Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-120324-PSA
December 3, 2024

Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

The FBI is warning the public that criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes. Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.[1] Since it can be difficult to identify when content is AI-generated, the FBI is providing the following examples of how criminals may use generative AI in their fraud schemes to increase public recognition and scrutiny.

AI-Generated Text

Criminals use AI-generated text to appear believable to a reader in furtherance of social engineering,[2] spear phishing,[3] and financial fraud schemes such as romance, investment, and other confidence schemes or to overcome common indicators of fraud schemes.

- Criminals use generative AI to create voluminous fictitious social media profiles used to trick victims into sending money.
- Criminals create messages to send to victims faster allowing them to reach a wider audience with believable content.
- Criminal use generative AI tools to assist with language translations to limit grammatical or spelling errors for foreign criminal actors targeting US victims.
- Criminals generate content for fraudulent websites for cryptocurrency investment fraud and other investment schemes.
- Criminals embed AI-powered chatbots in fraudulent websites to prompt

victims to click on malicious links.

AI-Generated Images

Criminals use AI-generated images to create believable social media profile photos, identification documents, and other images in support of their fraud schemes.

- Criminals create realistic images for fictitious social media profiles in social engineering, spear phishing, romance schemes, confidence fraud, and investment fraud.
- Criminals generate fraudulent identification documents, such as fake driver's licenses or credentials (law enforcement, government, or banking) for identity fraud and impersonation schemes.
- Criminals use generative AI to produce photos to share with victims in private communications to convince victims they are speaking to a real person.
- Criminals use generative AI tools to create images of celebrities or social media personas promoting counterfeit products or non-delivery schemes.[4]
- Criminals use generative AI tools to create images of natural disaster or global conflict to elicit donations to fraudulent charities.
- Criminals use generative AI tools to create images used in market manipulation schemes.
- Criminals use generative AI tools to create pornographic photos of a victim to demand payment in sextortion schemes.

AI-Generated Audio, aka Vocal Cloning

Criminals can use AI-generated audio to impersonate well-known, public figures or personal relations to elicit payments.

- Criminals generate short audio clips containing a loved one's voice to impersonate a close relative in a crisis situation, asking for immediate financial assistance or demanding a ransom.
- Criminals obtain access to bank accounts using AI-generated audio clips of individuals and impersonating them.

AI-Generated Videos

Criminals use AI-generated videos to create believable depictions of public figures to bolster their fraud schemes.

- Criminals generate videos for real time video chats with alleged company executives, law enforcement, or other authority figures.

- Criminals create videos for private communications to "prove" the online contact is a "real person."
- Criminals use generative AI tools to create videos for fictitious or misleading promotional materials for investment fraud schemes.

Tips to protect yourself

- Create a secret word or phrase with your family to verify their identity.
- Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic teeth or eyes, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, lag time, voice matching, and unrealistic movements.
- Listen closely to the tone and word choice to distinguish between a legitimate phone call from a loved one and an AI-generated vocal cloning.
- If possible, limit online content of your image or voice, make social media accounts private, and limit followers to people you know to minimize fraudsters' capabilities to use generative AI software to create fraudulent identities for social engineering.
- Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and call the phone number directly.
- Never share sensitive information with people you have met only online or over the phone.
- Do not send money, gift cards, cryptocurrency, or other assets to people you do not know or have met only online or over the phone.

If you believe you have been a victim of a financial fraud scheme, please file a report with the FBI's Internet Crime Complaint Center at www.ic3.gov. If possible, include the following:

- Identifying information about the individuals including name, phone number, address, and email address.
- Financial transaction information such as the date, type of payment, amount, account numbers involved, the name and address of the receiving financial institution, and receiving cryptocurrency addresses.
- Describe your interaction with the individual, including how contact was initiated, such as the type of communication, purpose of the request for money, how you were told or instructed to make payment, what information you provided to the scammer, and any other details pertinent to your complaint.

[1] *Synthetic content* refers to the class of media generated or manipulated by machine-learning-based techniques. ↩

[2] *Social engineering* is the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. ↩

[3] *Spear phishing* is a directed attempt to trick a specific user or group of users into clicking on a malicious link or opening an attachment in an email that incorporates information intended to increase the chance of success. ↩

[4] *Non-delivery scams* occur when payment is sent, and goods or services are never received, or are of lesser quality. ↩