



Are You the Next Target of a Scam?

Don't take the bait!

Your tax payment bounced, your account is overdrawn, there's a problem with your 401k, or a Nigerian Prince desperately needs your help. Most of us at some point have received random urgent emails trolling for financial information or asking us to click a link to win a huge prize. It's a common scam known as "phishing", and if you fall prey to this crime, you risk having your bank account pillaged or your identity stolen. Phishing scams can take a variety of forms, but one thing they have in common is they cost consumers and businesses millions, even billions of dollars per year. With technological advancements, scammers are becoming more sophisticated. Learning how to quickly spot these scams will prevent you from becoming their next unsuspecting victim.

Mortgage Fraud

There are many types of schemes, including foreclosure rescue, loan modification or reverse mortgage scams, and all contain some type of material misstatement, misrepresentation or omission of information relating to the property or potential mortgage.

Unauthorized Credit Card Charges

Scamming occurs when a company that has your credit card information on file makes unauthorized charges and hopes the victim either doesn't notice or thinks reversing the charges will be too much trouble. To get your credit card information, some companies will offer a "free trial" and then sell the credit card information to another disreputable group.

Computer Intrusion Scams

In frauds such as the Nigerian e-mail scam, the scammer claims to desperately need short-term financial assistance to see them through a crisis with the false promise of full reimbursement and a generous cash gift for their assistance.

Overpayment Scams

Fraudsters negotiate contracts requiring payment to their victims. Ultimately, the victims receives an illegitimate payment larger than the amount owed, and then scammers instruct their victims to wire the money back to them. Several varieties of this scam exist, such as secret shopper, pet schemes, and false roommates.



SMS Phishing- "Smishing"

Smishing, a combination of text messaging (SMS) and phishing, is another scheme designed to trick people into divulging sensitive information via a Web link and false website, or a telephone number. The recipient might receive a text appearing to be from a trusted source such as a financial institution, asking to verify account information, or a retailer offering a free gift. Many people don't realize that their mobile phone is another source for scam artists who use the immediacy of text messages to their advantage.



Ways to Protect Yourself from Mass Marketing Fraud

- * **Never "verify" account information via email**-- Your bank and legitimate companies will not ask you to disclose account information via email
- * **Watch out for links**--Don't click any links in an email claiming to be from a bank or financial institution
- * **Steer clear of "urgent" messages**--Don't respond to emails or texts that warn of consequences unless you validate your information. Contact the company directly using a telephone number or Web address you know are genuine
- * **Be cautious with attachments**--Unless you trust the source and you're expecting them, it's best to avoid opening attachments or downloading files
- * **Do not send money via wire or electronic money transfer**--Unless the entity whose legitimacy is personally known to you or you personally initiated the contact with the entity



For a Free Home Evaluation, Call Us Today!

Keller Williams SD Metro
2250 Fourth Ave FL 3
San Diego, CA 92101
Broker DRE #01295699

kw
KELLERWILLIAMS

Leon Alchalel
C: 619-517-8609
E: Leonalchalel@kw.com
CAL DRE #01507076

Dawn Ramos
C: 619-889-9592
E: Dmramos4@gmail.com
CAL DRE #01940779

If you already have a brokerage relationship with another agency, this is not intended as solicitation.
All information deemed reliable but not guaranteed.