# Phishers can use social Web sites as bait to net victims

May 24 2007

Internet sites such as MySpace and Facebook are popular ways for friends to stay in touch, but they also can be used by cyber sharks posing as "friends," enabling them to steal personal and financial information.

That's one of the conclusions found by researchers at the Indiana University School of Informatics. In their study, "Social Phishing," the scientists claim to have established for the first time a baseline for the success rate of individual phishing attacks, both traditional and with social context.

Phishing is duping someone into giving up private data -- such as credit card and Social Security numbers -- by masquerading as an authority. This is usually accomplished through e-mail or instant messaging, directing the recipient to a fraudulent Web site that appears legitimate.

"Phishing has become such a prevalent problem because of its huge profit margins, ease in launching an attack and the difficulty of identifying and prosecuting those who do it," said Filippo Menczer, associate professor of informatics and computer science. "Our study clearly shows that social networks can provide phishers with a wealth of information about unsuspecting victims."

Menczer was joined by Markus Jakobsson, associate professor of informatics, and computer science graduate students Tom Jagatic and Nathaniel Johnson. Their study is scheduled to appear in the October 2007 issue of Communications of the Association of Computing

Machinery.

Their phishing expedition was spawned in April 2005 as a Web-mining student project at IU's Bloomington campus. It was approved in advance by the IU-Bloomington Human Subjects Committee, which is responsible for reviewing and approving research activities involving human subjects and data collection. The researchers also worked closely with the university's information technology policy and security offices.

"The attempt in performing such an experiment was to quantify -- in an ethical manner -- how reliable social context would increase the success of a phishing attack," Menczer said.

No personal information or any other sensitive data was collected from those who responded to the simulated phishing attack.

The researchers began by harvesting freely available information by crawling social network and blogging Web sites, allowing them to easily build a database with tens of thousands of relationships.

"This could be done using off-the-shelf crawling and parsing tools, accessible to anyone with introductory-level familiarity with Web scripting," said Jagatic. "For the purposes of our study, we focused on a subset of targets affiliated with IU by cross-correlating the data with IU's address book database."

Jagatic said this was done to guarantee that all subjects were IU students, which was part of the approval to perform the experiment on human subjects.

The experiment spoofed e-mail messages to two groups of students: One group received messages from senders they thought to be friends, while the other group received e-mail from strangers. Both groups were asked

in their e-mails to visit an external Web site and enter their university ID and password.

Sixteen percent of students receiving e-mail from strangers took the bait, while 72 percent receiving e-mails from "friends" on their social networking sites gave up the information.

"We were astonished by that 72 percent response rate," Jakobsson said.

And for good reason: Surveys by the Gartner Group report that about 3 percent of adult Americans are successfully targeted by phishing attacks each year, an amount that might be conservative given that many are reluctant to report they have been victimized, or may even be unaware of it.

The study suggests that some countermeasures can be taken to thwart social phishing. Digitally signed e-mail could verify the identity of senders. A second line of defense might be a browser toolbar, alerting Web users about spoofing attempts. A third countermeasure would be improved spam filters that detect spoofed emails by analyzing the email path information. Finally, another technique might be to provide users with a secure path for entering passwords, alerting users that they are trying to authenticate to an unknown site.

"Our study also points to the need for extensive educational campaigns about phishing and other security threats," said Jakobsson. "Efforts such as SecurityCartoon.com aim to make typical Internet users less vulnerable by heightened awareness of the dangers of phishing, the importance of reporting attacks to which they fall victim, the ease of spoofing, and the possible uses -- and abuses -- of personal information posted on the Web."

Jakobsson and Steven Myers, assistant professor of informatics, are the

co-editors of *Phishing and Countermeasures*, a 736-page tome exploring the sophisticated methods cyber crooks use to steal financial and other personal information from consumers, and to conduct corporate and military espionage.

Source: Indiana University