# Real Estate Advisor

## Online phishing scams – 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 that they cost consumers and businesses millions, even billions of dollars per year.

## Here are some Common tricks:

### 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 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.

### Mass phishing

High-volume "mass phishing" campaigns are sent by fraudsters to thousands or millions of consumers, and often appear to be from larger banks, Internet service providers, retailers, or the IRS. Victims are randomly chosen via sophisticated tools used to scan the Web and harvest email addresses, or through purchased or stolen lists. Many online users have learned to spot these emails, which are often suspicious and vague--with salutations such as "Dear customer." According to Cisco Security Intelligence Operations, only about three percent of mass phishing emails are opened, yielding the attacker an average of $2,000 when the scam succeeds.

### Spear-phishing

Personalized phishing attacks, known as "spear-phishing," target fewer individuals than mass phishing campaigns, but the scammers are careful to choose people most likely to open the emails. Messages tend to look authentic, address their victims by name, contain a personal tidbit about the individual (such as employment), and seem to come from companies the victims have a business relationship with. Oftentimes, these emails contain links to fake sites or attachments with malware that can relay passwords and account numbers to the scammers. The payoffs are higher for cybercriminals – approximately $80,000 per victim, according to Cisco.

# 7 steps to protect yourself

## 1. Never "verify" account information via email

Your bank and legitimate companies will not ask you to disclose account details via email. Never give out your personal financial information in response to an unsolicited email, text, or phone call.

## 2. Watch out for links

Don't click any links in an email claiming to be from a bank or financial institution. If you scroll your cursor over a suspected link, your browser should show the actual address you'll be taken to. If it's different from the address of the legitimate website, then clicking may take you to a fraudulent site.

## 3. 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.

## 4. Be cautious with attachments

Unless you trust the source and you're expecting them, it's best to avoid opening attachments or downloading files.

## 5. Look closely at spelling

Many phishing emails and websites include spelling and grammatical mistakes--errors your real bank or account provider would never make in a professional customer email.

## 6. Make sure websites are secure

When conducting online business, make sure sites feature a lock icon and an "https" URL to indicate security.

## 7. Safeguard your computer

Purchase up-to-date security software to prevent spam, viruses, and spyware.

With the speed and convenience of email and text, it's likely that tech-savvy con artists will at some point attempt to steal your money or identity. By knowing more about phishing scams, you'll be able to recognize potential threats and avoid being hooked.

LINDSEY REALTY, Debra Lindsey, Broker
P O Box 777
Shreveport, LA 71162

LINDSEY REALTY,
Debra Lindsey, Broker, 0995690271
LINDSEY REALTY
P O Box 777
Shreveport, LA 71162

FAX 800.406.2665
318.990.2737
lindseyrealty@gmail.com
www.lindseyrealty.us

LINDSEY REALTY



*High Tech, High Touch, High Performance!*