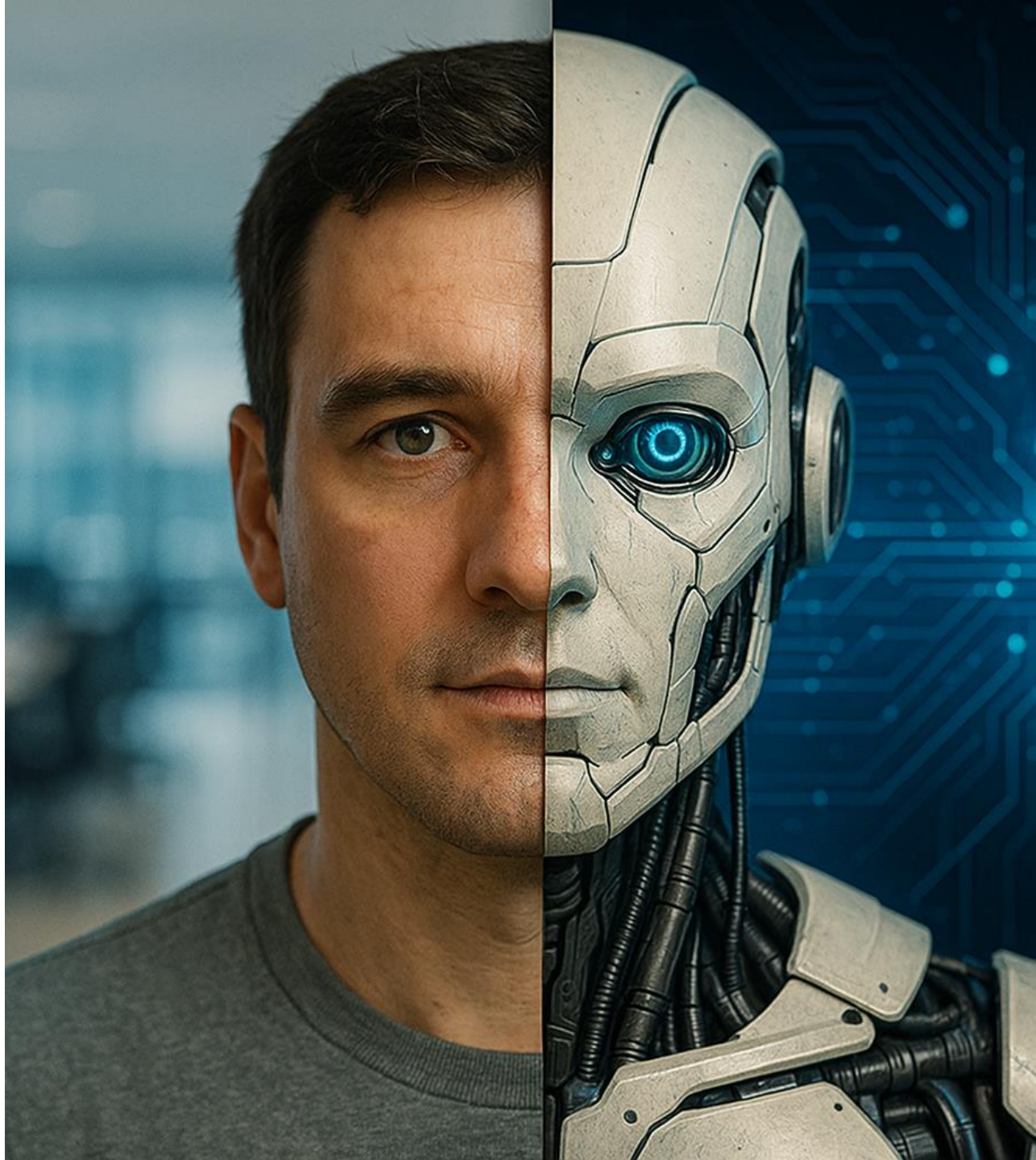
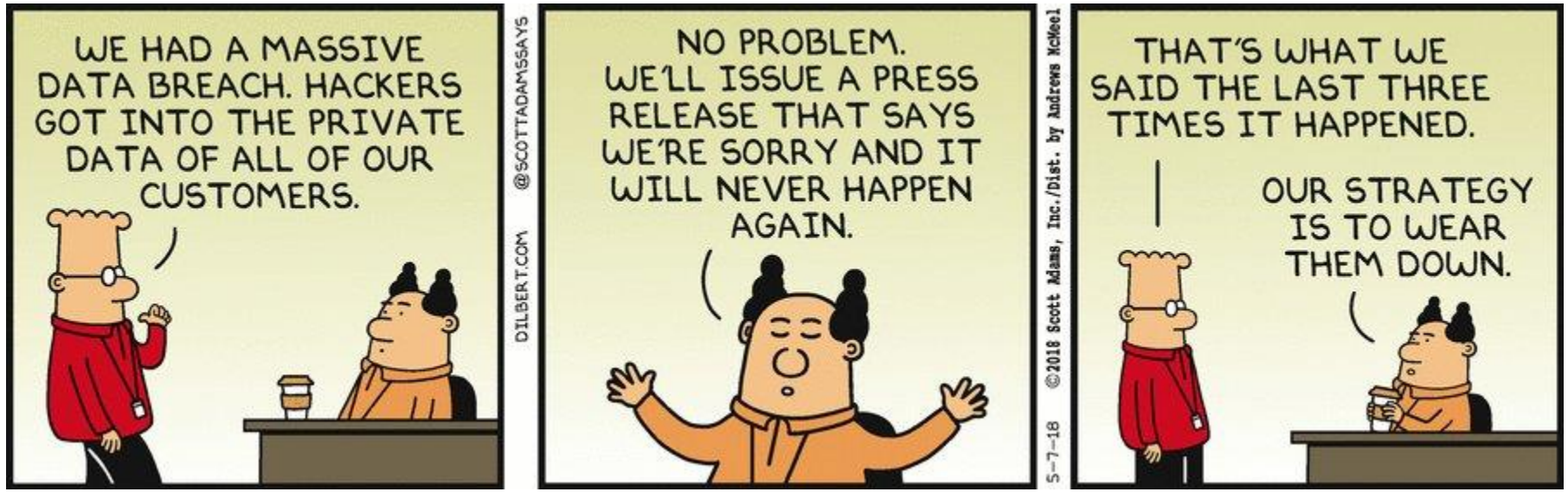
Deepfake 101: How to create and spot deepfakes



