# More Internet users may be taking phishing bait than thought

October 13 2006

A higher-than-expected percentage of Internet users are likely to fall victim to scam artists masquerading as trusted service providers, report researchers at the Indiana University School of Informatics.

"Designing Ethical Phishing Experiments: A study of (ROT13) rOnl query features," published online, simulated phishing tactics used to elicit online information from eBay customers. The online auction giant was selected because of its popularity among millions of users-and because it is one of the most popular targets of phishing scams.

The study, one of the first of its kind, reveals that phishers may be netting responses from as much as 14 percent of the targeted populations per attack, as opposed to 3 percent per year.

Phishers send e-mail to Internet users, spoofing legitimate and well-known enterprises such as eBay, financial institutions and even government agencies in an attempt to dupe people into surrendering private information. Users are asked to click on a link where they are taken to a site appearing to be legitimate. Once there, they are asked to correct or update personal information such as bank, credit card and Social Security accounts numbers.

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. Other

surveys may result in overestimates of the risks because of misunderstanding of what constitutes identity theft.

In contrast, experiments such as the one conducted by IU researchers Markus Jakobsson and Jacob Ratkiewicz have the advantage of reporting actual numbers.

"Our goal was to determine the success rates of different types of phishing attacks, not only the types used today, but those that don't yet occur in the wild, too," said Jakobsson, associate professor of Informatics. Jakobsson also is an associate director of the IU Center for Applied Cybersecurity Research, which studies and develops countermeasures to Internet fraud.

Ratkiewicz and Jakobsson devised simulated attacks where users received an e-mail appearing to be legitimate and providing a link to eBay. If recipients clicked on the link they were in fact sent to the eBay site, but the researchers received a message letting them know the recipient had logged in. The researchers specifically designed the study so that all they received was notification that a login occurred, not the login information (such as the recipient's eBay password) itself-unlike a real phishing attack, which is designed to harvest passwords and other personal information.

The study 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 experiment was unusual in that it did not involve debriefing of subjects, given that this step was judged to be the one and only aspect of the experiment that could potentially pose harm to subjects, who might be embarrassed over having been phished or wrongly conclude that sensitive information had been harvested by the researchers.

"We wanted to proceed ethically and yet obtain accurate results," said Ratkiewicz, a computer science doctoral student.

One experiment they devised was to launch a "spear phishing" attack in which a phisher sends a personalized message to a user who might actually welcome or expect the message. In this approach, the phisher gleans personal information readily available over the Internet and incorporates it in the attack, potentially making the attack more believable.

The researchers used three types of approach statements: "Hi can you ship packages with insurance for an extra fee? Thanks" … "HI CAN YOU DO OVERNIGHT SHIPPING? THANKS!" … and "Hi, how soon after payment do you ship? Thanks!" In a large portion of the messages, the user's eBay username was included in the message to make it appear more similar to those eBay itself would send.

"We think spear phishing attacks will become more prevalent as phishers are more able to harvest publicly available information to personalize each attack," Ratkiewicz said. "And there's good reason to believe that this kind of attack will be more dangerous than what we're seeing today."

Source: Indiana University