INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC

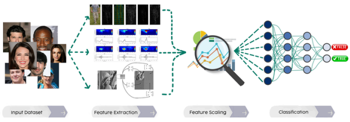
DOI No. 10.5281/zenodo.17083981

AUGUST 2025

CYBER BULLETIN

CEO Deepfakes Rising

Deepfakes: AI Posing Risks 1.

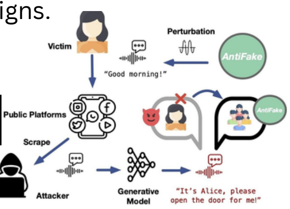


GANS (DEEP LEARNING)

TARGET: Government, Businesses and the general public domain.

IMPACT: Misinformation, election manipulation, political instability, financial fraud, scams, and erosion of trust in digital content.

MITIGATION: AI-based detection tools, strict regulations, global policies and public awareness campaigns.



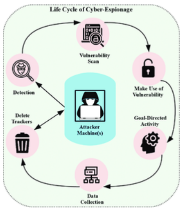
Deepfake CEO Scams 3.

AI VOICE

TARGET: Corporate employees, especially finance and IT staff.

IMPACT: Financial losses, data breaches, reputational damage and erosion of trust in this single scams can cost millions.

MITIGATION: Employee training on red flags, multi-step verification for sensitive requests and AI-based detection plus multi-factor authentication.



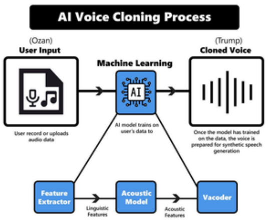
Geopolitical Cyber Espionage 5.

CREDENTIAL THEFT

TARGET: Energy and critical infrastructure sectors, including government and industrial networks in Europe and South Asia.

IMPACT: Loss of confidential data, operational risk to critical infrastructure, and long-term strategic intelligence compromise.

MITIGATION: Restrict VPN use to approved apps. Regularly rotate and monitor privileged credentials. Deploy EDR to detect unusual VPN activity and train users on risks of unauthorized VPN tools.


AI Voice Cloning Process
(Ozan)
User Input
Machine Learning
(Trump)
Cloned Voice
AI
User record or uploads audio data
AI model trains on user's data to
Once the model has trained on the data, the voice is prepared for synthetic speech generation
Feature Extractor
Linguistic Features
Acoustic Model
Acoustic Features
Vacoder

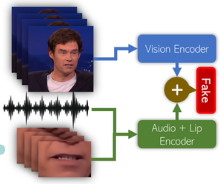
CEO Impersonation Scams 2.

AI VOICE CLONING

TARGET: Corporate executives (CEO, CFO, senior leaders), finance teams, IT admins and employees with privileged access.

IMPACT: $200M+ financial losses, legal exposure from data breaches and reputational damage from loss of trust.

MITIGATION: Apply Microsoft's July 2025 patch. Restrict SharePoint access to internal/VPN networks.



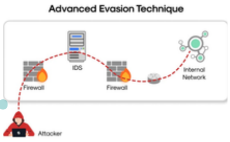
Multimodal Deepfake Fraud 4.

COMBINED AI-GEN CONTENT

TARGET: Employees and the public, vulnerable to complex fraud scenarios.

IMPACT: High risk due to tech gap—human detection accuracy is low (images ~62%, videos ~24.5%), AI detection can lose up to 50% accuracy in real-world cases.

MITIGATION: Employee and public training to spot inconsistencies, human-centric awareness programs, and continuous education alongside technical defenses.



Ransomware Resurgence 6.

DETECTION EVASION

TARGET: Healthcare, logistics and government organizations

IMPACT: Systems encrypted and sensitive data leaked ransom demands between $5M–$15M. Some campaigns used exfiltration-only tactics skipping encryption to evade detection.

MITIGATION: Maintain offline backups and test recovery. Network Segmentation to isolate critical assets. Use AI Detection for anomaly and exfiltration monitoring

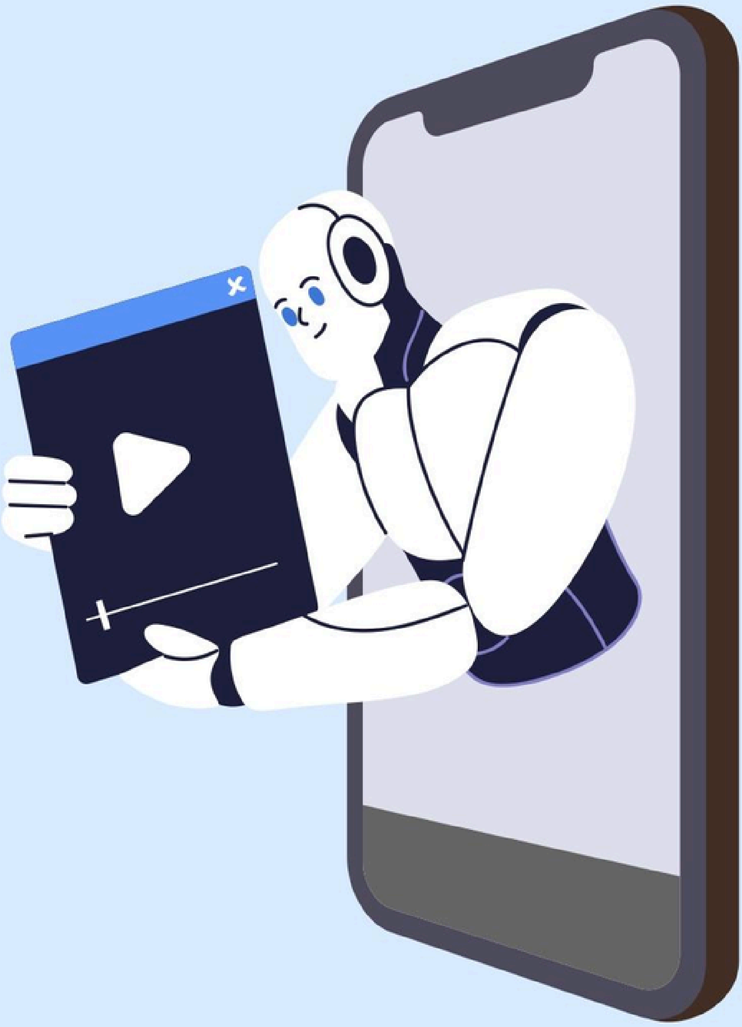
इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

iSEA
www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

CYBER SECURITY

POSTER OF THE DAY



Stay alert for AI-generated deepfake videos and voice scams

Fraudsters now use advanced AI to convincingly mimic loved ones or officials

Making verification through a second channel is essential

#Deepfake
#VoiceScam
#AIFraud

Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

myGOV
मेरी सरकार

Indian Cyber Crime Coordination Centre

सी-डैक
CDAC

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
ANAMTA ANSARI | AREEBA KHAN | ANWAR AHMAD

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application