Fred Kwong, Ph.D - DeVry University, CISO

Disclaimer

This presentation and statements herein constitute the views and options of the speaker alone and are not to be construed or interpreted as views and opinions of any other source, including any company or organization with which the speaker is employed or affiliated in any manner.



About Me

CISO
10 Years

SECURITY
25 Years

IT
28 Years

Finance, Manufacturing, Telcom, Education, Insurance, Technology

About DeVry

DeVry University

1931
Founding
DeForest's Training School opens to prepare students for careers in electronics, film and radio.

1955
Accreditation
Associate degree program in Electronics Engineering Technology earns TAC of ABET accreditation.

1998
Online Pioneer
DeVry begins offering online programs, extending access to learners everywhere.

2002
University Era
DeVry Institute and Keller Graduate School merge to become DeVry University.

2025
Modern Milestones
New brand identity launches, and tuition freezes for the sixth year demonstrate commitment to students.

Cybersecurity Learning

Stackable Pathways
Certificates, associate, bachelor's, graduate certificates, MBA and master's programs build on one another.

Cutting-Edge Curriculum
Topics span AI fundamentals, ethical hacking, incident response and cloud security.

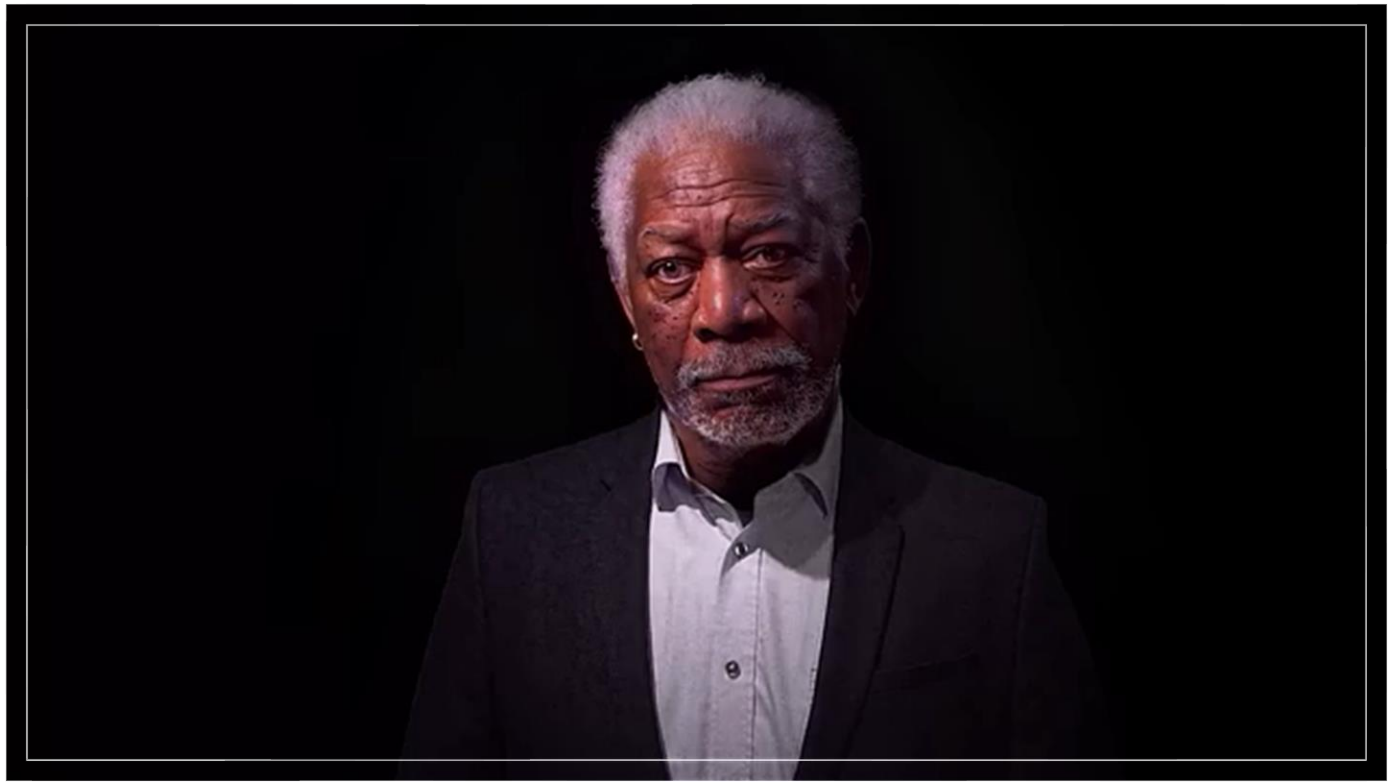
Hands-On Training
Experience immersive simulations in our cyber range and Cyber Skills Training Platform.

Recognition & Certs
NICCS/CAE-C/HLC designations and courses that prepare you for Security+, CEH, CISA & more.

Deepfakes

What is a Deepfake?

A deepfake is an image, video, audio recording, or text that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.



Why should we care about deepfakes?

