CYBERFRAUD

Protecting Yourself From Real Estate Cyber-fraud

Sensitive information plays a critical role in your real estate transaction, and it's imperative that this information remains safe and protected. We strive to provide Stewart Trusted ProvidersTM with peace of mind in knowing that their personal, non-public sensitive information is protected through Stewart's data security and email encryption. But, as a Stewart Trusted Provider, there are steps you can take to protect yourself from cyber-fraud, too.

Recently, there has been a wave of cyber-fraud. Cybercriminals hack into the email accounts of real estate agents or other persons involved in real estate transactions. These "hackers" are patient; they sit and wait until they discover useful information to assist in the scam and trick you into sending money through a wire transfer to a bank account that appears to be legitimately owned by a party involved in the transaction (but is not). The hackers send an email that appears to be from an individual involved in the transaction (a practice called spoofing).

At first glance, these spoofing email addresses appear legitimate but often have one additional letter or some other minor variation from the actual email address (for example, msmith@stewartttitle.com instead of msmith@stewarttitle.com). These spoofing emails advise the recipient (often the buyer) 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 hacker's account and, most often, lost forever.

Recognize common indicators of cyber-fraud:

- Emails requesting last-minute changes to wiring information (e.g., particularly changes in the beneficiary and/or receiving bank)
- Requests for wire transfers late in the day or week or outside of business hours
- Emails with poor grammar and/or typographical errors
- Slight, typically unnoticeable-at-first-glance changes in the email address

stewart title | AGENCY SERVICES

Suggested best practices for transmitting and receiving sensitive information:

- Send emails with sensitive, personal information, through encrypted email only.
- Verify requests to change wiring instructions through a trusted method (like a phone number previously verified); never use the phone number in the email.
- Verify wire transfer requests to locations outside normal business areas.
- Never click on any links in an unverified or unexpected email.
- Always question attachments and links that are sent unencrypted.

What to do if you believe you are a victim of cyber-fraud:

- If money was wired in response to fraudulent wiring instructions, immediately call all banks and financial institutions that could put a stop to the wire or your funds.
- Contact your local police or local municipalities' real estate fraud division.
- Contact any other parties who may have been exposed to the cyber-fraud so that appropriate action may be taken.
- Change all usernames and passwords associated with any account that you believe may have been compromised.
- Report any cybercrime activity to the Federal Bureau of Investigation Internet Crime Complaint Center www.ic3.gov/complaint/default.aspx.

stewart title | AGENCY SERVICES