NEW YORK STATE SENATOR

James L. Seward

Socialize Safely In Cyberspace

JAMES L. SEWARD October 14, 2010

The Internet is a revolutionary, world-changing innovation. While it continues to enrich our lives in new and profound manners on a daily basis, there is a dark side that everyone should keep in mind.

October is National Cybersecurity Awareness Month (NCSAM) sponsored by the Department of Homeland Security. The goal – encourage people to protect their computers and our nation's critical cyber infrastructure.

The theme this year is "Our Shared Responsibility," referring to the important role each of us plays in securing our part of cyberspace. The actions we take may differ based on our personal and professional responsibilities. However, if each of us does our part—whether it's implementing stronger security practices in our day-to-day online activities, making sure the right tools are in place, raising awareness in the community, educating young people or training employees—together we will be more resistant and resilient, protecting ourselves, our neighbors and our country.

One of the top cybersecurity concerns is the growing number of social networking websites. Facebook, Twitter, MySpace and similar websites offer a wonderful method to connect and reconnect with friends and family while at the same time providing on-line predators and

identity thieves with an opening to invade our lives. The National Cyber Security Alliance has a number of suggestions on how to stay safe when utilizing these sites, including:

• Privacy and security settings exist for a reason. Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way;

• Once posted, always posted. Protect your reputation on social networks. What you post online stays online. Think twice before posting photographs you wouldn't want your parents or future employers to see;

• Keep personal info personal. Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking;

• Protect your hardware. Safety and security start with protecting computers. Install a security suite (antivirus, antispyware, and firewall) that is set to update automatically. Keep your operating system, browser, and other software current as well and back up computer files regularly;

• Know and manage your friends. Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life;

• Be honest if you're uncomfortable. If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let him know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. Post only about others as you would have them post about you;

• Use strong passwords. Make sure that your password is long, complex and combines letters, numerals, and symbols. If you need to write down your password to remember it, store it somewhere away from your computer;

• Be cautious about messages you receive on social networking sites that contain links. Even links that look they come from friends can sometimes contain malware or be part of a phishing attack (attempts to collect personal information).

These tips and additional cybersecurity advice can be found at staysafeonline.org.