



The Bridge

The Journal of the Memphis PC Users Group

Volume 21 Number 6

June 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
PowerPoint Trainer	Page 4
May Meeting Report	Page 5
SIG News	Page 5
More Phish in the Sea	Page 6
Two New Books from Que	Page 10
Out for Review	Page 11
Event Calendar	Page 12

Main Meeting Wednesday, June 22 Southwest Tennessee Community College

5983 Macon Cove, Memphis

MEETING LOCATION

Fulton Room 118

First Floor - Fulton Engineering Building

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

June Main Meeting . . .

Join a roundtable discussion on spyware. We all hate it, but what are we doing about it, and are we getting any results? Share your experiences-what works and what doesn't. Bring along a friend!





The School Bell

News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Many different security organizations do surveys. They try to get a representative sample of computer users, study their behavior, and then make their best guess of what's really going on in the world. Because of differences in the way they survey, seldom do two or more organizations ever agree on how many computers are this way or that way, or which trend is most prevalent. But most recent surveys have been in total agreement that computer vulnerabilities and malware attacks are much worse than previous estimates. The number of unpatched, vulnerable PCs in the general population is much higher than anyone thought. Probably more than one-third of all PCs are open to worms and Trojans that turn a normal PC into a "zombie" for criminal use.

Most users never know that their PCs have become zombies. Everything usually works the same, although sometimes a bit slower. Unless the PC becomes corrupted in some manner, it will be connected to the Internet and serving a dual function—regular computer and zombie—twenty-four hours each day.

The researchers at the HoneyNet Project deliberately left a network of PCs vulnerable to several types of malware to find out how they would be used once they had "gone over to the dark side" as zombies. They discovered four distinct ways the zombie PCs can be used for illegal purposes.

Some of the PCs hosted fake Web pages of legitimate sites, such as banks or financial institutions. With a page here and a page there, a group of zombies can look like a Web server and operate as a

phishing destination. Other PCs were used to send out spam email advertising the location of those zombies posing as Web pages. Still another group of PCs were performing redirection services, re-routing traffic away from legitimate Web sites and toward the bogus phishing pages. Lastly, some compromised PCs were sending out actual spam and phishing email messages over botnets. Did your PC participate in a similar illegal operation? If it's not patched and updated, it very well may have!

The HoneyNet Project concluded that forwarding spam and participating in phishing attacks are becoming much more widespread than the traditional zombie role of Denial of Service (DoS) attacks, and that the phishing schemes are very well organized. They observed that many Web pages of legitimate businesses were pre-built days in advance and stored until they were brought online very quickly to support a phishing spam attack being launched.

Another general conclusion reached by more than one survey organization should come as no surprise to anyone; there is a "clear connection between spamming and phishing" using zombies. Some of the surveys also found zombie PCs were being used to conceal illegal financial transactions.

Maybe PC zombies and phishing aren't enough to convince everyone to get those critical updates and patches installed. After all, they cause no observable damage to the PC or its user. But another recently discovered attack against vulnerable PCs puts the risk right in the living

room. Trojan software installed on a PC when visiting a malicious Web site encrypts all of the user's personal files. Then the Trojan program notifies the user that a tool must be purchased from a specific Web site in order to decrypt the files and make them usable again. The tool is simply a decryption program with the encryption key already defined.

The Trojan encrypts files with extensions like .doc, .xls, .qpw, .dbx and .txt, ignoring the majority of application program files that can be restored from original CD ROMs with relative ease. This scheme takes advantage of users who do not back up their personal files to media that does not remain in the PC. With backup files in an area inaccessible to the Trojan, everything can be restored if necessary. Backup files stored on a second hard drive inside the PC can also be encrypted by the Trojan, so they could be as useless as no backup files at all.

Security professionals are calling this encryption and extortion scheme "ransomware" and they classify it as only a modest threat at the present time. Since it is not self-propagating, like a virus, its ability to spread is limited. Also, the payment requirement is a weakness, since money transactions are usually traceable. The first instances of ransomware investigated by the FBI contained a demand for \$200 (160 euro) and the encryption used was fairly simple. An unrelated party was able to crack the key and restore all of the files without resorting to paying the ransom.

