HUMBOLDT ASSOCIATION OF REALTORS®

Don’t Get Played: Real Estate & Tech Scam Alert

A member resource for HAR REALTOR® and Affiliate members

Wire fraud and impersonation scams cost real estate consumers hundreds of millions of dollars a year — and criminals now use AI to make them harder to spot. Know the red flags, and share them with your clients.

1 Wire Fraud & Closing Instructions

- Never trust wiring instructions received only by email — confirm any account or routing number by phone, using a number you already have on file, not one in the email.
- Tell every buyer and seller early: your brokerage and the title company will NEVER change wire instructions by email.
- Watch for last-minute “urgent” changes near closing — that pressure is the scam.

2 Phishing & Spoofed Emails

- Check sender addresses closely — scammers use domains that look nearly identical to a real title company, lender, or brokerage.
- Don’t click links or open attachments from unexpected emails, even ones that look like they’re from a colleague or MLS.
- Hover before you click: the display name can lie, but the actual link address usually gives it away.

3 AI Voice & Video Deepfakes

- A cloned voice or video call from a “client” or “broker” urgently requesting funds or personal data is a growing tactic — verify with a callback to a known number.
- Agree on a verbal “safe word” with clients for anything involving money or sensitive documents.
- Be cautious with voicemail greetings and social media videos; scammers harvest voice and image samples from public posts.

4 Seller & Title Impersonation

- Vacant land and absentee-owner listings are common targets for fraudsters posing as the seller.
- Verify seller identity with photo ID and, when possible, a face-to-face or video meeting before listing.
- Be alert to sellers who refuse in-person meetings, push to close fast, or want proceeds sent overseas.

Lock Down Your Own Accounts

- Use multi-factor authentication on email, MLS, and transaction platforms.
- Use unique, strong passwords — never reuse your email password elsewhere.
- Be skeptical of unsolicited “IT support” or password-reset calls and texts.
- Report suspicious emails to your broker or IT contact before forwarding or replying.

If You Suspect Fraud — Act Fast

1. Contact your bank or the receiving bank immediately and request a wire recall.
2. File a report at IC3.gov within 24–72 hours for the best chance of recovery.
3. Notify your broker, the title company, and all transaction parties right away.

NAR Wire Fraud Resource Center