The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE RISE OF CYBERCRIMES WITH AI: DEEPFAKES

~Aaysha Khan

With the rapid advancement of AI and machine learning, we have reached some great milestones, implementing technology in medical sciences and data driven business decisions. However, we have also delved deeper into a new horizon of scams and frauds such as video deepfakes and voice phishing.

The Deepfakes enabled fraud made up 11% of all fraud globally in 2025. One such case was the Arup deepfake scam that cost the Hong Kong based company 25 million dollars, because of a video deepfake when fraudsters impersonated the company CFO, hence tricking the employee to transfer funds. In 2026, Deepfake attacks are now linked to 1 in 5 biometric fraud attempts. In business, 41% of organizations experienced a deepfake combined with social engineering on an audio call and 35% on a video call. While in case of fraud and scams, the statistics show 46% of fraud experts have encountered synthetic identity fraud, 37% voice deepfakes, and 29% video deepfakes.

The word deepfake is derived from the combination of the word “deep” referring to deep learning and “fake”. Deepfake as a technology is referred to as synthetic (altered) media is any content, such as audio, images, or video, created by artificial intelligence which includes deepfakes or “the manipulation of existing media (image, video, and/or audio) or the generation of new (synthetic) media using Deep Learning -based approaches. The most commonly discussed deepfake data are fake face images, fake speech forgeries, and fake videos that combine both fake images and fake speech forgeries”.

These trigger safety issues not only for high profit businesses but also common people that are the target for AI scams.

One of the most prevalent dangers of it today is the generation of fake biometric data and media forensics. Deepfakes specifically target the verification processes that organizations rely on: a voice on a phone call, a face in a video meeting, or an email.

The number of deepfake files has grown from approximately 500,000 in 2023 to an estimated 8 million in 2025, as reported by Cybersecurity Drive.

Previously done only by mimicking a person's voice over phone call, by using their publicly available data to trick the victims into sending money or divulging sensitive information, usually in a panicked distressed voice to induce urgency.

The danger is heightened with the ease of technology as a scammer can easily use a short video from 3 to 10 second clip on social media to produce a convincing video call with little to no programming experience. Similar to voice phishing scams, that require real voice samples from an audio, there are deepfake videos that require sample images and videos to make realistic deepfakes.

Considering prevalence in sharing voice notes, recording as well as posting videos on YouTube and sharing reels on social media, gives easy access to people hoping to trick. Messages can vary from a related person stating they've been in a car accident or lost their phone and wallet.

People who have reported losing money, 36% said they lost between $500 and $3000 while 7% reported a sum of anywhere between $5000 and $15000. In a scenario of bank verification with KYC, the scammers can impersonate higher ranking bank officials or even law enforcement officers to obtain OTP for bank account actions.

While financial fraud is currently the most prevalent and damaging type of deepfake scam by bypassing biometric security and impersonation, others also include Elder scam (tricking elderly/ grandparent), Romance scams, Fake celebrity/Influencer interaction that can lead to loss of finance.

Some subtle signs for detecting a scam include: -

- Robotic or flat tone of voice.
- Weird pauses, unnatural tone or breakage.
- Not able to answer a new question differently or repeated/same response to altered question
- Unrealistic blinking and breathing patterns
- Edge of faces or hair might seem blurry, distorted and may glitch
- Face seems to have different lighting, or varied colouring as compared to background and surroundings

There have been significant focus and efforts to combat and differentiate deepfake and figure solutions on an organisational level.

In the Indian context of laws, On 10th February, 2026, the Government strengthened the regulatory framework by amending the IT Rules, 2021 to address harms arising from synthetically generated information (SGI), including deepfakes and AI-generated content.

The deepfake detection initiatives include:

- Saakshya, multi-agent framework developed by IIT Jodhpur & IIT Madras for deep fake detection
- AI Vishleshak for improving Audio-Visual forgery detection system
- IIT Kharagpur's project on Real-Time Voice Deepfake Detection System

In spite of the government initiatives, one needs to be alert and equipped with awareness to combat such unfortunate scenarios as precaution is better than cure. Protecting yourself can include establishing codewords with family, and friends in case of emergency situations, or asking questions only they would know based on recent scenarios, not giving into panic and rather verifying the request or call by calling the person with a different number or message app is good practice as well.

Citations

- Enes Altuncu et al., *Deepfake: Definitions, Performance Metrics and Standards, Datasets, and a Meta-Review*, 7 Frontiers in Big Data 1 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11408348/.
- Amy Bunn, *Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam*, McAfee Blog (May 15, 2024), https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/.
- Catherine Chipeta, *Deepfake Statistics 2026: Key Facts for CFOs and Finance Leaders*, Eftsure (July 9, 2026), https://www.eftsure.com/statistics/deepfake-statistics/.
- Jayachander Reddy Kandakatla, *Deepfakes and Digital Safety: A Citizen's Guide to AI Scams*, Vikaspedia (Jan. 24, 2026), https://en.vikaspedia.in/viewcontent/education/science-and-technology/deepfakes-and-digital-safety-a-citizen%E2%80%99s-guide-to-ai-scams?lgn=en
- *A Guide to Deepfake Scams and AI Voice Spoofing*, McAfee (2024), https://www.mcafee.com/learn/a-guide-to-deepfake-scams-and-ai-voice-spoofing/.
- Nadia Naffi, *Deepfakes and the Crisis of Knowing*, UNESCO (2025), https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing.
- Srini Tummalapenta, *How a New Wave of Deepfake-Driven Cyber Crime Targets Businesses*, IBM: Think Insights (2024), https://www.ibm.com/think/insights/new-wave-deepfake-cybercrime.

- *What Is a Deepfake?*, Proofpoint (2026), https://www.proofpoint.com/us/threat-reference/deepfake.
- Press Info. Bureau, Gov't of India, Ministry of Electronics & IT, Press Release No. 2295500, Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes (Aug. 6, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295500&reg=48&lang=2.