

## Preventing Fraud: Internet 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 scams and suggestions on how you can be aware and help protect yourself against identity theft.

### Phishing and Spoofing

This is when a criminal will send you a phony message or a website link that appears to be from a legitimate business. They will directly request that you provide personal financial information, such as:

- **Name and address**
- **Social Security Numbers**
- **Credit card numbers / bank account numbers**
- **Pin numbers / passwords**

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 that you have won a contest or 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 provide 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 solicitation requesting that you deposit a check or pay a fee to collect a prize.

Please report any suspicious emails or contacts that are using the First Community Bank name directly to: [SecurityOfficer@FCBConnect.com](mailto:SecurityOfficer@FCBConnect.com)