STAR Watch

Statewide Technology Assistance Resources Project

A publication of the Western New York Law Center, Inc.

Volume 7 Issue 4 **September 2003**

HELP! Internet Explorer is Running Slow!

There are a lot of nosy people out there. Some of those nosy people have gone to great lengths to try to find out about you and how you use your computer. Whenever you download "free" computer applications (or sometimes even updates to software that you paid for), the developers of those freebies may have included some "snoopware" that can collect information about you and your computer habits, and then send it to any number of interested parties. Usually, you are not told about the existence of the snoopware nor can you prevent its installation without canceling the installation of the intended product. (Some people argue that there is a fine but discernable line that separates snoopware from viruses. We see no difference.)

Snoopware can track the sites you have visited on the Internet or profile your shopping habits in order to target you for a deluge of spam. If you use a computer program to manage your household or business finances, snoopware can potentially extract information about bank accounts and credit card numbers and disseminate it.

It could also cause major problems for your computer by altering important computer settings and/or slowing it to a crawl. While each of these uninvited guests is recording who-knows-what, they are taking up memory and using CPU cycles. Then, when you connect to the Internet, the snoopware uses up the bandwidth that you paid for to blab all of your personal information. On frequently used computers, it is not unusual to find several dozen snoopware modules skulking about.

The end result is a computer with extremely degraded performance.

Believe it or not, snoopware is easy to remove—and it's free.

A company in Sweden has made available a product to hunt down and eliminate snoopware. This product will search through your hard drive, identifying and quarantining each and every snoopware module that it finds. To get a copy of this program:

- Go to: www.lavasoft.de
- On the left side of the screen, click on the "Ad-Aware" (not "Ad-Aware Professional" or "Ad-Aware Plus"; They are not free.) The "Ad-Aware" information screen will be displayed.
- On the right side of the screen, locate the "Download" information box; then click on the "Our software" link under it. The "Download screen will be displayed.
- Download a copy of Ad-Aware 6 Standard Edition from one of the listed sites; follow the instructions for installing & running the program.

In this issue…

HELP! Internet Explorer is Still Running Slow!

When that computer on your desk was new, it seemed like your web browser was a lot faster. Now, everything seems to take longer. Is it just your imagination playing tricks on you? Maybe not. There are a couple settings in Internet Explorer that might be causing computer to slow down when surfing the Internet.

In a less-than-perfect attempt to improve the performance of Internet Explorer, Microsoft reasoned that many web pages are revisited while users surfed the 'net. If the objects that make up those revisited web pages could be temporarily saved on the hard drive, any time the user returns to that web page, time could be saved because Internet accesses could be avoided. This would be especially useful for very slow (dialup) connections.

When Internet Explorer is installed, it allocates a fixed percentage of your C: drive to use for Internet temporary storage space and keeps items in it for up to 20 days from last use, depending on whether the allocated amount of space has been used up. If you have a small hard drive, a reasonable amount of space is allocated, but if you have a large hard drive a huge amount of space is allocated. Depending on the size of the hard drive, there may be more than a Gigabyte (1,000,000,000 bytes) of disk storage allocated to Internet temp file storage. A huge amount of disk space can contain a huge number of files, especially if the files are small (like most object files for the web pages). There could be thousands of files in the Internet temp storage area.

Whenever Internet Explorer begins to load a web page, it searches the temp storage folder for each of the objects that are part of the web page. If it does not find the object in temp storage, it then downloads the object from the website. Even on the fastest computers, searching through thousands and thousands of objects on disk takes a substantial, noticeable amount of time. The temp storage idea was meant to improve performance, not make it worse. Fortunately, this problem is easy to correct:

