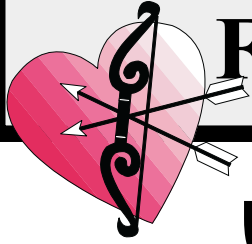


# MID-CITIES PC USERS' GROUP

## February 2001 Newsletter



## Wait! Don't Forward That E-Mail

By Julia Scheeres of Wired Magazine

A simple JavaScript could make millions of e-mail accounts vulnerable to what basically amounts to illegal wiretapping, a privacy group reported Monday. The code enables e-mail to be traced and read by embedding a 20-line script into JavaScript/HTML-enabled messages.

"It's a security flaw inherent in the design," said Stephen Keating, executive director of the Privacy Foundation. "It's hard to know how widely it's been used. But history shows that Web bugs like this are quickly incorporated into surveillance techniques."

### MEETING NOTICE

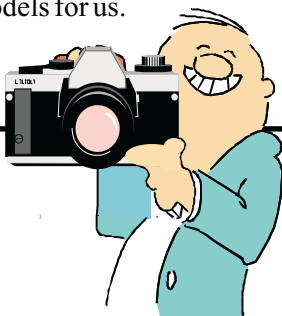
by: *George Miner*

**When:** Tuesday, February 13th,  
7:15 PM

**Where:** Old Bedford School (1800  
block of Bedford Road)

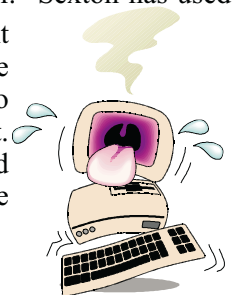
**Program:** **Hermillo**, a photo & video specialist with *Wolf Camera* will discuss the basics of digital photography. He will also talk about the variety of digital cameras on the market, and will demonstrate several models for us.

**Bring a  
Friend!**



Keating said the foundation spent two weeks testing the discovered bug by an engineer from British Columbia on different e-mail systems. Outlook, Outlook Express and Netscape 6 all use JavaScript/HTML-enabled e-mail by default and are vulnerable to the bug, he said. For the script to work, both the sender and recipient of the tapped message must use an HTML/JavaScript-enabled e-mail reader. Users of the AOL and Eudora e-mail application don't appear to be affected by the bug, Keating said. And it also doesn't affect Web-based e-mail, such as Hotmail. But some HTML-enabled e-mail readers, such as older versions of Netscape Messenger, pass along the wiretapping script without executing it themselves, he said. "To protect themselves, an organization would have to make everyone that works for them turn off JavaScript in e-mail," he said. The bug could be used to monitor confidential messages and to harvest e-mail addresses for spamming purposes, he said. In business, it could be used to glean inside information as a proposal spreads through a company's internal e-mail system. In the military, the consequences could be much more dire. The bug is easy to use and modify. David Martin, a computer science professor at the University of Denver, quickly intercepted a message this reporter forwarded to a colleague with his own version of the bug. And while using the bug is illegal, it is also very hard to trace, said Philip Gordon, a wiretapping expert with the Denver law firm Horowitz & Wake. "Typically illegal wiretapping doesn't come to light except in connection with the investigation of something else," said

Gordon. "It's constructed in a such a way that the actual person who planted the bug would be hard to find." The Privacy Foundation alerted Microsoft and Netscape to the problem and asked both companies to stop making their e-mail readers HTML and JavaScript-enabled by default. Netscape recommended that users change the preferences on their e-mail readers if they were worried about being victimized, but said the company had no plans to change the default settings. "Netscape is working on a fix to block the exploit," Netscape spokesperson Catherine Corre said. The bug-blocking software should be available in a "couple days." Microsoft didn't return calls for comment. The foundation has published instructions for turning off JavaScript in Outlook Express 2000, Outlook Express 5, and Netscape Messenger 6 on its website. The vulnerabilities of e-mail are nothing new to hard-core techies. E-mail may have come a long way since the text-only days, but the "new and improved" versions have also introduced security risks such as worms, Trojans and viruses. "People are now sending programs which run automatically on your computer through e-mail," said Richard Sexton, a Canadian Internet developer. "It's kind of like everyone on the Net can use your computer." Sexton has used his Eudora Light version 1.5.2 since 1994 and has no plans to update it. "HTML is a bad idea for e-mail," he said.



