



STOP | THINK | CONNECT

INFO: stopthinkconnect.org

EMAIL: info@safteyandsecuritymessaging.org

Safety Tips for Social Networking

Social networking sites such as Facebook, Twitter and LinkedIn have become extremely popular in recent years. They're a great way to keep family and friends updated on your life and connect with colleagues and communities that share your interests. You can use social networks to build a positive online reputation. The first step is **STOP. THINK. CONNECT.**

Protect Your Personal Information.

Since social networking sites are about sharing, you may be prompted or tempted to reveal personal information. Make sure you are comfortable with the information you share. Draw the line between what's okay to share and what's best kept private.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you log into that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit who you share information with.
- **Your online reputation can be a good thing:** Recruiters often respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.

Connect with Care.

When you use social networks you are joining a global community. Therefore, it's smart to approach social networking with a degree of caution. Remember that people may not be who they say they are. If one of your friend's accounts is compromised, you could get spammy and suspicious posts.

- **When in doubt, throw it out:** Links in tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete.

Be a Good Online Citizen.

Social networks work best when people maintain the same level of courtesy online as they would in the real world.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you.**
- **Know what action to take:** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Keep a Clean Machine.

You can't be safe and secure if the technology you are using is vulnerable.

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

STOP. Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK. Take a moment to be certain the path is clear ahead. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Additional resources:

- Facebook Help Center: <http://www.facebook.com/help/>
- Twitter Help Center: <http://support.twitter.com/>
- LinkedIn Help Center: <https://help.linkedin.com/>