ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Monthly Security Tips
NEWSLETTER

Tacoma

September 2013 Volume 8, Issue 9

Social Networking Sites: Security and Privacy Issues

From the Desk of Paul Federighi, Chief Information Security Officer

Recent hacks involving several high-profile social networking accounts once again highlight the potential vulnerability of social media. The sheer volume of users and the information that gets posted on social media sites create plenty of opportunity for an attacker to use social engineering or other methods to gain access to the accounts of individuals and organizations. The more information you post, the more your security and privacy are at risk.

What Precautions Should I Take on Social Networking Sites?

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, anti-spyware software, and a firewall and keep these applications and operating system patched and up-to-date.

- Be cautious when clicking on links. If a link seems suspicious, or too good to be true, do not click on it...even if the link is on your most trusted friend's page. Your friend's account may have been hijacked or infected and now be spreading malware.

- If you are going to request that your account be deleted, first remove all of the data. Request that the account be deleted, rather than deactivated.

- Type the address of your social networking site directly into your browser or use your personal bookmarks. If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen

- Be cautious about installing applications. Some social networking sites provide the ability to add or install third party applications, such as games. Keep in mind there is sometimes little or no quality control or review of these applications and they may have full access to your account and the data you share. Malicious applications can use this access to interact with your friends on your behalf and to steal and misuse personal data. Only install applications that come from trusted, well-known sites. If you are no longer using the app, remove it. Also, please note that installing some applications may modify your security and privacy settings.

- Use strong and unique passwords. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised. Use different passwords for different accounts, and do not use a password you use to access your organizations network on any personal sites you access.

- Be careful whom 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 comments. Once information is posted online, it can potentially be viewed by anyone and may not be able to be retracted afterwards. Keep in mind that content or communications on government-related social networking pages may be considered public records.

- When posting pictures, delete the meta data, which includes the date and time of the picture.

- Do not announce that you are on vacation or away for an extended period of time.

- Configure privacy settings to allow only those people you trust to have access to the information you post, and your profile. 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.

- 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.

For More Information:

For additional information, please visit:

- STOP.THINK.CONNECT Social Networking and Cyberbullying Tips: http://stopthinkconnect.org/resources/viewimageembed/?id=341

- US-CERT Socializing Securely: Using Social Networking Services http://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf

- Facebook: A Guide to Privacy: http://www.facebook.com/privacy/explanation.php

- Sophos: Facebook Security Best Practices: http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx

- Twitter: Protecting and Unprotecting Your Tweets: https://support.twitter.com/articles/20169886-how-to-protect-and-unprotect-your-tweets

Brought to you by:

CENTER FOR INTERNET SECURITY

MULTI-STATE Information Sharing & Analysis Center

STOP | THINK | CONNECT