Social Networking Sites

What is a social networking site?

A social networking site (SNS) is a web-based service that allows communities of people to share common interests and/or experiences. Rather than using direct point-to-point communication to stay in touch (e.g., face-to-face, phone, text/video messages), SNSs allow users to publish information that can be read later by other users (a one-to-many form of communication) and follow their friends' postings and provide comments.

SNSs provide innovative methods for interacting with friends through third-party applications, such as simple games (tic-tac-toe, paper-rock-scissors), interactive maps to show places visited across the world, and quiz/trivia games which allow for score comparison with others. Many SNSs also allow users to logon from mobile devices that have web browser access to the Internet, allowing them to check and update their accounts from virtually any location with a Wi-Fi or cellular signal.

What are the security concerns?

OPSEC – SNSs promote "social behavior" and encourage users to share information and inherently trust the information from those they are connected to within the SNS. Once information is posted or uploaded onto an SNS, it should no longer be considered *private*. Even if the SNS has strong *privacy settings*, that privacy is completely dependent on the security of the web application. On some SNSs, third-party add-ons have elevated privileges, giving them access to additional private information such as home addresses or birthdays (Mary Landesman, "Cyber Thieves Target Social Sites," *BBC News Online*). Savvy attackers may also aggregate information from multiple sites to gain access to private information (e.g., online banking records, email). For example, personal information posted to an SNS (e.g., birthday, pet's name) could be used to compromise security credentials (e.g., password, pin, security questions) for that site or other sites, giving an attacker access to private information.

Cross-Site Scripting (XSS) – These attacks are a type of code injection, generally in the form of a browser-side script (OWASP, Cross-Site Scripting). Many SNSs allow users to post comments and messages in plaintext, HTML, or active content (e.g., JavaScript, Flash). If these posts contain malicious content, a user's web browser could be forced to perform a variety of unintended actions such as downloading malware, surfing to a malicious website, or even causing a Denial of Service (DoS) on the user's network.

Impersonation – Impersonation of a friend or colleague can be used to trick SNS users into providing private information or downloading malicious third-party applications or content. In most cases, SNSs perform only a basic check, such as email validation, to confirm a user's identity.

Malicious Content – SNSs allow users to share a variety of multimedia content, from images to video clips to documents. This advanced content has the potential to contain malicious code, which under the correct circumstances may cause the user's browser to download malware or perform other unintended actions.

SNAC DoD, 9800 Savage Road Ft. Meade, MD 20755-6704 410-854-6632 DSN: 244-6632 FAX: 410-854-6604 www.nsa.gov/snac
SNAC@radium.ncsc.mil

An example of how these security concerns can be exploited is detailed in the following: John Smith has a profile on *CoolSNS.com*. Users can find John by searching, but his profile information is visible only to those authorized by him. He receives a connection request from Sally Jones, and because he recognizes her name from a prior technology conference, he accepts her request. The "Accept" means that John has authorized Sally – or rather, anyone logging in from or impersonating Sally's account – to view information posted on his profile. A day or so later, Sally sends John a link to a third-party application. Thinking "this is from Sally so I can trust it," John adds the application to his account. Immediately, a popup displays saying "This application requires an update of Endure Media Player. Please click 'OK' to run 'endure_mp.exe' for the update." Trusting Sally, and wanting to experience this application in its entirety, John clicks "OK." By clicking "OK," John unwittingly downloads malware, which not only infects his local computer, but also spreads throughout his entire organization's network causing loss of data and productivity.

What should I keep in mind when using SNSs?

Although quite advanced, social networking sites are simply websites. Safe web browsing practices and OPSEC awareness are the best mitigation strategies for protecting your information. Below is a list of technical and behavioral best practices that can be implemented to mitigate the risks of using SNSs.

Technical Best Practices

- Ensure your operating system and web browser are up-to-date with the latest patches (System and Network Analysis Center IAD, "Defense Against Drive-by Downloads," NSA/CSS).
- Maintain a blacklist of blocked sites for your network.
- Update your virus scanners with the latest definitions and patches, and scan often.
- Do not browse the Internet from privileged accounts such as root or Administrator.
- Enable Data Execution Prevention (DEP) in the OS to prevent buffer overflow attacks (System and Network Analysis Center IAD, "Data Execution Protection," NSA/CSS).
- Install an application firewall or Host Intrusion Prevention System (HIPS) and enable whitelisting.
- Apply Software Restriction Policies (SRP) on machines running Microsoft Windows platforms (XP/Server 2003 and newer). SRP keeps a whitelist of allowed executables, preventing the installation of malicious downloads.

Behavioral Best Practices

- Perform a risk assessment before posting information about you or your organization. Never post any sensitive information, and post information as if privacy or filtering settings do not exist within the site's functionality. Sensitive information (e.g., address, phone number) should be left off all social networking sites.
- Before accepting a friend/connection request, confirm with them either verbally or face-to-face. This ensures that the involved accounts are neither compromised nor impersonated.
- Be selective of which third-party applications to add to your profile. There is no guarantee that third-party applications have been reviewed or officially approved by the parent SNS. These applications could contain malicious code attempting to exploit your account and the site at large.

References:

Cyber Thieves Target Social Sites – http://news.bbc.co.uk/2/hi/technology/7156541.stm
Cross-Site Scripting (XSS) – http://www.owasp.org/index.php/XSS
Defense Against Drive-by Downloads – http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf
Data Execution Prevention (DEP) – http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf