Feds bolstering online banking security

October 19 2005

Federal banking regulators are ordering financial institutions to bolster their Internet security by the end of next year, hoping to halt identity theft. But experts tell UPI's The Web that the measures still may not be strong enough, and may, in the words of Mark D. Rasch, senior vice president and chief security counsel of Solutionary Inc., a Bethesda, Md.-based IT developer, inspire "false confidence" among consumers.

The Federal Financial Institutions Examination Council sent a letter last week to U.S. banks indicating that it was no longer permitted for banks to allow access to online banking accounts with just one form of technology authentication -- a PIN number or a password -- because hackers are too savvy to be stopped by such trifling security.

In its letter the council noted, "Single-factor authentication as the only control mechanism is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."

The government wants banks and other financial institutions to provide two or more forms of online authentication for customers. This may include technology that creates distinct passwords every time one tries to log into an account, as well as fingerprint and handwriting analysis.

This is the approach that has been taking by some financial institutions already. "E*Trade Financial was the first financial services firm in the United States to offer two-factor authentication via a token to its retail customers, earlier this year," a spokeswoman for E*Trade, Tina

Martineau, based in suburban Boston, told The Web. "The security program is voluntary and more than 20,000 tokens have been distributed to date."

Experts noted that multifactor authentication might increase the amount of customers who conduct banking services online, for about 26 percent of bank customers refuse to use the Internet due to safety concerns today. "Many banks and financial institutions have been moving in the direction of strong or multifactor authentication to secure their environment and protect their user community," said Chris Dircks, a principal consultant at the PA Consulting Group, an international IT firm. "Those organizations slow to adopt these technologies will continue to be a target of fraud technologies that are virtually eliminated by multifactor authentication -- phishing, pharming, keylogging."

Dircks said tokens are an interesting technology. They are similar to smart cards in that they store information about one's identity digitally and can be used on laptops or regular PCs. But other technologies are emerging that may be even more effective in the future. "Advances in biometrics continue to make that technology a more plausible and reliable solution," said Dircks. "Many hardware manufacturers provide biometric support technologies in their production systems, and, when combined with a PIN, allow an organization to comply with multifactor authentication with little or no hardware deployment to its user community."

One factor that the government cannot regulate easily, however, is the banking customer, experts said. Hackers will now target these customers directly -- and become more innovative in doing so -- if IT security is increased. "The customer has always been the weakest link," said Sachin Varghese, a computer-security specialist at Paladion Networks, based in suburban Washington, D.C.

A number of IT players will benefit from the ruling, Varghese told The Web, including RSA, VeriSign, Fortress Technologies, Symantec and Biolink. "Federal regulators will have taken a giant step in the right direction," Varghese said.

But some experts are still skeptical and think the regulations simply cannot stop the inevitable -- depraved criminals coming for your money.

"When the Big Kahuna hits online banking, Katrina, Rita, northeast floods and 9/11 will look like mosquito bites by comparison," said Art Gillis, a banking-technology consultant at Computer Based Solutions Inc. in Dallas. "And bank regulatory agencies will act like the FBI, CIA and FEMA. They did their best, but it was the other guy's fault. There is no absolute protection against cyberspace crime because as in the law of physics, for every action there is an equal and opposite reaction."