



## Security and Privacy on Social Networking Web Sites

### WHAT ARE THE SECURITY AND PRIVACY ISSUES ASSOCIATED WITH SOCIAL NETWORKING WEB SITES?

Social networking web 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 that 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 knowingly 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Security number, street address, phone number, financial information, or confidential business information should not be published online.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 PRECAUTIONS SHOULD I TAKE?

The following tips may help you to retain 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, do not share confidential information. 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 RESOURCES

For additional information on the current cyber security trends, please visit:

- DIR Monthly Cyber Security Tips Newsletter: Social Networking Sites: How To Stay Safe – [www.dir.state.tx.us/security/reading/2009%20CyberSecurity%20Tips/200904cybersec.htm](http://www.dir.state.tx.us/security/reading/2009%20CyberSecurity%20Tips/200904cybersec.htm)
- OnGuardOnline – [www.onguardonline.gov/topics/social-networking-sites.aspx](http://www.onguardonline.gov/topics/social-networking-sites.aspx)
- StaySafeOnline – National Cyber Security Alliance: [www.staysafeonline.org/blog/staying-safe-social-media-web-sites](http://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](http://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](http://www.us-cert.gov/cas/tips/ST06-003.html)

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit [www.dir.state.tx.us/security/reading](http://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](http://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:	Powered by:	Distributed by:
 <b>MS-ISAC</b> <a href="http://www.msisac.org">www.msisac.org</a>	 <b>US-CERT</b> UNITED STATES COMPUTER EMERGENCY READINESS TEAM <a href="http://www.us-cert.gov">www.us-cert.gov</a>	 <b>DIR</b>  <b>Secure Texas</b> <a href="http://www.dir.state.tx.us/securetexas">www.dir.state.tx.us/securetexas</a>
Copyright Carnegie Mellon University   Produced by US-CERT		