Social Networking Risks 101

Collaborative Web Technology sites, like Twitter and Facebook, are fun and allow users to upload and exchange pictures, text, music, and other types of information. The sites are meant to get as many users in one place as possible on one platform, which makes these sites a huge target for bad guys. For example, in 2009, hackers managed to hijack the Twitter accounts of more than 30 celebrities and organizations, including President Barack Obama and Britney Spears.

Listed below are some of the main risks and how to protect yourself.

Risk	Explanation	Protection Strategies
Password sloth	Using a weak password and/or the same password on all sites. If that password is discovered via a hack or accidental leak on one site, it provides bad guys a way into all the other sites.	Pick strong passwords. Use different passwords for different purposes.
Plain old TMI — too much information	It's a great idea to let your neighbors know you're going on vacation so they can keep an eye on your house. It's NOT a great idea to post those vacation plans on public Internet sites.	Think like a bad guy and what he could do with your personal information, like your birthday, town of birth, or family tree (use it for identity theft).
Your personal "brand"	Consider the perception others may form when viewing your pictures or reading your posts. The world (including present and potential future employers, your parents, kids, and co-workers) may be looking at your angry, immature posts for years.	Protect your personal brand. Think twice before clicking submit or send. Don't engage in "Tweet rage," or send email or post any content when you're drunk, angry, upset, or excessively tired.
Beware of scams	These are active attempts by bad guys to get you to • Share information you shouldn't (passwords, sensitive data, company secrets), or • Click on a link you shouldn't (because it leads to a website infected with malware).	Like with email scams, beware of the social networking tricks: • Using celebrity gossip and news events to get you to click on a link that actually leads to a malicious site or that installs malware. • Using a friend's hacked account to get you to trust the message, link, or attachment. • Using messages like, "OMG! Did you see this picture of you?" to pique your interest to get you to click on a link and enter your login information (on a fake login screen). • Using a quirky application (like an online quiz or poll) where you end up subscribing to services without realizing it.