



The Bridge

The Journal of the Memphis PC Users Group

Volume 20 Number 6

June 2004

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
The Wizard's Tips	Page 3
Turbo Backup 3.2	Page 4
Apress Books	Page 5
May Meeting Report	Page 6
Secure Clean 4.0	Page 7
Go Phish!	Page 8
Managing Data-MS Excel	Page 12
Out For Review	Page 13
Event Calendar	Page 14

Main Meeting Wednesday, June 23 Southwest Tennessee Community College

5983 Macon Cove, Memphis

MEETING LOCATION

Farris Meeting Room C

Second Floor - Farris Building

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

JuneMeeting - Virtual Reality

Gil Hennon will explain the technology that makes it possible to put objects and people in places where they aren't, including video demonstrations of the Total Immersion product from D'Fusion of Suresnes, France. These demos were highlights at the last Scottsdale Electronic Technology Show and knocked the socks off Gil and other viewers when D'Fusion's optical trickery was recently shown here in Memphis. Come and see why you may never again be able to believe what you see!





The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Which worm was the worst so far this year? Was it Slammer? Was it Blaster? Some security professionals believe it was the Witty worm.

What's that? You never heard of Witty? It didn't get much attention when it struck last March. After all, it only infected about 12,000 computers. But what makes Witty special is that it infected 100% of the computers it targeted. It also moved extremely fast, completing all of those infections in less than an hour. And while it was on the loose, it destroyed the hard drive data on every computer that it infected.

Bruce Schneier, the Chief Technology Officer at Counterpane Internet Security, Inc., raised the red flag on overlooked Witty. After studying the worm, he found ample reason to declare it the most evil piece of code he has ever seen. Bruce is also afraid that Witty is only a hint of much worse to come.

The Witty worm infects across the Internet using a unique IP address generating utility. It examines each computer it encounters and only infects those running the BlackICE firewall. That's why it didn't infect as many machines as Blaster and Nimda, but it did infect every vulnerable computer on the Internet that was running BlackICE firewall software. Witty exploited a security flaw in the firewall—a flaw for which there was already a corrective patch. Every unpatched host around the entire world was infected within 45 minutes after Witty was publicly released.

Besides being a perfectly targeted, nimble infector, Witty left a trail behind of unbootable computers, inaccessible hard

drives, and corrupted data files. It randomly erased 64 Kb sections all over every drive it could find, damaging both system files and data. Like the worms that attacked Microsoft vulnerabilities, Witty took advantage of users who procrastinated and did not install critical security patches when they were available. Twelve thousand BlackICE firewall users learned the hard way why it is extremely important to keep current with critical security patches. Don't let your guard down! Bruce Schneier and his security conscious peers believe plenty of Witty variant worms are getting ready to attack other applications with security flaws.

Changing the subject entirely and more pleasantly, many Memphis PC Users Group members will remember Gene Barlow of User Group Relations, Inc. Gene visited our group many times over the past years representing PowerQuest and demonstrating Partition Magic, Data Keeper, and Drive Image. He was and still is a recognized guru in the areas of backups, security, utilities, and Windows in general.

These days, Gene is on a new "quest" with the opening of usergroupstore.com, and I quote his own words of what the site offers. "We plan to make this store a learning experience for you. Along with the store items, you will find educational materials, technical articles, and user group evaluations of the various products. So, spend a while browsing the shelves and learning about the technology behind these exciting products.

"To help introduce this user group store, we are offering some great bundle

prices on many of our most popular products. We also expect our popular PowerQuest products to go up in price as we negotiate a new contract with Symantec. So check out the great prices now and get your order in quickly to take advantage of these grand opening specials.

"The user group store is divided into six different departments with many exciting products in each. When you decide on which items to purchase, click on one of the "Buy Now" buttons to be taken to our secure web order form. Complete the order form including the special order code of UGUGS04. We will receive your order shortly after you submit it. We normally ship all products by the following morning. So place your order today and you should have your products in just a few days."