Although ransomware has a way to go before it will be a workable threat, security analysts call it "fully malicious" and indicative of the growing trend of malware authors becoming or working with criminals to exploit PC vulnerabilities for profit. It also exploits the anonymous nature of the Internet at a time when regulatory agencies are looking for ways to limit anonymous Web activity.

MPCUG Education Services can give you lots more tips for staying away from zombies and ransomware. Join the Wizards session every month prior to the main meeting and keep your computer healthy.

*Genius is one percent inspiration
and ninety-nine percent perspiration.
- Thomas Edison*

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

PowerPoint Personal Trainer

Book Review

Review by Megan Hefner

Now I am a superhero. Just ask my *PowerPoint* personal trainer. Throughout my college career, *PowerPoint* has become a close friend. Every semester I find myself creating presentations using this program. I thought I knew all of the ins and outs. Turns out I was wrong.

PowerPoint Personal Trainer starts with the very basics and by the end shows you all of the tricks of the trade. You can't mess up – just follow the steps.

O'Reilly's *Personal Trainer* is very easy to read and follow. For those who have to budget their time, it's laid out in a very logical manner. Each instruction comes with an actual example from *PowerPoint* so that you can see what it would look like. Visuals always seem to stick with me longer than words alone. Every chapter also has a review section at the end. (For those who REALLY don't have a lot of time.) The review section includes a summary, quizzes and homework

A CD is also included with *the Personal Trainer*. It

contains an "interactive simulation" of *PowerPoint* in "bite-sized lessons." The CD is easy to install and navigate. Lessons include formatting, editing, working with multimedia and more.

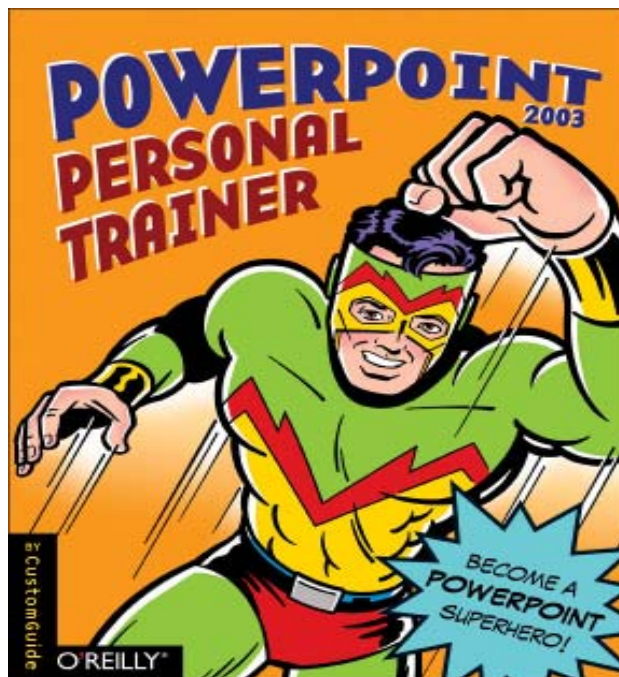
From quizzes to homework to simulated lessons, the *Personal Trainer* is built to stick with you. I could read the book and have to go back to it several times while I am creating a presentation. Or I could spend a couple of hours working through the book and CD and become thoroughly competent in *PowerPoint*.

After checking out the *Personal Trainer*, I wish that I could roll the clock back and add sound or movie

clips to my last presentation. Now I know how. "Eye of the Tiger" would sound great in my presentation about the University of Memphis.

Presentations don't all have to look the same; with the *Personal Trainer* you can learn how to keep your colleagues and clients awake with unique backgrounds, animation and multimedia. In a time where no one has time, think above and beyond, or up, up, and away with the *Personal Trainer*. You too can become a PowerPoint superhero!