$1.33

The average cost of creating a deepfake

Cost for malicious actor to reach 100,000 social media users

$0.07

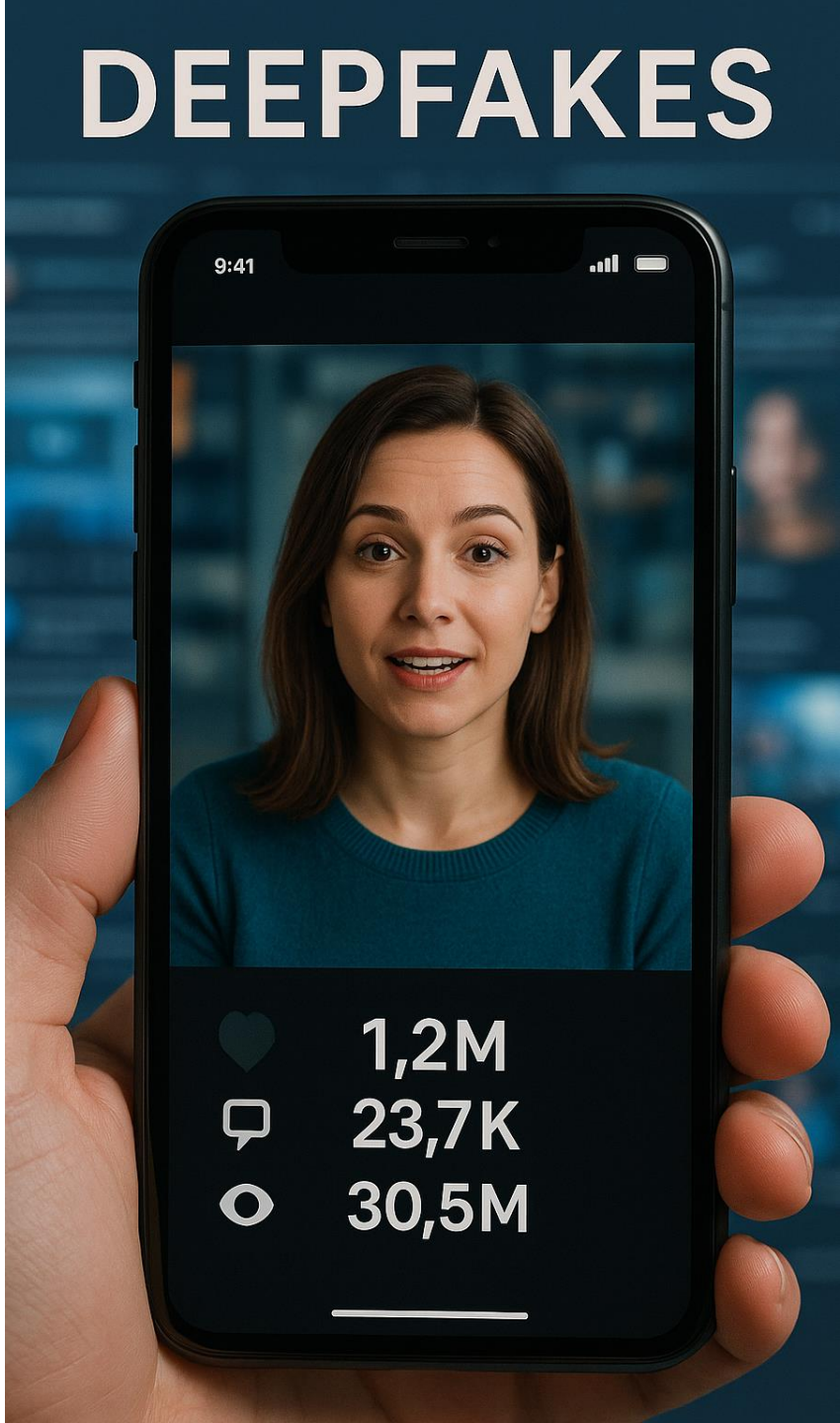
The World Economic Forum's Global Risks Report 2024 ranks AI-fueled disinformation as the **number one** threat the world faces in the next two years.

