Monthly Cyber Security Tips

# NEWSLETTER

March 2010 Volume 5, Issue 3

## Security and Privacy on Social Networking Sites

From the DoIT Office of Security Services

## What are the security and privacy issues associated with social networking sites?

Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe. While there can be benefits from the collaborative, distributed approaches promoted by responsible use of social networking sites, there are information security and privacy concerns. The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information. The same technologies that invite user participation also make the sites easier to infect with malware that can shut down an organization's networks, or keystroke loggers that can steal credentials. Common social networking risks such as spear phishing, social engineering, spoofing, and web application attacks attempt to steal a person's identity. Such attacks are often successful due to the assumption of being in a trusting environment social networks create.

Security and privacy related to social networking sites are fundamentally behavioral issues, not technology issues. The more information a person posts, the more information becomes available for a potential compromise by those with malicious intentions. People who provide private, sensitive or confidential information about themselves or other people, whether wittingly or unwittingly, pose a higher risk to themselves and others. Information such as a person's social security number, street address, phone number, financial information, or confidential business information should not be published online. Similarly, posting photos, videos or audio files could lead to an organization's breach of confidentiality or an individual's breach of privacy.

## What are the precautions I should take?

Below are some helpful tips regarding security and privacy while using social networking sites:

- Ensure that any computer you use to connect to a social media site has proper security measures in place. Use and maintain anti-virus software and keep your application and operating system patches up-to-date.

- Use caution when clicking a link to another page or running an online application, even if it is from someone you know. Many applications embedded within social networking sites require you to share your information when you use them. Attackers use these sites to distribute their malware.

- Use strong and unique passwords. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised.

- If screen names are allowed, do not choose one that gives away too much personal information.

- Be careful who you add as a "friend," or what groups or pages you join. The more "friends" you have or groups/pages you join, the more people who have access to your information.

- Do not assume privacy on a social networking site. For both business and personal use, confidential information should not be shared. You should only post information you are comfortable disclosing to a complete stranger.

- Use discretion before posting information or commenting about anything. Once information is posted online, it can potentially be viewed by anyone and may not be retracted afterwards. Keep in mind that content or communications on government-related social networking pages may be considered public records.

- Configure privacy settings to allow only those people you trust to have access to the information you post. Also, restrict the ability for others to post information to your page. The default settings for some sites may allow anyone to see your information or post information to your page; these settings should be changed.

- Review a site's privacy policy. Some sites may share information such as email addresses or user preferences with other parties. If a site's privacy policy is vague or does not properly protect your information, do not use the site.

## Additional Information:

- MS-ISAC Monthly Cyber Security Tips Newsletter: Social Networking Sites: How To Stay Safe www.msisac.org/awareness/news/2009-03.cfm

- OnGuardOnline: www.onguardonline.gov/topics/social-networking-sites.aspx

- StaySafeOnline – National Cyber Security Alliance: www.staysafeonline.org/blog/staying-safe-social-media-web-sites

- Social Networking Privacy - A Parent's Guide: www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm

- US-CERT--Staying Safe on Social Network Sites: www.us-cert.gov/cas/tips/ST06-003.html

**For more monthly cyber security newsletter tips visit:** www.msisac.org/awareness/news/

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, noncommercial purposes.*

***Brought to you by:***

MS-ISAC

*www.msisac.org*