

## Defining Common Scams:

**Phishing** is the criminal fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by claiming to be a trustworthy entity in an electronic communication.

Communications claim to be from popular social web sites, online payment processors, or IT Administrators.

### **Example:**

Phishing is typically carried out by email or instant messaging and it often directs users to enter details at a fake website almost identical to the legitimate one.

### **How to Avoid:**

- Be suspicious of any email with urgent requests for personal financial information
- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic
- Avoid filling out forms in email messages that ask for personal financial information

## Resources

**NM Attorney General**  
[www.ago.state.nm.us](http://www.ago.state.nm.us)

**NM Securities Division**  
[www.rid.state.nm.us/securities](http://www.rid.state.nm.us/securities)

**Social Security Administration**  
[www.ssa.gov](http://www.ssa.gov)

**Better Business Bureau**  
[www.bbbsw.org/](http://www.bbbsw.org/)

## 13th Judicial District

**Cibola County**  
515 High Street,  
Grants, New Mexico  
87020  
505)285-4627

**Sandoval County**  
1500 Idalia Road  
Bernalillo, New Mexico  
87004  
(505) 867-2386

**Valencia County**  
101 South Main Street,  
Suite 201  
Belen, NM 87002  
(505) 861-0311

## Scam Awareness



## Don't Become a Victim

**Lemuel L. Martinez**  
**13<sup>th</sup> Judicial District**  
**Attorney Serving Cibola,**  
**Valencia & Sandoval**  
**County**

**Credit Card Fraud** a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. It is often used in identity theft.

**How to Avoid:**

- Shred all credit card applications you receive.
- Never leave your credit cards or receipts lying around.
- Shield your credit card number so that others around you can't copy it or capture it on a cell phone or other camera.
- Keep a list in a secure place with all of your account numbers and expiration dates, as well as the phone number and address of each bank that has issued you a credit card.

**Advance-Fee Fraud** usually begins with a letter, fax or e-mail sent to a selected recipient but actually sent to many making an offer that will ultimately result in a large payoff for the intended victim.

**Example:**

The **419 scam** originated in Nigerian. It was first used to scam business investor interested in shady deals in the Nigerian oil sector. The 419 scam has spurred imitations from other locations

in Africa, Asia and Eastern Europe, and, more recently, from North America, Western Europe and Australia.

**How to Avoid:**

- Do not open emails with subject lines that says something like “From the desk of Mr. [Name]”, “Your assistance is needed” and so on.
- Look out for stories sent from unknown sender, often a government or bank employee, who knows of a large amount of unclaimed money.
- Advanced payment is usually requested by wire transfers.

**Pyramid Scheme** is a non-sustainable business model that involves the exchange of money primarily for enrolling other people into the scheme, without any product or service being delivered. Pyramid schemes are illegal in many countries, including the United States.

**Health Insurance Fraud** an intentional act of deceiving, concealing, or misrepresenting information that results in health care benefits being paid to an individual or group.

**How to Avoid:**

- The coverage offered to you costs 25 percent or more below the norm, yet promises generous benefits and a large provider network.

- The plan readily accepts people with serious illnesses and other medical conditions that other plans normally reject.
- The insurance has few or no underwriting
- The plan isn't licensed in your state, and the agent (falsely) assures you the federal ERISA law exempts the plan from state licensing.

**Charity Scams** often set up quasi-legitimate agencies so that, at first glance, they look real; they may also name themselves something similar to other legitimate charities.

**How to Avoid:**

- These scam artists use all of the standard methods to collect 'donations' for their charity scams -- tables at the local mall, going door-to-door, email, and telemarketing.
- They may even carry 'ID' in the name of the charity, complete with a logo.

