DEEPFAKES AND AI IMPERSONATION CREATING A NEW CHALLENGE FOR CAMPUS SECURITY

August 4, 2026

Artificial intelligence is rapidly changing higher education, but it is also creating new opportunities for fraud, deception, and social engineering. Free AI tools can now generate convincing voices, images, videos, and emails that make it increasingly difficult to distinguish legitimate communications from fraudulent ones. As these technologies become more accessible, colleges should begin considering how they may affect both cybersecurity and physical security operations.

Deepfake technology has the potential to target campus security in several ways. An attacker could use AI-generated voice cloning to impersonate a college executive requesting after-hours building access, manipulate employees into bypassing security procedures, or create convincing emails that appear to come from leadership. Institutions are also seeing AI used to create fake student identities, phishing campaigns, and misinformation designed to exploit trust and create confusion.

Fortunately, technology alone is not the answer. Security experts emphasize creating a culture of verification. Employees should feel comfortable slowing down and independently verifying unusual or urgent requests, particularly those involving building access, financial transactions, sensitive information, or emergency decisions. Simple practices, such as confirming requests through a second communication method or following established authentication procedures, can significantly reduce the likelihood of a successful impersonation attempt.

***My Real-World Example**: I needed to update the bank account used for my direct deposit. Although I submitted the request using my official work email account, the Finance Department did not process the change based solely on the email. Instead, they followed up with a phone call to verify my identity before making the update. This simple secondary verification step helped ensure the request was legitimate and protected against the possibility of email compromise or AI-enabled impersonation. It serves as an excellent reminder that even requests appearing to come from trusted sources should be independently verified before action is taken.*

As AI continues to evolve, campus security professionals should work closely with information technology, emergency management, and institutional leadership to ensure policies, training, and response procedures evolve as well. Building awareness today will help institutions remain resilient against the increasingly sophisticated threats of tomorrow.

Provided by your "Collaborators in Risk Management"

DMI
DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES

Questions to Consider

- Would your staff recognize an AI-generated voice or email impersonating college leadership?
- Do employees know how to verify unusual or urgent requests before taking action?
- Have campus security and IT discussed how AI impersonation could affect emergency response, access control, or visitor management?
- Does your institution have a process for reporting suspected AI-generated fraud or impersonation attempts?

Resources

- Higher Ed Institutions Ramp Up Defenses Against Deepfakes (EdTech Magazine)
- Defending Against Data Breaches in the Age of Deepfakes (Campus Technology)

Lance Klukas, Campus Security Consultant

Districts Mutual Insurance & Risk Management Services
lance@districtsmutualinsurance.com | 715-563-6006