

Special Alerts

SA-183-2009
October 27, 2009

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Fraudulent E-Mails Claiming to Be From the FDIC
Summary: *E-mails fraudulently claiming to be from the FDIC are attempting to trick recipients into installing unknown software on personal computers. These e-mails falsely indicate that recipients should download and open a "personal FDIC insurance file" to check their deposit insurance coverage. The "insurance file" may actually be a form of spyware or malicious code and may collect personal or confidential information.*

The Federal Deposit Insurance Corporation (FDIC) has become aware of e-mails appearing to be sent from the FDIC that are asking recipients to download and open a "personal FDIC insurance file" to check their deposit insurance coverage. These e-mails are fraudulent and were not sent by the FDIC. The FDIC is attempting to identify the source of the e-mails and disrupt the transmission.

Currently, the subject line of the fraudulent e-mails includes the wording "check your Bank Deposit Insurance Coverage." The e-mails state: "You have received this message because you are a holder of a FDIC-insured bank account. Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets."

The e-mails ask recipients to "visit the official FDIC website" by clicking on a hyperlink provided, which appears to be related to the FDIC and directs recipients to a fraudulent Web site. The Web site includes hyperlinks that appear to open forms. However, it is believed that clicking on the hyperlinks will cause an unknown executable file to be downloaded. While the FDIC is working with the United States Computer Emergency Readiness Team (US-CERT) to determine the exact effects of the executable file, recipients should consider the intent of the software as a malicious attempt to collect personal or confidential information, some of which may be used to gain unauthorized access to online banking services or to conduct identity theft. Financial institutions and consumers should NOT access the Web site or download the executable files provided on the Web site.

Information about counterfeit items, cyber-fraud incidents and other fraudulent activity may be forwarded to the FDIC's Cyber-Fraud and Financial Crimes Section, 550 17th Street, N.W., Room F-3054, Washington, D.C. 20429, or transmitted electronically to alert@fdic.gov. Information related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at <http://www2.fdic.gov/starsmail/index.asp>.

For your reference, FDIC Special Alerts may be accessed from the FDIC's website at www.fdic.gov/news/news/SpecialAlert/2009/index.html. To learn how to automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Director
Division of Supervision and Consumer Protection

Distribution: All FDIC-Insured Institutions

Note: Paper copies of FDIC Special Alerts may be obtained through the FDIC's Public Information Center, 1-877-275-3342 or 703-562-2200.