PowerPoint Personal Trainer. 2004. O'Reilly. 315 pages with CD. \$30



May Meeting Report



Microsoft Digital Image Suite 10 and Photo Story 3

The May meeting presentation came from Microsoft's Mindshare program. Although we did not have Digital Image Suite 10 software to perform the demonstration portion of the presentation, the scripted slide show contained sample screens and walked the audience through several typical digital image editing scenarios. There are four main parts to the Suite: The Import Wizard, the Sorting and Organizing viewer, the "Fix-up" tools, and the Online Print Wizard.

Digital Image Suite 10 imports photos from digital cameras and cell phones. The Organizer allows a user to assign a caption to each photo as well as keywords for sorting, flags as reminders of what to do with the photo, and a rating of one to five stars designating the quality of the photo. Some photos have small defects, such as "red eye" from flashbulbs too close to the camera lens. These small defects can be "auto-fixed" in many cases, and if more work is required, the Suite contains a complete set of image editing tools. The Online Print Wizard can locate the nearest Microsoft photo-finishing partner. An automated tool identifies the images to be printed and determines whether the finished prints are to be mailed to the user or picked up at the finisher. Some finishers can have prints ready an hour after the images have been electronically received.

A second part of the Mindshare program was a demonstration of Photo Story 3. This program is a free download from Microsoft's Web site. It requires Windows XP and needs Media Player 10. After showing the Photo Story 3 slides, Gil Hennon used the Photo Story software to produce a multi-image story of a day at the beach. Photo Story contains fades and dissolves similar to Microsoft's Movie Maker, and motion/zoom within an image. Narration and music can be added as well as text captions on each photo. The interface is easy enough to use that children can be encouraged to make stories from their own photos.

SIG News

Hardware SIG by Jim Ingram

Our project was to evaluate and analyze the CPU of Jim Holland, whom I met at the main MPCUG meeting nearly two weeks ago. Holland Printing Co. is on Poplar just a few of blocks west of the Library, so I stopped by and picked up his old Sony PC because he could not be at the meeting. We only had six at the meeting.

It only has a 6MB (yes, SIX MB) hard drive. I had downloaded Belarc.com's Advisor to a floppy and ran the program on the PC. Mike Davidson figured that the CD-ROM not connected and that a controller was not working. He connected it and later disconnected it), for the DVD-ROM was OK. His Hard Drive had only 16 MB of capacity used – 4.4 MB free. He will have to have a larger Hard Drive for it to be much help. He says that he is going more into direct mailing.

Holland is not a computer person (no e-mail or internet ISP). This PC was a gift from his brother. He wants to learn how to use it in his business. There were a few programs on it – spreadsheet, MS Word 2.0, MS Office and several small other programs by a company that no longer exists. Holland says that his printing business has suffered because his old customers are now using computers to do what he used to do for them.

More Phish in the Sea

Editorial

by Gil Hennon

You can be a phishing victim even if you don't have a computer! I learned that yesterday when I got a phone call from a slick, well-practiced scam artist. Like just about everyone else, we belong to a wholesale club where we purchase items for our business and home. There is an annual fee of \$30.00 to continue our membership which we usually pay in the store when it is due. Yesterday's caller told me our membership in this club was about to expire. He knew our names, addresses, and how many cards we have issued, and he said he could renew our membership for \$45.00 while we were on the phone.

What saved me from falling for the scam was an alarm that goes off inside my head when anyone says "give me your credit card number." Those words trigger an instantaneous "time-out" for me—a pause where I mentally step back and look at what I'm doing. If I'm in a store with my card in hand, or I've called or gone online to make a purchase, the pause is hardly noticeable. I've already made a decision to purchase something. But when a request for a credit card hits me blind-side, everything stops long enough for some serious and suspicious consideration.

So I told the caller that I didn't have time to handle the renewal right then, and asked for a number where I could call him back. He didn't like that, but when it became obvious I wasn't going to cough up a card number, he gave an 888 number and left me, probably to go pursue a fresh prospect. When I asked my wife if our membership needed renewal, she said it was just renewed a couple of months ago. Then she called the manager of the wholesale club's local store. He confirmed that

they do not renew by telephone. They mail a renewal notification and the cost is \$30.00. The manager said he would inform their home offices about our experience.

