups and criminally-oriented mailing lists.

Vulnerable computers that don't get tangled in an Instant Messaging trap are most likely to become ensnared in a botnet, where they can be used for a variety of purposes. Gathering confidential information, key logging, and forwarding spam are the most lucrative uses of a botnet, but some are used to wage "cyber war" on other botnets, usually by launching Denial of Service (DoS) attacks

against the controlling servers of a rival botnet.

DoS can also be used against the Web sites of legitimate corporations and organizations. Yahoo, Google, eBay, Microsoft, and Bank of America have all been plagued by DoS attacks from botnets in the past year. Most botnets are populated with eight to ten thousand individual zombie computers. When this many computers simultaneously attempt to communicate with a single server, responses cannot go out as fast as new requests come in. The server comes to a halt as unprocessed requests back up in the queue. Server administrators call it a "meltdown." Occasionally several botnets will be consolidated for a special purpose. At least once a botnet of fifty thousand zombies was created as an experiment, so super botnets are possible, but difficult to control. The damage that one could do is hard to imagine.

One creative individual set up a botnet specifically to cheat in online games. His force of zombies probed the Internet for other computers with the "Diablo II" game installed, then stole important objects that a player had earned or found and put them into designated places in the game's virtual world where the botnet master would know where to find them. Then, on eBay, he auctioned the location of the objects to other players.

While many botnets are established and expanded by infecting PCs with viruses or worms, one well-known spyware house found itself in trouble with the law for installing software to create a spam-forwarding botnet with an additional illegal payload. Like a bad penny, the Cool Web Search (CWS) spyware empire comes back to haunt us regularly and usually with some new twist of tactics that the anti-spyware products aren't yet prepared to handle. Those who have already encountered CWS know that it corrupts a PC's system settings in order to "hijack" the browser

and force all Internet activity to Web sites controlled by CWS or its associates. Most of these sites are pornographic or sites selling various products, and there are literally thousands of sites all over the world associated with CWS. Browsing to one of these associate sites, either accidentally or intentionally, is like painting a target on your computer. Abandon hope, all ye who enter here!

Every PC that visits a CWS associate Web site comes away with more than the user ever expected. Even having the current operating system critical patches and up to date virus and spyware definitions can't protect a computer from all of the CWS surprises. Their software changes often, sometimes several times per day, and no anti-virus or anti-spyware product can keep up with all of the variations. A PC with vulnerabilities will get even more attention there—as many as forty-five different spyware and Trojan programs have been installed on a previously clean computer with just one visit to a CWS associated Web site. Anyone who has been there can also tell you that CWS is the dickens itself to eradicate. They use every trick in the book to protect their software once it has taken control of a PC. Most infected users had to finally resort to a complete system reload in order to get rid of CWS.

Even using all those nasty tricks, CWS has, until recently, kept its toes on the line between legal and illegal exploits. It takes over a computer and limits its use in many ways, but remained within the gray area that law enforcement has to ignore. Then, early in August, researcher Patrick Jordan at Sunbelt Software Inc., an up-and-coming anti-spyware company, deliberately allowed a test PC to become infected with the latest version of CWS. What surprised him was that one of the Trojan programs installed with CWS immediately turned the PC into a spam zombie and began to make calls back to a

remote server. This was unusual behavior unlike any CWS infection he had seen before. Patrick successfully logged into the remote server and found that it was selling something; it was selling confidential information, and that information was being harvested by a sophisticated form of keystroke logging. The calls he had seen going to the remote server were reports of his own activities!

Additional investigation by Patrick and other Sunbelt Software researchers uncovered usernames, passwords, real names, addresses, bank and credit card account numbers, and even transcripts of chat room conversations being collected and sold on the remote server. Names and passwords that could be confirmed as belonging to active accounts on eBay were available for sale. One of the bank accounts for which credentials could be purchased was a major corporation that had, at the time, over \$350,000.00 in the account. As Sunbelt cooperated with the FBI in the investigation, it became very obvious that they had uncovered a “massive identity theft ring.”

While the ID theft server itself was located in Texas, the domain names it hosted were located outside the United States. Sunbelt's president, Alex Eckleberry, called the server a “massive repository of stolen data.” They were able to watch it replenish its storehouse of information in real time, and Eckleberry said that the huge size of the log files being handed indicated that thousands of PCs were reporting back regularly. Eric Sites of Sunbelt, who also investigated the stolen ID sales Web site said that, “the way the data is laid out, the quality of it—it's very easy to go through it and use it for nefarious purposes.”

