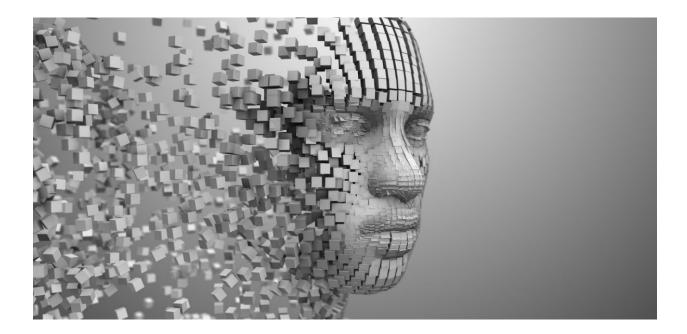
Cybercriminals are using artificial intelligence to impersonate agents and other parties to a real estate deal. Here's how you can stop them.



You've probably seen "deepfake" videos online purporting to show a person doing or saying something that they never actually did. It's one of the <u>dangers of artificial intelligence</u>: Savvy users can imitate or replace a person's face or voice to create highly convincing video or audio forgeries and manipulate or deceive audiences. Deepfakes are often used against political or public figures to disrupt discourse. But how can deepfakes put your real estate business at risk?

- 1. Al can create fake listings, like fraudulent rental ads, to defraud consumers.
- 2. Deepfake videos can trick agents into taking listings or writing virtual sales contracts for properties that don't exist or are not representative of the actual condition of the property.

- 3. Al can create fake reviews or video testimonials for real estate agents or brokers. Fraudulent reviews may convince consumers—or even other real estate pros—to work with agents who have ethical, disciplinary or criminal issues.
- 4. Deepfakes can be used to slander, defame or damage an agent's reputation by depicting him or her saying things that were never said.
- 5. Deepfakes can impersonate real estate professionals in order to gain access to sensitive information about clients and defraud them.
- 6. Fake Al-generated property tours online could deceive buyers and agents about property condition.
- 7. Deepfake videos can be used to lure agents into virtual meetings with a cybercriminal who poses as a legitimate party to the transaction.
- 8. Cybercriminals can use AI to impersonate clients and seek unauthorized information about a property, net proceeds from a sale, confirm financial information from lenders or get employment details.

One of the most significant risks of AI in real estate has to do with wire fraud. The use of deepfakes has made wire fraud even more challenging to detect. Case in point: In 2019, a cybercriminal used AI voice technology to trick the CEO of a U.K.-based energy firm to transfer \$243,000 to a secret account.

To protect buyers and sellers from such risks, you must take the necessary steps to ensure that your clients' identities and transactions are secure. This includes verifying identities, implementing secure payment procedures and adopting strict security measures.

You should consistently advise clients of the prevalence of wire fraud in the real estate industry as well as potential deepfake crimes. One step to prevent wire fraud is to put a warning in your email signature. (The National Association of REALTORS® provides a <u>template</u>.)

Steps to Protect Against Deepfakes

- Stay informed. Know the latest developments in deepfake technology, and be aware of the potential ways cybercriminals could use it to harm the real estate industry. It's imperative for brokers to provide regular cybersecurity training. Technology changes quickly.
- Verify information. Be cautious with any information or media related to real estate. Regardless of the source—whether it's a lender, colleague or client—take steps to verify the authenticity of the information before acting on it. Reach out directly to the source to confirm, and make sure to communicate via an email address or phone number you know to be authentic.
 - •Use secure communication channels. Use domain-based and encrypted email and messaging apps rather than free email accounts when communicating with clients or colleagues about sensitive information related to real estate.
 - •Use watermarks on real estate documents. To guarantee the authenticity and integrity of real estate documents and materials, employ watermarks and other authentication techniques to detect any unauthorized modifications.
 - Educate others. Teach your fellow real estate pros and consumers about the dangers of deepfakes and the importance of being vigilant.

It's important to note that deepfake detection tools are still in the early stages of development and may not always be effective at detecting all deepfakes. However, there are several software tools that can be helpful. Two popular and highly rated ones are ZeroGPT(link is external), a free resource with a 98% accuracy rate, and Sensity(link is external), a deepfake detection tool that uses artificial intelligence to analyze facial expressions and other video features to determine if they have been altered. It also helps verify ID cards and documents. Integrating ChatGPT, artificial intelligence and deepfakes into the real estate industry brings benefits and potential risks. As technology continues to evolve, real estate pros and consumers need to stay informed and take action to mitigate the potential dangers of these technologies. By being cautious, verifying the authenticity of information and transactions and implementing proactive measures, you can ensure a more trustworthy and secure real estate market for all stakeholders.

•