Privacy Tips for Social Networking

Social networking sites like Facebook, Google+, Twitter, Foursquare, LinkedIn and others are extremely popular. They're a great way to keep family and friends updated on your life and to connect with colleagues, business associates, and communities that share your interests. You can use social networks to build a positive online reputation.

Protect Your Personal Information.

Because social networking sites are about sharing, you will undoubtedly share personal information on your profile page. Make sure you are comfortable with the information you share, and use privacy settings to protect your information.

- **STOP. THINK CONNECT.** Think carefully about the kinds of information, comments, photos and videos you share online.
- **Know your audience:** Consider who may have access to your profile: family, friends, friends of friends, your school, college admissions officers, potential employers. Use available privacy settings to manage your audience.
- **Own your online presence**: When available, set the privacy and security settings on websites to your personal comfort level for information sharing. Do not rely on "recommended" settings or default settings. Make your own decisions. It's okay to limit who you share information with. It is okay to not accept a friend request.
- **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 digital environment.
- **Your privacy is only as protected as your least reliable friend allows it to be:** Keep in mind that privacy settings protect information from people you choose to exclude from your personal networks. When you choose to share information with friends, those friends can make their own decisions about forwarding your content. Avoid sharing compromising photos and information. Think carefully before sharing.
- **Make passwords long and strong**: Combine capital and lowercase letters with numbers and symbols to create a more secure password. To protect your privacy, don't share your passwords with others.
- **As a general rule, do not share the following information on a profile page**: your phone numbers, home address, full date of birth, travel plans, social security number, passwords, family financial information, bank or credit card numbers.

Be a Knowledgeable User.

Understand that participating in a social network is not "free." Even if you do not pay money to be part of a network, you are sharing your data with the network, and that data has value.

- **Learn about apps before you download them**: Understand that apps often require access to your personal information.
- **Understand the business model for the network that you use:** Advertisers are interested in your information, and you can receive targeted ads in the context of a social network.
- **When in doubt, throw it out**: If one of your friend's accounts is compromised, you may receive posts that appear to be from a friend but that are actually spam or phishing attacks.   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.
- **Log out when you are done**.

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.

- **If you would not do or say something in person, do not do it online.**
- **Respect the privacy of others.**
- **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. If you are a teenager, report the problem to your parents or an adult you trust as well.