The Trojan installation by Cool Web Search was not typically what anti-spyware software products look for. Had it not been for Patrick Jordan's sharp eyes and curiosity about something that didn't

look quite right, the identity theft activity might have gone undetected for some time. Being part of an installation process that includes many obvious spyware programs also aids in concealing the Trojan infection. And rather than being a run-of-the-mill keystroke logger, this one hides what it is doing by using the Windows clipboard and the "Auto-Complete" feature in Internet Explorer, which remembers account numbers and passwords and fills them in automatically as a convenience to the user. By taking information from operating system components rather than from the keyboard buffer, the CWS Trojan program wasn't triggering any of the alarms that watch for suspicious activity inside the PC.

Another big advantage to the Trojan using the "Auto-Complete" feature was that the data it captured was already labeled and sorted. Rather than the collecting server having to figure out what part of the captured strings of characters were account numbers or other confidential information, it was already identified as such. The log files being sent to the remote server contained standard labels for each piece of data. Harvesting the important stuff was merely a matter of quickly scanning the logs for the right labels. This kind of efficiency was very important because of the massive quantity of data constantly coming in. Hundreds of thousands of infected machines were sending in log files hourly or whenever the file reached a pre-determined size. During their investigation, Sunbelt researchers saw confidential financial details of thousands of customers at about fifty international banks. There was sufficient authentication credentials available to get into those victims' accounts. They also saw credit card account numbers, expiration dates, security codes, names, and addresses. Everything that a criminal needed to use the credit card account immediately was right there and ready to

buy.

This was the first instance of this type of Trojan program being used in identity theft operations. It has been used in the past by pornography and software pirate sites. Sunbelt Software's researchers believe that the Trojan and its server had been harvesting confidential information for about three weeks before Jordan noticed it. Eric Sites summed up how easily an innocent victim can be infected by CWS. "Type in a Web link and your machine is infected. You do not have to click on anything. The Web site forces the installation. This version of the Trojan is very successful. It is small, hard to detect, the file has a very innocuous name and does not cause any problems to the machine." The CWS Trojan is a nightmare for computer users. Until Sunbelt and the other anti-spyware companies developed definitions to identify and disable the Trojan, it is doubtful that the victims had any ideas that their PCs were infected.

Sunbelt's findings about CWS and the remote server have been provided to the FBI and an investigation is in progress with cooperation from law enforcement agencies in other countries. Some doubt exists on how deeply the Cool Web Search organization is involved in the identity theft operation. They do install various types of software for paying third-parties along with their own browser hijacker and spyware, so there is a possibility that the CWS organization was unaware that something they were handling had illegal purposes. CWS has been careful to stay just within the law in the past, so the Trojan is not typical of what their developers produce. Regardless of whether or not CWS becomes implicated in the identity theft investigation, there won't be much sympathy for them. Just about anyone who has been infected with CWS would like to see that organization get what's coming to it.

Book 'em, Dan-O! Put 'em behind bars!

# Managing Your Money and Investments with Microsoft Excel

## Book Review

Reviewed by Rick Fischer

I've been intrigued by financial models for years. It probably dates back to a graduate class I took at the University of Southern California in the 1970s called deterministic models for decision making. We did everything by hand (and small calculator), but I could see that one day computers had the potential to bring these powerful tools to just about everyone.

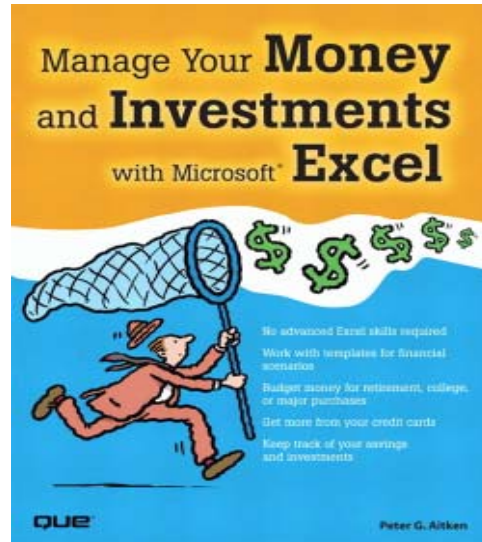
Of course, that day is here.

