



Productivity

September/October 2008

To Block or Not to Block? Social Networking Sites in the Workplace

There's no doubt that social networking sites are a relevant part of the everyday lives of people at home as well as in the workplace. People are realizing these sites have impact not only in terms of personal growth and relationships, but also as tools for staying connected in business.

The recording industry recently demonstrated the growing importance of social network sites when BusinessWeek reported that Warner, Sony BMG and Universal launched an endeavor with MySpace in which the social networking giant will allow users to listen to and watch music content and purchase related merchandise and tickets on its site. Certainly, there are business reasons to employ these sites.

But like all worthwhile technology tools, this one, too, comes with pitfalls. The increasing use of social networking sites in the workplace can have serious security and productivity implications for companies, which is why more and more companies are choosing to block or limit the use of these sites.

Scammers are coming up with new ways to steal information and corrupt computers through sites such as LinkedIn, Plaxo, MySpace and Facebook. One such method is the Nigerian 419 advance fee fraud scams, which experts say has popped up recently on these sites.

According to Paul Wood, senior security analyst at MessageLabs, "We've seen one example of Nigerian 419 recently where the fraudster had created a fairly convincing-looking page on LinkedIn to give credibility to their background in the business they were trying to promote." In these cases, scammers may use e-mail correspondence to prompt unsuspecting users to visit their profiles and learn about their fake personas. The aim is to provide a false sense of trust so users will be convinced to do business with them — and ultimately give them money.

In some cases, a scammer will claim to be someone you know, "pretending to be that person in order to gain access to your profile, your friends list, or other information you might be willing to give them," explained Wood.

Another trick is the use of fake embedded videos on otherwise legitimate-looking websites. "You might see [what looks like] a link to a YouTube video with the YouTube logo, but in fact it's just a spoof. When you attempt to view the video, you are asked to download a codec that supports the video's format. In most cases, what you downloading is malware.

In order to protect yourself, Wood suggests verifying the identity of people who claim to be someone you know and also being skeptical of videos and links that may appear to be legitimate.

“If somebody says, ‘I’m so-and-so that you used to work with several years ago,’ do you have another means of contacting that person?” Wood said. “Don’t take it at face value; [on the computer, people] tend to be more trusting than if [they] were face to face meeting somebody for the first time. [On the Internet], there are so many other factors that you miss out on, like body language.”

These sites also can cause a lag in productivity. “If someone’s spending too much time online or addicted to playing Scrabble with somebody on Facebook, then they might not be doing their jobs,” said Wood. This is another reason why companies need to adopt policies regarding acceptable Internet use on the job.

Some companies choose to completely block social networking and blogging sites, and others allow some use of these sites at specific hours, such as lunchtime. Excessive blabbing on social sites can generate unwanted gossip about a company and its plans, while unscrupulous competitors can social-engineer employees into revealing intellectual property. An employee’s mere presence on a social network also sends a signal: job titles, experience, friends and family, and contact information can all be combined to where competitors can draw reasonably accurate organizational charts of a company, its suppliers, partners and clients.

What’s important, said Wood, is accounting for the “three prongs” of web policies. “You have to look at the policies appropriate to your business: the user training and awareness side of it as well as the educational aspects internally, to make sure employees understand the potential risks — the social engineering threats — that they may come into contact with. “The third part is having the tools and technology in place to protect employees so they don’t visit a site that may harbor malicious content,” he concluded.

Minimizing Social Network Risk

Realizing that perceived security gaps could lead individuals and companies to shun their sites, big names like Facebook and LinkedIn allow users to adjust how much information — posts, photos, online status and other factors — others may access.

Facebook’s [privacy site](#) describes several such controls. Users can reduce what appears in their profile and what information about their online activities is public, such as their use of specific Facebook applications. Users can also block specific users from seeing more than a limited profile or from finding a user via search.

Facebook also limits the ability of search-site Web crawlers to harvest user information, saying in its privacy policy, “Facebook limits access to site information by third party search engine ‘crawlers’ (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond a user’s name, profile picture, and limited aggregated data about the users profile (e.g. number of wall postings).” LinkedIn is the most business oriented social network, and its users seem generally aware of the need to behave professionally. The site provides a wide range of tools for customizing views, such as the ability to change whether people you’re connected to can see just those you both have connections with, or your entire connections list.

These types of features increase social networks’ corporate usability. However, at the end of the day, specific company policies that limit what employees may share online might create the biggest payoffs, like resistance to social engineering, preservation of the company’s and employees’ reputations, and preservation of trade secrets and internal company structure.

Excerpts from two articles: Certification Magazine, May 12, 2008, by Meagan Polakowski. www.certmag.com/articles and IT Security Magazine, Social Network Security Hazards, July 25, 2007 by Paul D. Kretkowski; www.itsecurity.com