National Cyber Security Alliance and National Consumer League Social Networking Security and Safety Tips

Social networking sites are the hippest new meeting places around. These sites enable people to post information about themselves and communicate with others around the world using forums, interest groups, blogs, chat rooms, email, and instant messaging. While you can make new friends through social networking sites, you may also be exposed to embarrassing situations and people who have bad intentions, such as hackers, identity thieves, con artists, and predators. Protect yourself by taking some common-sense precautions.

- **Guard your financial and other sensitive information.** Never provide or post your Social Security number, address, phone number, bank account or credit card numbers, or other personal information that could be used by criminals.
- **Picture social networking sites as billboards in cyberspace.** Police, college admissions personnel, employers, stalkers, con artists, nosy neighbors – anyone can see what you post. Don't disclose anything about yourself, your friends, or family members that you wouldn't want to be made public. And remember that once information appears on a Web site, it can never be completely erased. Even if it's modified or deleted, older versions may exist on others' computers. Some social networking sites allow users to restrict access to certain people. Understand how the site works and what privacy choices you may have.
- **Be cautious about meeting your new cyber friends in person.** After all, it's hard to judge people by photos or information they post about themselves. If you decide to meet someone in person, do so during the day in a public place, and ask for information that you can verify, such as the person's place of employment.
- **Think twice before clicking on links or downloading attachments in emails.** They may contain viruses or spyware that could damage your computer or steal your personal information – including your online passwords and account numbers. Some messages may "spoof," or copy the email addresses of friends to fool you into thinking that they're from them. Don't click on links or download attachments in emails from strangers, and if you get an unexpected message from someone whose address you recognize, check with them directly before clicking on links or attachments.
- **Protect your computer.** A spam filter can help reduce the number of unwanted emails you get. Anti-virus software, which scans incoming messages for troublesome files, and anti-spyware software, which looks for programs that have been installed on your computer and track your online activities without your knowledge, can protect you from online identity theft. Firewalls prevent hackers and unauthorized communications from entering your computer – which is especially important if you have a broadband connection because your computer is open to the Internet whenever it's turned on. Look for programs that offer automatic updates and take advantage of free patches that manufacturers offer to fix newly discovered problems. Go to www.staysafeonline.org or www.onguardonline.gov to learn more about how to keep your computer secure.

- **Beware of con artists.** Criminals scan social networking sites to find potential victims for all sorts of scams, from phony lotteries to bogus employment and business opportunities to investment fraud. In some cases they falsely befriend people and then ask for money for medical expenses or other emergencies, or to come to the United States from another country. Go to www.fraud.org to learn more about how to recognize different types of Internet fraud.