JS|HELD

PERSPECTIVES

The Dark Side of Artificial Intelligence: Scams and Frauds

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

If you checked the news lately, you have probably seen or heard about the latest advancement of Artificial Intelligence (AI). Notably, the advancement of AI and deepfake technology convinced the actor, filmmaker, and studio owner, Tyler Perry to indefinitely pause his $800 million movie studio expansion.[1] So what exactly is AI and deepfake technology and how will it impact everyday people?

AI is technology that enables computers to simulate human intelligence and problem-solving skills, whereas deepfake is synthetic media that has been digitally manipulated to replace and mimic one person's likeness.

AI has involved itself in nearly every aspect of modern daily life. We see it now on websites we visit, and we are greeted with AI-powered chat bots for customer service online. However, with the advancement and seemingly helpful progress of AI, there is a darker reality – the potential of AI for exploitation and manipulation through scams and frauds. As AI continues to advance, so too, do the tactics used by malicious actors to deceive and defraud unsuspecting individuals and organizations.

THE RISE OF AI-POWERED SCAMS

AI, with its ability to analyze vast amounts of data and mimic human behavior, has become a powerful tool for scammers. These perpetrators leverage AI tools to orchestrate sophisticated scams that are often difficult to detect and combat these schemes. One prominent example is the use of AI-generated deepfake content, where scammers use machine learning techniques to manipulate audio and video recordings, creating convincing but entirely fabricated content.

Specifically, AI voice cloning is on the rise. According to the computer security company McAfee, approximately 77% of AI voice scam victims lost money.[2] When we answer a phone and hear the voice of a loved one or close friend on the other end, we instantly know and trust that voice. It is reasonable to believe that if a loved one or close friend called, we would recognize their voice and speaking habits. However, according to McAfee, voice-cloning tools are capable of replicating how a person speaks with up to 95% accuracy.

We unknowingly give cybercriminals the data to replicate our voice and likeness. With the use of video-based social media platforms, such as TikTok, Instagram, and others, users unknowingly create a template for fraudsters to clone our voice and likeness. Based on a survey conducted by McAfee, in the United States, approximately 52% of adults share their voice at least once per week.[3] Cybercriminals now have access to specifically target individuals by cloning their intended target's voice, based on our own use of these social media platforms.

The rapid rise of AI and the advanced schemes from cybercriminals created the need for the Federal Trade Commission in 2023 to create a new division, the Office of Technology, specifically to identify and keep up with the advancements of AI and to maintain their ability to protect consumers.[4] The advancement of AI is generating enough noise and attention for the federal government to attempt to stay ahead.

MANIPULATING BEHAVIORAL DATA FOR FRAUDULENT PURPOSES

Deepfake technology and AI has been exploited in various ways, from impersonating public figures to creating fraudulent videos to trigger a panic. One example of how damaging and convincing AI has become is a deepfake viral photo circulating on the internet in 2023 showing the Pentagon in Washington D.C. on fire after an alleged explosion. This deepfake created a panic and a temporary dip in the stock market.[5] While this image was later determined to have been created by AI, the image was still convincing enough to cause panic and impact the stock market.

[1] https://www.hollywoodreporter.com/business/business-news/tyler-perry-ai-alarm-1235833276/
[2] https://www.mcafee.com/zh-tw/consumer-corporate/newsroom/press-releases/press-release.html?news_id=5aa0d525-c1ae-4b1e-a1b7-dc499410c5a1
[3] https://www.mcafee.com/content/dam/consumer/en-us/resources/cybersecurity/artificial-intelligence/rp-beware-the-artificial-impostor-report.pdf
[4] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work
[5] https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai

Additionally, deepfake technology can be convincing and seemingly real enough to have an employee of a company to send millions of dollars to cybercriminals. An employee at a multinational firm received an email seemingly from the company's Chief Financial Officer (CFO), to send a large sum of money in an unusual transaction. Rightfully so, this request raised some red flags to the employee, and it was thought of as a standard phishing email. However, the employee subsequently joined a video conference call with the "CFO" and "other members of staff" that the employee recognized based on their looks and the way they sound. After the video conference call, the employee felt comfortable to proceed with the unusual transaction. However, the alleged CFO and staff members that the employee spoke to were all part of an AI deepfake operation. The employee was convincingly duped to send approximately $25 million to the cybercriminals.[6]

