

EMAIL FRAUD RED FLAGS

Email fraud is on the rise, 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

- 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 (e.g. o1drepublictitle@OldRepublicTitle.com) 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? Keep in mind that Old Republic Title® does not wire funds to third-party bank accounts.

- 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 EMAIL FRAUD

- Slow down and read every email carefully – even those that appear to come from a trusted source.
- 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 the wiring instructions 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).

For more information, please contact your local Old Republic Title representative, or visit our website at **oldrepublictitle.com**.