

ASK THE COMPUTER SURGEON

Net Threats – How to Stay Safe On-Line?

This is the second in a series on the serious matter of Internet Threats. These “threats” (the risk of having your identification stolen) keep the act of going online a risky and ever growing, dangerous venture.

There are now thought to be more than 200,000 malicious programs in existence - the vast majority of which are aimed at subverting Windows PCs. According to one report, these problematic programs can arrive via e-mail, instant messenger, through your internet connection or even your web browser if you visit the wrong website. The threats are so numerous and appear so fast that Windows users might feel under siege. However, you don't need to be helpless victims. You have control and you can take a stand.

A local company, Protectus®, has provided a great “security tips” pamphlet that lists the TOP 10 Personal Security Tips for the average computer user. They are:

1. Use a security software suite that includes anti-virus, firewall, and anti-spyware. Configure it to automatically receive updates. We have also included a link to a selection of some free security programs:
<http://www.download.com/Antivirus-Firewall-Spyware/?tag=dir>
2. Keep your Windows operating system updated using the “Windows Update” selection found under All Programs (clicking the Start button will take you to the Programs section). These updates fix the bugs that allow for many security vulnerabilities. Likewise, you can set this to update automatically.
3. Keep your applications (i.e., MS Office suite) updated as well. The vendor's website normally provides an update mechanism.
4. Never open unexpected email attachments even if it appears to come from a known sender. An unexpected attachment may contain a virus.
5. Avoid shared folders and peer-to-peer file sharing whenever possible. Many security threats spread via file sharing.
6. Routinely back-up important files and folders at least once a week.
7. Avoid those “free software or free screensavers” offers, they probably contain spyware.
8. Use passwords that do not contain familiar numbers or phrases such as Social Security Numbers, birthdates, family member's names, the street you live on or the like. Best practice is to include numbers, letters and punctuation in your passwords. Don't use the same password for everything. The best way to remember passwords and keep them difficult to decipher is to create a common phrase. For example the following would be considered a strong password and yet easy to remember: *Is@wTh3Lite!*
9. Never reply to requests for passwords or personal information. A legitimate company you do business with will never ask you for these – especially on-line. They'll also never ask you to login to a website to “fix” your account.
10. Shutdown your computer when it's not in use. In the very least, disconnect the internet connection if you need to keep your PC running for other tasks.

There is no single cyber security practice or technological solution that will prevent online crime. These recommended security practices highlight that using a set of practices that include Internet habits as well as technology solutions can make a difference. For further information and a deeper exploration of this important topic, visit the following websites:

- <http://staysafeonline.org/basics/index.html>
- <http://staysafeonline.org/basics/quiz.html> (this is a self test to see how secure you are)
- <http://www.ftc.gov/bcp/online/pubs/alerts/idsalrt.shtm>
- <http://www.cert.org/homeusers/HomeComputerSecurity>
- <http://look-both-ways.com/blogs/blog/archive/2007/06/04/956.aspx>
- <http://www.haltabuse.org/resources/online.shtml>

In the next article, we will discuss: Does it Pay to Pay? What Security Software Should I Use? To view the first article in this series, visit our website www.compusergeon.com.