So, whenever you are looking for high quality software, be sure and compare prices at Gene's user group store - www.usergroupstore.com. Don't forget to enter the special order code UGUGS04 to get his best price. Gene also welcomes comments and suggestions by email to gene@ugr.com.

For another good deal, be sure to join the Wizard session each month before the main meeting. Bring your computer problems to the MPCUG Wizards crew and let their years of experience guide you to the best solution. They really know computers!

The Wizard's Tips

One often overlooked useful tool in Windows is the "Send To" folder. It is one of the tools that appears on the menu when you right click on a Windows icon. The default destinations set up during the Windows installation are the floppy drive, the "My Documents" folder, and the Desktop. Some applications also put their shortcut in this folder, but many do not.

You can add a shortcut to any folder or application to your "Send To" folder. "Send To" is located in your "Documents and Settings." Open the "Send To" folder, then drag a shortcut from another folder or application into it. If you have a couple of folders where you store lots of files, put shortcuts to them in "Send To" and pop new files into those folders with just a quick right click.

I also put a shortcut to "Notepad" in my "Send To" folder. Then, when I see a readme.txt or other file I want to read, I just right click and "Send To" Notepad.



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

TurboBackup 3.2

Software Review

Reviewed by Rick Fischer

In my review of TurboBackup 2.2 in January I made several suggestions on how the product might be improved. That's one of the perks reviewers have. You should also know that all our reviews are sent to the vendors immediately after the newsletter is released.

When I sent the January issue of the *Bridge* to Yao Chu at FileStream he responded immediately. "Thank you for your review and suggestions. Sorry that we beat you to it. It seems, however, all your wishes have come true."

Chu then outlined the list of changes in version 3.0:

- backup data, files and folders directly to CD-R/RW, DVD (+/-) R/RW without additional software
- backup music files (.wav format) directly to Audio CDR without additional software
- added emergency backup format (.tbz) with

drive information

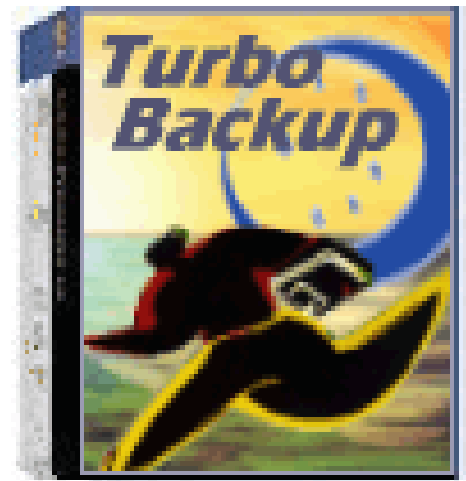
- added duplicate files and folders format without compression
- added *Outlook* template for single-click or scheduled backup
- added "NT System State" template (ntbackup) for backup
- added backup LOG file to journal and track backup activities
- completely updated HTML Help
- new online Help with How To's at www.filestream.com/turbobackup/help

Wow! I didn't wish for all of these, but I did wish for direct copy to CD and an alternative to printing out the Help files as a manual.

So, how does it work in practice?

Well, the new "how to's" on the Web are the same as what you will find in the Help file in the program. You won't need to go both places. I still prefer a manual, and it remains on my wish list.

How the changes in the



program were implemented took some getting used to. A lot had changed. I think it would be easier had I not used a previous version. My understandings from ver 2.3 led me down some wrong paths at first.

I easily saved my files to the C: drive and to a zip disk. After I got oriented I was able to burn files to my CD.

You know you need to do regular backups. Give *TurboBackup* a try.