$1,000,000,000,000

Expected global cost of deepfake fraud in 2024

How bad is it?

Statistic/Fact	Value/Percentage
Deepfake video growth (2019–2024)	+550%
Total deepfake videos (early 2025)	95,820
Deepfake incidents increase (Q1 2025 vs. 2024)	+19%
Consumers encountering deepfakes (last year)	60%
Deepfake fraud as % of all fraud (2025)	6.5%
Companies/consumers victimized by deepfakes	40%
Human detection accuracy	~50%



Weaponized deepfakes

60 MINUTES - NEWSMAKERS ›

How con artists use AI, apps, social engineering to target parents, grandparents for theft

60

BY SHARYN ALFONSI
UPDATED ON: AUGUST 27, 2023 / 7:08 PM / CBS NEWS

CNN World Africa Americas Asia Australia China Europe India More

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 min read · Published 2:31 AM EST, Sun February 4, 2024

BUSINESS INSIDER

A couple in Canada were reportedly scammed out of $21,000 after getting a call from an AI-generated voice pretending to be their son

Britney Nguyen
March 6, 2023 · 3 min read

Reuters World Business Markets Sustainability Legal Commentary Technology Investigations

Brazilian scammers, raking in millions, used Gisele Bundchen deepfakes on Instagram ads

By **Debora Ely**
October 3, 2025 6:42 PM CDT · Updated October 3, 2025

Aa

A.I. Audio

https://cybernews.com/security/how-ai-voice-cloning-threatens-th

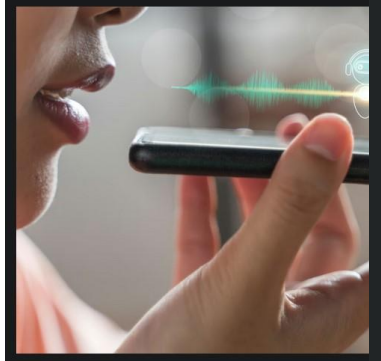
cybernews® News Editorial Security Privacy Crypto Tech Resources Tools Reviews Follo

Home » Security

How AI voice cloning threatens the security of bank systems

Updated on: 09 March 2023

Neil C. Hughes, Contributor



By Shutterstock

https://www.pcgamer.com/anger-from-voice-actors-as-nsfw-mods-use-ai-deepfakes-to-replicate-their-vo

News > Skyrim

Anger from voice actors as NSFW mods use AI deepfakes to replicate their voices: 'This is NOT okay'

By Harvey Randall published July 06, 2023

Skyrim VAs are speaking out about the spread of pornographic AI mods.

THE WALL STREET JO

English Edition ▾ | Print Edition | Video | Audio | Latest Head

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts

PRO CYBER NEWS

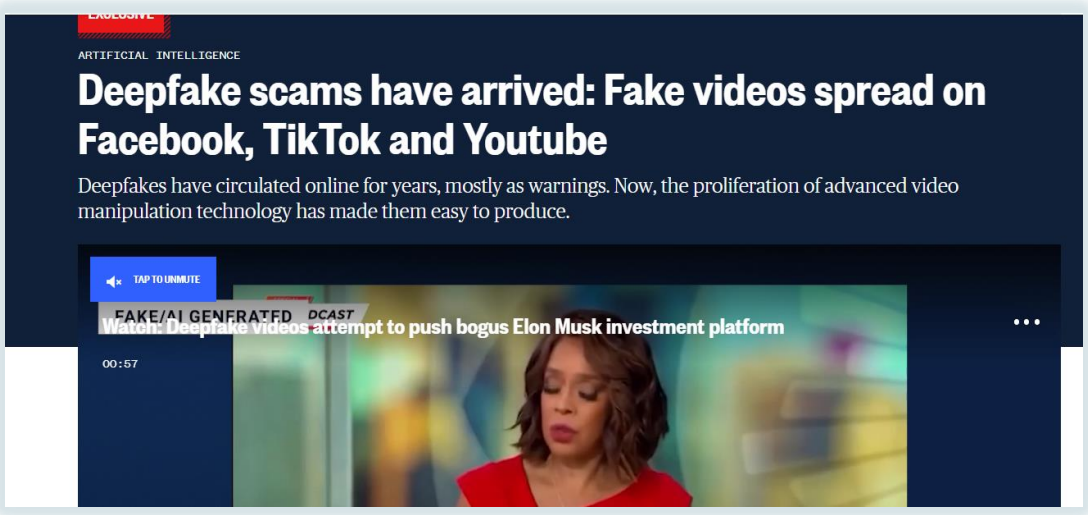
Fraudsters Used AI to Mimic CEO's Voi Cybercrime Case

