In this second of two parts, friend and colleague Jan S. Buitron, MSIA, CISSP, MCSE, continues her analysis of security and social networking. The rest of today’s column is entirely her work with minor edits.

* * *

Pictures from a Picnic

Facebook affords opportunities for Internet thieves to invade businesses. In an example provided by network infrastructure provider Terramark (with the victim company and employee names anonymized), hackers hijacked a Facebook account belonging to “Bob,” a male employee at a financial institution, and sent a link to an unsuspecting female employee named “Alice” at the same firm. There had been a company picnic the previous weekend, and the e-mail from the hijacked account belonging to Bob promised pictures from the recent picnic. Alice clicked the link, expecting to see pictures of the company picnic. It appeared that nothing happened, but she had downloaded a keylogger onto her company laptop. The thieves then obtained the female employee’s remote company login and proceeded to breach a vulnerable, unpatched server inside the financial services company network.

Fortunately for the financial institution, the thieves were not adept at hiding their activities. More than one person in the company had received the fake link and complained to the corporate administrator that the link to the pictures was not working. The administrator got suspicious and found the breach after closely examining corporate system event logs. It had all started with an employee using Facebook on a company laptop.

I strongly recommend that government agencies and businesses avoid using social-networking sites to post internal operating information. It is a dubious exercise, at best. At worst, organizations are exposing themselves to considerable risk of security breaches.

Casually posting detailed information (e.g., through tweets) from high-security personnel – especially about absences from work such as their whereabouts on vacation or at conferences – may give industrial spies valuable information for penetration through social engineering. Recently Thomas Ryan, co-founder of Private Security, carried out what is now called the “Robin Sage Experiment” by posting a fictitious female character as a ‘cyber threat analyst’ who is 25 years old with 10 years information security experience (why did no one notice this?). He added a flirty picture of “a cute girl from an adult website”
experiment/ and in less than a month, ‘she’ had over two hundred contacts in the military and intelligence communities. Worst of all, those contacts revealed national secrets readily to their new contact.

Readers with an investigative streak will quickly establish that I do use LinkedIn, the professionals’ social-networking site. I feel confident about the safety of using LinkedIn because numerous members of the cybersecurity community use LinkedIn. LinkedIn is designed for the business and privacy-minded. A member of LinkedIn has greater command over what others see in their public profile. LinkedIn has granular controls, allowing the user to block specific details of his\her profile from public view. You can choose to show or not show your picture, your location or even your last name < http://www.cio.com/article/485489/LinkedIn_Privacy_Settings_What_You_Need_to_Know?page=2&taxonomyId=3055 >.

In contrast, Facebook recently reduced its users’ abilities to manage what others see in their personal data. Facts like your current city, educational level and employment will be public information unless they are deleted < http://www.eff.org/deeplinks/2010/04/facebook-further-reduces-control-over-personal-information >.

Finally, the LinkedIn user also has final choice and control when it comes to establishing a connection. One users can ‘invite’ another to connect but the connection is not finalized until the invited person approves the connection. These are the reasons why I use LinkedIn, rather than Facebook, Twitter, or Friendster.

* * *

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.