\$29.95 special price

<http://www.filestream.com/turbobackup>

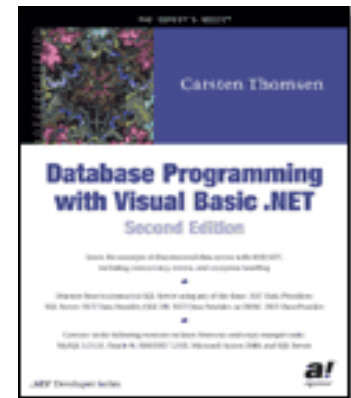
***Results! Why, man, I have gotten a lot of results!
I know several thousand things that won't work!
-Thomas A. Edison***

Apress Books in the PCUG Library

Database Programming with Visual Basic.NET, Second Edition

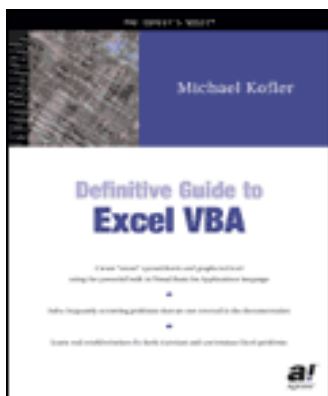
You can read *Database Programming with Visual Basic .NET, Second Edition* cover-to-cover, or use it as a reference book for its many listings with ready-made solutions of “drop-in” code. This book will teach you the concepts of disconnected data access with ADO.NET; how to create various database details, such as tables, constraints, projects, stored procedures, views, and triggers; how to use SQLXML 3.0 with SQL Server 2000; how to incorporate message queuing into applications using MSMQ 3.0; and more. You’ll learn how to master ADO.NET both from within the VS. NET IDE and programmatically.

One of the most popular features carried over from the first edition is the real-world sample application that Carsten builds throughout this book. It’s a user management system that’s based on SQL Server, Active Directory, and Message Queuing. With this example code, you can connect to SQL Server using any of the three .NET Data Providers: SQL Server .NET Data Provider, OLE DB .NET Data Provider, or ODBC .NET Data Provider. The example code also includes how to connect to and manipulate data in MySQL 3.23.51 or later, *Oracle 9i* or later, *Microsoft Access 2000* or later, and, of course, SQL Server. You will also find guidance on connecting to SQL Server 2000 using the SQLXML 3.0 plug-in to transfer data using XML from managed code or HTTP. Exchange Server 2000 data manipulation is also covered, with original working code.



Database Programming with Visual Basic .NET, Second Edition is the ultimate resource for developers needing to master database programming. Carsten Thomsen is a Microsoft MVP.

Database Programming with Visual Basic.NET, Second Edition by Carsten Thomsen. 2002. 959 pages. \$60. www.apress.com



Definitive Guide to Excel VBA

Michael Kofler has written a book that serves not only as a reference, but also focuses on solutions to frequently occurring problems. Kofler introduces *Excel* programming, and then provides a systematic explanation of VBA and the *Excel* object library in a problem-solving mode. He covers all of the essential topics in *Excel* programming from automatically displaying different views of data to accessing databases through ADO. Compact syntax references at the end of each chapter offer the overview not provided by Microsoft’s official documentation.

Definitive Guide to Excel VBA by Michael Kofler. 2000. 866 pages. \$50. www.apress.com

May Meeting Report

At the May meeting, Rick Fischer showed the first CD-ROM of the Total Training Adobe Acrobat 6.0 training suite. We watched excerpts in the allotted time that covered the Acrobat environment, navigation, the toolbar, setting preferences, and search tools. These topics were about half of the first CD-ROM and there are two more CD-ROMs in the suite, covering Acrobat 6.0 in depth. Rick also had Total Training CD-ROMS on Adobe Photoshop and on Digital Photography that we can show at future meetings.

Total Training has a special 10% discount offer running through August for Memphis PC Users Group members. See the ad below for more information and visit their Web site at www.totaltraining.com for complete information on all of their training programs.

Rick also passed out information on a User Group Members survey about Internet services preferences. All who participate in the survey will be entered into a drawing for one of five Canon PowerShot S230 digital cameras. The survey is strictly for research and all answers are anonymous. No one responding will be contacted further unless they are one of the five prize winners.

