Apr. 17, 2007

Back in 2005, I wrote an article on this same topic for this magazine. At that time, many people were calling for the abandonment of Internet Explorer in favor of FireFox, Netscape, Mozilla or some other browser because supposedly they were more secure and less vulnerable. Two years later, that drum beat has ended because those other browsers proved just as vulnerable. With the release of Internet Explorer 7, Microsoft has adopted many of the concepts I discussed in my article from two years ago and has added some functionality that makes it easier to use the security zones.

Why is this important to accountants?

Well, many of these alternative browsers are still not completely compatible with some of the accounting applications used in firms. In addition, things have changed in government (more regulation) and in the technology industry (more identity theft, phishing scams, Nigerian hoaxes, and many other security threats not even imagined two years ago). Just recently, the computers at the credit card processing company for several stores in a major retail chain were compromised by hackers. Identify theft and credit card thefts are the two most rapidly growing crimes in the world. Organized crime has gotten involved. Accountants who fail to take proper precautions to protect themselves, their networks and their clients' data open themselves up to the potential for a security breach either inside or from outside their firms.

When the Internet was still in its infancy (1995), Microsoft integrated the functionality required to make the Internet work into the primary code area of Windows. Ten years later, this proved to be a tragic mistake as the denizens of the Internet figured out how to use this to gain access to Windows, bypass security and

cause all kinds of mischief. Microsoft has gotten religion and released what I

security level. The next zone is Local Intranet, which covers websites, 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, which is used to specify internal or external websites that you specifically trust will not harm your computer. By default, this zone is set to low. The final zone is Restricted Sites, which is the place to specify websites 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 the settings in these four zones.

It is not enough to stress the importance of using these new zone settings to protect your computer from predators on the Internet. Each of these zones provides and controls how web-based content (whether in an e-mail, on a website or in some Trojan you just opened) is going to work on your system. The more secure the settings the better.

Here's a brief review of the settings for each zone:

- Internet should be set to medium high,
- Local Intranet should be set to medium low,
- Trusted Sites should be set to medium,
- Restricted Sites should be set to high, and
- Local Machine should be set to low.

(Note: You cannot directly control the Local Machine settings, and this one does not appear in the list. It is set to low by default and cannot be changed easily.)

For added protection, you can set the Internet zone to high, but this will break the browsing experience. It will also stop websites from adding tracking cookies, pop-up

ads, spyware, Trojan horses and other malware in the Internet zone by blocking

medium setting, which is the same as the default setting for the Internet zone. Most legitimate websites are designed to display properly with a medium setting. By adding the website being viewed to Trusted Sites, the content will display properly when visiting that website. 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 sites, the adding of Trusted Sites becomes less and less necessary.

Creating the Trusted sites list can be very time consuming, but it 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 to these malware products. You will soon learn how to spot the characteristics of a poorly displaying website due to blocked content. This will help you to know when you need to add the site (if you desire to add the site) to the Trusted Sites list.

Local Intranet

Local Intranet works in much the same way as Trusted Sites, with one exception — the settings are lower. Sites added to this security group should be limited to sites that are inside your perimeter firewall or those sites you trust explicitly to never have any type of content harmful to your computer. The process is exactly the same as the Trusted Sites area. Use this zone very sparingly for websites outside of the local network because you never know when a site changes its privacy policies or becomes compromised by a hacker.

Restricted Sites

Using Restricted sites is very uncommon, but this zone would be utilized in the case where you do not trust a site but need to obtain content off the site. Perhaps you are

visiting a site in a country known to traffic in stolen information. You might add

stopping the problems before they start, you are better prepared than the next person who doesn't. Learn and use the new tools as built, and you will have a better, more secure browsing experience.

Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.