

In a continued effort to alert and educate our customers regarding identity theft schemes, we will post special alerts on the homepage of our website as they become available. The FDIC has recently made us aware of a new “scheme”. Please read the alert below. If you have any questions or concerns, please do not hesitate to contact us.

SPECIAL ALERT

SUBJECT: Fraudulent E-Mail Claims 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 install software that was developed by the FDIC and other agencies. The software may be a form of spyware or malicious code and may collect personal or confidential information.*

The Federal Deposit Insurance Corporation (FDIC) is aware of e-mails appearing to be sent from the FDIC that are asking recipients to install unknown software on personal computers. Currently, the subject line of the e-mail includes the phrase “Urgent Notification - Security Reminder.” The e-mail is fraudulent and was not sent by the FDIC.

The fraudulent e-mail describes “a small client utility”—referred to as “ProBank”—that recipients are asked to install on home and business computers. The e-mail claims: “...this utility only starts whenever an online session is opened with a Financial Institution insured by the FDIC, thus it will never interfere with any programs installed on your computer. Please help us combat fraud by installing, ProBank on any computer that is used to open an Online Banking session.”

The e-mail requests that recipients click on a hyperlink that appears to be related to the FDIC, which directs recipients to 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 on-line banking services or to conduct identity theft.

Consumers should NOT access the link or download the executable file provided within the body of the e-mail.

The FDIC is attempting to identify the source of the e-mails and disrupt the transmission. Until this is achieved, consumers are asked to report any similar attempts to obtain this information to the FDIC by sending information to alert@fdic.gov.

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-4004, 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>.

The Bank of New Madrid will never contact you by e-mail, by phone, or by mail requesting your personal information. Before you ever give out any of your personal information, verify it is a legitimate organization or person you are speaking with.

For more information regarding identity theft, and other fraudulent schemes, please click on the Consumer Education link found on this website.