Social Networking Tips

Some days, we need a special assistant, it seems, to run all of our social media accounts. As soon as you learn Facebook or Twitter, the rest of the world moves on to Tumblr or Reddit. This month, the CISOs share some tips to avoid risky social networking.

Take the following precautions when accessing social networks:

- Keep private information private. Do NOT post your social security number, banking PIN, or other personal information.
- Use the social network’s privacy and security settings to control who sees what you post.
- Only approve friend requests from people you know. Remove threatening or harassing people from your friends lists, block, or report them to the site administrator.
- Use strong passwords as discussed last month.
- Use a different password for every online account you have. Keeping written passwords is not the best idea; however, if you do have to write them down, keep them in a secure place.
- Avoid sharing your social media password with others.
- Beware of instant messages and emails with links that may contain malware or phishing scams. Many hackers will want to steal your password.

Remember the following tips when you are on social networking sites:

- **Once posted, always posted.** Protect your reputation – what you post online stays online, even if you delete it.
- **Your online reputation IS your reputation.** Show your smarts, thoughtfulness, and mastery of the environment.
- **Personal information is personal.** The more details you post, the easier it is for a hacker or someone else to steal your identity, access your data, stalk you, or even rob your empty house while you are on vacation.
- **Consideration is key.** Let a friend know if you are uncomfortable about an inappropriate post, and respect other people’s privacy too.