

PHISHING, VISHING AND NOW 'SMISHING'

EUGENE, Ore. (4/22/08)--A type of fraud that scammers are using called "**smishing**" is gaining prominence as a way to fraudulently obtain consumers' personal information.

Smishing is text-message fraud that occurs when criminals, posing as financial institutions, attempt to dupe mobile-phone users into sending personal information through text messages.

Oregon Community CU (OCCU), a \$388 million asset, Eugene, Ore.-based institution, is under attack from fraudsters sending cell phone text messages that state "Your Oregon Community CU account is closed due to unusual activity." The message then requests that recipients call a phone number in Florida.

Recipients should not reply by texting, nor respond to the phone number listed.

OCCU said it has received thousands of phone calls from worried people, not just members. Since the credit union is the largest in the area, scammers probably sent the text message to the entire list of Oregon phone numbers hoping to trick as many members as possible to fall for it.

Source: Credit Union National Association (CUNA).

Protect Yourself

As a reminder, JDCU and other **legitimate** companies and financial institutions, **DO NOT ask for this information via email, phone or text-messaging**. If you are concerned about your account, contact the organization using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address.

If you believe you're a victim of a "Phishing", "Pharming", or "Smishing" scam, file a complaint with the Federal Trade Commission (FTC) at www.ftc.gov. Visit the FTC Web site at www.consumer.gov/idtheft to learn more about how you can protect yourself and visit our "[your privacy & security page](#)" for more information and resources.