Also remember that SoftwareCINEMA (www.software-cinema.com) is continuing its user group member 25% discount through July 13st on products like the Photoshop Digital Imaging program seen at the April meeting. Use discount code UG304 when ordering.



**TOTAL TRAINING
PROUDLY PARTNERS WITH THE
Memphis PC USERS GROUP**

**TO OFFER ITS MEMBERS
10% OFF**

**When you call in to 1-888-368-6825
and reference offer code: USRGP2004**

**Visit our web site www.totaltraining.com
for information on all of our training products**

**Offer valid through August 31, 2004; cannot be combine with any
Other offer; is valid ON ALL Total Training Products**

SecureClean 4.0

Software Review

Reviewed by Rick Fischer

I was really surprised. I use Norton *SystemWorks* regularly. I use *Ad-aware* and *Spybot*. Yes, I use both.

My surprise was with all the crud *SecureClean* found.

Sensitive Internet data - 24 instances. It found my daughter's old instant messenger passwords. I don't even remember her using my computer. She's been out of the house and on her own for two years now. Yet, there it was. There were remnants of an old AOL account I didn't even remember being loaded on my computer. I didn't use it, but sensitive logon information was still there.

It found what I suppose was some of my son's log-in passwords. He has had his own computer for several years. Yet, there they still were. It found two instances of my social security number stuck in a cookie. Not good.

There were 1,342 discarded files gathering dust. Over 1,100 URLs were being stored for no good reason. Eight hundred thirty-four cookies and adware were logged.

It found 54,219 instances of temp files and Internet histories.

If my termite exterminator regularly missed that many bugs, I'd fire 'em.

SecureClean is extraordinarily easy to use. You scan and you clean. It tells you what it found. You decide what you want to do with it. I don't believe I could select one cookie to save and another to remove. You deal with them in categories. I cleaned them all up. And, I was pleased that I could still log on to the Internet when it was all finished.

Members of our User Group know that deleting a file in Windows doesn't really delete it in the sense that it "erases" it. To do that you have to overwrite the ones and zeroes that made up the original file.

SecureClean does that. That means that you will want to use *ScanClean* regular as part of your preventative maintenance plan. WhiteCanyon says it is the only program to "safely erase all previously deleted e-mail messages stored inside e-mail archives and popular e-mail programs. . . ."

And, you'll want to use it before you retire or give away your computer. You may be giving away a whole lot than you intended.

I reclaimed 248MB on my hard drive. Nothing to sneeze at. *SecureClean* has earned a spot as part of my regular maintenance program.

SecureClean 4.0
\$40 on CD
WhiteCanyon Software
www.whitecanyon.com



 98/Me/NT/2000/XP

by Gil Hennon

Crime doesn't pay—or so they say. But computer crime seems to be paying well enough to have become one of the fastest growing industries in the world. For the past year, scams and computer fraud have been so successful that organized crime took note and decided to enter the business. Between September 2003 and March 2004, computer crime grew a phenomenal 772%. The growth rate parallels a similar increase in identity theft, which isn't always computer related. Many forms of identity theft are based upon theft of a person's credit cards, mail, or maybe a wallet. Most computer crime can be considered a sub-set of identity theft, because account numbers, passwords, PIN numbers, and other personal information are stolen from computer user victims.

Most of the new computer crime is described as "phishing." Until recently, phishing was a "social engineering" exploit. Users were tricked into revealing confidential information and numbers through a plausible-sounding lie. In the past few months, the phishers have grown smarter. They have figured out ways to get the same data without needing the victim's participation. It is entirely possible now to have credit card and bank account information stolen without noticing that anything is amiss.

The information that phishers want spans an impressive range of online and financial institutions. Elaborate and highly creative phishing schemes have targeted users of EBay as well as customers of U. S. Bancorp. While these and other institutions notify users and customers of the risks, they try to keep it low-key. They

give their warnings with a light touch, hoping not to frighten anyone badly enough to make them stop using the online services. And although most online activities are still safe and secure, there is enough phishing going on to require serious attention.

