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 to each other from around the world. On these sites, you create an account, post information about yourself, and share information with your friends, family and fellow co-workers. You can also track others to learn what they are currently 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 is set up differently, but they are all designed to allow you to 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 many risks 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 and personal photos and events in your life. The concern is, if you're not careful, sharing all this information can harm you.

Criminals and attackers look for highly personal information. Based on details of your life you've shared, they may be able to guess your passwords, impersonate you online, or even steal your identity. You should never post personal details such as your birth date, home address, or identification numbers.

In addition, organizations hiring new employees or universities reviewing new students 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 family to see, you 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 it, and with whom.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

Your Privacy Settings

Most social networking sites such as Facebook offer privacy controls. These are settings 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 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 often 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 shouldn't post it.

2. Others Posting Information About You

Even more challenging to control is 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. Always inform your friends what information they can and cannot share about you. If they are not sure, have them ask before posting.

It is also wise to review their sites to 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 website's abuse center.

3. Third Party Apps and Games

Some social websites have additional third-party programs, such as games you can install. 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 infect your computer or access your private information.

4. Trusting Others

One of the exciting features about social networking is the ability to quickly and easily interact with others. The issue is these websites make it easy for attackers to impersonate people you trust. Only accept friends or contacts you know. If you blindly accept any request to join your network, then you have no privacy protection.

Another common attack occurs when criminals hack an account on a social networking site and 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. When people visit the websites or install the program, 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, confirm it is your friend and not a criminal or virus that has taken over their account. When in doubt, call your friend to verbally confirm the request.

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 different passwords for your personal and work social networking accounts.