AI CAN BE A CPA'S POWER TOOL

With the rise of cybercriminals using AI and the tools available for their own personal gain, these same tools can be used by accountants and CPAs to assist with their day-to-day tasks. Some of the benefits associated with AI for CPAs and accountants, include bookkeeping automation, client communication, data analysis and fast tax research.[7] According to a study from the University of Pennsylvania, approximately 24% of top-performing client advisory services are using AI in their practices.[8] As AI continues to advance it will be reasonable to assume that more accounting and CPA firms will use AI in their practices.

SAFEGUARDING AGAINST AI-POWERED SCAMS

In considering the benefits of AI and accounting, here are some tips and good practices that should also be considered to protect ourselves from AI-powered scams:[9,10,11]

- **Set your social media pages to private:**
  - Do not accept profiles or connections you do not know.
- **Be mindful of what you post:**
  - AI-driven scams use our information posted on social media as a way to mimic their target.
- **Do not trust your caller ID:**
  - If you get a call from the "bank," "credit card company," "Internal Revenue Service," or other callers, hang up or decline the call. Wait for a voicemail, if any. Then look up the phone number, located on the back of your credit card, bank statement or other reputable source and call directly.
- **Do not be click happy:**
  - Do not click on a link in an email or text message without first verifying it is something you are expecting, and the sender is legitimate.
- **Using safe words with family:**
  - In the unfortunate event you receive a phone call from someone that is claiming to be a family member, utilize a safe word. In your inner circle, (i.e., parents, spouse, children) have a unique word that they can use to fully convince you that they are indeed your relative / loved one.
- **Implement anti-deepfake technology:**
  - There is technology that makes it more difficult for cyber criminals to steal your voice.[12]

[6] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/
[7] https://tax.thomsonreuters.com/blog/how-do-different-accounting-firms-use-ai/#:~:text=Bookkeeping%20automation%3A%20AI%2Dpowered%20software,of%20manual%20errors%20for%20firms.
[8] https://www.journalofaccountancy.com/news/2023/nov/how-artificial-intelligence-can-help-save-accounting.html
[9] https://states.aarp.org/arizona/chatbots-and-voice-cloning-fuel-rise-in-ai-powered-scams
[10] https://www.mcafee.com/blogs/family-safety/how-to-protect-your-family-from-ai-scams/
[11] https://www.cnbc.com/2024/01/24/how-to-protect-yourself-against-ai-voice-cloning-scams.html
[12] https://www.scientificamerican.com/article/how-to-keep-ai-from-stealing-the-sound-of-your-voice/

CONCLUSION

As technology continues to advance, we must adapt quickly to protect ourselves from the changing environment. The use of AI and the benefits that stem from it can be useful for businesses and people to enhance our daily routines. However, with the benefits of AI there will always be the opposite. As this technology continues to evolve, we must continue to stay at the forefront and not become victims to these schemes.

ACKNOWLEDGEMENTS

We would like to thank Jacob R. Hough, CFE, for providing insights and expertise that greatly assisted this research.

Jacob R. Hough, CFE, is a Senior Consultant in J.S. Held's Economic Damages & Valuations practice. Jake joined J.S. Held in January of 2024 as part of J.S. Held's acquisition of Forensic Resolutions, Inc. Jake has nearly a decade of experience quantifying economic claims in dispute. He has extensive experience analyzing financial and nonfinancial data, conducting thorough analyses, and assessing economic damages in personal injury, wrongful death, and commercial damages, among other areas. He has comprehensive experience determining economic damages in numerous jurisdictions throughout the United States.

Jacob can be reached at jacob.hough@jsheld.com or +1 856 433 6433.