@ISACA
RELEVANT, TIMELY NEWS
Volume 17, 18 August 2010

Five Things to Think About When Using Social Networking

By John P. Pironti, CISA, CISM, CGEIT, ISSAP, ISSMP

1. The most effective approach to use when considering social networking within the enterprise is “embrace but educate.” There is a great demand for and business benefit associated with using social networking. Users should be educated on the expectations and risks associated with using social networking in both their professional and personal lives. They should also be reminded of their obligations concerning corporate data security, privacy and employee conduct, which they agreed to as part of their terms of employment.

1. Social networking is often used for social engineering attacks. Adversaries are actively compromising social networking user accounts and using them to send malware and links to connected users from trusted connections to increase the likelihood that their attacks will be successful. Individuals are more likely to accept links and information from someone they trust than a random e-mail or message from a stranger.

2. Social networking content has an unknown lifespan. Individuals should be made aware that once they post information including pictures, video and personal details to a public social networking site, the data may follow them for the rest of their lives. Students and young people are especially vulnerable to this fact since many organizations now include public social networking sites in their background checks for employment.

3. Most public social networking sites do not have adequate authentication or identity verification capabilities. Social networking sites can be and have been used by individuals to pose as others to attempt to discredit, steal identities or use other identities in an effort to gain the trust of vulnerable targets. Most social networking sites use basic identity-verification techniques such as e-mail address validation and links within e-mail messages sent to the registered address. Setting up false e-mail accounts easily defeats these methods.

4. Privacy in public social media sites is not easily achieved. Free to the user, public social media sites are typically funded by their ability to sell targeted advertising

capabilities and marketing data to organizations. To demonstrate the value of these data, the site needs to be able to perform data mining and identification operations among all of the data posted to the site. The end-user license agreement (EULA) users agree to when joining public social media sites often include clauses that state that users should not expect privacy of data that they post and the site can use posted data for revenue-generating activities once the user has posted the data.

Click here for a complimentary download of ISACA's white paper titled *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*.

John P. Pironti, CISA, CISM, CGEIT, ISSAP, ISSMP, is the president of IP Architects LLC.