Fishing vs. phishing

by Onell R. Soto

Four years ago, Mouses Keshishyan sent dozens of unsolicited e-mails to America Online members telling them to verify their credit-card information on fake AOL Web sites he set up.

Then he had the information sent to his own e-mail box.

COMPUTER THIEVERY - 'Phishing,' where identity thieves fish for personal information by sending e-mail and creating bogus Web sites, has progressed to a multibillion-dollar problem for banks, online retailers and other companies. CNS Photo Illustration.It was a "state of the art" fraud for its time, an FBI agent said recently. And it led to a felony fraud conviction in August for Keshishyan, 22, who never used the purloined credit-card numbers.

But that type of scheme - known as "phishing" because identity thieves fish for personal information by sending e-mail and creating bogus Web sites - has progressed to a multibillion-dollar problem for banks, online retailers and other companies - $2 billion in 2006 by one estimate.

On Dec. 18, a San Diego federal judge fined Keshishyan $1,000 and ordered the California State University Los Angeles student to perform 240 hours of community service during a three-year probation term.

It was the first phishing-related prosecution anyone can think of in the area.

But it probably won't be the last.

Most people simply ignore or delete e-mails that ask them to go to Web sites and give personal information. But as many as 5 percent of those who get such e-mails are fooled, a study found.

Victims are vulnerable regardless of education, age, gender, previous experience or hours of computer use, according to another study.

ROGUE PROGRAMMERS

In October, the Anti-Phishing Working Group, a computer and financial industry alliance, found 37,444 new bogus Web sites - traps for unsuspecting computer users. A year earlier, it found 4,367.

Thieves have banded together and specialized, experts said.

Rogue programmers in the United States develop software that can set up the bogus Web sites, send realistic-looking e-mails and surreptitiously install programs that capture passwords.

Criminals in Eastern Europe, Asia or elsewhere use the software to deploy the Web sites, send out millions of e-mail messages and compile personal information in a few days, then deactivate the Web sites.

The information is sold to the highest bidder, and money launderers then post online job announcements to get unsuspecting people in the United States, where most of their targets are, to help them turn the credit-card numbers and other information into cash through bank transfers or by reshipping illicitly purchased goods.

As the criminals have gotten more sophisticated, law enforcement is fighting back, though with limited success.

"Many of the people that are behind phishing are overseas, which makes it dramatically difficult," said Mitch Dembin, a San Diego-based federal prosecutor and a national expert on computer crime.

He said charges are filed "whenever we can find someone in the United States that did it."

The criminals are adept at hiding their locations, often using computers they control from far away, and that makes for long hours for detectives.

"It's not as easy at it seems on CSI," Dembin said.

Keshishyan's Web sites were investigated by a San Diego cybercrime squad with FBI agents who work with industry experts to identify criminals. The squad continues to work on phishing cases, though agents won't talk about those investigations.

IDENTIFYING CRIMINALS

Agents have hooked up with a San Diego company called Secure Science Corp. to find out who's behind phishing attacks.

The company monitors Internet communications among identity thieves and has identified more than 55 groups that plot phishing crime, said Lance James, a co-founder and chief technology officer of Secure Science Corp.

The biggest threat comes from small programs called spyware that can secretly record what computer users type and send the information to the thieves. The programs are often installed when people visit Web sites from links in e-mails they receive, James said.

He said his company in 2006 recovered 5 million to 6 million stolen credit-card numbers from the thieves by gaining entry into the computers the thieves set up to collect the information.

He said his company helps identify groups for law enforcement agents to investigate.

James said his company often notifies banks before customers realize there are problems.

"A lot of it is old-fashioned detective work," he said.

INTERNATIONAL EFFORT

Federal authorities are uniquely suited to investigate such crimes because of the interstate and international connections, James said.

Indeed, the FBI is working with agencies in other countries, said San Diego office spokesman Darrell Foxworth.

U.S. officials are working with other countries to bring criminals to the United States to face charges or have them prosecuted overseas, said Dembin, the federal prosecutor.

"We've had to redo all of our extradition treaties," he said.

But prosecutions will remain a rarity, said Jay Foley, executive director of the San Diego-based Identity Theft Resource Center.

Phishing criminals move too fast for law enforcement, and it's up to the financial industry to tell people they won't be asked for personal information through e-mail, he said.

"It's a case of chasing smoke and mirrors," Foley said, noting how a scammer with a laptop can set up shop for a few days using a public connection, then disappear.

"Law enforcement will not be the answer to this, unfortunately, as much as I would like them to be," he said. "We can't expect them to do the impossible."

As for Keshishyan, the UCLA student "just succumbed to his own abilities and a little bit of greed," Dembin said.

"He's appeared to have turned his life around dramatically," the prosecutor said. "He's a very good student, but he will have to deal with a felony for the rest of his life."

Defense lawyer Mark Bledstein said Keshishyan was remorseful for his crime. Bledstein wouldn't comment further.

Fishing vs. phishing by Onell R. Soto