**Case Study: The Rise of Deepfake Attacks in Corporate Fraud**

**Introduction**

Deepfake technology, once a novelty, has rapidly evolved into a serious cybersecurity threat. By using artificial intelligence to manipulate audio and video, attackers can convincingly impersonate trusted individuals, leading to significant financial and reputational damage for businesses. This case study examines two high-profile deepfake scams that showcase the growing risk of deepfakes in corporate fraud, highlighting the techniques used and the lessons businesses can learn to protect themselves.

**Scenario 1:** [**Deepfake Audio CEO Fraud – A UK Company Loses $243,000**](https://www.trendmicro.com/vinfo/au/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company)

In a notable case from March 2019, a U.K.-based energy company fell victim to a sophisticated deepfake audio attack that resulted in the loss of USD $243,000. According to *Trend Micro*, attackers used AI to clone the voice of the company’s CEO and impersonated him over a phone call. The fraudster, mimicking the CEO’s voice with near-perfect accuracy, instructed the company’s finance director to urgently transfer funds to a Hungarian supplier.

The finance director believed the request was legitimate due to the strikingly accurate voice reproduction, including the tone, accent, and mannerisms of the CEO. Following the CEO’s "instructions," the finance director transferred the funds as requested, believing it was a routine business transaction.

Only after the funds were transferred did the company realise that the call was a deepfake, and the real CEO had no knowledge of the transaction. The money was immediately sent to a series of bank accounts in different countries, making it impossible to recover. This incident highlighted how deepfake technology can be weaponised to bypass traditional trust mechanisms and trigger large-scale financial fraud.

**Scenario 2:** [**Deepfake CFO Scam in Hong Kong – $25 Million Loss**](https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html)

A more recent and devastating example took place in Hong Kong in 2024, as reported by *CNN*. In this case, cybercriminals used deepfake technology to impersonate the Chief Financial Officer (CFO) of a large corporation. By cloning the CFO’s voice, attackers managed to convince another senior executive to transfer $25 million to a fraudulent account, believing it was part of an urgent business transaction.

The criminals orchestrated the scam using a combination of deepfake audio and hacked email communications. The senior executive received a phone call from what seemed to be the CFO, requesting the large transfer to finalise an important acquisition. The fake CFO’s instructions were reinforced by carefully timed emails that aligned with the company’s ongoing operations, further legitimising the request.

As with the U.K. case, the deepfake technology was so convincing that the senior executive had no reason to doubt the legitimacy of the call. By the time the fraud was discovered, the funds had been transferred through multiple offshore accounts, making recovery impossible.

**Tactics and Techniques of Deepfake Scams**

In both cases, attackers used deepfake audio technology to impersonate high-ranking executives and orchestrate fraudulent wire transfers. Deepfake audio is created using AI algorithms that analyse voice recordings of a target, allowing the attackers to reproduce the person’s speech patterns, tone, and accent with remarkable accuracy.

The success of these scams also relied on the attackers' deep understanding of the companies they targeted. In the Hong Kong case, the criminals had gained access to internal communications, likely through email phishing or another form of data breach. This allowed them to time their attacks perfectly, aligning with the company’s ongoing operations and avoiding suspicion.

Additionally, the use of deepfake technology, combined with phishing or insider knowledge, enables criminals to bypass traditional authentication methods, such as recognising a voice on the phone or relying on an email’s content. This makes deepfakes particularly dangerous, as they exploit human trust and familiarity in ways that conventional cyberattacks do not.

**Lessons Learned: Protecting Against Deepfake Attacks**

These deepfake scams highlight the urgent need for organisations to strengthen their defences against voice-cloning and deepfake technology. According to the *SANS Institute*, businesses should consider the following steps to mitigate the risk of falling victim to similar attacks:

1. **Implement Multi-Factor Authentication (MFA)**Relying solely on verbal instructions or email authorisation is no longer sufficient. Organisations should require multi-factor authentication (MFA) for any sensitive financial transactions, ensuring that additional layers of verification are in place before funds can be transferred.
2. **Use Code Words or Specific Verification Procedures**To counter the threat of deepfake audio, companies can establish specific code words or unique questions that are only known between executives, especially for urgent or high-value transactions. This extra layer of verification can help differentiate between legitimate requests and fraudulent ones.
3. **Raise Employee Awareness**Cybersecurity training should now include information about the potential risks posed by deepfake technology. Employees must be made aware that convincing audio and video impersonations can occur and that unusual requests for transfers or sensitive information should always be verified through multiple channels.
4. **Monitor Unusual Activity**AI-powered tools can also be used to detect anomalies in communication or financial behaviour. For example, sudden or unusual requests for large financial transfers can be flagged and investigated before being processed.
5. **Limit Public Availability of Voice Data**Executives, especially those in high-risk roles such as CEOs and CFOs, should limit the amount of publicly available voice data that could be used to create deepfakes. Minimising public speaking engagements or ensuring that voice recordings are not easily accessible can reduce the risk of becoming a target.

**Conclusion**

The cases of deepfake audio fraud against the U.K. energy company and the Hong Kong corporation underscore the significant threat that deepfake technology poses to businesses. By combining AI-driven voice cloning with social engineering, attackers can manipulate trust and exploit vulnerabilities in traditional business processes.

Organisations must recognise that deepfakes are not just a theoretical concern but a growing and real threat in the cybersecurity landscape. Implementing stronger authentication measures, training employees, and staying vigilant for unusual behaviour are crucial steps in defending against these highly sophisticated attacks. As deepfake technology continues to advance, businesses must adapt their security protocols to stay ahead of cybercriminals and protect their assets from future deepfake fraud attempts.