EUSTIS FAMILY OF COMPANIES

PHISHING ATTACKS ARE MORE RAMPANT THAN EVER BEFORE

Unfortunately, no matter what companies do, some phishing emails will always make it to the inbox. And those messages are extremely effective—97% of people around the globe cannot identify a sophisticated phishing email. That's why we want to educate you.

Here are 10 tips on how to identify a phishing or spoofing email. Please feel free to share this with anyone monitarily in your financing process.

TIP 1: Don't Accept Wire Requests

Your mortgage provider will never send you a request to wire funds via email. Do not open a wire request via email unless its securely sent directly from the closing/title company. Always double check your wire instructions by calling the closing/title company directly or contact your mortgage expert.

TIP 2: Look But Don't Click

Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in the website address directly rather than clicking on the link from unsolicited emails.

TIP 3: Check For Spelling Mistakes

Legitimate businesses are serious about their branding. They usually do not have major spelling mistakes or display poor grammar.

TIP 4: Analyze The Salutation

Is the email addressed to a vague "Valued Customer?" If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

TIP 5: Don't Give Personal Information

Mortgage companies and other businesses will never ask you for your personal credentials via email. Do not give them up.

TIP 6: Urgent Or Threatening Subject Line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or your account had an "unauthorized login attempt."

TIP 7: Review The Signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details. Cross check any phone numbers given in the signature against previously received emails.

TIP 8: Don't Click On Attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you.

TIP 9: Don't Trust The Display Or Header

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address.

TIP 10: Don't Believe Everything You See

Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it's legitimate.

WHEN IN DOUBT CALL 844-586-0075 AND VERIFY WITH YOUR TRUSTED CONTACT.