Social Networks

Social networks are online communities focused on interaction among friends, families, and others who may share similar interests. Social networks allow people to communicate in many ways including email, instant messaging, forums, and blogs.

1. Social Networking Concerns

Are social networking sites safe? Although social networking sites are not inherently dangerous, because of their open nature, and anonymity, users may not realize the potential dangers. However, every user should understand these risks and know how to address them. Some statistics indicate the following:

- 74% of social network users have given out at least some personal information. This information can be used to steal their identity.
- 83% of social networkers have downloaded content from another user. Content from untrustworthy sources can contain viruses, worms, or Trojan horses.

The following are some examples of the potential threats that exist on social networking sites:

Identity Thieves try to find out all they can about you so they can steal your identity, use your credit cards, or create new credit cards and loans in your name. There are millions of identity theft victims each year.

Predators prowl the Internet looking for victims. They rely on the anonymous nature of the Internet to hide their true identity and malicious intent.

Con artists will try to trick you into giving them money. They may claim to be with charities or have a great investment opportunity for you. Remember – if it sounds too good to be true, it probably is.

Cyberbullies and cyberstalkers use the social networking sites to embarrass, intimidate, or stalk someone.

Virus writers and other scammers send you files to download and links to malicious sites. Their goal is to infect your computer with software they can use to steal information from you. Sometimes they try to take control of your computer to use it to infect other computers or send spam to other people.

2. Protect Yourself

Protecting information is the key. Below are some examples of how you can keep your information protected while using social networking sites:

- When establishing your account, adjust your profile until you are comfortable with the amount of protection provided to maximize your security.
- Make sure your anti-virus and anti-spyware software are installed and up-to-date.
- Choose your screen name carefully – do not include any information such as your name, age, sex, city, or employer.
- Never post anything you would not want to have distributed publicly.
- Never post personally identifying information such as: SSN, first and last name, address, driver's license, telephone number and e-mail address.
- Be careful posting any pictures; they can be altered and re-posted anywhere on the Internet.
- Don't click on any links or open files that can be downloaded.
- Monitor your children's activities online; teach them to protect their information.

3. Internet Lingo

As computers have transformed communications, at the personal and business levels, a new language has emerged: Internet lingo. Acronyms such as WYCM (Will You Call Me?), or ROTFL (Rolling on the Floor Laughing) or character symbols called Emoticons such as :) (happy face) are just examples of everyday cyberspace shorthand. Many teens use these and other similar acronyms and symbols to convey emotions, moods, feelings, love, hate, and almost everything in between.

To keep kids safe online, it is important for parents to decode this lingo. Dictionaries, glossaries and translators are available online that parents can use in decoding Instant and Text Messages that kids might be exchanging with other peers.

4. Remember that Cyber Security is Everyone's Responsibility

By protecting yourself and the systems entrusted to you, you are protecting your co-workers, your entire organization's network and data.

Cyber Security Is OUR Shared Responsibility

5. Resources

More information on safe surfing and social networking can be found at these valuable sites:

- **MS-ISAC:**
  www.msisac.org/awareness/news/2009-03.cfm
- **US-CERT:**
  us-cert.gov/cas/tips/ST06-003.html
- **StaySafeOnline:**
  staysafeonline.info/practices/index.html

Disclaimer: These links are provided because they have information that may be useful. We do not warrant the accuracy of any information contained in the links and neither endorse nor intend to promote the advertising of the resources listed herein.

Social Networking Sites

State of Hawaii

Information & Communications Services Division

Contact Information

Information & Communications Services Division (ICSD)
Cyber Security Team

http://cybersecurity.hawaii.gov
ICSD.CyberSecurity.Mailbox@Hawaii.gov

Brought to You by the MS-ISAC

Multi-State Information Sharing and Analysis Center

www.msisac.org