

Consumer **ALERT**



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

Spoof Credit Union E-mails Could Ruin Consumers' Holidays

A new, dangerous identity theft scheme is targeting credit union customers across the country. According to consumer and credit union groups, spoof e-mails are directing credit union customers to call a telephone number and confirm their personal information. Consumers who make the call do not reach their credit union, but instead end up on the telephone with a scam artist who wants to steal their identity.

Savvy consumers have increasingly learned to identify and delete spoof e-mails that falsely appear to originate from legitimate banks or credit card companies. Known as “phishing,” these e-mails direct consumers to a decoy Web site that allows the scammers to collect all the information they need to empty the customers’ bank accounts and ruin their credit.

“Phishing” scams have been around for years, but increasingly sophisticated criminals now send e-mails instructing consumers to call a telephone number instead of clicking on a link. This tactic, known as “vishing,” can be especially effective because consumers who encounter a live person are much more likely to let down their guard.

The latest “vishing” scam immediately disarms consumers by specifically warning about similar schemes. One recently circulated e-mail reads:

Dear Credit Union Customer,

We regret to inform you that we have received numerous fraudulent emails which ask for personal account information. The emails contained links to fraudulent pages that looked legit. Please remember that we will never ask for personal account information via email or web pages.

Because of this we are launching a new security system to make Credit Union accounts more secure and safe. To take advantage [sic] of our new consumer Identity Theft Protection Program we had to deactivate access to your card account.

**WRITE TO: Greg Abbott, Office of the Attorney General, PO Box 12548,
Austin, TX 78711-2548 • (800) 252-8011 • www.oag.state.tx.us**

To activate it please call us immediately.

The e-mail provides a telephone number with a U.S. area code, adding to its air of legitimacy. In an especially brazen move, the e-mail offers identity theft tips and links to the Federal Trade Commission's identity theft prevention Web site. Consumers who think the e-mail is legitimate call the number and furnish sensitive information to a person they believe is a trusted credit union employee. Only when their identity is stolen do they realize it was all a scam.

These "vishing" scams combine the "phishing" ploy with a Web-based telephone scheme. The telephone numbers that appear in these e-mails are set up through VoIP, which is an Internet-based telecommunications service. Even though the phone number appears to be based in a familiar U.S. area code, the scammers are most likely in other countries and impossible to track down.

Consumers who receive this or any other unexpected e-mail or phone call seeking personal information should not respond. Consumers who have concerns about their account should contact their credit union by calling the telephone number that appears in the local directory or on their periodic statements. Never click on a link or call a telephone number that appears in an unexpected e-mail.

Sincerely,

A handwritten signature in black ink that reads "Greg Abbott". The signature is written in a cursive, flowing style.

Greg Abbott
Attorney General of Texas

**WRITE TO: Greg Abbott, Office of the Attorney General, PO Box 12548,
Austin, TX 78711-2548 • (800) 252-8011 • www.oag.state.tx.us**