There really isn't much difference between the phone call I received and an email that tries to get my personal information by directing me to a bogus Web site. Both scams are well prepared, plausible, and falling for them can be much too easy. The only difference is the medium used to deliver the scam.

Luckily, I've seen plenty of phishing scams on my computer, so the same alarms triggered when one came by a different route. Unfortunately, according to the Annenberg Public Policy Center at the University of Pennsylvania, many Americans are dangerously ignorant about phishing and fraud, online and otherwise. In a recent study, they tested 1,500 adult Internet users on their knowledge of online security and privacy. Most failed the "true-false" test, answering less than seven of the seventeen questions correctly. Almost half could not identify a phishing scam email when it was shown to them, and three-quarters thought that when a Web site has a privacy policy, it means they do not share any personal information. The sample population was selected randomly, and included people who use the Internet and computers at both home and work. Perhaps they would have been more suspicious of a phone call like the one I received than they would be of an email phishing expedition. I hope so, but I'm not putting down any bets.

Another study was done at the behest of the Anti-Phishing Working Group and findings were discussed at an email security conference. Cyber crime special-

ists concluded that today's hackers are turning to fraud at an alarming rate. The study analyzed data from a "honeypot" network. "Honeypots" are pools of intentionally vulnerable computers that lure malicious hackers to see what they will do there. During the second half of 2004, their "honeypot" recorded a 360% increase in phishing and pharming email as compared to the first half of the year. During the entire year, the "honeypot" attracted more than 10 million phishing scam email messages!

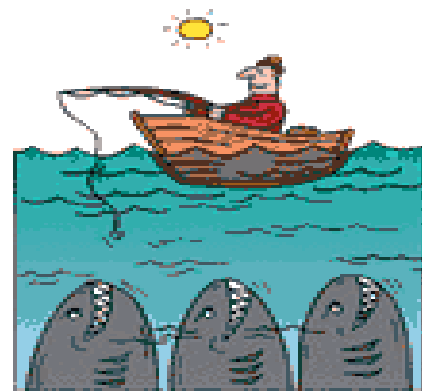
The networked computers also were infected by a variety of "drive-by" software installations attempting to use the "honeypot" computers as remote controlled zombies on a botnet. Most of these "drive-by" infections attacked one of 21 vulnerabilities identified in Microsoft Internet Explorer. Based on this experience, the researchers concluded that more than half of all malware now being created is intended to harvest confidential information. Researcher Dan Hubbard saw the trend influenced by the money involved, noting that the "profit motive for phishing is very sizable. The hit rate is high, and the financial returns are quite good." Going beyond phishing, into taking over servers and poisoning Domain Name Servers may be even more profitable and comparatively safer, since the methods are more sophisticated and do a better job of covering a hacker's tracks.

The hacking "profession" is also undergoing similar significant changes. The days of the "jack of all trades" hacker are almost gone and specialization has become the key to greatest success. Some hackers create zombie botnets, then "lease" them to other hackers who perform the phishing and pharming operations. The information collected is sold to a third party, often another hacker, who prepares and packages it for the "cashiers" who actually use the stolen informa-

tion to perform illegal or fraudulent financial transactions. The resulting, ill-gotten proceeds pass

through secret bank accounts and businesses where money is "laundered" into revenue appearing to originate from legitimate sources. Hackers specializing in the various process levels sometimes even advertise their services on their Web sites, newsgroups, and blogs.

Specialization not only puts the most capable person into each job, but also provides greater protection for those at each layer. True identities are seldom used between the layers, insulating the phishers and zombie masters from the cashiers and the street-level operatives. Exposure of one level does not jeopardize the entire hierarchy and allows each level to operate autonomously and most profitably. By far, the most organized and successful hacker community in the world now operates from Russia. Malware of every sort is created and distributed from the various Russian states to customers in nearly every country on earth. Software has become such a large and profitable business in Russia that it is often said that Russia is where hackers eat caviar. Good, experienced programmers in Russia tend to be the best paid in the whole world and the market there for both legitimate and criminal software is booming and profitable. Computer fraud accounted for 2.45 billion Rubles in losses inside Mother Russia, last year, but the bulk of Russian malware is sold to clients outside the country. A significant majority of viruses, worms, Trojans, spyware, and spamming tools are created by Russian hacker teams.



