



# The Bridge

The Journal of the Memphis PC Users Group

Volume 20 Number 7

July 2004

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
FormTool2004	Page 4
Out for Review	Page 6
June Meeting Report	Page 7
Phighting Phishing	Page 8
Event Calendar	Page 12

## Main Meeting Wednesday, July 28 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.

## **July Main Meeting**

Plans were not complete for the July meeting by the newsletter deadline. Come and see something none of us are expecting. For even more fun, bring along a friend.





# The School Bell

## News From MPCUG Education Services

By Gil Hennon, Education Services Coordinator

Will Rogers once said, "I don't make jokes. I just watch the government and report the facts." Not many folks are still around who were here when Will said that, but we certainly know exactly what he meant. Sometimes it seems like there must be a sign on the door of the chambers of Congress requiring members to disengage their brains before coming inside.

The latest "joke" to come out of the U. S. Senate is a proposed bill aimed at stopping peer-to-peer file swapping networks. In reaction to a federal judge's ruling in April that file sharing networks are legal to operate, the Senators decided we need a law to stop our children from embarking upon a life of crime by downloading music.

What makes the bill even more laughable is that our esteemed members of Congress obviously had no ideal of what a peer-to-peer network was when they decided it should be verboten. Any connection that allows two computers to exchange data without going through a server qualifies as a peer-to-peer network. Napster, StreamCast, and Grokster are not the only forms of peer-to-peer. Almost every business in the world uses some form of peer-to-peer networking. Yet the Senators—a lot of them—and a bipartisan crowd as well-worded a law so broadly and badly that it probably makes illegal the connecting of two computers together for any purpose at all.

The moment this woofer is passed, all U. S. business, finance, government, and services must come to a halt! No more scanning bar codes at the checkout

counter-price look ups access protected content databases. No more police and FBI checking databases for information on criminals (the real kind, not just the ones created out of thin air by clueless lawmakers) and no more Internet. All of that "computer talking to computer" stuff will carry a prison sentence!

I don't like pointing fingers, but our own Tennessee Senator Bill Frist, the Senate Majority leader, is one of the misguided co-sponsors of this awful piece of legislation. Even before it was introduced on the Senate floor, critics were raising their voices, but apparently Congressional deafness is an epidemic only surpassed by technical cluelessness. As proposed laws go, the "Inducing Infringement of Copyrights Act" (IICA) is short and to the point. In less than two pages, it makes illegal anything and anyone aiding the act of duplicating copyrighted materials. Senators Orrin Hatch and Patrick Leahy were a lot more long-winded as they introduced the bill. Their speeches claimed that this law is necessary to stop companies and corporations from encouraging America's children to commit crimes, to halt the spread of pornography, and to protect the profits of Sony and similar businesses that sell copyrighted products. One could wonder how our country has existed and prospered for so long without this legislation!

What neither Senator mentioned was that their bill is so broadly worded that just about anything can be an aid to copyright violation. Hardware and software of all sorts is used to exchange data over both formal and ad hoc peer-to-peer

networks. Other aids, which the law could also make illegal, easily include Tivo set-tops and VHS recorders, audio tape recorders, computer "capture" devices and related software, and probably copy and/or FAX machines. The opportunities for litigation based on this law are endless. The IICA ought to be renamed the "Lawyers' Full Employment Act." Congress has already given us too many bad laws. Let's hope our legislators figure out how much damage this one could do, and dump it where it belongs!

Just to show that laws and judgments can be goofy even when statutes are carefully enacted, a court ruling will allow a woman to sue her grocery store over their discount card policy. Now, it would be logical to assume that Jill Crowson of Clyde Hill, Washington took offense at the store "mining" her data and intruding on her privacy, but that's not the issue. She's sore because the store didn't intrude on her enough! She bought beef at her local QFC store and later learned that it might have been tainted with mad cow disease. Jill contends that the QFC store chain should have used discount card data to identify her and other customers who bought the beef and should have warned them about it.

