ChannelWeb

# Corporations Need Security For Social Networking Apps

(URL: http://www.crn.com/security/215600025)

## By Scott Campbell, ChannelWeb

### 4:01 PM EST Fri. Feb. 27, 2009

Facebook CEO Mark Zuckerberg was on "The Today Show" Friday defending the social networking platform's user policies for its 200 million members.

While Facebook has come under fire for its reported claim to own members' information in perpetuity, it hasn't stopped rampant growth of the company founded in 2004. Zuckerberg told "Today Show" host Matt Lauer that a million members a week are added in the United States alone.

What he didn't say is that it's likely that some of them are malicious, and that corporations and individuals need to take steps to ensure their security.

Some companies try to limit their employees' social networking at work while other businesses encourage it as part of the business process. But to date, there hasn't been enough communication or policies drafted to ensure confidential information remains that way, according to Ian Amit, director of security research at Aladdin Knowledge Systems, an Arlington Heights, Ill.-based security applications vendor.

"It's already prevalent in most midsize to large organizations. Most large organizations acknowledge they can't block social networking. Everyone they hire now expects accessibility to social networking. If an organization is trying to bring in new people, they can't enforce a policy that says they don't allow it."

The range of security threats around social networking sites, including LinkedIn, MySpace, Facebook and others, ranges greatly, Amit said.

Much of Web 2.0 is unmonitored, with unsupervised content being generated by everyone. Attacks can come from malware or malicious code that entices users to click on the links, which could allow a hacker to gain information about you or your company, he said.

"Another threat that is more relevant to businesses is personality hijacking. You can create a profile for people who are not on social networking, and with enough public information it looks like that profile is the person's real profile," Amit said.

Eventually, the fake profile can be used for slander or defamation to business espionage or financial fraud, he said.

"In the news, we've seen some recent examples for some activity. One example is a Facebook user who had their password stolen. The [hacker] started telling this person's friends that they were stuck on a business trip and that someone stole their wallet and can they help him out. They tried to social engineer the friend to send some money over," he said.

Another example is a soccer player in Italy, Alessandro Del Piero, who was victimized by a fake Facebook profile created in his name. Over time, the fake profile gained a legion of fans as friends. The creator started adding racial remarks and references to Nazi Web sites, Amit said.

"It caused a lot of turmoil in Italy and he [Del Piero] is suing Facebook," Amit said.

Closer to home, Amit said it's possible for someone to create a profile of a senior corporate executive that over time might be used to access information he or she might not otherwise be able to obtain.

"That's really easy to do. At the Black Hat conference in [Washington], D.C., a few days ago, a researcher had a great lecture about how you could create a fake profile for some company's employee, based on aggregate information from other profiles, like an alumni group. You start with office politics and friendships and you can infiltrate that space, create a fake resume, send messages. You can manage to get a lot of info [pertaining] to that business that was unknown to the public."

So what's a company to do? Education for employees is important. You can enforce some procedures such as no chatting via Facebook or sharing information with LinkedIn's Huddle Workspaces, Amit said.

"We did run into a few cases where [business] customers were impacted. They found out inadvertently that someone inside their business had linked to a fake profile. Someone noticed they had a LinkedIn profile that they didn't create. The guy lectured a couple of times so people had his bio," Amit said.

Social networking security breaches also can occur to people who belong in groups, such as those organized by graduating classes.

"In anticipation of the new year, [fake profilers] signed up for that group. Whoever opens that group is planting the seeds for all of those spammable mailing lists of university graduates," he said. "Can you imagine having the MBA list of Harvard? That's priceless."

In most cases, the perpetrators take great pains to ensure they don't get caught, he said.

"This is not Sarah Palin's e-mail getting hacked into by a guy using his own PC," he said.

By using an anonymous proxy on the Web, someone can impersonate whomever he or she wants to with little chance of being traced, Amit said.

"There are so many moving elements. You have to go through the ISP, the application provider, a potential proxy provider and hope they provide all the details. Knowing the volume of transactions, it's literally looking for a needle in a haystack," he said.

Aladdin recently started providing security functionality adapted for social networking and there also are reputation-tracking services and brand-recognition tracking services that can help spot fake profiles early on, Amit said. "They categorize [results] by new sites, social networking tools, analyst sites, to give you a view of how your brand is doing on the Web," he said.

---