US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Socializing Securely: Using Social Networking Services

Mindi McDowell and Damon Morda

Social Networking Serves Many Purposes

Social networking is a way for people to connect and share information with each other online. Millions of people worldwide regularly access these types of services from mobile devices, applications, and websites. According to statistics published by some of the most well-known social networking services, there are more than 500 million active users on Facebook[1], 175 million registered users on Twitter[2], more than 100 million users on MySpace[3], and more than 80 million members on LinkedIn[4].

People may use social networking services for different reasons: to network with new contacts, reconnect with former friends, maintain current relationships, build or promote a business or project, participate in discussions about a certain topic, or just have fun meeting and interacting with other users. Some services, such as Facebook and Twitter, have a broad range of users, while others cater to specific interests. For example, LinkedIn has positioned itself as a professional networking site—profiles include resume information, and groups are created to share questions and ideas with peers in similar fields. On the other hand, MySpace is known for its emphasis on music and other entertainment. There are also social networking services that have been designed specifically to reconnect former classmates.

Sharing Information Presents Risks

When you share information online, you need to understand the potential risks, and you need to be wary of what you share and with whom.

Attacks and Unintended Information Disclosure

Attackers may use social networking services to spread malicious code, compromise users' computers, or access personal information about a user's identity, location, contact information,

[1] Facebook Factsheet (http://www.facebook.com/press/info.php?factsheet) (accessed January 3, 2011)

[2] About Twitter (http://twitter.com/about) (accessed January 3, 2011)

[3] MySpace Fact Sheet (http://www.myspace.com/pressroom/fact-sheet/) (accessed January 3, 2011)

[4] LinkedIn: About Us (http://press.linkedin.com/about) (accessed January 3, 2011)

and personal or professional relationships. You may also unintentionally reveal information to unauthorized individuals by performing certain actions. The following are some common threats to social networking services.

- **Viruses** – The popularity of social networking services makes them ideal targets for attackers who want to have the most impact with the least effort. By creating a virus and embedding it in a website or a third-party application, an attacker can potentially infect millions of computers just by relying on users to share the malicious links with their contacts.

- **Tools** – Attackers may use tools that allow them to take control of a user's account. The attacker could then access the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also pose as that user and post malicious content.

- **Social engineering attacks** – Attackers may send an email or post a comment that appears to originate from a trusted social networking service or user. The message may contain a malicious URL or a request for personal information. If you follow the instructions, you may disclose sensitive information or compromise the security of your system.

- **Identity theft** – Attackers may be able to gather enough personal information from social networking services to assume your identity or the identity of one of your contacts. Even a few personal details may provide attackers with enough information to guess answers to security or password reminder questions for email, credit card, or bank accounts.

- **Third-party applications** – Some social networking services may allow you to add third-party applications, including games and quizzes, that provide additional functionality. Be careful using these applications—even if an application does not contain malicious code, it might access information in your profile without your knowledge. This information could then be used in a variety of ways, such as tailoring advertisements, performing market research, sending spam email, or accessing your contacts.

Professional and Personal Implications

You may risk professional opportunities, personal relationships, and safety by posting certain types of information on social networking services.

- **Business data** – Posting sensitive information intended only for internal company use on a social networking service can have serious consequences. Disclosing information about customers, intellectual property, human resource issues, mergers and acquisitions, or other company activities could result in liability or bad publicity, or could reveal information that is useful to competitors.

- **Professional reputation** – Inappropriate photos or content on a social networking service may threaten a user's educational and career prospects. Colleges and universities may

conduct online searches about potential students during the application process. Many companies also perform online searches of job candidates during the interview process. Information that suggests that a person might be unreliable, untrustworthy, or unprofessional could threaten the candidate's application. There have also been many instances of people losing their jobs for content posted to these services. Although the legality of some of these terminations is still being debated[5], posting certain comments may affect your credibility and professional reputation.

- **Personal relationships** – Because users can upload comments from any computer or smart phone that has internet access, they may impulsively post a comment that they later regret. According to a survey conducted by Retrevo, "32 percent of people who post on a social networking site regret they shared information so openly."[6] Even if comments and photos are retracted, it may be too late to undo the damage. Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache.