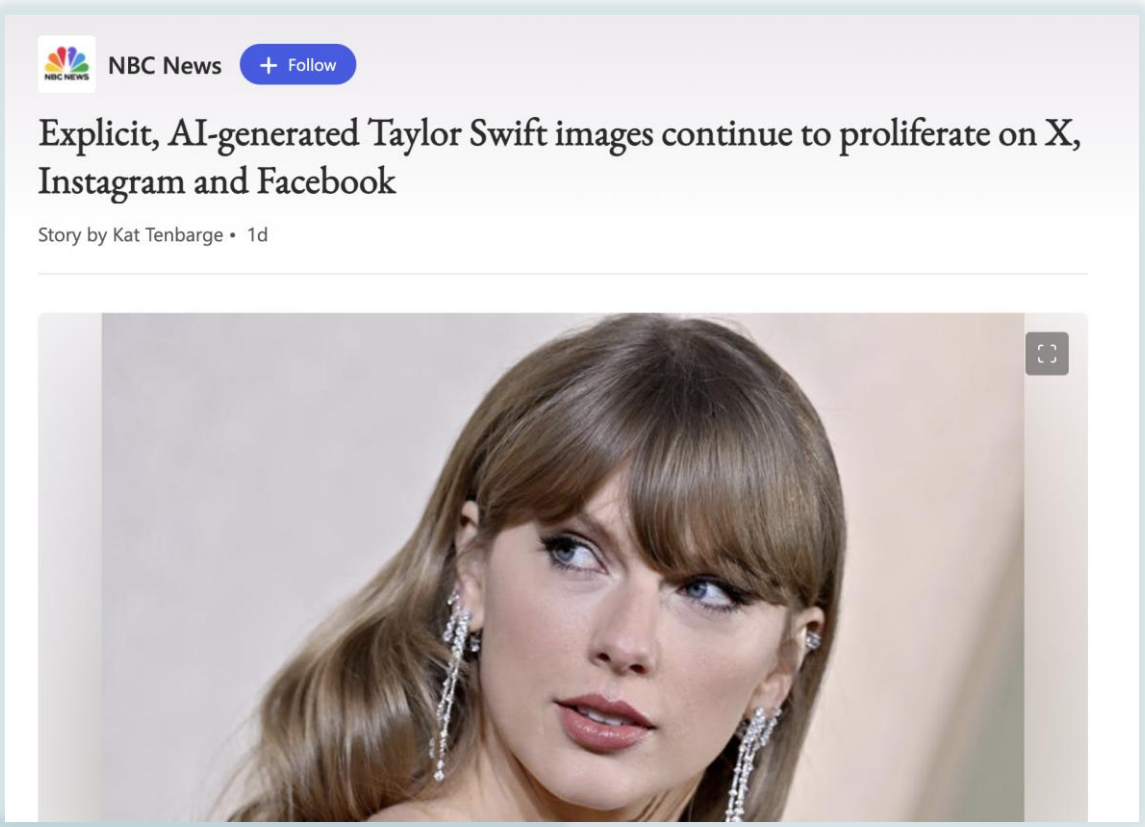
Scams using artificial intelligence are a new challenge for companies

Biden robocall tells New Hampshire Democr te Tuesday

ent imitation or digital manipulation of the president's voice, says, "Voting this Tuesday onl licans in their quest to elect Donald Trump again."