The store and its parent corporation were negligent, she contends. Since she was registered and used her QFC Advantage Card, her name, address, phone number, and purchases were all known to the store and should have been used to notify purchasers to return possibly tainted meat. The QFC store chain argued before the King County Superior Court that food warnings and recalls are traditionally the responsibility of the news media. Grocery vendors do not, in most cases, contact customers about recalls or similar problems. The grocery chain asked the judge to throw the case out of court, but he ruled instead that Crowson's suit can proceed.

So while stores in most states are being sued for collecting and selling too much information about their customers, one in Washington state is being sued for not being nosy enough. It's a real shame that Will Rogers won't have something to say about that!

MPCUG Education Services can't fix goofy laws or goofy lawsuits, but it can help you get more value out of your computer and your time at the keyboard. Join the Wizard session each month before the main meeting. Bring a question or problem, and whatever documentation you can about how it all came about. You'll get good advice from the Wizards!

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](http://www.mpcug.org)  
Information Line: 901-375-4316

### Reviewed by Rick Fischer

I remember going to an IMSI press conference at a COMDEX in Atlanta. It was more than 10 years ago. I was impressed with the niche products they offered people like me. They are still hanging in there, and it's a tough market.

*FormTool* is one of their niche products. We looked at their *ClipArt* product in the April issue.

Today I can build forms in *Word*, *Publisher*, *Excel*, *PageMaker*, *QuarkXPress* and *Access*. And, these are just the programs that come to my mind. There are probably more.

And, if you only want to make the occasional form for work or for personal use, I'd suggest you stick with what you know. But, *FormTool* really is different.

### A blend

*FormTool* is an interesting blend of a layout program, like *Publisher*, and a database program like *Access*. And, you get 600 templates that are ready to use, or ready to edit.



By now we are used to drag and drop elements. *FormTool* has it. We are used to having complete control over the appearance of those elements, once selected. *FormTool* has it.

I thought *FormTool* was just for making paper forms. It can make paper forms, but it can store data derived from those forms. And, that database can be queried to give you the information you might need for your desk or enterprise. That's a lot of power.

And, if you don't want to mess with *FormTool's* database, you can input and output data to *Act*, *Excel*, *dBase*, *Access*, *FoxPro SGL*, *Oracle*, *Paradox* and more.

And like an *Excel* sheet, your forms can execute math functions and fill in designated

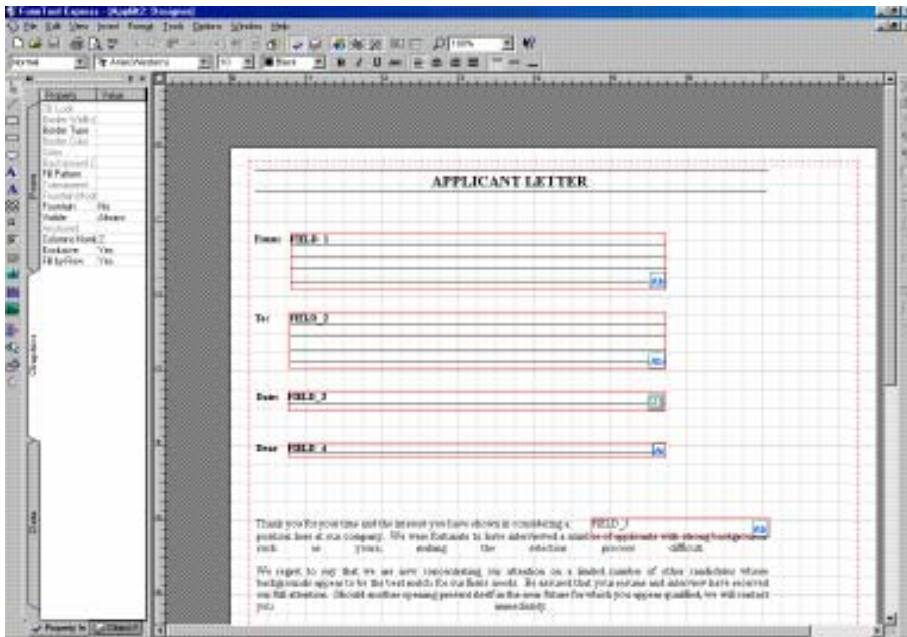
cells. The version I tried would compute all the fields in the templates. To create your own forms with active math functions, you will need *FormTool ver 5*.

