



Phishing On the Rise

As many as 12% of consumers are fooled by these scams

By *The Point Staff*
December 29, 2005

Phishing On the Rise

As many as 12% of consumers are fooled by these scams

Phishing has become an increasingly widespread and costly type of computer intrusion, according to a recent Financial Crimes Enforcement Network (Fincen) report. In its SAR Activity Review, the agency said reported intrusions were on the rise and that phishing was the "most pervasive and most effective manner" used to illegally access a financial institution's computer systems.

Phishing also has become more expensive. Between 2000 and 2003 most institutions that reported such an intrusion said it did not result in any financial losses. "In the fourth quarter of 2003 and throughout the first two quarters of 2005, however, filers indicated violation amounts within a range of \$1 to \$9,999 more commonly than violation amounts equal to zero," the report said. "This clearly indicates an emerging trend in actual losses reported by financial institutions."

Phishers send phony e-mails disguised as legitimate communications from financial institutions or other organizations to gain access to sensitive information that can then be used to draw funds from a consumer's account.

Though phishing falls into a broader fraud category known as "spoofing," the practice "should be a larger cause of concern because it occurs with far more frequency than instances of direct attacks on financial institution-hosted servers," the report said.

It cited industry estimates that as many as 20 out of 1,000 recipients of a phisher's e-mail will respond. However, Fincen also noted that other experts said the ratio "may be closer to 1 in 8."

Policymakers continue to focus on breaches at third parties like processors, but filings describing such an event have "disappeared during the last eight quarters," the agency said. By contrast, in 2001 and 2002, such intrusions were the ones most commonly reported by financial institutions. Consumers' hunger for online services plays into the hands of fraudsters, the report concluded. "Evidence suggested financial institution customers are increasingly seeking online services, but this need to be 'connected' may expose customers to scam artists seeking account information."

Phishing also appears to be a problem financial institutions have difficulty fighting. The report recounted an unspecified institution that detected a bogus Web site designed to look like its own. When contacted by the financial institution, the site's owner "refused to disable the site and threatened a civil suit if the institution contacted him again."

Financial institutions have also suffered through other kinds of attacks. The report cited another institution where an "angry customer engaged in a campaign of targeted spam on the institution's customer-support mailbox."

"Apparently, the customer was angry over a failed transaction, which he claimed lost him considerable amounts of money," Fincen reports. "In addition to threats and libel in the e-mails, the filer reported the e-mail attack rendered the institution's exchange server useless for 24 hours."

In the five-year period that ended June 30, financial institutions filed 3,726 suspicious-activity reports identifying phishing and other computer intrusions. The filing rate increased dramatically in 2003 and 2004, when nearly 70% of the reports were filed. Though the filing rate for computer intrusions has dropped off slightly in the first half of this year, the agency concluded that "growth is still the prevailing trend."

Attempts to hack directly into a financial institution's computer systems have largely been unsuccessful, according to Fincen. During the two-year period that ended June 30, there were five filings that indicated hacking attempts, none of which worked.

"Nothing in the last eight quarters indicated institution-hosted servers were particularly vulnerable to hacking attempts," the report said.

SIDEBAR

UW CU Beefs Up Anti-Phishing Measures

University of Wisconsin Credit Union in Madison has become the first customer to test Corillian Corp.'s second anti-fraud product.

Corillian's Intelligent Authentication software evaluates members' online habits, including the hardware they use to access a Web site, how they access the Internet, their location, and the time of day they tend to conduct their online banking. Such patterns "are very typical and predictable," Eric Bangerter, the credit union's director of Internet services told the *American Banker* newspaper. The credit union tried to develop a similar tool on its own but gave up last year because it could not devote the resources to it, Bangerter said.

The credit union is testing the software and expects to incorporate it into its logon next month.

Jim Maloney, the chief security executive at the Hillsboro, Ore., banking technology vendor, said the software works by keeping a file of the last 50 "access signatures" for each member, detailing how and when they used the credit union's online banking site. When members try to log in, the software will permit them to access the site immediately if their usage patterns match previous habits. If someone's login attempt does not match the attempts on file, Intelligent Authentication will ask the member doing the login a series of questions.

Maloney said the data the software collects is "the same information that ends up in the Web log" of visitor data that many companies already store. UW Credit Union also uses Corillian's consumer online banking software, and Bangerter said he plans to buy Corillian Fraud Detection System, which was introduced in July 2004.

Corillian Fraud Detection examines the Web logs of visitors to a Web site to determine if any visitors may have been using the site to create a counterfeit site that could be used for phishing. Maloney said criminals who visit financial institution sites to duplicate them for phishing scams have distinctive patterns. They use the fake sites to trick people into revealing personal information that could be used for identity theft.

Maloney said companies can use Corillian's anti-fraud products even if they do not use its online banking software. Corillian's two anti-fraud products complement each other, Maloney said. "From CFDS, we have lists of PCs and IP addresses that correspond to phishers," he said. Some countries are known phishing havens, and "we can say 'always block' or 'always challenge'" them.

About the Author

The Point Staff

thepoint@cuna.com

This article has been provided to you by *The Point for Credit Union Research & Advice*. If you would like to see more articles related to this topic or other information, visit thepoint.cuna.org for a FREE 30 day trial subscription to *The Point*.