By today's standards, the first instances of online phishing were pretty crude. The basic scam used an email message to a PayPal or Microsoft Wallet user saying that a system glitch or other problem had occurred. It asked for a reply containing the user's login and password. Often these email messages were written in broken English with grammar errors and misspellings. Only the very gullible fell for these scams.

Lately, though, highly elaborate preparations are in place before a phishing expedition is launched. Web sites of financial institutions are duplicated in great detail, and even navigating beyond the initial screen brings up pages that appear completely bona-fide. Only by digging deeper into the site does one begin receiving "page not found" error messages. Also, the phishers use pop-up fields to place an image of the duplicated institution's URL over the actual site URL displayed in the navigation window. Some put another pop-up of a "secured" padlock or key over the correctly displayed open lock or broken key. Even very sharp users can be fooled by these counterfeit Web sites. Law enforcement agencies say that a well made counterfeit site will extract confidential information from 5% or more of those who are lured there.

Other phishing scams don't try to fool the user with look-alike Web sites. They



operate more secretly, installing keystroke logging software on an unsuspecting user's computer. At regular intervals, this software sends all captured keystrokes to its home site, where it is examined for passwords, account numbers, and other confidential information. The software required to do this is compact, reliable, and available from any number of hacker sources. Lately an empty email message with no subject line contains an embedded, hidden link that downloads the keystroke logging software from a Web site. This occurs without the user's knowledge. All that is visible is a blank email message that is usually trashed without any second thoughts. But by then the deed has been done and the logger is running silently in the background. Fortunately, most of these loggers can be caught by anti-virus or anti-spybot software. Also, keeping current on operating system and browser patches prevents Web sites from installing software without some alarm being given.

Still another phishing scheme exploits a Microsoft system feature known as the HOSTS file. The ideal behind having a HOSTS file is good: It keeps the addresses of remote computers and supplies them to the browser as needed. This reduces the computer's dependency on Domain Name Service (DNS) servers. Recent

phishing scams change the information in the HOSTS file. Originally this was a virus/worm authors' trick. They used it to redirect connections away from anti-virus sites. When a phisher takes over the HOSTS file, connections to financial sites are redirected to the phisher's look-alike, duplicate Web site. Sometimes, to prevent suspicion, the HOSTS file is left alone. Instead, a Registry entry is installed that directs Windows to use a different file to perform the HOSTS function. The result is the same. Users go to the bogus Web site instead of where they intended. All of this happens secretly, with no indications given to the user that anything is amiss.

Brian Livingston, who keeps track of Windows problems at www.briansbuzz.com, recently had a detailed description of one of these HOSTS hijackings. The fake Web site he described looked exactly like the real thing. Only a few small details would tip off a careful user that things were not what they seemed to be. One was the security certificate. The site actually had one, but the name on the certificate was not what the site should have had. Some links on the page did not go where the real site would have taken a user. And the bogus site did not automatically insert the user's login name in the field, as the real site would have done after reading the cookie. These are subtle differences, and they could easily go unnoticed by a trusting user or one who is in a hurry. Brian suspected that the HOST file had been hijacked by a hacker tool called `Worm_Dumarai` or one of its variants. This worm sets up a keystroke logging program and sends information captured to a server in Russia.

What does a user have to do to prevent being taken in by a phishing scam? Some of the safeguards needed are technical, using security software, applied along with a healthy dose of suspicion and

some good, old common sense.

First, make sure all critical security patches are installed on the operating system, Web browser, email client, and other applications that access the Internet. An open port or a badly coded buffer is an invitation for a worm or Trojan program to take up residence.

Second, run a current version of a good anti-virus/anti-worm software. The major vendors are Symantec, McAfee, and Trend Micro. There are other good ones too, so look for one that updates its definition files at least once a week and is convenient to use. Some folks say they don't care about convenience or ease of use, but I'll bet that unfriendly software doesn't get used very much.

