How fake sites trick search engines to hit the top

December 8 2009, By JORDAN ROBERTSON , AP Technology Writer

Security researcher Jim Stickley displays logs on his laptop from Internet scams he created for a study for a California financial institution at his home in La Mesa, Calif., Monday Dec. 7, 2009. Stickley's study showed some of the most trusted Internet search engines gave high ratings to fraudulent web sites. (AP Photo/Lenny Ignelzi)

(AP) -- Even search engines can get suckered by Internet scams. With a little sleight of hand, con artists can dupe them into giving top billing to fraudulent Web sites that prey on consumers, making unwitting accomplices of companies such as Google, Yahoo and Microsoft.

Online charlatans typically try to lure people into giving away their personal or financial information by posing as legitimate companies in "phishing" e-mails or through messages in forums such as Twitter and

Facebook. But a new study by security researcher Jim Stickley shows how search engines also can turn into funnels for shady schemes.

Stickley created a Web site purporting to belong to the Credit Union of Southern California, a real business that agreed to be part of the experiment. He then used his knowledge of how search engines rank Web sites to achieve something that shocked him: His phony site got a No. 2 ranking on Yahoo Inc.'s search engine and landed in the top slot on Microsoft Corp.'s Bing, ahead of even the credit union's real site.

Google Inc., which handles two-thirds of U.S. search requests, didn't fall into Stickley's trap. His fake site never got higher than Google's sixth page of results, too far back to be seen by most people. The company also places a warning alongside sites that its system suspects might be malicious.

But even Google acknowledges it isn't foolproof.

Some recession-driven scams have been slipping into Google's search results, although that number is "very, very few," said Jason Morrison, a Google search quality engineer.

On one kind of fraudulent site, phony articles claim that participants can make thousands of dollars a month simply for posting links to certain Web sites. Often, the victims are asked to pay money for startup materials that never arrive, or bank account information is requested for payment purposes.

"As soon as we notice anything like it, we'll adapt, but it's kind of like a game of Whac-A-Mole," he said. "We can't remove every single scam from the Internet. It's just impossible."

In fact, Google said Tuesday it is suing a company for promising "work

at home" programs through Web sites that look legitimate and pretend to be affiliated with Google.

Stickley's site wasn't malicious, but easily could have been. In the year and a half it was up, the 10,568 visitors were automatically redirected to the real credit union, and likely never knew they had passed through a fraudulent site.

"When you're using search engines, you've got to be diligent," said Stickley, co-founder of TraceSecurity Inc. "You can't trust that just because it's No. 2 or No. 1 that it really is. A phone book is actually probably a safer bet than a search engine."

A Yahoo spokeswoman didn't respond to requests for comment. Microsoft said in a statement that Stickley's experiment showed that search results can be cluttered with junk, but the company insists Bing "is equipped to address" the problem. Stickley's link no longer appears in Bing.

To fool people into thinking they were following the right link, Stickley established a domain (creditunionofsc.org) that sounded plausible. (The credit union's real site is cusocal.org.) After that, Stickley's site wasn't designed with humans in mind; it was programmed to make the search engines believe they were scanning a legitimate site. Stickley said he pulled it off by having link after link inside the site to create the appearance of "depth," even though those links only led to the same picture of the credit union's front page.

The experiment convinced Credit Union of Southern California that it should protect itself by being more aggressive about buying domain names similar to its own. Domains generally cost a few hundred dollars to a few thousand dollars each - a pittance compared with a financial institution's potential liability or loss of goodwill if its customers are

ripped off by a fake site.

"The test was hugely successful," said Ray Rounds, the credit union's senior vice president of information services.

Stickley's manipulation illuminates the dark side of so-called search engine optimization. It's a legitimate tactic used by sites striving to boost their rankings - by designing them so search engines can capture information on them better.

But criminals can turn the tables to pump up fraudulent sites.

"You can do this on a very, very broad scale and have a ton of success," Stickley said. "This shows there's a major, major risk out there."

Robert Hansen, a Web security expert who wasn't involved in Stickley's research, said ranking high in search engine results gets easier as the topic gets more obscure. An extremely well-trafficked site such as Bank of America's would always outrank a phony one, he notes.

Still, Hansen said, criminals have been able to game Google's system well enough to carve out profitable niches. He says one trick is to hack into trusted sites, such as those run by universities, and stuff them with links to scam sites, which makes search engines interpret the fraudulent sites as legitimate.

"I don't think we're anywhere near winning" the fight against such frauds, said Hansen, chief executive of the SecTheory consulting firm.

Roger Thompson, chief research officer for AVG Technologies, who also wasn't involved in the research, said search results can be trusted, for the most part.

"But the rule is, if you're looking for something topical or newsworthy, you should be very cautious about clicking the link," he said. That's because criminals load their scam sites with hot topics in the news, to trap victims before the search engines have a chance to pull their sites out of the rankings.

"The bad guys don't have to get every search," he said. "They just have to get a percentage."

Consumers can protect themselves from scam sites by looking up the domain at http://www.whois.com , which details when a site was registered and by whom. That can be helpful if the Web address of a phony site is similar to the real one.