

# Is the World Wide Web Too Much Like the Wild Wild West?

## Internet Security Issues

By Jim Calloway, Director, OBA Management Assistance Program

The World Wide Web seems more like the Wild Wild West these days. The digital equivalents of robbers and gun-slingers seem to be hiding around every corner.

Item: An eastern Oklahoma lawyer reports that her computer is infected with malware that alternates between delivering pornography and apparent news items from *Good Morning America*. Despite sending the computer off to a professional technician for a "cleaning," the infection reappears as soon as she tries to use it again for work. Numerous other Oklahoma lawyers report similar problems.

Item: A Spanish newspaper reported that a contributing factor in a Spanair plane crash which killed 154 people in Madrid two years ago was a Trojan infection on the main airline computer system, which clogged the system and caused a failure to trigger an alarm about technical faults.

Item: An August 2010 article in *The New York Times* "Web Photos That Reveal Secrets, Like Where You Live" discusses Adam Savage, host of the popular science program "MythBusters," posting a photo of his car parked outside of his house on Twitter



with the tweet "now I'm off to work." Because the iPhone he used automatically inserts geotags that reveal the coordinates of the exact longitude and latitude of where photos are taken — someone who knew of this could easily locate his home and would also know that he just left it. (Note: One can disable the geotagging feature of the iPhone camera if desired).

Item: According to security software vendor McAfee, one tenth of websites devoted to the actress Cameron Diaz contain malware designed to steal information from the computer of the visitor. McAfee noted finding about six million malware infected systems and that apparently over 55,000 new types of malware come out every day.

Item: In August 2010, the U.S. Department of Defense publicly expressed concern over China's rapidly evolving cyber-warfare capabilities. U.S. government computer systems

and others around the world continue to experience intrusions that "appear" to originate within China, according to the Pentagon.

Item: In August 2010, the Federal Aviation Administration announced that its computer systems remain vulnerable to cyber attacks despite improvements in the past year.

Item: A staggering 92 percent of all e-mail is now spam and over 40 percent of that came from a single botnet, the Rustock botnet, according to Symantec's August 2010 MessageLabs Intelligence Report. (A botnet is a large collection of computers that have been compromised and can be operated collectively by the one who set it up, known as the "bot herder.") The report also found that one out of every 328 messages contained a virus and one out of every 363 was a phishing attack (an e-mail designed to get one to give up personal information like passwords, credit card numbers or bank account numbers).

Item: Recently the Internet security firm Panda Labs reported its discovery that 25 percent of newly created worms are specifically

designed to spread through USB storage devices. This is not limited to USB flash drives, but includes other USB-connected devices as external hard drives, digital cameras, MP3 players and smart phones.

Item: *The Wall Street Journal* completed a series this summer about how privacy is compromised at the most commonly visited websites. *The Journal* catalogued tracking files that were placed on computers at the top 50 most visited websites and the results were stunning. "The 50 sites installed a total of 3,180 tracking files on a test computer used to conduct the study. Only one site, Wikipedia.org, installed none. Twelve sites, including Dictionary.com, Comcast Corp.'s Comcast.net and Microsoft Corp.'s MSN.com, installed more than 100 tracking tools apiece in the course of *The Journal's* test." The information obtained from these tracking files creates a profile of users that is then auctioned off to various corporations. A credit card issuer may only display the less attractive card options when you visit their website based on this profile.

Malware is a term used to collectively refer to all of the various bad things that your computer may "catch" online. These include computer viruses, trojans, adware, spyware and other tracking software.

In the early days of the Internet, one Oklahoma law firm installed one computer with Internet access in their library, which was not connected to any other computer. E-mail, electronic filing and online legal research have done away with that setup

now, but maybe they were ahead of their time.

As the *WSJ* series points out, spyware is used for illegal purposes such as stealing credit card information and also for legal, but ethically questionable practices, like collecting and auctioning off the records of your Internet activities.

