Profitable phishing schemes slyly tinker with our heads, then rip us off

January 22 2015, by Pat Donovan

Vishwanath is a professor of communication at the University at Buffalo. Credit: Credit: Douglas Levere

In the first study of its kind, researchers at the University at Buffalo have found evidence that the incredible spread of email phishing scams may be due to phishers' increased use of "information-rich" emails that alter recipients' cognitive processes in a way that facilitates their victimization.

The study, "Examining the impact of presence on individual phishing

victimization," was presented at the 48th Hawaii International Conference on System Sciences, held Jan. 5-8 at the University of Hawaii.

Arun Vishwanath, professor of communication at the University at Buffalo, and co-author of the study, says "information-rich" emails include graphics, logos and other brand markers that communicate authenticity.

"In addition," he says, "the text is carefully framed to sound personal, arrest attention and invoke fear. It often will include a deadline for response for which the recipient must use a link to a spoof 'response' website. Such sites, set up by the phisher, can install spyware that data mines the victim's computer for usernames, passwords, address books and credit card information.

"We found that these information-rich lures are successful because they are able to provoke in the victim a feeling of social presence, which is the sense that they are corresponding with a real person," Vishwanath says.

"'Presence' makes a message feel more personal, reduces distrust and also provokes heuristic processing, marked by less care in evaluating and responding to it," he says. "In these circumstances, we found that if the message asks for personal information, people are more likely to hand it over, often very quickly.

"In this study," he says, "such an information-rich phishing message triggered a victimization rate of 68 percent among participants.

"These are significant findings that indicate the importance of developing anti-phishing interventions that educate individuals about the threat posed by richness and presence cues in emails," he explains.

The study involved 125 undergraduate university students—a group often targeted by phishers—who were sent an experimental phishing email from a Gmail account prepared for use in the study. The message used a reply-to address and sender's address, both of which included the name of the university.

The email was framed to emphasize urgency and invoke fear. It said there was an error in the recipients' student email account settings that required them to use an enclosed link to access their account settings and resolve the problem. They had to do so within a short time period, they were told, otherwise they would no longer have access to the account. In a real phishing expedition, the enclosed link would take them to an outside account/phishing site that would collect the respondent's personal information.

Vishwanath says 49 participants replied to the phishing request immediately and another 36 replied after a reminder. The respondents then completed a five-point scale that measured their use of systemic (critical thinking) and heuristic information processing in deciding what to do with the email. When a few other variables were factored in, the phishing attack had an overall success rate of 68 percent.

"With email becoming the dominant way of communicating worldwide," Vishwanath says, "the phishing trend is expected to increase as technology becomes more advanced and phishers find new ways to appeal to their victims.

"While these criminals may not be easily stopped, understanding what makes us more susceptible to these attacks is a vital advancement in protecting Internet users worldwide."

Provided by University at Buffalo