On the other side of the coin, slow, but steady progress is actually being made to stop the spread of malware and eliminate some of the fraud that permeates computer networks and especially the Internet. In May, the U. S. Federal Trade Commission launched a cooperative effort with similar bureaus in more than twenty foreign countries to reduce and perhaps eliminate the use of zombie networks to forward spam email. Since the first, and usually the most difficult step in shutting down a zombie network is identifying the computers that are unknowingly participating in spamming, an important part of the FTC's effort is going into education. Major ISPs are being shown how to recognize zombie behavior on their networks and how to better block out zombie creating software before it reaches their customers' computers. Some of the effective tactics include rate-limiting controls on the number of messages a client is allowed to send and establishing quarantine areas on gateway servers where suspicious email can be held and inspected prior to forwarding. The FTC is also encouraging ISPs to provide customers with software tools that disable or remove zombie Trojans from their computers.

Although ISPs are sometimes slow to embrace filtering and other methods that may leave them open to charges of censorship or violation of free speech, they also have a vested interest in eliminating spam. Every ISP loses a significant amount of expensive bandwidth to spam, and the problem has grown to proportions that no ISP can afford to ignore any longer. Zombie network investigators say that an average of 172,000 new zombies appear on the Internet every day. Less than one-fourth of these new zombies are in the United States, but the U. S. still leads all other countries, followed closely by China. Dmitri Alperovitch, a research engineer with CipherTrust, who tracks

zombie networks warns that they are probably one of the "most critical security challenges on the Internet."

To illustrate the gravity of the zombie problem, CipherTrust established the "ZombieMeter" which can be viewed at www.ciphertrust.com. It's an eye opener. With the FTC and government agencies of other countries working to help ISPs shut down zombie networks without violating the rights of bona-fide users, we hope to see a reduction in zombie forwarded spam in the near future. Any improvement here will also hurt the criminal phishing community, since spam is their most popular method for attracting gullible users to fleece. Keep an eye on that "ZombieMeter." If it starts going down, that's good news!

Another win for anti-spam troopers occurred when Scott Richter, who calls himself the "King of Spam" and "Super Spammer," filed for bankruptcy in the U. S. Federal Court of Colorado. Richter complained that his business is still profitable, but being battered by legal fees. All of those fees are the result of Richter's bad judgment; he really annoyed a company named Microsoft and the Attorney General of New York. Although New York settled their case, Microsoft wouldn't let the spammer off so easily. At the time of filing bankruptcy, Richter's company claimed assets of less than \$10 million and liabilities of more than \$50 million. While in operation, the company emailed more than fifteen million spam messages per day.

Hitting the spammers goes after the mechanism used to facilitate phishing and malware distribution. Senator Patrick Leahy (D-VT) introduced a bill in Congress that addresses the upper level of the crime, where the fraud resides. His Anti-Phishing Act of 2005 outlaws the use of look-alike Web commerce sites that fool consumers into divulging account numbers and other personal information.

Penalties of up to five years in prison and fines up to a quarter of a million dollars could be handed down by judge or jury. Leahy's bill adds pharming as a punishable act, and unlike a different version that failed in 2004, the new bill allows prosecution for creating a bogus site, rather than requiring someone to have been harmed before the law can be applied. Law enforcement officers hope this would be a help in apprehending and prosecuting phishers. They find that all too often the phishers strike and then disappear, covering their tracks long before an investigation can be initiated. Leahy claims that parody and consumer protest sites would be exempt, and only sites created with the intent to commit fraud would be prosecuted. While introducing his bill, Leahy referenced statistics from January, 2005 showing that the number of unique phishing Web sites was increasing by 47% per month. As initially written, the bill may be a little too specific, given the talent that online criminals have shown in finding ways to get around already existing fraud laws. They react and adapt quite quickly to both preventive and enforcement measures taken against them. Leahy's bill will be modified as it moves through both houses of Congress, hopefully adding some flexibility without losing any of its sting.

