



Are you Using Basic Internet Security Practices?

Kelli Tarala

originally printed November, 2008

A lot of people living in Sarasota County have Internet access in their homes. This marvel of modern technology allows us to read and reply to email, shop online, and complete school projects. We access the 'information superhighway' via cable modems, Digital Line Subscriber (DSL) service, or other high speed access devices. These connections to the Internet are considered always turned on. This means your computer is always visible on the Internet. It is like having the windows and doors to your home always open without locks or shades!

Almost 25 years after the introduction of the personal computer (PC), research has shown that a majority of US Internet users are failing to use even the most basic of Internet security tools. This research conducted by the NCSA (National Cyber Security Alliance) is being used to promote National Cyber Security Awareness Month. The research indicated that there is a sizeable gap between the protection that Internet users think they have and what is actually installed on PCs.

Even if you are only connected to the Internet some of the time, the information on your computer is vulnerable. While it is easy to think that no one could possibly be interested in your old home computer, it is simply not the case. Having an Internet connection always on is convenient for us, and it is also convenient for cybercriminals. Cybercriminals from around the world can sweep through thousands of random addresses on the Internet looking

for computers that they can exploit. What they can do is really quite scary. Without any visible signs or warnings, cybercriminals can infiltrate your computer system to obtain personal information about you or to use your computer to attack other computers.

In celebration of National Cyber Security Awareness Month, here are some tips to securing your home computers. More tips can also be found at the following website:
<http://www.staysafeonline.info/>

Use an anti-virus software program and be sure to keep your anti-virus software up-to-date.

Many anti-virus packages support automatic updates of virus definitions. Anti-virus software scans incoming email and files for malicious code by comparing files to virus definitions.

Use a firewall

A firewall is a protection tool that guards against intrusions from the outside. Firewalls block communications from and to sources you do not permit. It is not important to understand how firewalls work. It is important to know why you need it. Some operating systems like Microsoft XP and Apple's Mac OS X Leopard come with a built-in firewall. Verify that the firewall has been turned on and updated regularly. Check your online "Help" feature for specific instructions.



Securing our Digital Future

Kelli Tarala

originally printed November, 2009

Use an anti-spyware software program and keep it up-to-date.

Spyware is software that secretly gathers information about you while you are surfing the Web. Some spyware gathers information about passwords and even credit card numbers! Anti-Spyware software works by periodically scanning your computer for spyware programs, and then allows you to remove any harmful surveillance software found on your computer. Some anti-virus software contains anti-spyware capability.

Don't open unknown email attachments such as jokes, games, or ecards.

Malicious code is often distributed via email by well meaning people sending amusing jokes or enticing programs. If you must open the attachment, we suggest the following procedure:

1. Be sure your virus definitions are up-to-date (see "Use anti-virus software" above)
2. Save the file to your hard drive
3. Scan the file using your antivirus software
4. Open the file

Home computers are favorite targets of criminals. By following these basic Internet Security Practices, you make it as difficult as possible for criminals to access your home computer; and your family's personal information.

Article reprinted courtesy

