Title:
Computer Security: Threats and Solutions

Word Count:
566

Summary:
Unfortunately, much of the common sense advice we follow when it comes to Internet security does little to combat the cyber-crime that is rampant. Here is the inside scoop....

Keywords:
virus,spyware,malware,cyber-crime,identity theft, internet security,Hassle-Free Computing.

Article Body:
When it comes to computer security, many of us live in a bubble of blissful ignorance. We might be vigilant and never open email attachments from people we don't know, we might take care to make sure an ecommerce site is secure before entering our credit card information, or we might even go so far as to install a standard firewall on our computers. Unfortunately, much of the common sense advice we follow when it comes to Internet security does little to combat the cyber-crime that is rampant.

Federal Trade Commission

Even the U.S. Federal Trade Commission, a governmental agency that is designed to help consumers, had to issue a press release stating that "consumers, including corporate and banking executives, appear to be targets of a bogus e-mail supposedly sent by the Federal Trade Commission but actually sent by third parties hoping to install spyware on computers."

There's little doubt that spyware, malware, and insidious virus attacks make any computer with Internet access vulnerable. But, because not all Internet security breaches are immediately apparent, people are often unaware that their seemingly hassle-free computing is anything but. The Federal Trade Commission offers seven guidelines to help consumer surf the Web safely:

1. Protect your personal information. For example, when shopping on an ecommerce site, make sure that the page where you enter your personal information is secure, as designated by "https" before the URL. It's important to stop identity

theft before it starts.

2. Know before you click. For instance, many cyber-criminals impersonate legitimate businesses, or send "phishing" email that asks you to click a hyperlink. Check out online merchants and never click on emailed hyperlinks unless you're certain of the source.

3. Update anti-virus, anti-spyware, and firewall software often. Hackers and others who engage in cyber-crime seem to always be a step ahead of the good guys. If your computer protection is outdated, you're vulnerable.

4. Use Web browser and operating system security features. Make sure your browser settings give you optimal privacy and security, and ensure that you update your operating system regularly to take advantage of security patches.

5. Safeguard your passwords. For example, create a unique password for each site you visit, and keep them in a secure place. Use letter, number and symbol combinations that can outsmart automated password detection programs.

6. Always do backups. If your computer does get a virus or a worm, your files may be goners. Make sure to regularly back up any important files and store them in a secure place.

7. Prepare for emergencies. If something does go wrong, such as your computer being hacked or infected, or if you accidentally divulge personal information, know what courses of action you should take to remedy the situation and prevent further problems.

A Hassle-Free Solution

Protecting your computer from all of the threats in cyberspace can seem like full-time job. Thankfully, there are companies who make it their business to offer individuals and businesses the most technologically advanced computer security solutions available. The best of these services offer PC maintenance, full system optimization, problem diagnosis and repair, installation assistance, and a full complement of professionally managed security services. Typically, you pay a small monthly subscription fee and in turn can surf the Web knowing that your computer is locked down and that you'll never again have to stay abreast of the latest security software or lug your computer down to a high-priced repair center.