



IT Security

Privacy, the Internet and Social Networking Sites

Author: Randy Bragg, MBA, MISM

2613 Manhattan Beach Blvd Suite #100

Redondo Beach California 90278

Phone: 310.297.3605

Fax: 310.297.3615

Toll Free: 800.241.6808

Privacy, the Internet and Social Networking Sites

During the past several years the Web 2.0 has revolutionized the use of social networking sites on the Internet. Today there are several hundred million users around the globe using both specialized and general social networking sites. Social networking sites can be great tools for meeting people and sharing information for a variety of reasons. Some of the more common types of social networking sites include:

Sports related sites - most professional and many other sports teams have social networking sites for fan clubs. These sites may include blogs, real time information on the team and its players and staff, sharing of pictures and videos, and a host of other activities.

Industry specific sites - many industry associations have social networking sites where members may share information and ask questions of other members on industry/work related issues. These sites tend to be more professional and business related and is primarily for knowledge sharing purposes.

Marketing sites - much like the industry specific sites by focused on sales and marketing. These sites are used by marketing professionals to network, share ideas and gain knowledge.

Subject specific sites - there are many social networking sites that focuses on one or a few subject areas. These sites tend to be a mix of knowledge sharing on the specific subject(s) mixed with some of the more social aspects such as meeting new people, sharing information and maybe even pictures, videos, etc depending on the subject(s) focused on.

Schools, universities, and education facilities - many education facilities use a version of social networking sites for students and/or alumni. These sites allow for the members to enter into discussions, share information and gain access to valuable resources for educational purposes. These sites are well regulated for content and security due to the government oversight of the education system.

Dating and meeting sites - these sites are specifically for the purpose of individuals to meet others and engage in relationship building whether it is for friendships or dating purposes. Users in these sites tend to share a lot of private information in the process of relationship building.

Work specific sites - many business organizations maintain some form of social networking site for business purposes. These sites are primarily focused on sharing of business knowledge and company functions. Much like educational sites, these sites are well regulated for content as well as security in most cases.

General social networking sites - by far the most dangerous of all types of social networking sites are the general sites; which are used by the general public to setup individual sites for the purpose of sharing information, pictures, videos, and all type of other information with friends, family and the general public. These are the sites that typically provide private vs. public sections to their users.

Depending on the type of site, the amount of information shared can range from basic contact information with blogs to full social networking sites that include the sharing of pictures, videos, messages, biographical information and blogs along with instant messaging, live discussions and video conferencing. Many of the more advanced sites include both private and public sections for each user so that some information can be restricted to certain other users while some information is public for all users to see.

There is no doubt that social networking sites are here to stay and they do serve many purposes and have many advantages. However, it is critical that users understand the privacy and security issues related with these sites and the potential implications.

First, what are the implications? Why should you be concerned? There are many reasons for concern and listed below are some of the top reasons:

- 1) Potential Employers - many potential employers and recruiters now search one or more social networking sites (or the Internet in general) as part of their hiring process for applicants. Information that counters claims made on your application, or that shows bad judgment may cause you that potential job. At the very least your new employer may know way more about you then you wanted them to.
- 2) Potential School/College/University Admissions - just as with potential employers, many admissions counselors and boards now search the Internet and/or social networking sites to evaluate the character of applicants for admissions. The information gained is considered public information and may be used in the application process.
- 3) Potential professional associations/certifications - professional associations and certification boards also search for information on applicants to gain knowledge on their character. This can become especially important when applying for professional certification such as BAR admissions to be a lawyer.
- 4) Parents/Significant Other/Family - your parents, family or significant other may become aware of information or compromising photos that they were never intended to see. The wrong information can be accessed by the wrong person which can prove to be detrimental to many types of relationships.
- 5) Coworkers/clients - coworkers or clients have access to all the information you post on these social networking sites. Just like family and friends, your co-workers and clients will now have access to any information you post. It is also important to remember that in business not everyone has the same values and morals. What may be an innocent picture or statement to you may be offensive to a co-worker or client.

- 6) Hackers - there is always the potential for hacker to access the "private" side of the social networking sites and release this information to the public. This does not have to be a case where a hacker is targeting you - a hacker may simply target an entire site and open the security to all users' private information. Now all the parties listed above also have access to all of your "private" information.
- 7) Accidental release of information - just like in the case of a hacker, it is always possible that due to some type of human error or computer glitch the "private" information within a site will be made public.
- 8) Law Enforcement - law enforcement agencies may use any information obtained on social networking sites in to open and investigation, or in the process of an investigation. Unless you want to end up on a show related to the "worlds dumbest criminals" it would be wise not to put any information related to criminal activities on a social networking site.

It is very important to note that (1) people do not have to "dig" to find the public information, a simple search will uncover the majority of it and (2) what is private may not always be private. There have been many security breaches where large amounts of "private" information were released into the public domain.

With all these potential hazards, what can be done to safely use social networking sites?

- 1) Password Security - use strong password security. Always use at least three of the following characters in your password - uppercase letters, lowercase letters, number, special characters such as *. In addition always use at least 6 to 8 characters in your password and NEVER use birthdates, kid's names, pet's names, parent's names or birthdates, city born in, etc. This will slow down hackers and prevent your ex-friends from guessing your password.
- 2) Privacy Statements/Policies - read the privacy statement and policies associated with the site. This will be downloadable on their homepage. Make sure the site does not retain private information one you delete your account. Make sure you are aware of when they can and cannot release any of your information to a third party without your consent.
- 3) Research Security Breaches - search the site on the three major Internet search engines and see if they have a history of security issues. Simply search the name of the site and "security breaches" and "release of information".
- 4) Screen what you say - be careful what you say. Never say anything you would not say in a public place like a store or restaurant. Never say anything you do not want heard by the people listed above. Remember, what is private today may not be private tomorrow so be very careful even when in private sections.

- 5) Screen Pictures and video - NEVER post any picture, anywhere on the site (public or private) that you do not want seen by your boss, significant other, parents, church, co-workers, friends, the local police and probation officer if you ever end up with one. NEVER associate a full name with a picture as this makes it very easy to search for. In the case of pictures and video never assume they will stay private. Remember, once they are released in the public domain they can NEVER be taken back.

- 6) Be careful what you allow others to have - be careful what information you allow your friends and family to have if you know the "love to post everything" on a social networking site. If they post it you run the same disclosure risks as if you post it yourself.

- 7) Screen name mean nothing - making statements that you would never normally make because you have a screen name provides no real security. Someone (probably a lot of people) know who is really behind that screen name. The confidentiality of a screen name is only good if no one knows or has access to it, including hackers or knowledge by accidental release.

- 8) Don't assume the private section is private - as mentioned several times already, what is private today may not be tomorrow. Hackers and accidental releases of information happen every day.

- 9) Remember, some private people today may not be tomorrow - forget all the hackers and accidents, you also have to deal with all the people you let in the private section who you no longer talk to that much or had a falling out with. They have all that information now and might just decide to make it public.

- 10) Remember, this is PUBLIC domain - most importantly, think. Every time you are going to say or post something just remember that you are in the public domain of the Internet; and this information may very well follow you for the rest of your life and be accessible to hundreds of millions of people.

Remember, social networking sites can be a great way to meet people, share information and gain knowledge but you must also be aware of the potential privacy and security risks, the potential ramification and the actions you need to take in order to avoid these issues..