Although most of us know there are some slick tools buried in *Excel*, few actually put them together in ways that represent real work.

Peter Aitken has done the research and put together some great *Excel* templates that help the average user solve real financial problems. And, he provides it on CD and explains it in his book. What more could you ask for?

### What's inside?

You get 22 templates covering various aspects of handling money and investments. Each template comes as the stand-



alone template and as a companion template with the data filled in as an example.

Some of the calculations parallel what you would get with Microsoft *Money* or *Quicken*, e.g., keeping your check register. Others help us with decisions like: should we rent or buy? Should I refinance my home mortgage? Do I have enough money saved to retire?

But this is much more than a set of templates with instructions. As you go through the chapters you *learn* about each of the topics. So, it's like Lou Dobbs meets Bill Gates.

That makes it very suitable as a gift for youngsters approaching adulthood. It would be a

great text for a personal finance class. My son is wrestling with many of these issues right now!

What user group members will appreciate is the explanation associated with each template. You can disassemble the template and fiddle with it (after you unprotect it). That way, you can modify the template and/or create entirely new functions built around the things you liked about what Aitken's design.

I modified his retirement template substantially to allow me to see a worksheet of the inputs to the main planner. Also, I plan to re-build my survey "sample size" template using principles I learned from this book.

I am very pleased with this book. I wouldn't be surprised to see this concept replicated for topics beyond money and investing, e.g., reasoning using probabilities and templates for the building trades.

Managing Your Money and Investments with Microsoft Excel by Peter G. Aitken. 2006. Que. 276 pp plus CD. \$25

# PC Annoyances, Second Edition

Book Review

Reviewed by John Schuster

I seem to make a habit of reviewing books that can't be reviewed. Don't misunderstand me. I don't mean I can't write about it. I only mean that, since it covers a great many topics, it doesn't lend itself to reviewing in the same way as might a tome entitled *Mastering Microsoft Excel*.

The best use for this type of book is to keep it near your computer and, when confronted with a problem, look at the index of this (and similar reference works) to try to solve the problem.

About the best that I can do is to look in the index and find a couple examples of problems that this volume addresses. Fair warning: sometimes the solutions require shareware or even commercial software. As a convention, this book uses "snipurl" to provide short links to what can sometimes be tediously long URLs.

1. Ever had to reinstall *Windows XP* and gotten annoyed at having to reinstall all the service packs separately?

The book points you to three sites that give detailed instructions for incorporating the latest service pack into your installation. The book doesn't tell you, but the term for this is "Slipstreaming." The sites are: BARTs page at <http://snipurl.com/bootcd>, HelpWithWindows.com at <http://snipurl.com/> Neroburn, and TackTech at <http://snipurl.com/roxiocd>.

2. How many of us have VERY long favorites lists and have no clue as to which links may be bad?

Enter AM-DeadLink, a free utility that you can get at [http://snipurl.com/am\\_deadlink](http://snipurl.com/am_deadlink).

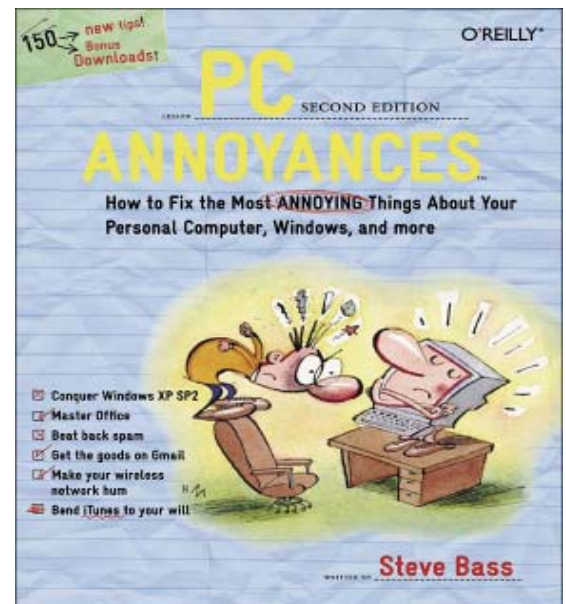
3. I have lots of MP3 files in a folder and would like a list of them to e-mail to my sister.

