



Helpful Tips

- ◆ Keep your system updated. Ensure that any computer you use to connect to a social networking site has proper security measures in place, including anti-virus and anti-spyware software, and a firewall. Make sure you keep them up-to-date.
- ◆ Use strong passwords. Protect your social networking account with a strong password. Do not share this password with anyone or use it for other sites.
- ◆ Be cautious when clicking on links. If a link seems odd, suspicious, or too good to be true, do not click on it...even if the link is on your most trusted friend's page. Your friend's account may have been hijacked or infected and now be spreading malware.
- ◆ Do not respond to an email requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- ◆ Be cautious about installing applications. Some social networking sites provide the ability to add or install third party applications, such as games. Keep in mind there is varying degrees of quality control on these applications and they may have full access to your account and the data you share.

CYBER SECURITY IS OUR SHARED RESPONSIBILITY



MULTI-STATE
Information Sharing
& Analysis Center™

A DIVISION OF



CENTER FOR
INTERNET SECURITY

www.msisac.org



STOP | THINK | CONNECT™