CYBER SECURITY newsletter

SOCIAL NETWORKING SAFELY

Problem

Social networking sites are one of the most exciting and powerful technologies on the Internet. These are virtual, online communities allowing people to connect from around the world. On these sites you create an account, post information about yourself, and then share that information with your friends, family and fellow employees. You can also track others and learn what they are doing. Different sites are used for different purposes. Sites such as LinkedIn are used for professional or work-related activities, while sites like Facebook are used for personal activities.

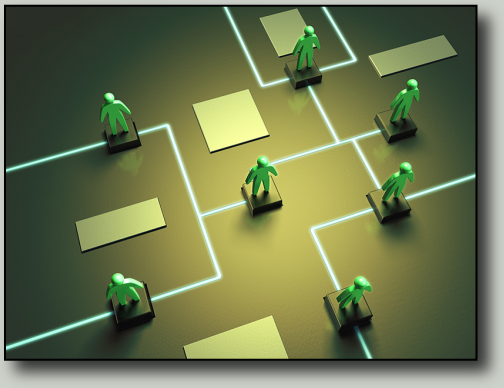
Each of these sites has a different set up, but they are all designed to let you decide what information you want to share, how often and with whom. Some people update their sites daily or even hourly, posting what they are doing, where they work, their hobbies, and their favorite music. What makes these sites so powerful is how easy it is to share with others and to watch and learn what others are doing. However, with these amazing capabilities come risks that you need to be aware of.

Solutions

1. Sharing Your Information: Social websites allow you to post and share a tremendous amount of information. Not only can you publish basic personal data, but also favorite songs and movies, personal photos and events in your life. The problem with all this information is that if you are not careful, it can harm you.

Criminals and attackers look for highly personal information. Based on the details of your life that you share, they may be able to guess your passwords, impersonate you online or even steal your identity. Be sure that you do not post personal details such as your birth date, home address or identification numbers.

In addition, organizations hiring new employees or universities reviewing student applications often do background checks on popular social networking sites such as Facebook. To protect your future, do not post any embarrassing information or photos of yourself. If it is something you would not want your boss or mother to see, then you most likely should not post it.



Social Networking

Social networking sites are powerful tools that allow you to communicate with friends and family around the world. However, be careful what you share, how you share and with whom.

University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Your Privacy Settings

Most social networking sites such as Facebook offer privacy controls. These are settings that you can configure to determine who can and cannot access information on your page. The intent is to give you the ability to publish private information, then share that information with only specific people. The problem with most privacy controls is they are complex. You may think your information is protected, but you may be surprised to learn that others can access it, such as Friends of Friends. Also, privacy controls may not work as you expect, so in some cases people who are not your friends or even third party applications can still access your information. Finally, even once you figure out the privacy options they can change.

The best way to protect yourself is to limit the amount of personal information you post. In fact, it is best to assume any information you do post will eventually become public, regardless of the privacy controls you use. If you do not want your boss, coworkers or family members to find out about it, you probably do not want to post it.

2. Others Posting Information About You: Even more challenging to control is the information others publish about you. You can control what is published on your page and who has access to it, but other people can publish information about you on their own sites. Photographs, videos or online chat sessions can easily be shared. Let your friends know what information they can and cannot share about you. If they are not sure, have them ask before posting.

It is also wise to view their sites and see what they have posted about you. Some social network sites will even notify you if others have posted information about you. In addition, many social networking sites have an abuse contact, if someone will not take down personal information about you then contact the websites abuse center.

3. Third Party Apps and Games: Some social websites have additional third-party programs such as games you can install. However, these programs are usually not developed or reviewed by the social networking website, instead they are developed independently by other individuals or organizations. Always be careful when using third-party programs as they can potentially actually infect your computer or harvest your information.

4. Trusting Others: One of the great things about social networking is the ability to quickly and easily interact with other people. The problem is these websites make it easy for attackers to impersonate people you trust. Only accept as friends or contacts people you know. If you blindly accept any request to join your network, then you really have no privacy protection.

Another common attack occurs when criminals hack an account on a social networking site and then pretend to be the victim. The criminal posts messages to all of the victim's friends, pretending to be the victim and tricking their friends to visit a website or install a program. If people visit the websites or install the programs, their accounts or computers are often hacked. Criminals are using your trust of others to attack you. So be careful: if a friend's request seems odd, be sure it is really your friend that is talking to you and not a criminal or virus that has taken over their account. When in doubt, call your friend on their mobile phone.

5. Work Information: Never post any organization related information on social networking sites unless you have prior permission. In addition, be sure you are using a different password for your social networking account than the password you use at work.