So what's a lawyer to do?

Let's think like lawyers and prioritize the issues. As repugnant as it may seem that the business community thinks it is OK to place secret snitches on your computer to profile you and then auction off the results, stopping that is beyond the scope of this article and the individual efforts of most of us.

First issue is that all of the spyware and malware could literally cause our computers to grind to a halt and become unusable. The second issue is that even if the malware and spyware does not kill the computer, the collective impact is to make it run slower and slower.

Lawyers do not want to put their business operations at risk due to a dead computer, whether it is a victim of malware, flood or fire. Backing up your data is your critical first step to avoid many technological disasters, including your computer dying from "malware overload." If you have IT staff in your firm, they are aware that this is their most important job. If you are in a smaller firm or a solo practitioner, then backup is your responsibility and one way to make certain there is no breakdown is have multiple layers of backups. You can use an online backup like OBA-endorsed CoreVault. But you can and should make a copy

of all of your files regularly on a portable hard drive or two. You can even copy forms, client documents and your case management data on a small flash drive as long as you make certain it is securely stored.

Of course, while good backup procedures help us recover from disaster, most of us would rather avoid disaster in the first place.

Practice safe computing. "Don't click on unfamiliar e-mail attachments" has become a bit of a cliché, but it bears repeating. Don't click on e-mail attachments unless you are expecting them — like a draft of a pretrial conference memo from opposing counsel on the day before it is due. Your bank probably isn't e-mailing you and if you need to check your account go to the normal website. Do not try to save time by clicking on a link in an e-mail you think is from your bank.

Never click on a pop-up window indicating malware has been detected on your computer and should be eliminated unless this message is from a software tool you have purchased and installed. Fake malware warnings and offers to clean your computer via pop-up windows are created by malware and clicking on the warnings can give you a massive dose of malware.

The required tools for protecting your computer sound intimidating to the amateur. But there's really no safe alternative. You need a firewall. You need antivirus software. You need antispyware software, if for no other reason but to regularly clean off those tracking cookies and tracking programs that *The Wall Street*

*Journal* tells us popular websites install on our computers.

## THE FIREWALL

Most PC users will want to activate their Windows 7, Vista or XP firewall. These products, particularly the later ones, do a decent job. Your Internet service provider likely also provides you some firewall protection. Larger firms may have a hardware/software combination firewall managed by their IT staff. These products do a good job. When you click on an e-mail attachment or a link to run a bad file, you are telling these products it is OK to let the process past the firewall. This is why it is so important that the computer user be cautious. Some users prefer purchasing a commercial firewall software product.

## WIRELESS SECURITY

Whether you have a wireless network at home or at work, it is no longer appropriate to have it wide open where anyone can log in. Leave that setting for the coffee shops and hotel chains to defend. You have to set up security and require a password to log in. If you have an open network and no longer have the instructions on how to configure it, you can locate them online at the wireless router company's website. But if you have an old "G" router, it may be simpler just to go buy a new faster "N" router that will come with all of the instructions right in the box and end up with faster Internet access in the process.

## MICROSOFT SECURITY ESSENTIALS

If you don't consider yourself a technology expert and use a Windows-based computer, then it is probably essential that you download and install

“...all of the spyware and malware could literally cause our computers to grind to a halt and become unusable.”

Microsoft Security Essentials, although some of the commercial products listed in the next section may be preferred by some. But Microsoft has provided a nice, free product that replaces its Microsoft Live OneCare.

“Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware and other malicious software. Microsoft Security Essentials is a free download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology. It's easy to tell if your PC is secure — when you're green, you're good. It's that simple,” according to the Microsoft website.