# The School Bell

*By Gil Hennon, Editor of the Memphis PC Users' Group*

Late last year we encountered an early example of a new breed of "virus," an email attachment that many users thought was part of a story about how the Seven Dwarves prepared a big surprise for Snow White. The surprise turned out to be a combination Trojan-worm-virus named W95.HYBRIS, which took control of WSOCK32.DLL in order to manipulate the computer's Internet sessions. Hybris uses idle time while connected to the Internet to download its own updates and patches. It also captures addresses from legitimate email, then sends its infection to these addresses.

Hybris was a turning point in rogue code development. Previously, most of the viruses spread by email attachment exploited specific security weaknesses in Microsoft Outlook. Users of other email client software might be vulnerable to infection, but usually could not spread the virus to other users. Hybris, in taking control of WSOCK32.DLL, the TCP/IP socket manager, was no longer dependent upon Outlook. This virus does not use the services of any email client program to capture addresses and send mail. It is a nasty bug and somewhat difficult to remove manually, but Hybris was only the beginning of our troubles.

In October, a Hybris-like virus called W95.MTX was released in Germany. By Thanksgiving, it was infecting U. S. computers. MTX can do all that Hybris does and adds a few more tricks of its own. MTX is also much more difficult to remove.

The virus arrives as a second email message, following behind a valid message from a legitimate sender. Usually there is nothing on the Subject Line and no text in the message area. The only content is the infection program, which may have any one of about thirty different names, including:

*matrix\_screen\_saver.scr  
new\_napster\_site.txt.pif  
win\_\$100\_now.doc.pif  
siecho\_no\_ie.exe  
protect\_your\_credit.html.pif  
me\_nude.avi.pif*

Clicking on the attachment creates an installation script named WININIT.INI. The next time the computer is booted, this script replaces WSOCK32.DLL with a variation of the file that it can control. It also corrupts the files EXPLORER.EXE and RUNDLL32.EXE to control user-run programs and system security. For example, the MTX virus scans the programs that are run on the system. When certain anti-virus programs are running, the virus will not run or it will drop copies of itself and start these too. Freshly dropped copies are named IE\_PACK.EXE, but they rename themselves WIN32.DLL the first time they are executed.

Another file that is dropped is MTX\_.EXE, a download manager that goes out on the Internet to get plug-ins and upgrades that increase the virus' capabilities. The registry is modified to start the download manager automatically each time the computer boots up while keeping the download manager invisible to the Windows Task List. Besides interfering with anti-virus software, MTX also keeps an eye on what Web sites the computer visits. Stopping at McAfee or Symantec causes MTX to crash the browser, or at the minimum, corrupt any file that is downloaded from these sites. While all of this is going on, MTX is also infecting files on all accessible drives. It infects EXE and DLL files greater than 8 kb in size, but skips any file whose byte size is evenly divisible by 101.

Regina Burns was infected by MTX before Christmas. She began to experience frequent, random system crashes and had trouble getting to some Web sites. She received an email reply

that warned her she was spreading a virus, but the combination of out-of-date virus definitions and MTX preventing the download of new ones left her with only manual removal as an alternative.

