The New Red Flags of Real Estate Fraud

FRAUD ALERT

AI is making real estate fraud faster and harder to spot. Cybersecurity experts urge agents to build verification into the transaction to avoid getting duped.

Think you know how to spot a fake? A familiar email, a trusted voice or even a building ID card—nowadays none of these necessarily proves you're dealing with the real person.

AI is giving scammers new ways to impersonate clients, agents and parties in a transaction, and it's making fraudulent messages harder to spot, cybersecurity experts said during a recent webinar, "Cybersecurity in the Age of AI," hosted by the National Association of REALTORS®' Tech & Innovation team.

Joshua Sklüt, CEO of SKLÜT, a biometric facial recognition company for buildings and a 2026 participant in NAR's REACH accelerator program, put the challenge simply: "You just don't know what's real until you can prove it. In the age of AI, proof is key."

An attacker can use AI to research a listing, build a profile of the agent and transaction, craft a convincing message, monitor an email thread and ultimately send fraudulent wire instructions timed to closing. A cloned voice or other manipulated media can add another layer of false credibility.

"Voice alone is no longer reliable proof of identity," said Sebastian Drywa, NAR's director of cybersecurity.

The Red Flags to Watch

AI didn't create phishing, business email compromise or impersonation scams, but "AI has weaponized them"—making these scams much faster to replicate, more targeted and more convincing, Drywa said.

Mike Woodward, NAR's director of data science, also warned that even a small amount of publicly available audio and video—a mere three seconds of it—or imagery can be used to create a convincing deepfake or synthetic media used to dupe unsuspecting parties in a transaction. That makes traditional cues—like recognizing a voice, an email address or even seeing a familiar photo—less reliable as proof of identity.

The speakers highlighted several warning signs real estate professionals should watch for, including:

A sudden change to wire instructions. Treat any new or change to payment information as a reason to stop and verify.

A request that doesn't fit the normal transaction pattern. An unusual request from a familiar looking contact can still be fraudulent.

Unexpected urgency. Pressure to act quickly—especially around money—should trigger more verification, not less.

A message or caller that seems unusually convincing. A familiar voice, email account or writing style is no longer enough to base identity or verification on.

Related: New NAR Fraud-Fighting Site Takes Aim at Real Estate Scams

Additional information - https://www.nar.realtor/news/real-estate-news/the-new-red-flags-of-real-estate-fraud

PROVIDENT TITLE COMPANY