Professionals: Don’t Use Facebook and Twitter

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Friend and colleague Jan S. Buitron, MSIA, CISSP, MCSE, contributes an interesting analysis of security and social networking. The rest of today’s column is entirely her work with minor edits.

* * *

The January 2010 “Security Threat Report: 2010” from SOHOS starts with a section on social networking sites; the summary includes the statements, “2009 saw Facebook, Twitter, and other social networking sites solidify their position at the heart of many users’ daily Internet activities, and saw these websites become a primary target for hackers. Because of this, social networks have become one of the most significant vectors for data loss and identity theft.” The section on social networking reports, “Companies now commonly use blogs to disseminate and share information. Forums serve as a form of technical support where professionals can troubleshoot with peers and colleagues. Meanwhile, many companies embrace Facebook and MySpace because the sites present a great way to connect with customers and spread the latest company news or product offerings to the public.”

Do you receive a steady stream of invitations to join Facebook, MySpace, and Friendster? I have been told repeatedly by friends and colleagues that I should post personal information on these sites, tweet on Twitter, and use some of the many other social-networking tools available. However, as a computer-security professional, I have purposely avoided joining Facebook and tweeting on Twitter.

It’s against my sense of personal security to use Websites asking for personal information unless I have a pretty good idea that they are secure. I like to use Netcraft’s Web phishing toolbar to avoid connecting to dubious sites. Unfortunately, from what I have researched about Facebook, MySpace and Twitter, I do not feel that they warrant my trust.

Vast Attack Surface

Businesses have taken to using social-networking sites to promote their services and to connect with prospective clients. While the trend may be progressive, it is also progressively risky. Facebook was designed by Harvard University student Mark Zuckerberg in 2004 as a project to keep students connected. It appears that Mr. Zuckerberg was not
familiar with techniques for developing secure Web-facing sites. The result was a non-secure application: a hacker’s paradise, but an end-user’s nightmare.

According to two Internet security researchers who presented at the Black Hat Briefings in 2008<http://searchsecurity.techtarget.com.au/tips/26279-Black-Hat-roundup-Social-networking-sites-insecure-by-design-How-to-bust-Vista-Bluetooth-hackable>, sites like Facebook and MySpace are eminently hackable for several reasons. Shawn Moyer, founder of consultancy Agura Digital Security<http://www.agurasec.com/> [and responsible for one of the funnier LinkedIn profiles (start at <http://www.linkedin.com/in/shawnmoyer>) that MK has ever seen], and Nathan Hamiel, founder of the Hexagon Security Group<http://hexsec.com/>>, presented evidence that social networks use “wide open” Application Programming Interfaces (APIs); this means that the applications used to run sites like Facebook and Myspace allow unrestricted application data interchanges. The attack surface is vast. The programming flaws “permit attackers to tap into user applications and exploit site code that’s wide open to cross-site scripting and other attacks.” It seems tantamount to hanging out signs on Facebook and Myspace that say, “Hack Me.”

** * * *

In the second of this two-part series, Jan Buitron discusses how social networking sites can be used for social engineering and looks at the safety of LinkedIn.

** * * *

Jan S. Buitron, MSIA, CISSP, MCSE, is a 2009 graduate of the Masters of Science in Information Assurance (MSIA<http://infoassurance.norwich.edu/> ) program at Norwich University. She is currently teaching classes in the MSIA<http://www.regisdegrees.com/online-degree-programs/masters-information-assurance.asp> program for Regis University, Denver.


Copyright © 2010 Jan S. Buitron & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.