### Example

Let's say I regularly check out tools or parts to others. Every time I check out a tool or part I could fill out one of the paper forms I created in *FormTool*. Better. Every time I checked out a tool or part, I would type the information directly in *FormTool* and have that information captured into the database. Yes, it can be used over a network.

### Send forms by e-mail

I'm sure this seemed like a good idea at the time, but. . . . You can send a form to someone as an e-mail attachment with an exe extension. I could send some of my forms to graduate students and have them fill them out and return them to me either by mail or by e-mail. When the form comes back as an attachment the content can be



incorporated directly into your database. But, who among you is willing to take a chance on an attachment with an exe extension?

### Manuals

I am pleased to say that *FormTool* comes with two excellent manuals on the CD. One is called the *FormTool Onscreen Users Guide*. This Guide gives you an overview of the layout functions. And, if you never planned to use the powerful database, you could stop here. I suspect they call it and *Onscreen Users Guide* so that you won't think you need to print it. It runs 101 pages. I don't want to read that many pages on screen.

The *FormTool Onscreen Reference Manual* is more detailed and covers working with the included

database. It runs 221 pages. No, I won't read it on screen either.

Whatever they are called, they really are done professionally.

### Lots of templates

I spent a lot of time just going through the templates that came with the program. There are still more online at [www.imsisoft.com/support/formtool/free\\_fprms.asp](http://www.imsisoft.com/support/formtool/free_fprms.asp).

*FormTool* includes a preview function. But, unless you are already familiar with the form, it isn't clear enough to help you make an initial selection. And, although the templates are already sorted into broad categories, I also found myself saving the forms I was interested in with a more complete name. A few of

the templates have names like U1142. A better name, in this case, would be "subcontractor agreement."

They have templates for: accounting, construction, human resources, personal forms (e.g., net worth), production management, real estate, sales, small business. If you ran a small business you will immediately use many of the forms that come with *FormTool*.

### Marketing Confusion

The box calls this product *FormTool 2004 ver 5 for Windows*. The Users Guide talks about *FormTool ver 5*. The installed program calls itself *FormTool Express ver 5*. It's confusing.

So I contacted IMSI and asked. They sent me a document that helped me separate the three variants of *FormTool*.

I am using *FormTool 2004 ver 5*. It has the 600 plus forms/templates, 200 label templates, the drag and drop editing tools, and complete database support.

There is a *FormTool 2004 ver 5*, yes, the same name, but sells for \$40. It allows me to do all that the basic program can do plus save forms as HTML.

The big package is

*FormTool ver 5*. It includes all the above features plus the ability to scan forms and import them directly into *FormTool*, it has built-in calculation functions and formulas, password protected signature fields, password control to protect form data, network administrator controls, label wizard, and direct connectivity with Access, Excel, dBase, FoxPro, Paradox, and most ODBC compliant databases.

One thing's for sure: you can't fuss at the price for the basic product. For a small or medium size business, it makes sense to try it for its very useful forms and consider using it for your database and main input device. There's a lot to like in *FormTool*.

Requires: Pentium 120 or faster. 32MB RAM. CD-ROM. 26MB free on hard drive. Windows 95 or newer (to XP).

\$20 for *FormTool 2004 ver 5*

\$40 for *FormTool 2004 ver 5* [with publish to HTML capability]

\$100 for *FormTool ver 5*

[www.imsisoft.com](http://www.imsisoft.com)

# Out for Review



Here is a list of software, books, or other products you can expect to see reviewed here in the coming months. These members checked out items to review for the benefit of all.

Windows Me: The Missing Manual	Greg Adams
Teach Yourself GoLive 5 in 24 Hours	Allison Banks
Teach Yourself Adobe Photoshop CS in 24 Hours	Judith Bogan
Windows Security Handbook	Dorothy Drum
The Little Web Cam Book	Mike Heinrich
Microsoft Works 7.0	Jim Ingram
Zoo Tycoon	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
Amazon Hacks	Vanessa Muldrow
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
SPSS	Jin Yang
Using Photoshop CS	Jin Yang

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

# June Meeting Report

---

Gil Hennon showed some of the graphic magic of D'Fusion "augmented reality" software. Augmented reality consists of taking a video of a real scene and adding computer generated objects or backgrounds. Either areas of the real scene are filled with real-time computer generated content, or an actor can hold a "sensor" that transmits to the computer the position of the hand. The computer then turns the virtual object as the sensor moves, keeping the object correctly aligned with the actor's movements. Light and shadows give the virtual object a very real appearance, and the virtual object can interact with or be deformed by contact with edge boundaries in the real world. For example, a virtual car cannot drive through an object on a table that is being used as a platform, or a virtual mallet is deformed when swung against a real object.

To increase the sense of reality, collisions of virtual objects with real objects, or with other virtual objects, trigger an appropriate computer generated sound effect, such as the noise of a blow or breaking glass. Total Immersion, the French company that makes D'Fusion, has designed a "virtual" harbor control system where ships entering and leaving the harbor are seen in their correct position and orientation on a computer screen, even though fog and darkness do not allow the ships to be seen by eye or optical enhancement. Another application allows prospective automobile buyers to "virtually drive" the car of their choice around the city of Paris.

The hardware that makes "augmented reality" possible consists of a few styles of cameras and sensors that record the real world and a Pentium 2.4 GHz PC running the D'Fusion software. A complete setup costs \$30,000.00 and up, depending on how many virtual objects will be augmented into a real scene. While it may look like an actor is just moving his hand to anyone walking by, those watching the screen will see him realistically swinging a broadsword, or perhaps a Jedi Light Saber. Anything you can imagine can probably be done in augmented reality.

## 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: \_\_\_\_\_

# Phighting Phishing: Identity Theft Revisited

*Editorial*

by Gil Hennon

Last month's article about "phishing" for confidential identity and account information attracted more comments than usual. The media and law enforcement have become aware of phishing as an opening ploy in identity theft crimes, and are giving it the serious attention it deserves. A recent, well publicized Shelby County Court trial—the one involving stolen Goldsmith's account numbers and gift cards—emphasized how commonplace identity theft crime has become. You don't have to be a rich, fat cat to attract a thief. Ordinary folks like you and me are victimized by fraud and impersonation every day.

In the local Goldsmith gift card fraud, the identity theft occurred inside a Tennessee prison. Inmates were working for a firm that subcontracts credit inquiries for financial institutions. One of those inmates had been convicted for writing bad checks. She recorded personal information and account numbers of Goldsmith's store customers and passed the data to an outside accomplice who purchased gift cards. Some of those on trial appeared to be innocent victims, who were unaware that they were handling stolen goods, but the inmate and her accomplice were convicted of fraud.

Last year nearly ten million Americans were victims of identity theft related fraud. Most of these crimes were small—typically credit card purchases of no more than \$500.00. Others were hit a lot harder when thieves were able to take over identities and open new credit card accounts, make automobile purchases, and occasionally even take out second mortgages on victims' homes. Discovery of these thefts puts "fraud alerts" on the accounts of the victims, effectively ruining their credit ratings and preventing them from performing any ordinary purchasing

or financial transactions. In addition to the personal costs and problems incurred by the victims, identity fraud crime resulted in \$48 billion costs to businesses in 2003.

The latest phishing attempts indicate two dangerous trends. First, more sophisticated software is being used to phish. Powerful hacker tools are being modified, especially those that operate silently in the background as they collect information and exploit security vulnerabilities that have not yet been patched. Second, more and more phishing exploits are targeting financial institutions like major banks, investment brokerage houses, and national credit organizations. The hackers and phishers are getting smarter fast, and they are more often trying to steal money rather than cause computer problems.

Many of the comments to *The Bridge* about the trial and the phishing article included personal experiences. Thankfully, most of these had happy endings. An alert and suspicious potential victim avoided a trap and averted an impending crime. Comments also included protection tips and several links to excellent Web sites that can help prevent identity theft or assist in the aftermath of being victimized. Here are some of the best links and recommendations.

## **Precautions to take to prevent identity theft:**

1. Purchase a good paper shredder. Before throwing in the garbage, destroy personal papers, credit account bills, pre-approved credit applications, "convenience checks," and other document that provide personal and financial information.
2. Make sure no one looks over your shoulder when you use ATM machines or phone cards.
3. When you purchase new checks, have them delivered to your bank for pick



up rather than mailed to your home.

4. Don't send mail from your home mailbox. Put mail in a secure USPS box.

5. Call credit card companies if statements do not arrive on time or replacement credit cards do not come in a reasonable time before old cards expire.

6. When a Web site asks for your mother's maiden name or some such proof of identity, don't use what they ask for, but use something else that only you can remember.

7. Question financial institutions, doctors' offices, etc. about how they handle your private information and dispose of their documentation. Make sure they shred it.

8. Don't carry any identification or credit cards in your wallet that you don't use regularly. Especially don't carry your Social Security number. Memorize it instead.

9. Never give any information to anyone on the phone whom you do not know. If a request might be genuine, get the person's name and call back on the public telephone number from the phone directory. Even when the request is genuine, only give information you feel they have a need to know.

10. Use only secure Internet sites for credit card purchases.

11. Try to avoid dealing with firms and organizations that use your Social Security number for identification. Respectfully ask them to use another ID form. Some will and some won't. (In California it is now illegal for any non-government

entity to ask for a Social Security number.)

12. Notify your bank or credit card issuer if there is anything that you do not recognize on monthly statements.

13. Order credit reports twice a year and check them for fraudulent usage. Correct any erroneous information in writing to the credit bureau. Use certified mail to get a delivery receipt. The credit bureau must respond within 30 days.

14. Take your name, telephone number, email address, etc. off of any promotional lists that you did not request.

15. Keep your purse or wallet in a secure place when at work or anyplace where they are not in your physical possession.

16. Do not use computer software that "remembers and fills in" your account numbers, passwords, PIN numbers, or other identification data.

17. When disposing of a used computer, remove the hard drive and crush it or otherwise physically destroy it so it can never work again.

18. If you will be away from home for several days, have the Post Office hold mail and pick it up when you return, or have a trusted neighbor or friend collect mail in your absence.

### **If you discover you have been the victim of an identity thief:**

1. Notify the major credit reporting agencies (Equifax, Experian, and Trans Union) by letter to attach a "fraud alert" to your accounts.

2. Request copies of your credit reports from the same agencies and examine them for unauthorized activity.

3. Close any accounts that have fraudulent charges. Open new accounts if necessary.

4. Contact all other department stores, utility companies, credit card issuers and businesses with whom you have credit accounts. Call them on the phone and follow up with a letter informing them that you have had fraudulent charges on other accounts.

5. Watch for unusual activity on credit card bills. Make sure you are receiving bills from all of your credit card companies.

6. Keep a list of all contacts you have with credit agencies, law enforcement, and financial institutions. Be able to document with times and dates all notifications and account discussions.

7. Report the incident to your local police or sheriff's department. Get a copy of their incident report and give copies to creditors with fraudulent charges and others that require proof of the crime.

8. File a complaint with the Federal Trade Commission. It will be used to cross-reference related complaints and for evidence against any apprehended criminals. In some cases of fraud, you may also need to file reports with the FBI or the U. S. Secret Service.

9. Your state bureau of investigation and local attorney general may have Web sites, toll free numbers, and other information specific to fraud and identity theft in your area. Check to see what resources they provide.

Here are links to the sites where the above recommendations were found. Much more information and additional details are available.

