Are You A Safe Cyber Surfer?

(NAPSI)-Are you a safe cyber surfer? The stakes are high if you're not.

Every time you buy stuff online, do your banking or pay bills over the Internet, check in with your office by e-mail or just surf the Web for fun, you open a gateway to the personal information on your computer-including credit-card numbers, bank balances and more. You may also be in for costly computer repairs and lost data, due to damaging computer viruses that can invade your computer through e-mail connections.

Fortunately, there are steps you can take to protect your computer, your information and your peace of mind from computer creeps who try to slow down a network operation, or worse yet, steal personal information to commit a crime. Here are some tips to help you, from the security experts at the Federal Trade Commission (FTC):

• Make sure your passwords have both letters and numbers, and are at least eight characters long. Avoid common words: some hackers use programs that can try every word in the dictionary. Don't use your personal information, your login name or adjacent keys on the keyboard as passwords-and don't share your passwords online or over the phone.

• Protect yourself from viruses by installing anti-virus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically.

• Prevent unauthorized access to your computer through firewall software or hardware, especially if you are a high-speed user. A properly configured firewall makes it tougher for hackers to locate your computer. Firewalls are also designed to prevent hackers from getting into your programs and files. Some recently released operating system software and some hardware devices come with a built-in firewall. Some firewalls block outgoing information as well as incoming files. That stops hackers from planting programs called spyware-that cause your computer to send out your personal information without your approval.

• Don't open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

• When something bad happens-you think you've been hacked or infected by a virus-

e-mail a report of the incident to your Internet provider and the hacker's Internet provider, if you can tell what it is, as well as your software vendor.

To learn more, visit the Web site at www.ftc.gov/infosecurity or call toll free 1-877-FTC-HELP (1-877-382-4357).