A.I Video Disinformation Campaigns






Deepfakes
2025

How Has Deepfake Tech Changed in the Last Year?

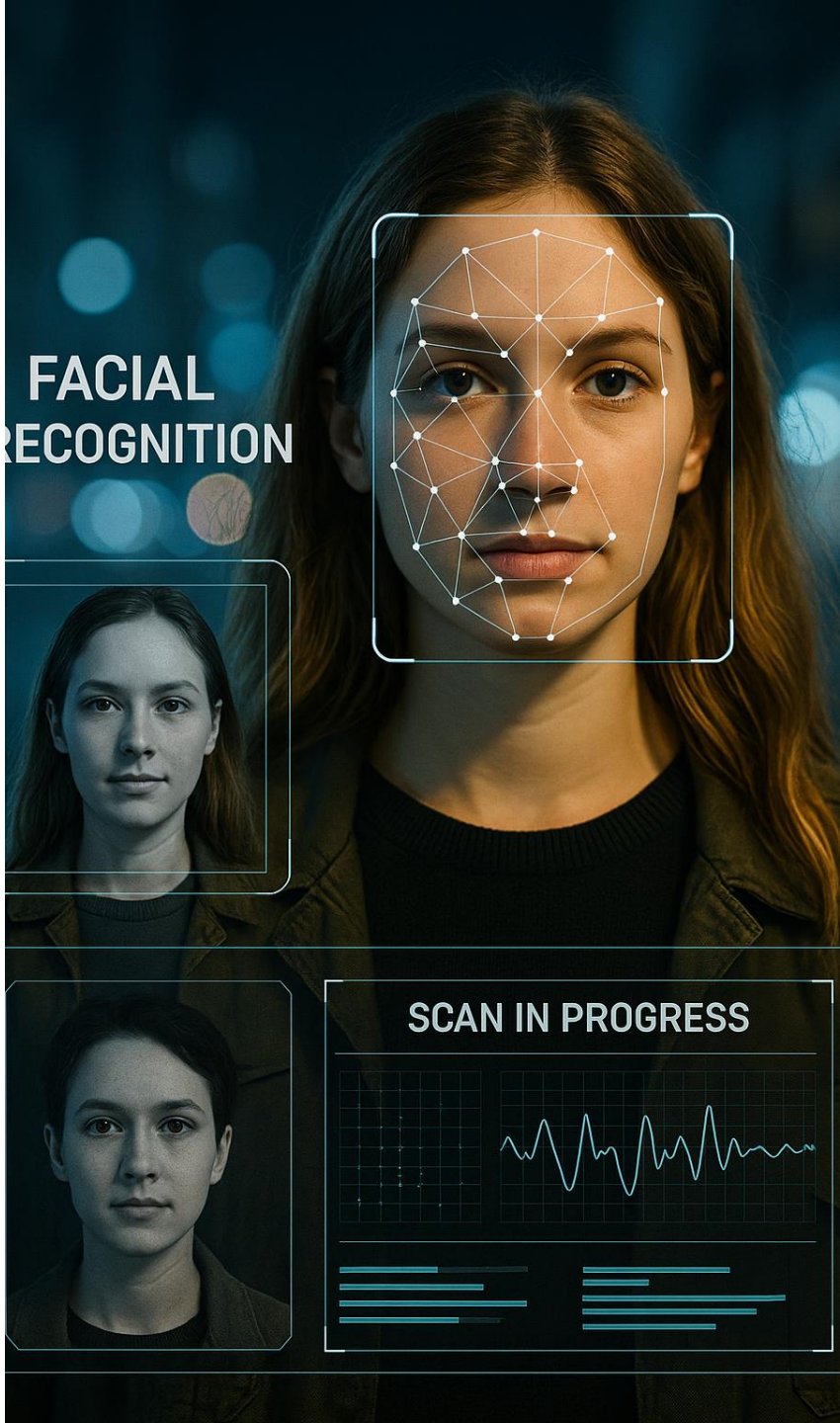
Enhanced Realism:
New models replicate subtle facial expressions, micro-movements, and emotional inflections, making detection by humans extremely difficult