Symantec has a "tool" called FIXMTX.EXE that removes the virus from the operating system. That was a start, but the virus was still spread widely throughout her hard drives. When new virus definitions could be installed, MTX infected files were found in lots of Netscape and Internet Explorer files, as well as in many "temp" files that had been created while the virus was present. Windows did restart after cleaning the virus, which is not a sure bet, but many system files were corrupted, so the operating system had to be reloaded. The same was true for browser software, although her email client software continued to work. About 600 files, most of them related to TCP/IP and other Internet or networking functions, were corrupted and had to be reinstalled. Removing the virus took many hours of work, and a few "left-behind" problems are still popping up to surprise us. Putting the system back the way it should be is taking a lot more time. The MTX virus is a very nasty bug, but don't take only my word for it. Here are Regina's own feelings:

*It all started in November when a friend in Dallas sent me an email. Later, he sent me an email saying his computer was sending out "messages" and to watch out. A virus!, a virus!, not "messages," my friend! Thus began my odyssey which would still be nagging me had it not been for Gil Hennon, an old friend who rescued me. This virus took at least 12 hours of work to remove. It caused me enormous inconvenience in that I couldn't send email from my computer; instead I used other web mail services such as mailstartplus.com to execute*

***Continued on Page 3***

# GOLDSTAR SITES

*from article written by Alan Cohen for Yahoo Internet Life Magazine December 2000*

## AskMe.com

You shouldn't need an expert to find an expert. AskMe's design is simple but smart: Browse the Yahoo!-like directory to zoom in on specialists in a huge variety of fields. Categories are extremely narrow, so you don't have to worry about I.M. Pei fans answering your question on medieval architecture. You can see all the topics an expert has signed up for, so you know if your forensic scientist also fields queries on teen relationships. The search engine is excellent; it lets you find experts and archived answers by keyword and other criteria, such as response time or rating. All these tools, combined with a large pool of enthusiastic experts, make AskMe your best bet for getting questions answered quickly and knowledgeably.

### **How they decided this one:**

**AskMe.com** - Finding An Expert: Pinpoint control: Keyword search lets you find experts by subject, response time, and rating. Choose multiple experts to ask directly, or post your query on topical open-question boards.

### **Getting Your Answer: - Rating A**

Questions can be targeted to specific experts, so answers were often detailed and knowledgeable. Search the huge database of archived answers by keyword.

### **Quality Control: Rating A**

When experts fail to answer, it's noted in their profile. So is average response time. To answer open questions, experts must be registered in that category, so you can report a bogus expert.

### **Extras: Rating A**

Superior organization makes navigation a breeze. Huge variety of topics, from archaeology to zoology. You can ask questions anonymously, with no link to your own profile.

## **Best Product Advice - Epinions.com**

Buying that new DVD player can be tricky when you've got 50 models to choose from. To the rescue: a host of sites linking you to reviews provided by consumers who have used the products. The best of this breed is Epinions, where reviewers are rewarded with Eroyalties (redeemable for cash) for crafting thorough, insightful reviews in hundreds of categories.

## **Best How-To Learn2.com**

Sometimes the expertise you need can't be summed up in an e-mail. Maybe you want to learn the Heimlich maneuver, for instance, or how to jump-start your car. In these cases you'll need a step-by-step lesson. That's where how-to sites come in, offering prepackaged tutorials on a host of common and not-so-common tasks. Our favorite is - Learn2.com. Its many guides, on subjects from changing your oil to building a snowman, are detailed but never intimidating. Instructions are clear and well written; illustrations help guide you through some complex jobs. Better still, the tutorials do more than get you from point A to point B: They consider every variable (don't perform the Heimlich maneuver on an infant, for example) and offer appropriate alternatives. Each how-to is loaded with tips and tells you what tools and how much time you'll need.

## **Best Directory of Expert Sites - AskA+**

Have a question about the NASA space program? Sure, you can ask it at one of the Q&A hubs and hope for the best. But wouldn't you rather talk to a real astronaut than someone who has read a lot of Arthur C. Clarke? The good news: You can. Many educational, corporate, and even military sites have a page where you can direct a question to a professional and get an insider's insight. The bad news: These pages are often buried within large sites. Happily, the Virtual Reference Desk's AskA+ Locator does a terrific

job of rounding up these resources. It describes each service—from Ask the Optometrist to Ask a Hurricane Hunter—and tells you who runs it, how quickly questions are answered, and if there is anything you can do for more-immediate assistance. So should you ever find yourself in a semicolon crisis, for example, you'll know to skip the Grammar Lady's Web site and go straight to her telephone hot line. <http://ericir.syr.edu/locator/>

## **Best Expert Bookmarks - Blink** <http://www.blink.com/>

Picking someone's brain is all well and good, but sometimes all you really need is an expert's list of bookmarks. Services such as Clip2 [[clip2.com](http://clip2.com)] and Blink let users organize their favorite links by topic and share them. So if you're looking for the best sites on marathon training, there's no need to spend hours with a search engine; instead, check out the sites that marathon runners like to visit. Blink wins our Gold Star for its variety and usability.

