Customer Advisory: Criminals Increasing Use of Generative AI to Commit Fraud

The availability of generative artificial intelligence technology makes it easier than ever to create false images, voices, videos, live-streaming video chats, social media profiles, and malicious websites designed to look like financial trading platforms. The technology is also increasingly being used in relationship investment frauds, the FBI recently reported.[1]

The technology is being used to improve website functionality and content. Criminals outside the United States commonly target U.S. residents. Generative AI tools are used to assist with language translations and correct grammatical or spelling errors that may have raised suspicions in the past. AI-powered chatbots may also provide the appearance of legitimacy or prompt victims to click on malicious links. The same AI capabilities make it easier and faster to create fake social media profiles that target people looking for friendship, trading information, or advice.

Images and Video

Criminals create realistic images for fake dating or social media profiles using AI. They make fraudulent identifications and forge government or financial documents to help their schemes. Perpetrators also use generative AI to produce convincing photos and videos to share with targets in private communications to "prove" the online contact is a "real person."

Technology can now be used to alter real-time video chats. With a smartphone app or free, open-source software, criminals could alter their appearance or use other images to change their facial features.

Protect Yourself

- Identify AI products by studying images and video for distorted hands and other imperfections. Listen carefully to vocal inflections, tone, and word choices. See the FBI's Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud to learn more.
- Tighten your social media account privacy settings to limit what others can learn about you or who can contact you. Do not respond to text messages, phone calls, or social media invitations from people you do not know.
- Never send cryptocurrency or other assets to people you do not know or have met only online or over the phone.
- Never share sensitive information with people you have met only online or over the phone.

Report Fraud: If you've been defrauded, report it to the CFTC at cftc.gov/complaint and to the FBI at ic3.gov. Your report may help others avoid fraud.

[1] See *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud,* https://www.ic3.gov/PSA/2024/PSA241203#fn1