

Keeping Safe on the Internet

Written by Stephen

Tuesday, 01 February 2011 21:00

Part 1: Just Browsing We're starting a new series of articles will hopefully advise readers as to some good habits to develop in order to limit exposure to viruses, malware, and other damaging agents on the Internet. Basic Internet usage has become a staple for many, but even with the ease of accessibility and use, the Internet is filled with dangers both to your computer and data as well as to your identity and reputation. The first of our entries to this series covers how you cruise around on the Information Superhighway. This series of articles will hopefully advise readers as to some good habits to develop in order to limit exposure to viruses, malware, and other damaging agents on the Internet. Basic Internet usage has become a staple for many, but even with the ease of accessibility and use, the Internet is filled with dangers both to your computer and data as well as to your identity and reputation. The first of our entries to this series covers how you cruise around on the Information Superhighway. Browsing the Internet has been likened to walking around the streets in a big city. As you walk, you'll find that there are many interesting locations to visit which are safe and secure, even welcoming. However, like all big cities, there are areas that are more dangerous, more seedy, and are not as welcoming to your curious eyes. While in a city, you may have the foresight to not walk down a dark alley, on the Internet, those signs might not be as obvious. Vigilance and caution are required to maintain a clean and safe surfing experience. A Gaelic proverb says that "he who lies in the mud will rise dirty". In a practical sense, this is true with content on the Internet. If you go to questionable websites which are off the beaten path and down the dark alleys, your risk of being exposed to viruses, malware and even identity theft and data corruption are significantly higher than if you stayed on the lit, well-populated streets. With that said, websites which feature hacking techniques and software, pirated software and pornography are danger zones for your computer. That's not to say that all sites that have that content are dangerous but you will have a greater chance of a compromise if you frequent that material. Being mindful of what you're clicking on can be very helpful. A technique used by hackers is called URL masking. When you see a link to a page in a browser, you can place your mouse over that link and it should tell you the address it will direct you to. In this example, I've highlighted the CNN link "Record snowfalls slam Northeast" and at the bottom of the screen, I see that it's going to send me to that URL. However, there are numerous examples on the Internet where you may hover over a link and it may look secure, but once you click the link and have been redirected, you will find the address does not match at all what you saw previously. Care is required, especially when performing online purchases as you may find you are supplying hackers with usernames, passwords, phone numbers, and even credit cards. There are some products which attempt to negate some of this risk, such as AVG LinkScanner, but knowledge is power. Even when browsing safe sites, you still can be found vulnerable. Pop-ups and ads are frequently misleading and will infect your computer with many varieties of spyware. Downloads, even from legitimate websites, can contain viruses if not properly scanned on your system. We'll be covering some of these dangers in more detail in later articles. One of the ways that you can start to secure your computer is a self-evaluation of your computer habits. If you find that you have, or have had, issues with spyware or viruses, perhaps you can modify your surfing habits. If that is not always an option, or you have issues with accidental infection, then perhaps using a different web browser might be advisable. Microsoft Internet Explorer is pre-loaded with Windows computers, but with its native ActiveX support, it often is the target of exploits which can put you at risk. Google Chrome and Mozilla Firefox are generally regarded as the two of the safest web browsers freely available. Opera, Apple's Safari, and Microsoft's Internet Explorer generally rank lower on the security scale. No amount of installed browsers

Keeping Safe on the Internet

Written by Stephen

Tuesday, 01 February 2011 21:00

can make you completely safe. You have to become street smart when navigating the Internet. Browse slowly, be mindful of where you are going, and use the tools at your disposal and you can enjoy a more peaceful visit to the Internet. Our entry next week will discuss downloading on the Internet. What are some things to keep in mind with where and what you download? We'll discuss that next. For more details on information and products covered here, please visit these (safe) links: ActiveX: <http://en.wikipedia.org/wiki/ActiveX> URL Masking: http://en.wikipedia.org/wiki/Domain_Masking AVG LinkScanner: <http://linkscanner.avg.com> Google Chrome: <http://www.google.com/chrome> Mozilla Firefox: <http://www.mozilla.com/en-US/firefox>