7 Deadly Sins of Web Surfing

These days, using the Internet is one of the most dangerous daily activities that you can undertake. Admittedly, the odds of bodily harm, other than carpal tunnel, are slim. The real danger lies in the potential impact web browsing can have on your personal identity and financial standing. Every computer connected to the Internet is a target of malware, viruses, and spyware, all of which are secretly installed onto your PC. The individuals behind these have one purpose in mind - to collect personal information about you *and* make money from what they learn about you. The following information is intended to simplify the process for you; however if you are heavily time or tech challenged, you can hire an IT professional to implement many of these safety features for you. Having the list will ensure that you cover all your bases.

Here are seven things you can do that can help you avoid the dangers:

1. *Don't have a good hardware firewall router.* Not having a good, separate active hardware firewall between your PC and your modem will let hackers have access to your network. A firewall is designed to permit or deny network traffic based upon a set of rules and it protects your networks from unauthorized access while permitting legitimate communications to pass. You want the firewall to have Denial of Service (DoS) protection and use Stateful Packet Inspection (SPI) to protect your network. (Just look for these on the box.)

2. *Don't keep your Antivirus updated.* With new viruses coming out every day, one sure way to get a virus is to not update your antivirus product. It's bad enough that new viruses can get through prior to the software companies devising a way to stop them, but once a solution is devised, you want to get it. Update this daily.

3. *Don't have antispyware.* Spyware infections are just as dangerous as viruses. They secretly collect pieces of information about you. With spyware present on your system, you may open yourself up to identity theft and credit card fraud. You don't want your PC "phoning home" with your personal information. Run an antispyware program at least weekly.

4. *Don't keep your web browser updated.* It's important to keep your web browser up-to-date with the latest patches. Patches are coming out much more frequently now than ever before. Familiarize yourself with the built-in safe surfing features, and tweak the settings to ensure a high degree of protection. The browser providers realize that they have competition and that customers are expecting them to help provide a safe browsing experience. Check for updates weekly.

5. *Don't keep Windows updated.* Again, patch management is a key to keeping your systems secure. Microsoft sends out security updates once a month on "Patch Tuesday". This is usually the second Tuesday of each month. Run the Windows Update as soon as they come out. This protects you from exploits to your from your OS, other Windows components, and the Microsoft Office Suite. Updates for other Windows products such as Microsoft Security Essentials (highly recommended) and Windows Defender are sent out much more frequently.

6. *Click on Pop ups.* Never click on a pop up – whether it is from an antivirus program, Adobe, some other software, or any other so-called updates. Always go to the website directly to update any programs on your PC. Follow this golden rule -> If you are not sure, <u>or even if you *are* sure</u>, *never ever click.*

7. *Click on a link in an Email* – especially if they are from a bank, credit card company, or services like PayPal. Only click on these if you want to let the world have your personal information. Never believe an email. Always go directly to the website by opening up a new browser session and do whatever you need to do. The same goes for Emails from social media sites.

Identifying where a link goes. One trick - If you hover over a link with your mouse, is should display the destination website in the bottom left or right of your web browser. Be sure to look at the last "www" address if there is more than one, as the last is the destination website.

Example:

www.website.com/..../www.badwebsite.com

Here is a link where you can find some great information and explanations about malware - http://www.kaspersky.com/threats_faq.

"Tech Talk" is authored by Chamber member John Kalli, CEO of Trinity Worldwide Technologies; and will cover important technical topics that we believe can help our members/readers. Basically, our goal is to provide you with the knowledge that can save you time, money and potential disaster. Trinity is a Microsoft Certified Partner, Microsoft Small Business Specialist and has vast experience in all realms of computer networking, repairs, installation and more. If you have any questions about the security of your IT network, Trinity Worldwide Technologies can help you by assessing your specific IT environment and recommending the proper security measures for your organization please contact John at JKalli@trinityww.com and see if you qualify for a no cost, no obligation assessment of your business' technology, you can reach them at services them at 732-780-8615. Visit them at www.trinityww.com.