Researchers fight phishing attacks with phishing tactics

October 2 2007

Early findings by Carnegie Mellon University researchers suggest that people who are suckered by a spoof email into visiting a counterfeit Web site are also people who are ready to learn their lesson about "phishing" attacks.

Phishing attacks have become a common method for stealing personal identification information, such as bank account numbers and passwords. Lorrie Cranor, associate research professor of computer science, said phishing often is successful because many people ignore educational materials that otherwise might help them recognize such frauds.

But in a laboratory study, the researchers fought "phire with phire" and found that when they sent their own spoof email to users and tricked them into visiting an educational Web site, those people tended to learn and retain more of the lesson about how to spot phishing sites.

Ponnurangam Kumaraguru, a graduate student in the School of Computer Science's Institute for Software Research, will present the study results Friday, Oct. 5 at the Anti-Phishing Working Group's (APWG) eCrime Researchers Summit in Pittsburgh. The summit, sponsored by the APWG and hosted by Carnegie Mellon CyLab, includes leading industrial and academic practitioners in the field of electronic crime research.

In the study, three groups of 14 volunteers participated in role-playing

exercises in which they processed email, which included a mix of phishing, spam and legitimate email. Those in the "embedded training" group, who were given anti-phishing educational materials after they had fallen for a phishing email, spent more than twice as much time studying the materials than those who were presented the materials without first being tricked. Those who were presented the materials without being tricked were no better at identifying phishing emails than those who received no anti-phishing educational materials. A week later, when the exercise was repeated, those in the embedded training group were significantly more successful in identifying phishing emails than those in the other two groups — 64 percent of phishing emails identified by the embedded training group versus 7 percent identified by the other two groups.

Cranor, director of the Carnegie Mellon Usable Privacy and Security Lab, said additional testing will be necessary to confirm these results. But the initial findings suggest that using the tricks of phishers, perhaps in a controlled environment, might be a good first step in educating computer users to protect themselves.

In addition to Cranor and Kumaraguru, the study team included faculty members Jason Hong and Alessandro Acquisti and graduate students Yong Rhee, Steve Sheng and Sharique Hasan. Their paper is available at www.ecrimeresearch.org/2007/pr … s/p70_kumaraguru.pdf .

According to the latest trend report for June, APWG detected 31,709 phishing Web sites, a drop of 6,000 from May, and 146 brands were hijacked, a slight decrease from May. But the number of unique phishing reports was 28,888 in June, up by more than 5,000 over May. The vast majority of attacks were in the financial services sector.

Source: Carnegie Mellon University