Consumer Guide: Spotting Deepfake Scams in Real Estate

Cyber-enabled fraud—use of the internet or other technology to steal money, data or identity—accounted for $13.7 billion in 2024, according to the latest data released by the FBI's Internet Crime Complaint Center (IC3). Among cybercrimes, the use of deepfake technology is a growing concern. Deepfake scams increased 40% year-over-year, according to the 2026 Identity Fraud Report by security firm Entrust. Here's what you need to know about deepfake scams to protect yourself during the sale or purchase of your home.

What are deepfakes?
Entrust defines deepfakes as "realistic, AI-generated fake videos, images or audio recordings that mimic a real person's likeness."

How are deepfakes used in real estate?
Scammers might use deepfake-generated audio or video to impersonate buyers, sellers, real estate agents, real estate lawyers, title agents or other professionals. By pretending to be real people involved in a real estate transaction, criminals can change the wiring or money transfer instructions to divert down payments or closing funds to their own bank accounts. They can also manipulate property photos or virtual tours to hide defects, exaggerate home features or even fabricate nonexistent properties to sell to unsuspecting buyers.

What can you do to protect yourself?

- Work with trusted professionals, like a real estate agent who's a REALTOR®, a member of the National Association of REALTORS®.
- Use a secure messaging system or encrypted emails (rather than a free email account) when communicating about a real estate transaction.
- Try to avoid entering into a transaction on a property you haven't seen in person or with a buyer or seller who communicates only electronically.
- Independently verify property documents and ownership through title companies and trusted parties. Never rely solely on digital copies that could have been altered.
- Ask for multifactor authentication before transferring funds or signing important documents. Many companies are now using a third-party verification tool, such as CertifID.
- Invest in fraud-detection tools that can detect deepfakes by analyzing facial movements in videos, voice anomalies and inconsistencies in digital images.
- Consider investing in an owner's title policy to safeguard against record fraud. The insurance protects you against forged deeds, fraudulent liens and fake owners.
- To verify instructions for wiring funds, always talk to the party who's receiving the funds by phone on a known number, or meet in person. Any urgent change in instructions—whether delivered through an email, audio message or a video call—is a red flag.
-

What should you do if you suspect a deepfake scam?

- Contact everyone involved in your transaction (real estate agent, lawyer, title company) to alert them to the suspected fraud so that they can exercise extra caution.
- Contact your local and state law enforcement.
- Report the incident to the FBI's Internet Crime Complaint Center (IC3)

Practices may vary based on state and local law. Consult your real estate professional and/or an attorney for details about state law where you are purchasing a home. Please visit facts.realtor for more information and resources.