Safety on social media

Facebook, Myspace, LinkedIn, Twitter, blogs, etc. The number of social networking sites and tools is exploding. Such sites have breached the walls of the corporate firewall, are a part of our most important smartphone apps, are a vital tool for any serious job search, and are the new way to connect with current and new friends. Using social networking tools and sites seems to be in direct conflict with another important principle of using the Internet – protect your identity from identity theft. Participating in online social networking sites leaves a trail of personal and professional information that can make stealing your identity or posing a corporate threat a whole lot easier.

Some tips to protect you and your company while on social media sites:

1. Beware of TMI (too much information): the five things you should never share
    - As obvious as it may seem, some still share this information;
        - Your ID number
        - Your phone number
        - Address and place of birth
        - Banking details and PIN numbers
        - Any passwords
2. Privacy options must be customised:
    - Don't assume you have to take whatever default settings the site gives you. Check out the settings, configuration and privacy sections to see what options you have to limit who and what groups can see various aspects of your personal information.
3. Limit your work history details:
    - Limit your work history details on sites like LinkedIn. If you feel you need the added information to help in a job search, expand the details during the job hunting process and then cut back later after you have a position, leaving just enough information to entice recruiters to contact you with interesting new positions.
4. Don't trust always verify:
    - If the content on the site doesn't look like or sound like the person you know, avoid it. E-mail or call your friend to verify the site is legit. Let them know, too, if you think someone else is faking your friend's identity online.
5. Control comments:
    - Anonymous blog comments (marked as anonymous) are fine but some people are leaving comments under someone else's name.
    - Contact the site administrator immediately if you find someone is impersonating you on a social networking site or in blog comments.
6. Avoid sharing any personal details:
    - You wouldn't put a note on your front door stating, "Away for the weekend… Returning on Monday. Why do it on social media?
    - Be aware of what information you put out there which others might use for immoral purposes.
    - Over time, seemingly innocuous information can be pieced together, giving lurkers a much more complete and rich picture of you, your family, your habits and other personal information.
    - Twitter is often used at conferences, parties and other social scenes where alcohol is consumed. That makes it even easier for personal details to slip out for the world to see. Twitter users frequently use it to communicate and share their travel woes, giving clue to others that you aren't at home, leaving your family or possessions at risk for intruders.
7. Google yourself:
    - As scary as this sounds…

- It is a good idea to search your name on Google and check out your profile as others see it on social networking sites. Understand where you show up and what information is available about you, and then adjust your profile, settings and habits appropriately. Don't worry, it's not vain if you only search your own name once a month or so. If you unexpectedly see your name in locations you don't frequent, it could give you a heads up someone else is using your identity online.

8. Do not violate your company's social networking policies:
    - Data leakage incidents (loss of corporate, confidential or customer information), making inappropriate public statements about the company, using corporate resources for personal uses and harassing or inappropriate behaviour toward another employee can all be grounds for reprimand or dismissal.
    - Social networking sites are another way those things can happen and they create an easy digital paper trail to investigate.
9. Empower yourself with knowledge:
    - Learn how sites can use your information.
    - Social network sites are typically free to use which means they are making their money by advertising to you. That means they are collecting information about you. Is your information shared with outside companies and partners? What information can third-party plug-in software, such as Facebook Applications, use from your profile or page content? Review the site's privacy policy and watch closely the privacy settings you can control.
10. Forget the popularity contest:
    - Put a number on something and suddenly you have a competition.
    - If you do get an unsolicited invite to connect, check them out first and try to figure out why you know them or if you even do at all.
11. Once posted, always posted:
    - Think twice before posting pictures you wouldn't want your parents or future employers to see.
12. Your online reputation can be a good thing:
    - So show your smarts, thoughtfulness, and mastery of the environment.
13. 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.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

1. Keep a clean machine:
    - Having the latest security software, web browser, and operating system are the best defences against viruses, malware, and other online threats.
2. Own your online presence:
    - When applicable, set the privacy and security settings on websites to your comfort level for information sharing.
3. Make passwords long and strong:
    - Combine capital and lowercase letters with numbers and symbols to create a more secure password.
4. Unique account, unique password:
    - Separate passwords for every account helps to prevent cybercriminals.
5. When in doubt, throw it out:
    - Links in email, 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.