

# Phishing attacks slam midmarket

By Shamus McGillicuddy, News Writer

**P**hishing attacks are moving downstream to the midmarket, forcing CIOs to take steps to protect their companies' brands.

"Certainly the criminals have moved downstream to smaller financial institutions," said Avivah Litan, a vice president and research director at Gartner Inc. in Stamford, Conn. "That's been the trend for well over a year, because the larger banks have employed services to take these phishing command and control services down. So criminals would rather use brands that are not going to go after them. It's easier to attack smaller banks that haven't geared up to protect themselves. They can go undetected. And as soon as they are detected, these smaller banks are caught off guard."

Litan said PayPal and larger banks are still the more frequent targets, but smaller financial institutions need to be prepared.

In its quarterly Brandjacking Index, which tracks online brand hijacking, phishing and other criminal attacks, online reputation protector MarkMonitor Inc. reported that 32.6% of all phishing attacks detected in the third quarter of 2007 were targeted at credit unions. Such financial institutions are traditionally smaller, with limited resources for dealing with such attacks.

Frederick Felman, chief marketing officer at San Francisco-based MarkMonitor, said medium-sized companies that get phished for the first time can see a profound effect on their businesses. The customer service and public relations efforts required to remediate an attack can be overwhelming, not to mention the sales that can be lost due to the reputation hit.

"Smaller brands are being phished," Felman said. "Over the last two or three years we've seen pockets of attacks on smaller players, attacks on credit unions and small online retailers."

"It's definitely not just a risk for the nation's and the world's largest financial

institutions. It's definitely a risk for smaller organizations."

Carolyn James, senior vice president and CIO of USA Federal Credit Union, a 225-person, \$700 million credit union based in San Diego that has historically served members of the U.S. armed forces, said her institution has been targeted by phishing attacks twice during the past year or so.

"We've had some phishing attacks that specifically spoofed our Web site," James said. "It was before we were doing multi-factor authentication. They were taking advantage of that, to get people to put their usernames and passwords into a Web site. We shut them down."

James said she became aware of the first phishing attack when MarkMonitor warned her company about it. She was not yet a MarkMonitor customer, but the company contacted her to tell her it had detected the attack.

"The first time we were phished we weren't a MarkMonitor client," she said. "We had to do a takedown ourselves. It took a day. The second time, MarkMonitor took down the site within 45 minutes."

James said protecting yourself from phishing attacks is a cultural issue to some extent. When she joined her credit union two and a half years ago, her organization had too many silos separating IT from the business. Many business units had online relationships with partners that IT had no knowledge of.

Through persistence and constant communication, James has gained more control over those relationships, especially those where credit union membership information is exchanged with partners. A breach of such information, such as a list of email addresses, could make customers vulnerable to phishing attacks.

"When you're in the contract review process, information services has to be included in the list of people who review

new vendors when we are going to exchange member information," she said. "We need some influence on that."

James said that in the online reputation world, she considers the CIO a chief information gatherer.

"I read online journals, attend webinars and conferences and talk to peers to learn about new vulnerabilities," she said. "Along with my team, we identify new solutions. I would not likely be able to afford some of the solutions that Bank of America or Wells Fargo would. But MarkMonitor is unique in that it is priced so that I can do what the big guys do."

Litan said smaller organizations should have a contract with a phishing site takedown service like MarkMonitor. While larger organizations that get targeted by phishing attacks daily will have large contracts for constant protection, smaller organizations can engage with a service provider for a standby service. In a standby mode, the service provider would be positioned to kick into gear quickly when a phishing attack takes place.

"These smaller banks get caught off guard," Litan said. "They have to sign up for a service to take on these phishers. They can't do it quickly. They have to sign a contract. It can take days. But some vendors will do the takedown right away if an agreement in principal is in place."

Litan said phishing attacks are further evolving, moving away from specific brands.

"They're being more generic so there's nobody going after them," she said. "When there's no brand involved, no one is going to spend the money to get rid of the phish. In the greeting card industry, one of the leading greeting card companies took one for the whole industry. So even though the phishers were using nonbrands, one big company thought it was damaging the industry's name. So they spent the money to take down the phishing attacks."

Reprinted with permission from SearchCIO-Midmarket.com, January 9, 2008.  
All Rights Reserved. FosteReprints: 1-866-879-9144