

## PREVENTING FRAUD: INTERNET SCAMS

### Recent Increase in Phishing Scams

**Keeping our Client's personal information secure and confidential is one of First Community Bank's highest priorities. Below are some of the most common types of Internet and Phone scams, along with suggestions on how you can be aware and help protect yourself against Identity Theft.**

Reports of increased Phishing, Vishing, and "SMS"ishing:

Using these techniques fraudsters pose as legitimate businesses and contact cardholders via email, voicemail, text to cell, or other wireless device. The fraudsters request a cardholder to key in their sixteen (16) digit card number, PIN and CV2 value (or similar combination of data).

In the latest cases they are **spoofing** legitimate merchant phone numbers, unlike some incidents in the past that we have seen where they set up a specific toll free number that could then be shut down. Spoofing is a way that the fraudster can arrange for the bank's phone number to show up on caller id through illegal sources and attempt to trick the intended victim out of confidential information. Never give any confidential information over the phone unless you originated the call and you know your local bank's number. **Do not return a call to an 800 # given by the solicitor on the phone.**

**First Community Bank will not send out these types of messages. If you ever receive this type of message with First Community Bank's name, please call our Information Security Officer at (707)636-9007.**

Pop-Up Advertisements:

Some advertisements "pop up" in a separate browser window advising you that you have won a contest and request that you participate in a survey to collect a prize. They may then ask that you provide personal information in order to receive your gift. By clicking on the link it is possible that you are also downloading viruses designed to capture or destroy information on your computer.

What Can You Do?

**Never** respond to emails that cannot be verified.

**Never** respond to personal information via e-mail

Contact the business by **using legitimate phone numbers to verify the request**

Enter websites **using your browser and not by clicking on provided links.**

**Be cautious** of any solicitations **requesting that you deposit a check or pay a fee to collect a prize**

**PLEASE REPORT ANY SUSPICIOUS EMAILS OR CONTACTS THAT ARE USING FIRST COMMUNITY BANK'S NAME DIRECTLY TO: [SecurityOfficer@FCBconnect.com](mailto:SecurityOfficer@FCBconnect.com)**