



Enterprise Information Security Office

Monthly Security Tips NEWSLETTER

September 2013

Volume 8, Issue 9

Social Networking Sites: Security and Privacy Issues

From the Desk of Thomas D. Smith, Chief Information Security Officer

Recent cyber attacks involving several high-profile social networking accounts highlight the potential vulnerability of social networking sites. The sheer volume of users and the information that gets posted on social networking 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 on social media sites, the more your security and privacy are at risk.

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

- Ensure your computer has proper security measures in place before connecting to a social networking site. Use and maintain anti-virus software, anti-spyware software, and a firewall. 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.
- Remove all personal data first when deleting a social media account. Request that the account be deleted rather than deactivated.
- Always type the address of your social networking site directly into an Internet browser or use personal bookmarks. Do not click on a link to your social networking site through email or another website. Chances are you might be entering your account name and password into a fake site where your personal information could be stolen by a hacker or cyber criminal.
- Be cautious about installing third party applications. Install applications that come from trusted, well-known sites. Some social networking sites provide the ability to add or install third party applications, such as games. When you download a malicious application, hackers may have the ability to gain full access to your account and the data you share. Malicious applications can use this access to interact with your friends on your behalf, steal, and misuse personal data. Installing some malicious applications may modify your security and privacy settings. If you are no longer using the application, remove it.
- Use strong and unique passwords. Use different passwords for different accounts, and do not use a password you use to access your organization's network on any personal sites you use. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised.
- 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 metadata, 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.
- 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 additional information, please visit:

- Enterprise Information Security Office Resources and Newsletters - <http://www.dhses.ny.gov/ocs/>
- 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>

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 some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