Phishing, pharming, identity theft, and credit card fraud are all crimes that became much more popular when perpetrated online. The relative anonymity of the Web reduces the risks a criminal takes while fleecing a victim. No face to face contact is required and if anything looks amiss, the criminal can disappear instantly, leaving hardly a trace behind. Ralph Basham, the director of the U. S. Secret Service addressed the RSA Security Conference in San Francisco during February. He spoke of increased activity by professional criminal elements in all types of online fraud. Organized crime has

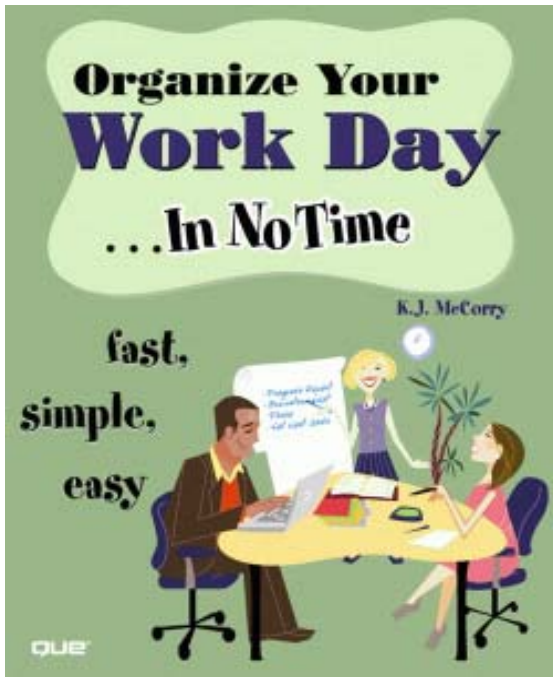
taken to the Web, astronomically escalating the scale of Internet crime. Basham noted that the use of malicious code and phishing schemes have made online crime highly profitable in a very short period of time, leaving law enforcement agencies and their conventional resources far behind. Credit card companies now measure their losses in billions of dollars, so it will not be long before online crime begins to noticeably impact the U. S. economy.

Another trend in online crime identified at the RSA Conference is the movement of criminals down the "food chain." Early computer crime was generally aimed at big corporations, especially financial institutions. Criminal hackers picked large targets where simple and crude system intrusion could reap large rewards. As these targets hardened their security and became more difficult to crack, the criminals moved down to smaller businesses and individuals. Even though the smaller targets are better protected than they used to be, they do not have the big bucks to spend on highly-effective security measures. For the criminals, the pickings are leaner, so they go after many more targets.

Perhaps the best weapon against fraud, either the online type or the con artist in your face, is a healthy dose of suspicion. Law enforcement officers say that some of the comments regularly made by fraud victims are, "It sounded too good to be true," or, "I kind'a had a bad feeling about it," or something very similar. Police wonder why victims didn't listen to their feelings instead of allowing themselves to be fleeced. Certainly we all want to believe our neighbors are good and honest people, but some of them just aren't. If a deal seems too good to believe, or something about it feels wrong, it's time to take a hike. Like the phone scam that was tried on me, when it smells fishy, it is very probably a phish!

Two New Books from Que Publishing

Book Reviews



Organize Your Work Day... in No Time reviewed by Rick Fischer

Que is putting their brand on some interesting new book projects. We'll be looking at two of them here.

Organize Your Work Day is intended to "bridge the gap between specific software how-to books and time management books." So, it's about your busy life and the principles and tools that can make it a little less hectic.

McCorry accomplishes this in three parts. In the first part we look at our lives and what we do with our time. She asks to us to consolidate our information (and do a major spring cleaning of the stuff we've been saving). Easier said than done. Then we group like things - called categorizing. Last, we find a place for the stuff we think we need to save. You wanted to find it again, didn't you?

