Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer | April 2009 | Volume 3, Issue 3

Social Networking Sites: How to Stay Safe

The popularity of social networking sites, such as MySpace, Facebook, Twitter, and others, has exploded in recent years, with usage in the United States increasing 93% since 2006[1]. The sites are popular not only with teenagers but with adults as well: the number of adult Internet users having a social networking profile has more than quadrupled in the past four years[2].

While there are many positive aspects of using social networking sites, it is also important to understand the potential security risks and to know what precautions to take in order to protect yourself and your personal information.

WHAT ARE SOCIAL NETWORKING SITES?

Social networking sites are online communities of Internet users who want to communicate with other users about areas of mutual interest, whether from a personal, business, or academic perspective. The specific functionality of the various sites may differ, but in general, the sites allow you to provide information about yourself and communicate with others through email, chat rooms, and other forums.

WHAT ARE THE SECURITY CONCERNS OF SOCIAL NETWORKING SITES?

Social network sites are growing in popularity as attack vectors because of the volume of users and the amount of personal information that is posted. The nature of social networking sites encourages you to post personal information. Because of the perceived anonymity and false sense of security of the Internet, users may provide more information about themselves and their life online than they would to a stranger in person.

The information that you post online could be used by those with malicious intent to conduct social engineering scams and attempt to steal your identity or access your financial data. In addition, the sites are increasingly sources of worms, viruses, and other malicious code. You may be prompted to click on a video on someone's page, which could redirect you to a malicious website, for example. If you are accessing a site that has malicious code, your computer could become infected. For examples of some common social networking scams, visit the Council of Better Business Bureaus (**www.bbb.org**).

It's also important to realize that information you post can be viewed by a broad audience and could have lasting implications. College admissions officers and school administrators, for example, do visit these sites, and in some cases, admissions have been denied to applicants or disciplinary actions have been taken because of information or photos posted online. Employers also review these sites for information about potential job applicants.

WHAT CAN I DO TO PROTECT MYSELF?

- **Make sure your computer is protected before visiting sites** – Make sure you have established a firewall and installed anti-virus software on your computer and that it is up-to-date. Keep your operating system up-to-date as well.
- **Be cautious in how much personal information you provide** – Remember that the more information you post, the easier it may be for an attacker to use that information to steal your identity or access your data.

[1] Netpop | Connect: Social Networkers 2008 – **www.netpopresearch.com/node/26552**

[2] Pew Internet & American Life Project – **www.pewinternet.org/topics/social-networking.aspx**

- **Do not assume you are in a trusted environment** – Just because you are on a page of someone you know, it is still prudent to use caution when navigating pages and clicking on links or photos, because links, images, or other content contained on the pages may include malicious code.
- **Use common sense when communicating with users you DO know** – Confirm electronic requests for loans or donations from your social networking friends and associates. The communications could be from someone who has stolen the credentials of the person you know with the intent of scamming as many people as possible.
- **Use common sense when communicating with users you DON'T know** – Be cautious about whom you allow to contact you or how much and what type of information you share with strangers online.
- **Understand what information is collected and shared** – Pay attention to the policies and terms of the sites; they may be sharing your email address or other details with other companies.
- **Make sure you know what sites your child is visiting** – Be involved in your children's activities and know with whom they are communicating and what information is being posted by them – or about them by others.

ADDITIONAL RESOURCES

For additional information on browser attacks, please visit:

- Netpop Research: **www.netpopresearch.com**
- Pew Internet & American Life Project: **www.pewinternet.org**
- List of social networking sites: **en.wikipedia.org/wiki/List_of_social_networking_websites**
- Social Networking Sites: Safety Tips for Tweens and Teens: **www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm**
- MySpace: Your Kids' Danger?: **www.cbsnews.com/stories/2006/02/06/eveningnews/main1286130.shtml**
- Hackers' Latest Target: Social Networking Sites: **www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html**
- Online Social Networking Dangers and Benefits: **web.pacific.edu/x4989.xml**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.
For more information on Internet security, please visit the SecureTexas website at **www.dir.state.tx.us/securetexas**.
SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC
www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
www.us-cert.gov

Distributed by: DIR Secure Texas
www.dir.state.tx.us/securetexas