

Risk Alert

Meaningful. Actionable. Timely.

May 20, 2024

Deepfakes in Higher Education

Deep fake technology, which employs advanced artificial intelligence and machine learning algorithms, is capable of producing highly realistic and difficult to detect audiovisual forgeries. These technologies can manipulate or generate video and audio recordings that falsely depict people saying or doing things they never did. In the context of higher education, the implications of this technology are particularly profound, encompassing academic, operational, reputational, legal and ethical, and social and psychological risks. Given these multifaceted risks, it is imperative that our management, faculty and staff understand the risks associated with deepfakes and methods they can employ to detect deepfakes.

Academic Risks:

Deep fakes can be used to create fraudulent academic presentations, research materials, or even entire lectures that could deceive students, faculty, and external academic bodies. This threatens the foundation of academic integrity and truth, pillars upon which educational institutions stand.

Operational Risks:

On the operational front, deep fakes could be employed in sophisticated cyber-attack strategies such as spear phishing. By impersonating trusted figures within the university, attackers could obtain unauthorized access to sensitive areas of the university's administrative and financial systems. Furthermore, these technologies could be used during negotiations or decision-making processes to mislead or manipulate outcomes.

Reputational Risks:

From a reputational standpoint, the misuse of deep fake technology can lead to severe consequences. For instance, a convincingly altered video of a university official could rapidly spread misinformation or harmful statements, potentially sparking public relations crises or damaging the university's credibility and trustworthiness on a global scale.

Legal and Ethical Risks:

There are also legal and ethical considerations. The unauthorized use of a person's likeness to create deceptive content not only raises privacy issues but could also lead to legal liabilities for the university if it is unable to prevent or respond effectively to such incidents. Additionally, there are ethical dilemmas associated with the handling and dissemination of synthetic media, which require clear institutional policies and guidelines.

Social and Psychological Risks:

Finally, on a social and psychological level, deep fakes could contribute to a broader erosion of trust within the university community. They can create confusion and mistrust among students and staff, impacting morale and the overall campus environment.

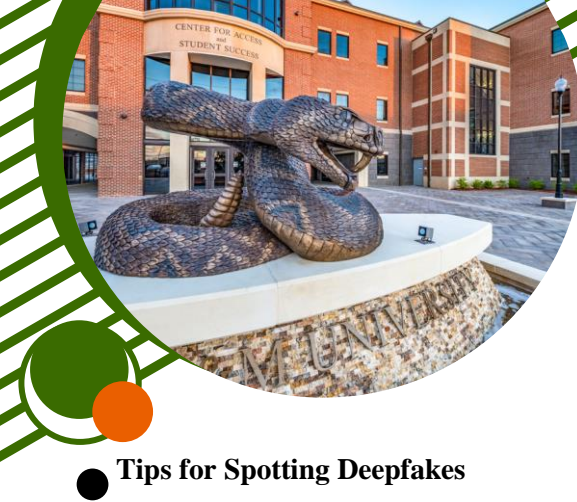


Alert Type

Awareness

Watch

Warning



"In the age of technological advancement, the threat of deepfakes presents a profound challenge to the integrity of academic discourse and the authenticity of educational content. As we navigate this evolving landscape, it is imperative for our institution to implement robust detection and verification mechanisms to safeguard our community from misinformation, preserve the credibility of our academic offerings, and uphold the trust placed in us by students, faculty, and stakeholders."

– FAMU Chief Risk Officer Deidre Melton

Tips for Spotting Deepfakes

1. Check for Inconsistencies in Speech and Lip Sync:

- **Audio Mismatch:** Listen for discrepancies between the visual lip movement and the audio. Delayed or mismatched speech can be a telltale sign of manipulation.
- **Artificial Sounds:** Pay attention to voices that sound flat or emotionless, as synthetic voices often lack the subtle inflections and emotional nuances of natural speech.

2. Analyze Facial and Body Movements:

- **Facial Expression Anomalies:** Look for irregularities in facial expressions. Deep fakes often struggle with accurately rendering emotions or facial movements like blinking and smiling.
- **Unnatural Movements:** Observe for any unnatural body movements. Smooth and fluid motion is difficult to synthesize accurately, leading to jerky or stiff movements in deep fakes.

3. Examine Visual Quality and Details:

- **Texture and Skin Tone:** Check for inconsistencies in skin texture or tone. Deep fakes may exhibit issues with rendering lifelike skin textures or maintaining consistent lighting effects on the skin.
- **Background Consistency:** Scrutinize the background for any signs of distortion or fluctuating quality, which can indicate video manipulation.

4. Use Technological Aids:

- **Reverse Image Search:** Employ tools like Google Images or TinEye to search for the origin of an image or to check if it appears elsewhere in a different context.
- **Deepfake Detection Software:** Utilize specialized software designed to detect deep fakes by analyzing the data for signs of digital tampering.

5. Listen for Audio Irregularities:

- **Background Noise:** Unusual background noise or fluctuations in audio quality can suggest manipulation, as can any mismatch in ambient noise levels when cuts or edits occur.
- **Voice Cloning Artifacts:** Be wary of slight distortions or oddities in speech patterns, especially if you are familiar with how the individual typically speaks.

6. Seek Confirmation of Media Provenance:

- **Metadata Analysis:** Inspect the metadata of files for signs of editing or for inconsistencies in the creation date and other digital fingerprints.
- **Verification from Source:** If possible, contact the original source or creator of the media to confirm its authenticity, especially for critical communications.

7. Professional and Academic Vigilance:

- **Education and Training:** Regularly update and educate staff and students on the latest trends in media manipulation and teach them how to use detection tools.
- **Policy Implementation:** Establish clear guidelines and protocols for handling and verifying media content, especially for academic submissions and official communications.



Chief Risk Officer:

Deidre.Melton@famuedu



Contact:

850-412-5479



ERM Coordinator:

William.Knight@FAMU.edu