*To be continued next month*



## **The School Bell**

*Continued from Page 2*

*email using my same email address.*

*I'm a self-employed writer, motivational speaker and communications specialist and email is critical in my business. I've lost countless hours trying to get this thing resolved. For several weeks my browser could not connect to any Web site.*

*While I had virus detection software, I didn't keep it updated (I know, shame on me). So, I had to learn a valuable lesson the hard way. Thank goodness for the Memphis PC Users Group and Gil.*

# THE MID-CITIES PC USERS' GROUP

The Mid-Cities PC Users' Group is a not for-profit organization whose objectives are:

- \* to provide a forum for the exchange of ideas and experience,
- \* education in the form of seminars and programs, and
- \* community as pertains to the computer industry.

Annual membership is \$24.00 per family with one vote per membership. Members are encouraged to notify the Membership Chairperson of any change of address as soon as possible to continue receiving their monthly newsletter. Please address any notifications to: Mid-Cities PC Users' Group: Attn. Membership Chair, P.O. Box 54141, Hurst, TX 76054

## 2000/01 OFFICERS AND BOARD MEMBERS

President	Steve Turner (817) 457-7131 president@mcpcug.org
VP Programs	George Miner (817) 292-3965 programs@mcpcug.org
VP Publicity	Don Helyer (817) 318-8475 publicity@mcpcug.org
Secretary	Sheryllynn Roberts (817) 531-7208 secretary@mcpcug.org
Treasurer	Tom Waak (817) 281-8950 Treasurer@mcpcug.org
Newsletter Ed.	Nancy Hester (817) 496-1961 newsletter@mcpcug.org
Member Chair	Anne Johnson (817) 268-6411 membership@mcpcug.org

# THE MID-CITIES PC USERS' GROUP NEWSLETTER

Published monthly by MCPCUG BOD and created using Corel Draw 8.0, a laser printer, and copied on a photocopier. Comments about the newsletter can be addressed to any officer or board member and constructive criticism is encouraged. Articles may be reproduced with proper credit given to *Mid-Cities PC Users' Group Newsletter*.

## CONTRIBUTING ARTICLES

**Article Style:** Type all copy flush left without justification; use word wrap feature for your paragraphs. This includes headings, by-lines, and the first line of each paragraph. Place a credit by-line (author's name) between the title and first paragraph. Leave no blank lines between paragraphs. Use only one space between sentences.

**File Formats:** MS Word or Word Perfect 5.0 is preferred. If formatting is crucial and you do not have access to Word Perfect 5.0 or Microsoft Word, send a hard copy to show the layout.

**Submitting Articles:** You may use one of two methods. Uploading the article to Nancy Hester at nancyhesterusa@netscape.net or you can hand them to her on diskette (3.5" preferred) during the general membership meetings.



Thanks a lot!

**Deadline:** The last Friday of the month prior to intended publication.

## Advertising Rates:

7½ in. x 9 in.	Full Page	\$40.00
7½ in. x 4 in.	Half Page	\$20.00
3¾ in. x 4¼ in.	Quarter Page	\$12.50
3½ in. x 2 in. Business Card		\$5.50

*Discounts: 3 months = 5%; 6 months = 10%. 1st month full price, discount applies to months thereafter.*

*Payment: required with 1st ad copy.*

Mid-Cities PC Users' Group  
PO Box 54141  
Hurst, TX 76054 <http://www.mcpcug.org>

**FIRST CLASS MAIL**