Third, get one or both of the leading anti-spybot programs—Lavasoft's AdAware and Spybot Search & Destroy. Both have free versions that do the basic functions and reasonably priced upgrades that add some features you might like to have. Like anti-virus software, these need definition file updates weekly. Out of date definition files cannot recognize the latest spybots.

Fourth, install a software firewall. The next service pack for Windows XP will add basic firewall protection into the operating system software. Until then, or perhaps even afterward, since the Windows firewall is said to work in conjunction with third-party firewalls, you need one like Zone Labs' ZoneAlarm. McAfee and Symantec also include a firewall application in their anti-virus security suites. The point here is to close up any ports open to the Internet and take a good look at any transactions that want access to the computer from the Internet or want to go from the computer out to the Internet. A good firewall will let you designate applications that are allowed Internet access, such as your email, browser, and necessary housekeeping

with your ISP. It will ask your permission for any other penetration before it is allowed to enter or leave your computer. The firewall alert will typically identify the IP address origin of incoming transactions. Outgoing transaction alerts will tell the application on the computer that is sending the transaction as well as the destination IP address. Unexpected outgoing transactions may indicate that a worm or spybot is on the computer and attempting to "phone home."

Additional firewall security comes with a hardware router. These are optional for most users, but they provide the best security and also have other benefits. If you want to connect several computers to a single Internet gateway, a hardware router is essential. Most routers have a built-in firewall that assigns unique addresses to all connected computers. It also closes the ports on those computers and only lets approved transactions come through to the internal network. If your hardware router is wireless, then you also need to enable WEP security. Some wireless routers offer additional security features, so consider WEP to be a minimum requirement. A combination of a hardware and a software firewall will prevent unauthorized access from either direction. Hardware firewalls are best at preventing outside access to the computers on the network. Software firewalls excel at preventing software on the networked computers from accessing the Internet without a users' permission.

In the suspicion and common sense area, ignore any email that asks for personal financial information or passwords. Legitimate financial institutions never ask for information by email. If you suspect that any email is not authentic, then do not click on any of the links or attachments contained in that message. If it comes from a company or person you don't know, but looks legitimate, make a

phone call to them before taking any chances. Like those blank email messages mentioned earlier, it may be difficult to know when one is dangerous. The combination of a firewall, anti-virus software that scans incoming email, and a utility that detects and removes spybots will considerably reduce the risk of harm by malicious email.

Only communicate credit card numbers, PIN numbers, and other confidential information while connected to a secure Web site. To insure that a pop-up isn't being pasted over the security icon, use a pop-up stopper. The best one we've used comes with the free Mozilla browser. There are other good ones, but you'll have to pay for them. Check anti-virus and security suites you have already purchased. Quite a few also contain a pop-up stopper that will do the job.

Either online or on paper, regularly check your bank and credit card statements. Make sure that all transactions are legitimate and inform the bank or card issuer if anything appears amiss. Also notify them if a statement does not arrive electronically or by U. S. Mail when it is supposed to.

The final question, which we hope never comes up, is what to do if you realize that you have been victimized by a phishing scam. The Department of Justice offers some guidelines, based upon what kind of information was compromised.

If you gave out your credit or debit or ATM card information, or if you gave out your PIN number, report the theft to the card issuer immediately. The back of most cards has a toll free number to use in this sort of situation. Let the company cancel the account and issue you replacement cards on a new account. Destroy the cards that went with the old account. For the next several months, review your billing statement carefully and report any unidentified purchases to the issuer right

away.

If you have given out your bank account information, report the theft to the bank immediately. Have them cancel the account and open a new one. If you use online banking, attempt to log in and change your password. The same steps would apply to other commercial accounts on which information has been compromised.

