Anti-phishing 'posses' hunt criminals

October 5 2005

California Gov. Arnold Schwarzenegger last Friday signed into law the first state legislation that penalizes fraudsters who steal online identities through "phishing" scams, but Internet companies and banks are not waiting for the law to stop the cyber-criminals and are actively taking covert measures to protect their customers, experts tell UPI's The Web.

"We generally find that law enforcement is so involved with other issues that phishing is low on their priority list," said Hugh Hyndman, chief operating officer of Toronto-based Brand Dimensions, an online brand consulting company, in an interview with The Web.

So private-sector companies are setting up private posses to chase down the cyber thieves. They are working with Internet service providers, Web-hosting services and even regional Internet authorities to alert them when a phishing phenomenon is discerned online -- when thousands of suspicious e-mails are sent from a site purporting to be a U.S. credit union but that originate in the Far East. They track down the very server that the fraudulent e-mail is coming from -- by its IP, or Internet Protocol address, and then work with established contacts to shut down the site and take it offline as soon as possible.

Phishing -- a form of online identity theft -- is on the rise. Organized criminals are attempting to steal personal financial data, like credit-card numbers, account usernames, passwords and Social Security numbers. They do this by setting up fake Web sites -- and sending out fraudulent e-mail to get Netsurfers to go to the Web site. A report from the Anti-Phishing Working Group indicates that, as of March of this year, there

were 2,870 active phishing sites around the world. That number had grown by 28 percent during the previous nine months. About 31 percent of those sites have a URL similar to the name of their target institution -- so as to dupe clients. The average fraudulent site is online for only 5.8 days -- making fast action against the fraudsters imperative.

"We attempt to black hole the site," said Hyndman. "We've cultivated relationships with ISPs around the world. We have a great Rolodex. They know us personally. We have the home numbers in China of many leading Internet people. They don't want to be a country that houses criminals. They put a lot of effort into it."

Larger banks and financial institutions -- Fortune 500 firms -- have had IT staff dedicated to this kind of thing in the past. But now, smaller financial institutions, credit unions, regional and local banks can use the consulting services to stop the criminals before they cause too much damage.

The counter-phishing system documents the process by which the phishers attack. Then it identifies and verifies where the attacks are coming from, and then takes down the servers. Information on the phishers is retained -- so as to spot their patterns in the future.

What's more, the counter-phishing sites are conducting what amounts to counter-intelligence against the phishers.

"We're monitoring what the criminals do with the information they obtain -- so we're setting up fake account names," said Kevin Prince, president of Red Cliff Solutions Inc., a Salt Lake City, Utah-based Internet security company, in an interview with The Web. "We then work with the banks to monitor these red-flagged credit cards and other accounts. Then we work with law enforcement to arrest the person."

The cost of buying a stolen identity is about $10 on the black market today. The price used to be $50. The false bank accounts provided by the anti-phishing experts "spoil the databases" of the criminals and make reselling the stolen names impossible, ruining the credibility of the criminals amongst their colleagues, said Prince.