<http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm> and

<http://www.consumer.gov/idtheft/> are operated by the Federal Trade Commission and they contain information for consumers and businesses. 42% of all complaints the FTC receives are identity theft related, so the site is one of the most complete with good explanations of the fraud related laws.

<http://www.usdoj.gov/criminal/fraud/idtheft.html> is the Department of Justice's excellent identity theft site. This was one of the first sites on the topic, and it has been consistently updated as information and resources improved.

<http://www.identitytheft.org/> is more personal and friendly. Mari Frank, herself a victim of identity theft, under-

stands the problems and frustrations and offers sympathetic help. Ms. Frank has written two books on the subject that victims have found invaluable.

<http://www.privacyrights.org/identity.htm> belonging to the Privacy Rights Clearing House addresses identity theft as well as privacy problems in financial and medical records, telephone communications, government records, internet access, and in the workplace. The site is bilingual (English and Spanish) and is operated by a non-profit public affairs corporation.

No matter how careful an individual may be in protecting confidential information, dealing with a sloppy vendor puts everything at risk again. Almost every company holds confidential customer data, so every computer and employee is a potential identity theft point. Here are some recommendations specifically for business security managers from Sarah D. Scalet, Sr. Editor of CSO Online magazine.

1. Practice good data hygiene. Provide the basic protections: Firewalls, background checks for employees who handle confidential information, and effective security policies. Those policies should include shredding sensitive documents and establishing audit trails.

2. Limit the use of personal information. Remove Social Security numbers from customer accounts and limit information access to only necessary employees. Make subcontractors and vendors comply with your security policies as a condition of doing business.

3. Keep customers informed. Let them know that your company won't ever ask for information by email. Make sure that employees know not to use email to ask for customer information. Ask customers who receive any such requests to report them to your security division.

4. Confirm information changes. Make sure that address changes are being made by the real customer and not by an identity thief. At the minimum, send an address change verification form to both the old and new address.

5. Keep up with technical solutions. Use secure verification methods to identify customers. Don't rely only on passwords or cookies to verify a user. Consider digital certificates or other reliable identification technology.

For more details on these five recommendations, and some chilling accounts of identity theft crimes and their effect on the victims, read Sarah Scalet's full article at [www.csoonline.com/read/030104/idtheft.html](http://www.csoonline.com/read/030104/idtheft.html).

Unless businesses and government offices handle personal information carefully, any precautions taken by individuals are useless. In a recent case, victims of more than \$8 million in identity thefts were related only by the fact that they all purchased cars from the same auto dealership. While police suspected that an employee of the dealership was selling personal customer information, it could never be proven, and the identity thief was never caught.

Two industry groups have been chartered to fight phishing. The Anti-Phishing Work Group (APWG) at [www.anti-phishing.org](http://www.anti-phishing.org) is lead by Microsoft, Verisign, Tumbleweed Communications, and a dozen other prominent technology firms. The Trusted Electronic Communications Forum (TECF) at [www.tecf.org](http://www.tecf.org) is a joint effort involving IBM, Target, Schwab, and other companies. Both of these new organizations intend to educate the public, lobby for effective anti-phishing laws, and find technological solutions to the problem. Both have acknowledged that the most valuable asset companies can have is the trust of its customers.

Phishing and identity theft crime have increased faster than any other illegal activities in a very short time period. Individuals, law enforcement, and impacted companies are having to play "catch-up" against a largely unknown criminal element. Phishing exploits the average individual's tendency to trust others and delay taking precautions until it is too late. Until an effective solution is found, we must all be vigilant or suffer the consequences.

-0-



**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](http://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**

**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
JULY 2004	5 	6 DOT.NET	7	8 VISUAL STUDIO	9	10 WEB WRITERS MS OFFICE
JULY 2004	12	13	14	15	16	17
	19 WORDPERFECT	20	21	22	23	24 INVESTMENTS
	26 CLIPPER	27	28 MAIN MEETING	29	30	31 
	2	3 DOT.NET	4	5	6	7 INTERNET HARDWARE
	9	10 	11	12 VISUAL STUDIO	13	14 WEB WRITERS MS OFFICE