Sometimes you can find evidence that you have been victimized by visiting your regular Web sites and looking for messages using your name or "handle" that were not left for you. One user discovered that his EBay credentials had been stolen when he noticed that he had made several bids on an item that he did not want. In cases like this, notify the Web site management. Many sites involved in buying or selling goods like EBay have a fast form to notify them of fraudulent usage. Close the compromised account and open a new one.

If your anti-virus software alerts you that there is a worm or Trojan installed on your computer, immediately attempt to clean off the infection. Once you are sure that your computer is clean, check sites and accounts recently used for indications that someone else has been there using your identification. If so, proceed with steps to close the account and open a new one. The keystroke-logging phishers seldom stop with just one site and password. They will have tried every possible location.

Other good sources of information concerning identity theft, credit card fraud, and phishing attacks are www.consumer.gov/idtheft, www.usdoj.gov/criminal/fraud/idtheft.html, and www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm.

Don't get caught in the "phish net!" Protect your computer and your identity before the phishers pay you a visit.

Managing Data with Microsoft Excel

Book Review

Reviewed by Rick Fischer

Managing Data with Microsoft Excel is based on user research that says that most users use *Excel* “more as a storehouse of data than as a tool for analysis.”

So, what does that mean? It means that folks tend to use *Excel* to store lists in columns and rows. Those lists typically contain text and numbers. I certainly find that I use it that way most of the time.

Carlberg offers that “this book shows you how to manage your data in ways that make it easier to analyze and summarize the information” (p. 2).

The first half of the book covers *Excel*'s built-in data management functions, e.g., worksheet, tools to filter and sort, pivot tables, and importing data from databases, text files and the Web. The second half covers Visual Basic for Applications (VBA). In particular, how to move data from *Excel* to a database. That's the overview. The better you know *Excel* and VBA, the more you will value this book.

This book is intended for the intermediate and advanced *Excel* user. This is the kind of stuff our SIG



leaders would spend weeks explaining to like minded members.

Let me share two topics I believe I (at my level) will use immediately: the list and the pivot table.

Lists

I collect information in lists for my job at the University. At least, I thought I collected information in lists. Now, I learn that I can gain some power by defining a group of cells as a “list.” I didn't even know there was a “create list” command. Once I do this I can access a “data form” that looks a lot like what I would see in my mailing label programs. And, I can add, delete and sort whole clusters of related information. I didn't know *Excel* could do this! I will definitely play with

this feature.

Pivot Tables

Previously I've read about pivot tables and have printed several tutorials on the topic from Microsoft's site. I just hadn't seen an application that related to me and my work. Carlberg includes “case studies” so you can see how many of the features can be used. This time I made the connection.

As an output from one of my lists I need to summarize data. I do it by hand and it is fine. The list is fairly small. But, what if the list was large? And, why wouldn't I want my list output automatically updated when I change any of the values in the list?

Now I can, and I know how. Carlberg walks you through the procedure showing what to select and what you will see on the screen. That's reassuring.

Reading the book has given me mental models of what is possible. Now, I need to take the book to the computer apply what I have learned.

Managing Data with Microsoft Excel
by Conrad Carlberg.

2004. Que. 344 pages. \$35.

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
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
Windows XP Pro (book)	Daniel Notowitz
FrontPage 2002 Unleashed	Carl Osborne
Using Excel 2003	Jim Redmond
HiJaak ver 5	John Schuster
Macromedia (book)	David Stowell
Windows XP (book)	Terry Thomas
eBay Hacks	Tommy Towery

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

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
JUNE 2004	7	8	9	10 VISUAL STUDIO	11	12 WEB WRITERS MS OFFICE
JUNE 2004	14 	15	16	17	18	19
JUNE 2004 	21 WORDPERFECT 	22	23 MAIN MEETING	24	25	26 INVESTMENTS
JUNE- JULY 2004	28 CLIPPER	29	30	1 	2	3 INTERNET HARDWARE
JULY 2004 	5	6 DOT.NET	7	8 VISUAL STUDIO	9	10 WEB WRITERS MS OFFICE
JULY 2004	12	13	14	15	16	17