



WIRE FRAUD RED FLAGS

Fraud is on the rise and now coming via text message with hackers posing as real estate professionals or title companies to trick customers into wiring closing funds to their accounts. Below are common “red flags” associated with these schemes, and tips for how to avoid becoming a victim.

UNSECURE EMAIL ACCOUNTS

- Be suspicious of any party that uses free, web-based email accounts for business transactions. These accounts are easily breached.

CHANGES OR ANOMALIES

- Watch for the word “kindly” in communications. While it is a nice word, it is unnecessary and outdated in American conversation, but it tends to be used in overseas phishing schemes.
- Pay careful attention to all email addresses throughout the transaction to make sure they are legitimate. Hackers often email from unsecure domains or fake domains that closely resemble real ones to trick their victims.
- Watch for sudden changes in grammar, terminology and verbiage. Be wary of spelling or grammatical errors, requests for secrecy or pressure to take action quickly.
- Be suspicious of emails that arrive at odd hours of the day or night.

PAYMENT INSTRUCTIONS

- Be wary of unusual payment amounts or payment requests to odd parties, unusual persons or international wires.
- Review the name(s) on all bank accounts. Does it match the name(s) of the party(ies) involved? Is it worded strangely?
- Always verify changes to payment instructions and confirm requests for transfer of funds from any party – especially last-minute wiring changes from financial institutions.

HOW TO AVOID WIRE FRAUD

- Slow down. Moving too quickly and not verifying information leads to mistakes.
- Err on the side of caution. Assume anything suspicious is fraud.
- Never reply to a suspicious email or act on any of the information in the message.
- Pick up the phone. Call all parties involved in the transaction using previously known, verifiable phone numbers before closing. Do not just confirm that wiring instruction were changed, verify that the account information in the instructions are correct.
- If you suspect fraud, act immediately. Contact your local law enforcement authorities, and file a complaint with the FBI's Internet Crime Complaint Center (IC3).



431 West Lancaster Avenue
Devon, PA 19333
tridentland.com