



For Immediate Release
February 22, 2005

District Attorney Nola Foulston reminds everyone to be wary of any solicitation, by e-mail or other means, requesting consumers provide bank account or other financial information.

The District Attorney has learned of an E-mail solicitation sent to consumers in the Wichita area from "Regions NET Online Banking." The E-mail is addressed, "Dear Client of the Regions Bank." It continues stating the technical services of the bank are carrying out a planned software upgrade and asks the reader to visit a link to start the procedure of confirming the customer's data. Once logged on to the link, one is requested to type in a first and last name, ATM/Debit Card, PIN, Expiration Date, Login ID, Password, and E-mail Address. This is a scam. It is not a legitimate communication from Regions Bank. If you receive one of these E-mails, Regions Bank is requesting that you forward it to phishing@regions.com

This E-mail differs from that which one would use if you were accessing your own account. In this scam using the Regions Bank name, the communication **is sent to you**. When you access your own banking information on-line, **you are the one sending the E-mail and accessing a secure site**. In other words, you are not solicited by your own bank using an E-mail.

This is a tactic used by criminals called "Phishing", because the tactic is similar to a fisherman casting bait into a pond hoping to deceive and catch a fish. Criminals are hoping local consumers will "take the bait" and provide the information so the criminals can access the bank account or fraudulently use the credit card of the unsuspecting consumer. **Legitimate financial institutions do not solicit customer account information from their customers.**

In the event you receive such a solicitation, **do not provide the information**. If you receive a request for information you believe may be legitimate, contact your financial institution before filling out forms or providing information. Often the financial institutions who are the subject of such attacks have warnings posted on their website outlining the known scams and providing details about the various techniques.

If any consumer has been the victim of such a scheme, please report the event to the Internet Fraud Complaint Center at <http://www.ifccfbi.gov/cf1.asp>

For more information, contact Sharon Werner, Chief Attorney, Consumer Fraud and Economic Crime Division, at 383-7921.

*Nola Tedesco Foulston
District Attorney*