You can download Microsoft Security Essentials here: [www.microsoft.com/security\\_essentials](http://www.microsoft.com/security_essentials) or here: <http://tinyurl.com/kwsxcu>

## ANTIVIRUS AND ANTISPYWARE SOFTWARE

As the reader has no doubt determined by now, using antivirus and antispyware products is a requirement these days for the small firm lawyer with no IT department assistance and for the home user as well. When I use

Google to search for these products, I am usually not happy with the initial results, which are mostly sales oriented. I tend to use the Google advanced tools to limit my searches to resources I trust that do software product reviews. These include sites like [www.pcmag.com](http://www.pcmag.com), [www.pcworld.com](http://www.pcworld.com) and [www.lifelife.com](http://lifelife.com) and <http://reviews.cnet.com/software>.

I would never install a free antimalware product without first reading a review of it from a trusted source. Even then, I'd see if I could download it from a site that I know is legitimate and has security safeguards like <http://download.cnet.com>. (I note that when I visited CNet while writing this article, five of the six most popular downloads were antimalware products).

In fact, *PC Magazine* reviewed several free anti-malware products in its “Best Free Software of 2010” feature. This part of the feature is online at <http://tinyurl.com/yjtl49k>. But for most lawyers, while free is nice, you really should upgrade to the paid professional version of these products, even though some free versions enjoy good reputations.

Personally, at home I have had good results from Webroot's Antivirus with Spysweeper.

When there are really bad malware infections on a computer, nothing seems to work as well as Malwarebytes Anti-Malware and their free and paid anti-virus tools garner great reviews.

Some infected computers will block one from visiting sites that provide malware cleaning and protection. For a

do-it-yourself cleaning of an infected computer, you can disconnect the computer from the Internet and load the free version of Malwarebytes Anti-Malware from a USB flash drive. The cleaning may take a few hours and may also convince you to buy their product.

Our operating systems have stronger defenses now as well. Windows 7 and Vista are sold with User Account Control (UAC), which will search for potential risks and immediately suspend operations if a problem is identified.

### **SOCIAL NETWORKING ISSUES**

Recently many Facebook users got messages from their Facebook friends on how they could get a brand new iPhone 4 for absolutely free. Just click this link. If they would just take a second to think about it, they might consider whether it is more likely that their friend has had his or her Facebook account compromised in some manner or there's a really a secret plan to give away free iPhones that hasn't been leaked to the media. There's no harm in reading these messages, but always send a message to your friend to confirm it really came from them before clicking on unusual

## **Starting Your Law Practice Program Dates Set**

- **Sept. 28 - Tulsa**
- **Oct. 5 - Oklahoma City**

For several years the OBA has presented The New Lawyer Experience Program a few days after the new members of the Oklahoma bar are sworn in. Although brand new lawyers are our target audience and attend in good numbers, we have always had a significant number of experienced lawyers in attendance. Some were changing their careers and others just wanted a refresher course on law practice management. This year we have decided to rename the program to better reflect the subject matter. It will now be called Starting Your Law Practice. It is still free, with a free lunch provided by Oklahoma Attorneys Mutual Insurance Company. But the curriculum has been redesigned to reflect the economic realities of opening a law practice in these challenging times. The program will be held Sept. 28, 2010, at the Tulsa County Bar Association and Oct. 5, 2010, at the Oklahoma Bar Center. More details can be found on the OBA events calendar at [www.okbar.org/calendar](http://www.okbar.org/calendar). To register, e-mail [marks@okbar.org](mailto:marks@okbar.org) or call Mark at (405) 416-7026.

links. You can still click away on the YouTube video links that they send you.

### **CONCLUSION**

One rule of thumb before installing these antim malware products is to set a restore point in case something unexpected happens. Generally speaking, it is a bit risky to run two antivirus software programs from different companies. It is likely they will conflict unless the real-time, on-access scanning is disabled

and even then there are no guarantees. There is no permanent harm from this. The computer may just run slow, lock or reboot frequently. According to online reports, running two antispyware solutions does not seem to create the same issues and one may find things that the other missed.

Hopefully, putting some of the "sheriffs" detailed above on the job will make you feel a little less like you are in the