DON'T FALL VICTIM TO

WIRE FRAUD

SHORELINE TITLE
A BSPOKE TITLE HOLDINGS COMPANY

Sensitive information plays a critical role in your real estate transaction, and it's imperative that this information remains safe and protected.

Scammers are increasingly taking advantage of homebuyers during the real estate closing process using a technique known as phishing, or spoofing. During a real estate transaction, they attempt to divert a homebuyer's closing costs and down payment into a fraudulent account by posing as a representative of the title company, lender, or real estate agent. For example, they may send an email advising the homebuyer that there has been a last-minute change to the wiring instructions and request that funds be sent to the new account information provided. By following these instructions, the funds are inadvertently wired to the scammer's account and, most often, lost forever. As a consumer, there are ways to identify and protect yourself from cybercrime.

STOP. CALL. VERIFY.

URGENT REQUESTS

Be cautious of emails requesting last-minute changes to wiring instructions, provide a strict deadline for performing an action, or are threatening in nature.

SENDER ADDRESS

Confirm that the sender email address matches the sender name or the reply-to email address. These spoofing email addresses appear legitimate but often have one additional letter or some other minor variation from the actual email address.

ATTACHMENTS & LINKS

Avoid clicking on any links or downloading attachments that could download malicious files to your computer without first confirming with your trusted representative.

MISSPELLINGS OR BAD GRAMMAR

Phishing messages often contain misspelled words or incorrect grammar.

IMPERSONAL GREETING

Phishing emails may use a generic greeting such as, "Hi Dear" or "Valued Customer".

EMAIL SIGNATURE

Check to see if the email closing is overly generic or doesn't match the company template.

WHAT TO DO IF YOU'VE BEEN TARGETED

If there is ever any doubt, call your representative directly to confirm any changes. Use a publicly listed phone number, or one previously given to you directly from the representative, not the phone number listed in the email. While it's easy to think you may not fall for this kind of scam, these schemes are complex and often appear legitimate. If you suspect you have been a victim of wire-fraud, contact your bank or wire-transfer company immediately. Ask for a wire recall. Reporting the error as soon as possible can increase the likelihood that you'll be able to recover your money.