Aug. 01, 2005

From the August 2005 Issue

For several months now, there has been a steady drumbeat to switch from using Internet Explorer to Firefox, Netscape, Mozilla or some other browser because supposedly they are more secure and have less vulnerability. Just in the last month, however, several of these alternative browsers have also had their share of vulnerabilities discovered and publicized in the media. Is any browser safe? Probably not!

Can you reduce your exposure? Yes, you can! In this article, you will discover how to secure Internet Explorer to reduce the exposure and eliminate the risks from spyware, viruses, Trojan horses and malware. This article will provide a way to stop these unwanted pests by using the functionality already built into Internet Explorer.

"Why is this important to accountants," you might ask? Aside from the fact that the alternative browsers are not compatible with several applications used in accounting firms such as QuickBooks, accountants have a duty as prescribed by several laws and our ethics code to protect client data from disclosure to third parties not authorized to view such data. Spyware, Trojan Horses and other items infecting our computers can and do expose client data to non-authorized individuals who should not have such information. HIPPA; Graham, Leach, Bailey; and Sarbanes-Oxley put restrictions on disclosures of information.

The AICPA has also said in its Ethics interpretations that failure to protect confidential client information may be grounds for an ethics investigation. States are also getting into the act by moving
forward with privacy laws
that can cause trouble for accounting firms and even those in industry if confidential

data is released to the public.

zones. By default, this zone
is set to a medium security level. The next zone is Local Intranet. This zone covers web sites, servers, and other internal components located on the network to which the computer is connected. By default, this zone is set to medium-low. The next zone is Trusted sites. This zone is used to specify internal or external web sites that you specifically trust will not harm your computer. By default, this zone is set to low. The final zone is Restricted Sites. The Restricted Sites zone is the place to specify web sites that could cause damage to your computer operating system or cause data loss if accessed. Each of these zones, separately and combined, provides the ability to control the browsing experience. The impact the Internet will have on your computer is controlled through these settings in these four zones.

As the vulnerabilities increase on the Internet, having the appropriate settings for each of these zones is important to maintaining a computer free of the junk floating around the Internet. The recommendations that follow are derived from personal experience as well as extensive reading on how the various spyware, viruses, Trojan horses and other malware find their way onto computers. If everyone would change his/her settings as recommended here, the malware generated on the Internet would become much less prevalent.

To stop web sites from adding tracking cookies,
pop-up ads, spyware, Trojan horses, and other malware, the Internet zone setting needs to be set at high — the same as the Restricted Sites setting. By choosing the high setting, all Java, Active-X and other "programming components" allowed by a lower setting are blocked from being able to execute. By choosing this setting, it causes any web-enabled content from the Internet to be blocked. For example, if you open an HTML-formatted e-mail, the policy settings here will prevent any hidden formatting from executing, such as an Active-X control that launches a Trojan horse from a web site or downloads a spyware application onto your computer. The

unfortunate impact of this change is that it blocks all content, so legitimate sites

web site because the underlying zone settings of Trusted sites are lower than the Internet zone settings.

If you are a frequent browser of the Internet and like to click on links, this solution may become very bothersome to you because you have to add sites all the time. However, if you are a general user of the web, once you have the site in your list of Trusted sites, the addition of trusted sites becomes less and less necessary. In Windows XP SP2 and Windows 2003 Server, Microsoft has made it easier to add sites by providing a "quick add" option that provides a dialog box to add the site on the fly. Wildcard characters are also allowed for content type (http, https, ftp, file, etc.) and for sub-domain, which makes the addition of a group of domains, sites or content type a much quicker process.

Creating the Trusted sites list can be very time consuming, but the time involved is still less than the cost of paying for the cleanup of spyware, viruses and other malware content on your computers or suffering through the performance loss due to these malware products. You will soon learn how to spot the characteristics of a poorly displaying web site due to blocked content. This will help you to know when you need to add the site (if desired) to the Trusted sites list.

Local intranet works in much the same way as Trusted sites, with one exception — the settings are lower. The recommended settings for Local intranet is medium-low. Sites added to this security group should be limited to sites that are inside your gateway perimeter firewall or those sites that you trust explicitly to never have any type of content harmful to your computer. The process of adding sites to this location is exactly the same as adding them to the Trusted sites zone. Use this zone very sparingly for web sites outside of the local network because you never know when a site is going to start changing privacy policies or adding content.

Restricted sites are infrequently used because the security zone settings are exactly

the Privacy tab to block cookies and stop pop-ups (if running Windows XP Service Pack 2). By changing the cookie settings to high, it makes control over what comes into your computer even stronger. Individual sites can be added in the same way as sites can be added under the security tab by clicking on the sites button and adding the name of the site for
which to allow cookies. You can also unblock pop-ups by clicking on the settings tab and adding sites to the allow list for pop-ups.

By using this built-in functionality, you can control and strengthen what is allowed on your computer and what is blocked from accessing your computer. This ability to increase and utilize the Security Zone tools for content provides the means to control the access to the system from only those sources you allow access. Mozilla, Firefox, Netscape and others may handle this in a different manner, and perhaps with a more friendly user interface, but there is no need to switch browsers to increase your security on the Internet. All you need is to utilize the tools already built into the operating system to safeguard your browsing,
help prevent malware from gaining a foothold on your computer and keeping the nastiness of the Internet off your computer. As with anything, utilizing the tools provided to lock the door will stop the problems from occurring in the first place. By stopping the problems before they start, you are certainly better prepared than the next person who doesn't take the necessary steps. Switching browsers may not be an option for some users, but learning how to lock the door and prevent the problems can is an option with Internet Explorer.

AUTHOR'S PERSONAL NOTE:
I have been using these settings for the past 18 months. During those 18 months, my computer has had no virus, spyware, Trojan horse, or other malware, even when running multiple spyware products and checking the system with multiple antivirus software products. Others have not been so fortunate. I know one individual who

lowered his Internet zone setting from the recommended high setting in this article

Sponsors.