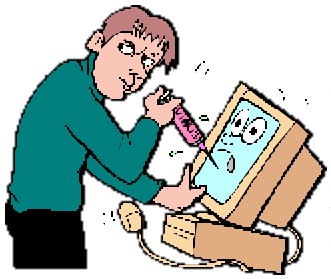
- Start up Internet Explorer
- In the "Tools" menu at the top of the screen, select "Internet Options…" The "Internet Options" screen will be displayed.
- In the "History" box, click on "Clear History". When this function completes, set "Days to keep pages in history" to 0.
- In the "Temporary Internet files" box, select "Delete Files…"
- Place a checkmark in "Delete all offline content", then click "Ok". Note how long it takes to complete this operation (this is approximately how long a search of the temp folder would have taken).
- Back in the "Temporary Internet files" box, select "Delete Cookies…" This will remove all of the old, expired cookies from your workstation.
- Click on "Settings…" The "Settings" screen will be displayed.

Set "Amount of Disk Space to Use" to 10-20 MB, which is a significant reduction from the original setting.

SoBig Virus

It's almost like the plot from a very bad horror film where the evil scientist attempts to take over the world by turning the citizens of a small town into robots who perform all kinds of terrible deeds. Basically, that's how the SoBig virus works. But instead of taking over the minds of human beings, it takes control of computers.

Unlike most other computer viruses of the past that were unleashed on the cyber community by someone with a little too much time on their hands, the SoBig virus appears to be a deliberate attempt by one or more spammers to deliver tons of spam and not get caught at it (and not pay for the bandwidth used to deliver it either).



It infects thousands of computers through a very simple means: User curiosity. The authors of the SoBig start the propagation of the virus by sending a very intriguing email containing the virus in an attachment to thousands of computer users. The message in the email directs the recipient to open the attachment. If the anti-virus software doesn't detect the virus in the attachment AND the user opens the attachment, the primary SoBig virus begins its sinister task.

First, it copies itself into the Windows folder. Then, it inserts entries into the system registry that will cause the virus to run whenever Windows is rebooted. While SoBig is running, it searches the local hard drive files for anything that looks like an email address and stores them. If the infected computer is on a network, it attempts to copy itself into the Startup folder of other workstations on the network if those folders are shareable.

At a predetermined time of day, the infected computers attempt to download a file from one web server that gives it the address of still another server. It downloads a secondary virus from the second web server and installs it. The secondary virus begins transmitting all of the collected email addresses to the spammer and sets up the workstation to become a email generator for the spam. At this point in time, the spammer can be confident that nothing can be traced back to him/her/it. Since the spam is actually generated on the infected workstation, there is no way to trace the origin of it beyond that workstation.

As the users of the infected workstations detect and remove the viruses or Internet Service Providers detect and stop the origins of the spam, the virus is slightly modified and the whole process is repeated.

The SoBig virus is actually very easy to thwart:

1. Make sure that your anti-virus software is up to date. It can't detect the latest incarnation of a virus if it's not kept up to date.
2. Don't open or view any attachment until it has been scanned by the anti-virus software.
3. No matter how much your interest is piqued, if you don't know the person who sent the email or the subject of the email is unusual: Don't open it! If there is a virus in the attachment, it cannot cause you any harm until you allow it to run. Remember, curiosity killed the cat.

Virus Protection on WNYLC Mail

Antivirus programs constantly run on the servers for WNYLC mail and WNYLC discussion groups. All mail that is sent to a WNYLC discussion group or to an address hosted on our server is scanned for viruses. Mail that is sent *through* WNYLC is also scanned for viruses. Both servers automatically check each hour for updated virus definitions and automatically apply new definitions. Over 150 viruses are blocked each day.

When a virus is found on mail sent to a WNYLC account, the virus is removed and an attachment called "*warn.txt*" is substituted for the virus. This file does not contain a virus. It is just a text file that tells the user that a virus was removed. The text file is also filled with spaces to fit the original file length. The scanning software doesn't change the mail file size because some mail protocols (like IMAP) may request the mail size first and then the mail body. Since the text file is the same size as the original infected attachment, all mail programs can still retrieve the cleaned message.