Try PrintFolder 1.2, a free utility (also works for other types of files) whose purpose is to save or print a list of files from any folder. Get it at <http://www.oreilly.com/pcannoyances>

That is a small sampling of the items covered in this book. The index, alone, is 12 pages long. This will give you some indication of the breadth of coverage. All in all, I consider this a reference book worth having and will be keeping it near my PC for that quick solution I sometimes need.

PC Annoyances, 2<sup>nd</sup>. ed. by Steve Bass. (2005). O'Reilly. 252 pages. \$20.  
<http://www.oreilly.com>

O'Reilly User Group Discount: 20% on all O'Reilly, No Starch, Paraglyph, Pragmatic Bookshelf, SitePoint, and Syngress books and conferences when you order direct. Include your User Group code: DSUG. Go to: [www.oreilly.com](http://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  
Teach Yourself GoLive 5 in 24 Hours  
Teach Yourself Adobe Photoshop CS  
in 24 Hours  
TIVO Hacks  
Home Theater Hacks  
Windows XP in a Snap  
Wipe Drive 3.0  
Windows Security Handbook  
Smart Home Hacks  
The Little Web Cam Book  
Microsoft Works 7.0  
How to Use Microsoft FrontPage 2002  
The Complete Idiot's Guide to Starting  
A Business Online  
User Interface in C#  
Maximum PC 2005 Buyers Guide  
Windows XP Personal Trainer  
Windows XP Pro (book)  
PC Hardware Annoyances  
Create Your Own Website  
Macromedia (book)  
Windows XP (book)  
Using FileMaker 7

Greg Adams  
Allison Banks  
Judith Bogan

Jacob Burke  
Osborne Burks  
Vicki Dabney  
John Dodson  
Dorothy Drum  
Megan Hefner  
Mike Heinrich  
Jim Ingram  
David Levine  
David Levine

Jim McGee  
Vanessa Muldrow  
Vanessa Muldrow  
Daniel Notowitz  
John Schuster  
Jesse Strauch  
David Stowell  
Terry Thomas  
Tommy Towery

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

# SIG News

## Hardware SIG Report by Jim Ingram

We met on Aug. 6th at the Poplar-White Station Library. We had two visitors who became members. Brenda and Ted Williams brought their CPU to the meeting for our wizards to evaluate. Their PC was evaluated, optimized, etc., and some problems were solved. They went away quite satisfied with the help and recommendations that they had received. We meet at the library at 10:00 AM on the first Saturday of each month—holiday weekends excluded, such as Labor day.



*The real problem  
is not whether  
machines think,  
but whether men  
do.*

*- B. F. Skinner*

# The Wizard's Tips

---



When Windows is installed on a PC, some basic management and diagnostic tools are also installed, such as a font management tool, printer and network diagnostics, and rudimentary utilities for adjusting the system configuration. Most users are never aware that there are many more useful and powerful tools on the Windows installation CD ROM. They are the Windows Support Tools and they are not part of a normal installation. They must be installed separately. Many of these tools are very useful, and one that the Wizard uses often is dupfinder.exe, the Windows duplicate file finder.

Before you can use the duplicate file finder, you have to install the Support Tools. It's easy. Just insert your Windows XP installation CD ROM. If it tries to start up automatically, click EXIT. Then open My Computer, right click the CD player, and choose EXPLORE. Go to the \support\tools folder and double click SETUP.EXE. Answer the typical questions and choose a COMPLETE installation. The Support Tools will be installed in the \ProgramFiles\Support Tools folder.

Now you're ready to find and clean out all of those duplicate files on your hard drive. Double click dupfinder.exe. It has a convenient Windows interface where you can select directories to compare. When duplicates are found, names, file sizes, and creation dates are displayed. The duplicate file finder allows you to delete or rename the extra copies. If you are unsure that a file will not be needed later, you can rename it until a determination of its value can be made. Note that the Wizard never deletes or renames files in the Windows folder, or any of its subfolders. Neither should you.

## 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
SEP 2005	12	13	14	15	16	17
SEP 2005	19	20	21	22 	23	24 INVESTMENT
SEP - OCT 2005	26 CLIPPER	27	28 MAIN MEETING	29	30	1 INTERNET HARDWARE
OCT 2005	3 	4	5	6	7	8 WEB WRITERS MS OFFICE
OCT 2005	10 	11	12 	13	14	15
OCT 2005	17	18	19	20	21	22 INVESTMENT