



Enterprise Security Office Monthly Security Tips NEWSLETTER

December 2011

Volume 6, Issue 12

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. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Staying Safe On Social Networking Sites

The popularity of social networking sites -- such as MySpace, Facebook, Twitter and others -- has expanded tremendously in recent years, with nearly two-thirds of Americans using these sites regularly.¹ The number of adult Internet users having a social networking profile has more than quadrupled in the past five years, according the Pew Internet & American Life Project. The sites are becoming more ubiquitous for both personal and professional activities. The sites also continue to serve as prime targets for malware distribution and scams. A recent study reported that 91% of respondents have received spam and 54% were targets of phishing attacks on social networking sites.² While there has been increased attention to addressing security concerns relating to social networking sites, you need to remain vigilant and take the necessary precautions when using them has never been greater.

What are the security concerns of social networking sites?

Social networking sites continue to grow in popularity as attack vectors because of the volume of users and the amount of personal information that is posted. The nature of social networking sites encourages you to post personal information. The perceived anonymity and false sense of security of the Internet may cause users to provide more information about themselves and their life online than they would to a stranger in person.

The information you post online could be used by those with malicious intent to conduct social engineering scams and attempt to steal your identity for access to your financial data. For example, many individuals are tempted to click on a video they see on a friend's page. Unfortunately, these videos may lead to a malicious website. When you access a site that has malicious code, your machine could become infected.

What can I do to be safe?

- **Keep your system updated:** Ensure that any computer you use to connect to a social networking site has proper security measures in place, including anti-virus and anti-spyware software, and a firewall. Make sure you keep them up-to-date. Keep your operating system updated and patched. Set the configuration to "auto update" so patches can be applied automatically without intervention.
- **Use strong passwords:** Protect your social networking account with a strong password. Do not share this password with anyone or use it for other sites. In addition, some social networking sites support features for stronger authentication, such as using one-time passwords when logging in from public computers or using your phone as part of the login process. Enable these features where possible. It is critical that passwords used on social networking sites not be used on other sites.
- **Links:** Be cautious when clicking on links. If a link seems odd, 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.
- **Scams:** Criminals take advantage of the open nature of social networking sites to defraud individuals. Such scams sometimes use the pretext of an offer for a job or money. Another common scam uses hijacked accounts to contact the victim's friends with requests for help, claiming that the person was robbed in

¹ <http://www.pewinternet.org/Reports/2011/Social-Networking-Sites/report.aspx>

² http://www.barracudanetworks.com/ns/news_and_events/index.php?nid=492

foreign country and needs money. Be cautious when contacted on a social networking site with a request for money or with an offer that's surprisingly good.

- **Privacy:** Do not assume privacy on social networking sites. 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. 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.
- **Personal Information:** Do not respond to an email requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- **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 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.

Resources for more information:

MS-ISAC Newsletter – Security and Privacy on Social Networking Sites

<http://msisac.cisecurity.org/newsletters/2010-03.cfm>

MS-ISAC Daily Tip – Stay Safe on Social Networking Sites

<http://msisac.cisecurity.org/daily-tips/Stay-Safe-on-Social-Networking-Sites.cfm>

US-CERT Cyber Security Tip – Staying Safe on Social Networking Sites

<http://www.us-cert.gov/cas/tips/ST06-003.html>

National Cyber Security Alliance – Protect Yourself: Social Networking

<http://staysafeonline.org/in-the-home/social-networking>

Facebook Security Guide (issued in October 2011)

<https://www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf>

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

Brought to you by:

