Computer Corner

Tips For Computer Safety

(NAPSA)—It's that time of year again as families and students are stocking up on school supplies and preparing for the upcoming school year. Back to school shopping goes beyond pencils and books since computers are now an integral part of school curriculums. Students and parents are utilizing computers and going online for everything from communication and entertainment to researching papers, completing homework assignments and so much more. However, this increased use of personal computers also comes with increased risk when going online. The threat of damaging viruses, spyware programs, phishing scams and other attacks are an all too common occurrence today. With increased use and reliance on the Internet comes a responsibility to adopt safe Internet practices in order to protect not only your own personal information, but information belonging to your friends, family members, teachers, etc.

The National Cyber Security Alliance, a public-private partnership whose sponsors include the Department of Homeland Security, Federal Trade Commission, and private-sector corporations, manages a resource Web site, www.staysafeonline.info, that offers tips and other useful information to help ensure your cyber safety throughout the school year. Below are a few basic tips to help you protect yourself:

• Install anti-virus software and keep it up to date. It is critical that you install anti-virus software on your computer. New viruses and new variants of established viruses/worms emerge daily so for anti-virus programs to be effective, they must be updated regularly. Check with the Web site of your anti-virus software provider for automatic updates.

• Use a firewall to protect your computer from intruders. Firewalls filter out unauthorized or potentially dangerous types of data, while allowing legitimate data to reach your computer. Firewalls also ensure that unauthorized individuals are not able to gain access to your computer while you're connected to the Internet.

• Don't get hooked by a spam or phishing scam. If you receive a suspicious e-mail from someone you don't know, don't respond and delete the message from your inbox. Never respond to e-mails asking you for personal or financial information—even if it looks like it has been sent by your bank.

Protect yourself online by following a few basic steps.

• Be sure to use parental controls. Children need special protection online. How much protection you put in place largely depends on the maturity level of your child. Parental controls are provided by some ISPs and are also available for purchase as separate software packages. Keep your computer in a central location in your home. Familiarize yourself with your children's online friends and what sites they like to visit.

• Be cautious when downloading files and attachments. Only download files and attachments from senders and web sites that you trust. Don't open an e-mail attachment—even if it appears to be from a friend or coworker—unless you are expecting it or know what it contains. Be particularly wary of emailed files with extensions like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd. You can help others trust your attachments by including a text message explaining what you're attaching.

• Install and run anti-spyware software regularly. Some spyware programs monitor your online activities, collect personal information while you surf the Web, and slow down the operation of your computer. Install anti-spyware software to help keep your computer free of adware and surveillance software. Some anti-virus software contains anti-spyware capability.

For more information on Internet safety visit the National Cyber Security Alliance at www.staysafeonline.info.