Because we run virus protection on our mail servers, some people ask us if they need to install virus protection on their machines. The answer is yes – for three reasons. First, viruses can be transmitted from scripts run on web pages. The Nimda virus, for example, can infect vulnerable Web sites by appending a script that could cause a browser to download the actual virus. Secondly, people can bring in disks with files that are infected by a virus. When the files are opened, the virus may spread across the internal network infecting other computers in an office. Finally, many people run multiple mail accounts or instant messaging (IM) on their machines. Viruses can come in through these other mail accounts (hotmail, msn, etc.) or through AOL or Yahoo IM accounts.

Symantec, the company that sells Norton Antivirus, still has a corporate giving program in place. The program allows non-profits to obtain free copies of antivirus software (there is a minimal handling charge). The application form is available at: http://www.symantec.com/corporate/software_gik.pdf. We have posted links to this application on www.wnylc.com. Just use the "News search" function to search for the word *donations*.

@#$&$#%*& Popup Ads!

You are working on your computer, minding your own business, your web browser is not even running, and Wham! A message is plastered in the middle of your monitor that says something like "If you don't want to be pestered by stupid, annoying messages like this one, come to our web site and for a small fee, we'll help you to get rid of this despicable form of spam".
After you have been hammered enough times by these annoying messages, you succumb to the hype and go to the named web site and get a sales pitch similar to this one from www.byebyads.com:

> *Have you been hit with unwanted advertising or Spam? The message you received is the newest form of Internet spam. You do not have to have an email account or even a web browser. You received this message due to a built in feature that Microsoft included in Windows XP, 2000, and NT.*
> *The worst part of all this is that some computer experts have indicated that it is also a potential SECURITY THREAT that hackers can use to infect your computer with a virus that is untraceable by current anti-virus software. Messenger pop-ups are defined to be pop-ups that are sent via the built in Windows Messenger Service, which means you do not even have to be at a web page to receive these types of pop-ups.*
>
> ***TO STOP THESE ANNOYING MESSAGES AND PROTECT YOUR COMPUTER WE HAVE A SOLUTION!"***

That is the sales pitch from a company that advertises their product by the exact means that their product is supposed to prevent. They say that they have a solution but we have an even better solution—and ours is free.

To get rid of some of those annoying popup ads…

- Go to the site: www.grc.com
- Click on the "Shields UP!!" icon. The "News & Views" page will be displayed.
- Click on "Shoot the Messenger". This will take you to the information and download page for this product. Before downloading, be sure to read the instructions on how to use this product.
- Click "Download" to get your copy of shootthemessenger.exe, a program that can shut off the ability of spammers to reach you with this form of advertising.

When the download finishes, run the program on your computer to stop any further annoyance from spammers using instant messaging.

WNYLC Web Statistics For September 2003

Total Hits 801,863
Total User Sessions 35,828
Average Hits/Day
(Monday—Friday) 28,101
Average User Sessions/Weekday . . . 1,415
Number of Pages Viewed 589,078
Average Number Of Pages
Viewed Per Day 19,002
Number of Documents Viewed . . 71,527

Accessed Using Internet Explorer . . . 95%
Accessed Using Netscape 2.3%
Operating Systems Used:
Windows 98 . . . . . 12%
Windows 2000 . . . . . 75%
Windows XP 8%
Windows 95 . . . . . < 2%
Windows ME . . . . . < 1%
Windows NT . . . . . < 1%
Macintosh . . . . . < 1%

WHO WE ARE

Joe Kelemen - Attorney
Kathleen Lynch - Attorney
Linda Hassberg- Attorney
Tom Karkau - Programmer
Brenda Pattison—Administrative Assistant


Wnylc@wnylc.com


716-855-0203


www.wnylc.net

Western New York Law Center, Inc.
295 Main Street, Suite 454
Buffalo, New York 14203