IU researchers warn of look-alike Web sites: HeraldTimesOnline.com  

IU researchers warn of look-alike Web sites

By Mercedes Rodriguez
August 4, 2008

INDIANA UNIVERSITY
IU researchers warn of look-alike Web sites

Lurking in inboxes all over the world are e-mails exhorting recipients to reactivate their suspended eBay or PayPal accounts — even though the recipient doesn’t have an account with either.

Chances are, those e-mails are part of phishing scams, ones that use convincing graphics and look-alike Web URLs to direct victims to unauthorized sites where crooks can gather their personal information.

Indiana University computer science researchers have completed a study indicating that hundreds of thousands of Web pages on some of the Web’s most popular sites are vulnerable to exploitation by phishing scammers.

Doctoral student Craig Shue, along with fellow doctoral student Andrew Kalafut and their adviser, assistant professor Minaxi Gupta, created software that allowed them to scan millions of Web sites for “open redirects,” a command that can send a user to a different page from the one clicked on. Sometimes, those redirects can be manipulated by scammers to surreptitiously send users to their own sites.

According to Shue, legitimate uses for redirects exist, for instance, when a Web site is easily misspelled.

Type www.googel.com into a Web browser and you’ll automatically be redirected to the correct site, www.google.com.

"When we came across what looked like redirects, most of them, about 81 percent, were not secure," said Shue.

That means those redirect commands were vulnerable to being hijacked to send users to the wrong Web site.

Hypothetically, "If I found a redirect on eBay’s Web site, I could set up a link that uses that eBay link to redirect to my own site," explained Shue.

Phishing scammers can send out e-mails containing Web addresses that look legitimate but actually redirect users to their own sites. Often, the phishers even copy the graphics from the real sites to fool victims further.

The study, which surveyed about 2.5 million sites and found more than 128,000 vulnerable redirects, began as a class assignment given by Gupta.

"We are excited at the prospect of making it into a company product. That would give us a lot of satisfaction because it is a real problem," Gupta said.

Gupta said it is not difficult for criminals to begin phishing schemes, as some of the tools necessary to pull off the several aspects of a scam are downloadable as phishing kits.

"Phishers don’t have to have any infrastructure, they don’t have to know any programming," she said.

Redirects to phishing Web sites are a problem for businesses. "They negatively impact their brand because they are allowing users to be defrauded through their site," said Shue.

The researchers’ findings were presented at the USENIX Workshop on Offensive Technologies in San Jose, Calif.

Story comments

Read all comments on this article (2) »

Post your comment:

Name to appear with this comment:

Your comment:

Some HTML allowed (Select the text and press button): bold italics hyperlink  
submit comment