The growing threat of spyware

July 27 2005

The Federal Deposit Insurance Corporation -- the New Deal-era government agency designed to restore confidence in the Great Depression-shattered banking system of the United States -- is now providing guidance to banks to protect themselves and their customers from spyware, the latest threat to the integrity of the banks, experts told UPI's The Web.

Millions of Americans, banking at institutions such as Wachovia and Bank of America, have had their private financial information stolen by hackers through spy software, downloaded unknowingly from the Internet.

"The information collected through spyware can be used to compromise a bank's systems or conduct identity theft," said Michael J.Zamorski, director of the FDIC's division of supervision and consumer protection in Washington. "So it is critical that banks stay vigilant about the risks involved with this malicious software, and take appropriate action so that they and their customers do not fall victim to it."

The FDIC recommends that banks consider threats from spyware as part of their risk-assessment process. They should bolster Internet security and enhance employee training to understand the machinations of hackers. Experts had a mixed reaction to the FDIC's plans. Terry Brown, chief executive officer of Caymas Systems in Petaluma, Calif., a network-security firm, said the government's recommendations do not go far enough and will not "significantly alter" the risks that consumers face.That is because a May 2005 study by the software lab at Carnegie

Mellon University in Pittsburgh -- financed by the science and technology directorate of the Department of Homeland Security -- found that the greatest risk to banks comes from insiders, and 49 percent of all network security breaches can be linked to employees, former employees, contractors and temporary workers. Still, the risk from spyware itself is significant, because 90 percent of spyware traversing the Internet is written for criminal purposes, according to Kaspersky Lab, an international anti-virus developer with an office in Woburn, Mass. "An entire industry exploded in 2004 as virus writers and hackers became increasingly involved with criminals to create malicious code," said Steve Orenberg, Kaspersky Lab's president.

The FDIC's guidance to banks may just be the first step by the government to protect consumers against hackers from Russia and China. Orenberg said some forms of e-mail advertising -- the lure that hackers use to plant spyware in PCs -- may be banned in the United States. Similar legislation may be introduced in Europe and other industrialized countries, he added.Another step may be mandating multi-layered authentication -- passwords -- for online banking accounts. "We believe the guidance regarding the bank's own infrastructure makes sense, since the bank can enforce it, but the guidance regarding consumers is naïve," said Naftali Bennett, chief executive officer of Cyota Inc.in New York City, an anti-fraud software developer for banks. "Banks cannot expect or enforce customers to keep spyware out of their computers, but banks can take steps to minimize or eliminate the damage that spyware causes."

Banking from public terminals, such as at colleges, libraries and Internet coffee shops, are a major problem, as most of those computers may be already infested with spyware, said Robert Siciliano, an ID-theft expert in Boston. Bennett suggested that banks begin to track and monitor all of the online transactions of their customers, from login to logout, to discern suspicious patterns. "Only by analyzing all transactions, invisibly

and in real-time, and invoking stronger authentication at the first sign of potential fraud, will banks be able to reduce the damage of spyware and Trojans," Bennett said.

Another potential solution is "smart cards," which can be created to contain a number of one-time-use passwords. Once employed, they are not usable again.Unless banks implement such solutions, they might have to give up e-mail marketing altogether and, like eBay, reduce or eliminate the use of e-mail ads, experts said.