In the second part we explore organizational tools - from paper to electronic databases. She offers suggestions for storing information on your computer and compares nine contact management-type programs.

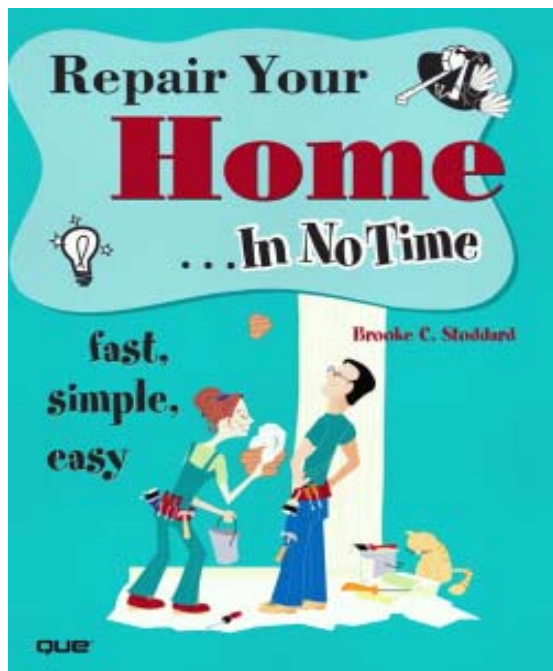
Part 3 is about managing your daily tasks, i.e., e-mail, projects, meetings and your day-to-day activities.

I know these are important topics. We are offered workshops on time management regularly at work. You must also understand that it will take time to apply the techniques suggested in the book. But, presumably, the benefits will be much greater than the costs.

It is an easy read and you can skip around if you are already familiar with the principles.

Organize Your Work Day... in No Time by K. J. McCorry. (2005). Que. \$17.

Repair Your Home... in no time reviewed by Rick Fischer



Now that you've found extra time in your life (see above) you can use that extra time to do home repairs.

Since I have been collecting books and articles on DIY topics for years (and I don't intend to throw them away), I was particularly interested in this book. It is no match for the encyclopedic sets of how-to books available to DIYers. There are pictures, but the description is carried largely through text.

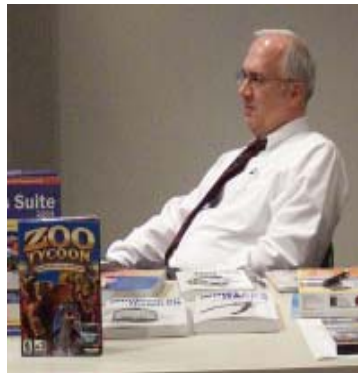
The repairs are organized around walls and floors, doors and windows, plumbing, simple electrical repairs, painting and wallpapering, and outdoor repairs.

What is different about this book is the chapter on a maintenance plan. I think most folks wait until something is really broken, before they pay attention. This is about spending a little to save a lot (later). What needs to be done in the fall? The spring? The summer? What can I do, and when should I bring in people who've done this before?

Following McCorry's advice, you should put the plan on your free-form database (*OneNote* or *InfoSelect*) or on a *Word* document that you can call up when needed. That's what I did.

Repair Your Home. . . in no time by Brooke Stoddard. (2005). Que. \$17.

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
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 Personal Trainer	Vanessa Muldrow
Windows XP Pro (book)	Daniel Notowitz
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
Photoshop CS	Jin Yang

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

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 2005	6	7	8	9	10	11 WEB WRITERS MS OFFICE
JUNE 2005	13	14 	15	16	17	18
JUNE 2005 	20	21 	22 MAIN MEETING	23	24	25 INVESTMENT
JUNE-- JULY 2005	27 CLIPPER	28	29	30	1	2 INTERNET HARDWARE
JULY 2005	4 	5	6	7	8	9 WEB WRITERS MS OFFICE
JULY 2005	11	12	13	14	15	16