



Louisiana Credit Union League
SCAM ALERT

Monday, September 14, 2009

Contact: Lacey Hyer, Public Relations Specialist
Louisiana Credit Union League • lhier@lcul.com • 1.800.452.7221, ext. 3100

Phishing Attacks Reported by Two Louisiana Credit Unions

Homeland FCU and Jefferson Parish Employees FCU are the latest targets of recent phishing attacks. Both members and non-members are receiving text messages informing them that their accounts have been closed, are negative, or are having suspicious activity. Recipients of the text messages are being asked to call a toll free number or visit a website in order to check the status of their account. These calls are not coming from a legitimate source and individuals should be reminded to never provide their personal private information.

Please remember that your members could potentially be contacted even though they are not a member of one of these credit unions. There have been cases where non-members were receiving the same text messages and phone calls. In one instance, a member from one credit union received a text on behalf of another. Criminals do not discriminate against credit card numbers from different financial institutions than the one they are "targeting." If the phone call references a specific credit union or bank and you enter a credit card number for another institution, your account can still be compromised.

Please be sure that you encourage everyone that receives one of these text messages and/or calls to report it to the FTC at 877-382-4357. The phone number that the call or text message is coming from is NOT important. The phone number they should report is the number they are being asked to call. Informing the FTC that there is a fraudulent 800 number activated will encourage the FTC to disconnect the number.

Additionally, please use this as a reminder to educate your members on the many scams out there, especially during hurricane season and the upcoming holiday season. Remember to review your own credit union's policies and procedures on a regular basis and make sure your staff is informed of the proper verification procedures for all transactions.