Web social networks friendly to identity thieves

Scam artists are taking advantage of a trusting arena to get members to divulge passwords and other information.

By Joseph Menn, Los Angeles Times Staff Writer
May 5, 2008

Michael Maris became an unwitting spammer.

The 22-year-old college student from Chicago received messages last year from annoyed friends on MySpace, wondering why he had used the social networking site to send them pitches for male enhancement products.

He checked his outgoing mail folder and discovered that someone had hacked into his account, then blasted the unsolicited messages to each of his 70 MySpace pals. Among the recipients were his nieces, ages 14 and 16.

"I couldn't believe that it happened," he said.

Social networking sites, which let users create detailed profile pages and connect with friends, are becoming the hot new thing for identity thieves, both amateur and professional. As improved spam filters and skeptical consumers make bogus e-mail less successful, scam artists are taking advantage of the atmosphere of trust that exists within these online circles of friends.

Symantec Corp., a tech security firm, recently reported that 91% of the bogus U.S.-based websites used in so-called phishing attacks during the second half of 2007 imitated the log-in pages of two unnamed social networking sites -- believed by industry executives to be the two biggest, MySpace and Facebook. Phishing tries to trick recipients into visiting phony websites and disclosing account numbers, passwords and other personal data.

"The bad guys are very adaptable. If something doesn't work, they come up with something new." said Kevin Haley, a product executive at Symantec. "Users feel more comfortable surrounded by their friends online -- what could be safer?"

Sometimes financial gain isn't the objective. Cyber-bullies have taken over the social networking accounts of acquaintances to post vicious rants or engage in mischief.

Frank Nein, a new-media executive in Los Angeles, is still perturbed that a man showed up at the home of his 12-year-old daughter after another girl impersonated her during MySpace chats.

Nicole Whiting, a 19-year-old nanny from Charlotte, N.C., fielded questions from friends about her new boyfriend, Patrick. They learned of the relationship on what they thought was her Facebook page.

One problem, she said: "I don't even know a Patrick."

It turned out that "some lonely guy" had copied her pictures from her MySpace page, borrowed her first name and created a Facebook profile for an imaginary girlfriend. Her problem ended after she tracked down Patrick and complained.

But experts warn that victims of more sophisticated scams won't get off so easy. The same kind of hackers who dreamed up e-mail scams featuring Nigerian dictators are now focused on cracking social networks to peddle products and engage in identity theft.

In more organized campaigns, scammers distribute free widgets that purport to help
users decorate their profile pages but secretly use the log-on information to spam their friends, as happened to Mars. Other crooks surreptitiously install software that records keystrokes to steal financial data, or they use personal details gleaned from the profiles to make e-mail fraud attempts more credible.

One common technique on social networking sites involves sending messages that appear to come from an online buddy, inviting the recipient to check out a new profile page. The page then asks the recipient to log in.

It's a scam. Although the page looks as if it's on MySpace or Facebook, thieves have set up to capture log-in names and passwords. The con artists can then try those names and passwords to gain access to e-mail accounts, financial accounts and other websites, given that many people use the same password widely.

For scammers, knowing the names of a target's friends can be a powerful tool. Last year researchers at Indiana University used simple tools to crawl through major networking sites and record the connections among Indiana students they found. They then sent e-mails that appeared to come from a friend also enrolled at the school.

About 72% of the recipients clicked on the e-mailed link and then entered their university user names and passwords at a fake site. In a control group where the e-mails came from strangers at the university, only 16% fell for it.

MySpace and other sites that rely on outside advertising networks also have been compromised by malicious banner ads that take advantage of security holes in users' Web browsers to install spyware. In addition, both MySpace and Facebook recently had security vulnerabilities in their systems for uploading photos. "Toolkits" for exploiting those vulnerabilities to forcibly install "malware" circulated rapidly in hacker communities.

Most attacks work only against people who lack updated firewalls, anti-virus systems and anti-spyware programs, but some can victimize anyone clicking the wrong link.

Parry Aftab, executive director of the nonprofit group WiredSafety, said the most pernicious attempts to get log-on information or install spyware remained phishing e-mails that appear to come from financial institutions. The account takeovers at social sites, by contrast, usually aim to send spam within a network, drawing people to porn sites or those selling questionable wares.

Major social networking sites are stepping up their defenses. Beverly Hills-based MySpace, which is owned by Rupert Murdoch's News Corp., now tries to have the Web links from its pages go through a sort of quarantine. When it recognizes that users are about to follow a link away from the site, MySpace flashes an explanation of the potential for fraud.

"MySpace employs a variety of technological, legal and policy solutions to protect our users from phishing attempts," Chief Security Officer Hemanshu Nigam said in a statement.

MySpace and Palo Alto-based Facebook Inc. declined to make executives available for comment.

"Facebook is committed to user safety and security and is constantly improving the site to provide new technology to catch phishers quickly and limit the damage they can do," it said in a statement. "We always encourage users to take precautions when clicking on any suspicious links and to only log in to Facebook from pages they know are legitimate."

Security experts said they expected identity theft and other scams on social networking sites to escalate.

Spam has evolved from advertising pitches to fake e-mails from banks and, most recently, highly targeted phishing attacks that focus on a given company's executives or customers. Some instances of that tactic, known as spear-phishing, rely on information about the targets gleaned from postings on Facebook, LinkedIn and other sites favored by professionals, experts said.

As the social networks do better at blocking fake or captured user accounts, the scams will become more harmful by automatically installing key-loggers and other data-stealing software, said Adam O'Donnell, director of emerging technologies at anti-spam firm Cloudmark Inc.

"As anti-spam improves, all the techniques they use for e-mail will work on social networks," he said. "This time, those techniques are going to have a much higher rate of success."

joseph.menn@latimes.com