Full-Body and Multimodal Synthesis:
Not just faces – now includes full-body gestures, synchronized audio, and even text manipulation

Real-Time Generation:
Live deepfake creation is now possible, enabling real-time video/audio manipulation in calls and streams

Accessibility:
User-friendly, open-source, and cloud-based tools have democratized deepfake creation

Adversarial Advances:
Deepfakes are now designed to evade detection tools, using adversarial machine learning



State of Deepfakes

Prevalence

- **+550% growth** in deepfake videos from 2019 to 2024; **95,820 videos** by early 2025
- **19% more incidents** in Q1 2025 than all of 2024
- **60% of consumers** have encountered a deepfake in the last year; only 15% have never seen one

Types & Targets

- **Fraud/Scams:** 31% of incidents; 6.5% of all fraud cases now involve deepfakes
- **Victimization:** 40% of companies and consumers have been targeted
- **Industries hit hardest:** IT (57%), law enforcement (56%), crypto (53%)

Impact

- **Financial:**
  - $25 million lost in a single deepfake voice scam (Arup, 2024)
- **Reputational:**
  - Celebrity and political deepfakes erode public trust and cause PR crises
- **Detection Difficulty:**
  - Human detection accuracy is barely above chance (~50%)
- **Public Trust:**
  - 68% of those familiar with generative AI are concerned about being deceived; 59% struggle to distinguish real from fake


Deepfake
Creation
(Demo)

Spotting Deepfakes

Pay attention to the face. High-end DeepFake manipulations are almost always facial transformations.

Pay attention to the cheeks and forehead. Does the skin appear too smooth or too wrinkly? Is the agedness of the skin similar to the agedness of the hair and eyes? DeepFakes may be incongruent on some dimensions.

Pay attention to the eyes and eyebrows. Do shadows appear in places that you would expect? DeepFakes may fail to fully represent the natural physics of a scene.

Pay attention to the glasses. Is there any glare? Is there too much glare? Does the angle of the glare change when the person moves? Once again, DeepFakes may fail to fully represent the natural physics of lighting.

Pay attention to the facial hair or lack thereof. Does this facial hair look real? DeepFakes might add or remove a mustache, sideburns, or beard. DeepFakes may fail to make facial hair transformations fully natural.

Pay attention to facial moles. Does the mole look real?

Pay attention to blinking. Does the person blink enough or too much?

Pay attention to the lip movements. Some deepfakes are based on lip syncing. Do the lip movements look natural?

AI Detection Capabilities

Trust as a Service:

1. Pixel Level Analysis
2. Audio Waveform Analysis
3. Metadata Analysis

AI Detection Providers:

Deepware Scanner – scanner.deepware.ai
Sightengine - sightengine.com/detect-deepfakes
Deep Fake Detector - deepfakedetector.ai
Sensity - https://sensity.ai/

Deepfake Countermeasures

AI-Based Detection:
Machine learning models analyze facial, vocal, and behavioral cues; current tools claim >90% accuracy for many deepfakes

Digital Watermarking & Metadata:
Embedding cryptographic metadata at content creation for provenance tracking

Content Authentication Standards:
Adoption of C2PA and similar standards for cross-platform verification

Biometric & Behavioral Analysis:
Analyzing blood flow, micro-expressions, and vocal inflections to spot fakes

Multi-Factor Authentication (MFA):
Extra verification for sensitive transactions and communications.