Generative AI Impact on Real Estate

Description

Generative AI is a branch of artificial intelligence that creates new content by analyzing existing data. It has many potential applications in real estate, such as generating property images, listing descriptions, and personalized marketing campaigns. However, generative AI can also be used for fraud, which poses risks and challenges for the industry.

How Generative AI Can Be Used for Fraud in Real Estate

Generative AI has opened up many opportunities for fraudsters to deceive people in real estate. However, by understanding the most common and dangerous ways in which they do so, you can protect yourself against these scams.

One of the most dangerous techniques is deepfakes and voice spoofing, where fraudsters can use generative AI to create fake images, videos, or audio clips of people such as real estate agents, buyers, or investors. These convincing deepfakes or voice-spoofing techniques can then be used to impersonate someone else and trick their targets into sending money, revealing sensitive information, or signing fraudulent contracts. For instance, fraudsters can use a deepfake video of a seller to convince a buyer to make a deposit for a property that does not exist or use a voice-spoofing clip of an investor to persuade a real estate agent to wire funds to a fake account.

Another way in which generative AI is used for fraud is through email phishing and text messaging. The AI can create convincing text content, such as emails or text messages, that mimic the style and tone of a trusted source, such as a real estate agent, buyer, seller, or investor. Fraudsters can then use these phishing or text messaging techniques to lure their targets into clicking on malicious links, downloading malware, or providing personal or financial information. For example, fraudsters can use an AI-generated email to pose as a real estate agent and ask a buyer to verify their identity or payment details by clicking on a link that leads to a fake website.

Lastly, generative AI can be used to create fake or manipulated listings to make properties look better than they really are. This can be done to attract more buyers, inflate the price, or hide the flaws or defects of the properties. For example, fraudsters can use a generative AI-generated image to add a pool, a garden, or a balcony to a property that does not have them or use a generative AI-generated text description to exaggerate the features or amenities of a property. Also, generative AI can be used to perpetrate seller identification fraud and wire transfer or check fraud, which has been a topic of increasing concern for the title industry.

By being aware of these techniques, you can protect yourself against fraudsters who use generative AI to deceive people in real estate.

How to Prevent and Detect Fraud in Real Estate Using Generative AI

Generative AI has been subject to fraudulent activities in the real estate industry, but it can also be used effectively to prevent and detect fraud. Real estate organizations can leverage generative AI to protect themselves and their customers from fraud by following these strategies:

- Choose a secure and reliable generative AI solution that meets their needs, budget, and security standards. The solution should also comply with relevant laws and regulations. It is essential to conduct regular monitoring, updating, audits, and tests to ensure accuracy and effectiveness.
- Verify and validate generative AI-generated content such as images, videos, audio, emails, texts, and listings. Confirm partiesâ?? identity and credibility with official records, reviews, or personal references. Use tools like reverse image search, watermark detection, or digital forensics to check content authenticity.
- Educate employees and customers on the benefits and risks of generative AI. Teach them to use it responsibly and recognize signs of fraud. Provide clear instructions and support during the AI process. Ensure compliance with confidentiality requirements when interacting with generative AI.
- Use multifactor authentication to secure online services and accounts that store or access sensitive data, such as customer information, payment details, or contracts. Adaptive authentication can adjust the required level based on the context and risk of the login attempt, such as the userâ??s device, location, or behavior.

Conclusion

Generative AI space is still evolving. Solid governance, policy enforcement, and continuous monitoring must be embedded in business processes.

Genady Vishnevetsky
Genady Vishnevetsky serves as Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building successful security programs and developing the defense against emerging threats, Vishnevetsky leads security, governance, and compliance programs for global enterprises. Genady holds the following cybersecurity and risk management certifications â?? Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified in Risk and Information Systems Control (CRISK).

Category

1. Cybersecurity
2. Digital Marketing

3. In the News
4. Uncategorized

Date Created
2023/12/21
Author
vltaexaminer