Euler Hermes Group Deepfake Forensic Analysis

By **Kevin Lanier** (https://westoahu.hawaii.edu/cyber/author/kevinl7/) on February 6, 2025

Executive Summary

In March of 2019, an unnamed company involved with Euler Hermes had $243,000 stolen from them by scammers who used a deepfake of the CEO to convince the company's leadership to wire the money to "his" account. The company was able to partially mitigate this through its Euler Hermes fraud insurance, updating its cybersecurity awareness and verification procedures as well as collaborating with law enforcement. The best practice in this situation would have been to have proper verification checks in place to stop the employees from getting to the point where they had clearance to transfer the money.

Background

An unnamed German energy company received a call from their CEO demanding an immediate transfer of $243,000 to an account of his in Hungary. [1] Several officials said the voice-spoofing attack in Europe is the first cybercrime they have heard of in which criminals clearly drew on AI.[2] AI is changing the world around us, and it's apparent that cybersecurity professionals will have an entirely new list of risks to consider because of it.

A deepfake is a specific type of synthetic media in which a person in an image or video is swapped with another person's likeness. [3] This can be a huge issue for companies who are unfamiliar with or unprepared to address the technology. A 2023 McAfee survey revealed that 70% of those involved said they weren't confident they could tell the difference between a cloned voice and a real one. [4] Alongside this, a statistic from security.org states that more than 10 percent of companies have dealt with attempted or successful attempts at deepfake fraud and the damages reached as high as 10 percent of the companies' annual profits. [5]

Impact

A deepfake scam can happen to any company, even a small family owned business. In fact, smaller companies with less familiarity with the technology are better targets for scammers than a company with a dedicated cybersecurity team. Deepfakes can be incredibly convincing and are anticipated to improve in quality with time. Technology is quickly advancing to the point where deepfakes will be able to respond to human speech and answer questions using known information about the individual. This readily available information gathered by simple reconnaissance methods such as checking the company's website or social media accounts. could allow the AI to pass verification checks and make important decisions regarding money or sensitive information.

Mitigation

In order to mitigate the risks of deepfakes, two methods of mitigation can be implemented by companies. The first method would be to implement and improve verifications needed for decisions involving money or sensitive information to be made at the company. Organizations could also implement software mitigation. According to NPR, Pindrop Security, AI or Not and AI Voice Detector all have deepfake audio detection tools which they claim are over 90% accurate at differentiating between real audio and AI-generated audio. [6] Although deepfakes will improve, so will the software used for detecting it. Adopting this technology is a great way for a company to layer its protection against deepfakes.

Relevance

Companies need layered protection against deepfake-based fraud. AI is rapidly improving and will only become more and more successful at stealing money and information from companies unless they have proper safeguards. Requiring the CEO to answer several security questions as well as providing sensitive information only they would be privy to hinders scammers from reaching their goal, further reducing risk . Deepfake detection software will also be valuable going forward because it will be able to flag potentially fraudulent videos, before suspicion is even required from employees.

References

[1] Perallis, J. (2019, September 3). Bandits Steal $243,000 With Deepfake Audio Mimicking CEO Voice. *Perallis*. **https://www.perallis.com/blog/bandits-steal-243-000-with-deepfake-audio-mimicking-ceo-voice** (https://www.perallis.com/blog/bandits-steal-243-000-with-deepfake-audio-mimicking-ceo-voice)

[2] Stupp, C. (2019, August 30). Fraudsters Use AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal*. **https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402** (https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402)

[3] Roth, E. (2020, January 7). Deepfakes, Explained. *MIT Sloan*. **https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained** (https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained)

[4]McAfee. (202#, Month #). **Artificial Imposters: Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam**. *McAfee Blog*. **https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/** (https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/)

[5]Security.org. (202#, Month #). **Deepfake Statistics**. *Security.org*. **https://www.security.org/resources/deepfake-statistics/#citations** (https://www.security.org/resources/deepfake-statistics/#citations)

[6] Chang, A. (2024, April 5). Deepfake Audio Detection. *NPR*. **https://www.npr.org/2024/04/05/1241446778/deepfake-audio-detection** (https://www.npr.org/2024/04/05/1241446778/deepfake-audio-detection)

RELATED POSTS

Forensic Challenges in Detecting Sniffing Attacks
10/24/2025
(https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/forensic-challenges-in-detecting-sniffing-attacks/)

Velociraptor Ransomware Forensic Analysis
10/17/2025
(https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/velociraptor-ransomware-forensic-analysis/)

RacoonO365 Forensic Analysis
10/10/2025
(https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/racoono365-forensic-analysis/)