Social Networking Safety Tips

Social networking is a method of communication with people through online platforms such as Facebook, LinkedIn, and Twitter. Over the years, social networking has become an important part of life for both adults and teens. The popularity is due to the ability of meeting the needs and interests of a vast majority of people. For teens it is a way to socialize with friends, by sharing the latest events, photos and videos. Adults use social platforms for the same reason as teens, while also utilizing each platform in a professional manner as well. It is a valuable tool for businesses in that it allows them to interact with like-minded professionals, customers and other businesses. With all the benefits social networking offers, it is easy to overlook the risks that are involved. Said risks include threats of criminal activity, such as, stalking, bullying, identity theft, and hacking. Also, users may fall prey to impersonators who can cause damage to their reputation and standing with the very people they are trying to network with. To make the best use of social networking while avoiding the risks, users will need to understand and follow a set of basic safety tips that are easy to remember and highly effective.

1. Be Cautious of Sharing Too Much

When utilizing a social networking website, people have the option of sharing personal details with friends and followers. While sharing some information is okay, other facts can reveal too much about who a person is. For the sake of personal safety, one should never reveal their date and place of birth, home address or phone number, as this could put them at serious risk for identity theft and fraud. In addition, it is extremely important that a person never reveal their credit card numbers, banking information, passwords, or social security number on any networking site. If such information is shared it would be very easy to fall victim to crimes ranging from stalking to identity theft.

2. Adjust Privacy Settings

Nearly all social networking sites have pre-set or default privacy settings. People often feel that these setting are sufficient enough and never put forth the effort to make changes. Altering one's privacy settings can allow the account holder to block strangers and people who are not friends with them from viewing his or her private information. These settings also limit what information is available in search results; for example, Facebook allows the account holder to modify their settings so only their friends, friends and networks, specific groups, or no one can see their status, photos, videos, likes, etc.. Privacy settings can be adjusted at any time; however, the account holder must log in to make adjustments.

3. Limit Details About Work History

On some social networking sites, such as LinkedIn, people are able to post resumes and other information that pertains to their work history. Work related information can reveal too much about a person's personal life and can give criminals such as hackers personal information which may help them to hack into one's account. The information that is found on resumes can also be used in identity theft.

4. Verify Who You Are Connecting With

There are a number of reasons why a person may put up a false account. If there is ever uncertainty about the authenticity of an account that claims to belong to a friend, is important to check with the individual for verification. These accounts may be setup in efforts to misrepresent themselves as another person in order to make false statements. This may be done to embarrass someone or to create problems that either of a legal or personal nature. False accounts may also be set up to for the purpose of sending people to malicious sites or with the intent of committing fraud.

5. Keep Control of Comments – Be Aware of Impersonators

Impersonation can be a problem when it comes to comments on networking websites. Typically, people who are misrepresented online only need to ask that the impersonator be removed. This can be a hassle, however, networking sites are beginning to require commenter's to go through an authentication process in which they are identified as registered users or not.

6. Don't Share Personal Details

Microblogging websites encourage people to share in the moment activities and slices of life. For people who enjoy this sort of social interaction, they may find that they are revealing too much about what is happening and as a result making themselves the ideal victim for thieves and other criminals. Because these networks are visible to practically everyone, a person should not reveal information that alerts criminals to their whereabouts or other actions. For example, a person should never reveal where they are vacationing, shopping, or traveling. It should also never be revealed when they expect to leave or return home.

7. Check Out Your Own Account

In order to ensure the security of one's account, it is wise to search for their profile from the prospective of someone who is conducting a search. This step will let the account holder know what others are able to view. When using a search engine to look for one's profile they will also be able to see if there are any false accounts set up in his or her name.

8. Know Employer Boundaries or Acceptable Use Policies

More and more frequently there are reports of people who have lost their jobs as a result of their activities on social networking sites. This can easily be avoided when employees review what policies their employer has in place. These policies may affect what a person can share in terms of pictures and/or writing. This is done to not only protect their reputation, but to also prevent data loss or loss of intellectual property.

9. Control What Information is Shared with Outside Sources

When a person joins a social networking site, they should understand how that site uses their private information. A user's personal details may be shared with partners, advertisers, or other outside companies. Reading the privacy policy of the social networking platform will explain exactly how private information is used. Unfortunately, people do not fully read these policies before agreeing to them. The privacy terms should be rechecked in the event that a company is sold as these policies may change.

10. Be Careful of Over-Friending

As a member of a social networking group, it can be exciting to gain new "friends" or followers. Looking through the network it is easy to find members with high numbers of friends, which can inspire a competitive streak in some. A high number of friends, however, is not always positive. Some "friends" can be problematic by introducing spam into one's timeline or some may even have criminal intentions. When accepting friends, choose people who are actual friends.

11. Consider Forming a New Social Network

Respected networking sites like Facebook and Twitter, are not the only social networking platforms available. The popularity of these sites make them larger than life and attract a large assortment of people with various agendas. However, people who are interested in interacting with a smaller, more intimate group of people should look into joining MeetUp, Ning, or FamilyLeaf. In some cases people are able to go through MeetUp to create a niche social network that will attract like-minded individuals within one's own community.

12. Single Sign-On: Open ID

Using a single sign-on for multiple platforms is one way people can reduce the likelihood of their passwords getting into the hands of identity thieves and hackers. OpenID is the most common single sing-on to manage various accounts.

13. What Goes Online Stays Online

When sharing information online it is important for people to realize the permanence of what they type or download. Once information goes on the Internet, through social networking, microblogging, etc., it is difficult, if not impossible to remove. In some instances, the information may even be captured via screen shot and used on blogs or news sites. Depending on what was originally submitted, the information can prove detrimental for future job prospects, relationships, and may even leave a person vulnerable to crimes.

14. Know How to Block Unfriendly Followers

Nearly every social networking platforms gives users a way to protect themselves from harassment or unwanted contact. When joining a social network one should familiarize themself with how to block another member. Once a person has been blocked, he or she will no longer have the ability to interact with the individual who has done the blocking.

15. Keep Passwords Strong

Security is as important for one's social network account as it is for their computer or any other account. Creating a strong password will prevent hackers from gaining access to one's account and using it to post spam or malicious attacks. When creating a password it is important to choose one that consists of no less than eight characters. The characters should consist of both letters and numbers and should be changed approximately every three months.