- **Personal safety** – You may compromise your personal security and safety by posting certain types of information on social networking services. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized. You may also risk the safety of your children by posting photos and personal details. For example, if malicious individuals are able to collect enough information, such as the child's name, school, activities, or details about the parents, they might be able to lure a child into a dangerous situation.

An important element to remember about social networking services is that users may post information about other people. Without even realizing it, you may put someone else at risk by posting a comment or photo that could compromise that person's privacy or security. Sometimes, posting negative content about someone else is intentional. Social networking services have become channels for conducting cyberbullying[7], a growing problem that can lead to significant psychological trauma.

Proceed with Caution

Social networking services are useful and enjoyable, but it is important to take proactive steps to protect your computer, your personal information, and your company data. By protecting yourself, you also help to protect the people you are connected to on these services.

---

[5] "Company Accused of Firing Over Facebook Post" (http://www.nytimes.com/2010/11/09/business/09facebook.html)

[6] "Report: One in Three Regret Posting Personal Information on Social Networking Sites" (http://www.dailytech.com/Report+One+in+Three+Regret+Posting+Personal+Information+on+Social+Networking+Sites/article18401.htm)

[7] "Dealing with Cyberbullies" (http://www.us-cert.gov/cas/tips/ST06-005.html)

Implement Security Measures

Taking general security precautions will reduce the risk of compromise.

1. Use strong passwords[8], and use a unique password for each service.

2. Keep anti-virus software[9] up to date.

3. Install software updates[10] in a timely manner, particularly updates that affect web browsers.

Follow Good Practices

Social networking services offer unique risks, and you can minimize these risks by adopting good security practices.

1. **Use strong privacy and security settings** – Take advantage of the security options provided by social networking services. When choosing appropriate options, err on the side of privacy to better protect your information. These services may change their options periodically, so regularly evaluate your security and privacy settings, looking for changes and ensuring that your selections are still appropriate. Also periodically review the services' privacy policies to see if there are any changes.

2. **Avoid suspicious third-party applications** – Choose third-party applications wisely. Look for applications developed by vendors you trust, and avoid applications that seem suspicious. Limit the amount of information third-party applications can access.

3. **Treat everything as public** – The best way to protect yourself is to limit the amount of personal information you post to these services. This recommendation applies not only to information in your user profile, but also to any comments or photos you post. It is important that you consider information that you post about yourself and about others, particularly children.

4. **Share only with people you know** – Although many users seek to establish as many contacts on these services as possible, consider sharing personal information only with people you know. If you expand your contacts beyond people you are sure you can trust, check the service's settings to see if you can group your contacts and assign different levels of access based on your comfort level. Attackers may adopt different identities to try to convince users to add them as contacts, so try to confirm that contacts are who they claim to be before giving them access to your information.

Regardless of how restrictive you make your security settings, they may not offer complete privacy. An attacker or application may take advantage of software vulnerabilities, or another user may repost your information. When using social networking services, be responsible and

---

[8] "Choosing and Protecting Passwords" (http://www.us-cert.gov/cas/tips/ST04-002.html)

[9] "Understanding Anti-Virus Software" (http://www.us-cert.gov/cas/tips/ST04-005.html)

[10] "Understanding Patches" (http://www.us-cert.gov/cas/tips/ST04-006.html)

always consider the risks. Operate as if all of the content is public, and only post information you would be comfortable sharing with other people.

Additional Resources

US-CERT Resources:

- "Staying Safe on Social Network Sites" (http://www.us-cert.gov/cas/tips/ST06-003.html)
- "Guidelines for Publishing Information Online" (http://www.us-cert.gov/cas/tips/ST05-013.html)

Other Resources

- "Seven Deadly Sins of Social Networking Security" (http://www.csoonline.com/article/496314/seven-deadly-sins-of-social-networking-security)
- "Social Networking and Security Risks" (http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf)
- "Risks and Benefits of More Open Social Networking" (http://www.epa.gov/oei/symposium/2010/gotta.pdf)