Journal of Information Systems Education

Volume 37
Issue 2
Spring 2026

Teaching Case

Seeing Is Not Believing: A Deepfake Video Call Scam at Pan-Asia Trading

Benjamin M. Ampel

Recommended Citation: Ampel, B. M. (2026). Teaching Case: Seeing Is Not Believing: A Deepfake Video Call Scam at Pan-Asia Trading. *Journal of Information Systems Education*, 37(2), 243-251. https://doi.org/10.62273/CVGA1145

Article Link: https://jise.org/Volume37/n2/JISE2026v37n2pp243-251.html

Received: August 7, 2025
First Decision: October 26, 2025
Accepted: December 16, 2025
Published: June 15, 2026

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems, 37(2), 243-251, Spring 2026
https://doi.org/10.62273/CVGA1145

Teaching Case
Seeing Is Not Believing: A Deepfake Video Call Scam at Pan-Asia Trading

Benjamin M. Ampel
J. Mack Robinson College of Business
Georgia State University
Atlanta, GA 30303, USA
BAmpel@gsu.edu

ABSTRACT

This teaching case uses a deepfake-enabled executive impersonation scam to help analyze cybersecurity failures and to design verification controls for communication environments. Pan-Asia Trading Ltd. is a fictional mid-sized firm that regularly conducts high-value monetary transfers. In early 2024, senior finance officer Grace Lee joins what appears to be a confidential video call with her CFO. However, the convincing face and voice are an advanced deepfake. The case examines failures in identity, authentication, and authorization, the role of AI-enabled deception, and the governance and privacy trade-offs faced by organizations. The case is designed for undergraduate and graduate courses in cybersecurity, information assurance, and MIS governance and supports experiential learning through realistic analysis of control gaps and AI-driven impersonation. The case emphasizes experiential learning around realistic AI-driven fraud scenarios and implementable verification controls.

Keywords: Cybersecurity, Generative AI, Social engineering, Teaching case

1. CASE SUMMARY

Organizations increasingly rely on video and voice channels to authorize sensitive actions. However, emerging AI techniques can erode assumptions about the trustworthiness of video and audio modalities. This teaching case is designed to help identify how cybersecurity can fail in such contexts, examine how AI-enabled impersonation reshapes organizational risk, and apply the People-Process-Technology triad to design a Minimal Verification Protocol for high-risk directives.

Pan-Asia Trading Ltd. (PATL) is a fictional mid-sized global trading company with regional headquarters in Hong Kong. The firm deals with high-value international transactions that require regular electronic fund transfers through its finance department. Grace Lee, a senior finance officer at PATL, manages daily payment operations and reports to the Chief Financial Officer (CFO). The company prides itself on a tight-knit corporate culture built on trust. Like many organizations, PATL has basic cybersecurity policies in place. However, employees have little exposure to advanced threats such as AI-driven social engineering (Young & Farshadkhah, 2023). In early 2024, PATL became the target of a sophisticated social engineering attack involving deepfake technology. Deepfakes are forms of synthetic media generated by AI (Vasist & Krishnan, 2022). This attack tested PATL's cybersecurity posture and organizational culture (Plachkinova & Maurer, 2018).

This teaching case narrates the incident from two perspectives. First, the case presents Grace Lee's experience as the victim deceived by a realistic video-call impersonation (Sipior, 2024). Second, the case presents David Park's role as the IT security manager leading the internal review. The case includes communication transcripts, an attack timeline, and a post-mortem memo to simulate a real-world scenario.

The case illuminates fundamental security and privacy concepts such as identity, authentication, AI-enabled threats, and governance in an accessible way for undergraduate and graduate level information systems students taking an introduction to cybersecurity or privacy course (He et al., 2013). Finally, the case provides detailed questions and a template for practice. As you read the narrative, pay attention to where identity, authentication, and authorization broke down during the incident, and consider how a more effective verification process could have altered the outcome.

2. CASE TEXT

2.1 The Finance Employee: Grace Lee

Grace Lee hurried into her office at 9:03 AM on Monday. She was juggling her latte and a stack of invoices. As a Senior Finance Officer, Monday mornings meant clearing weekend payment requests. Grace settled into her office and logged into her email. Grace noticed a message marked "Urgent" from Michael Chan, PATL's CFO and her direct supervisor.

Oddly, the email was not from Michael's usual corporate address. Instead, it came from what looked like his personal Gmail: michael.chan.patl@gmail.com. The subject read, "Urgent Confidential Meeting 10 AM Today." Grace's brow furrowed. Michael never used personal email for work matters. Still, the message was urgent and felt like it came from Michael (shown in Exhibit 1).

***From**:* Michael Chan <michael.chan.patl@gmail.com>
***To**:* Grace Lee <grace.lee@patl.co>
***Date**:* Mon, Jan 8, 2024, at 8:47 AM
***Subject**:* Urgent Confidential Meeting at 10 AM Today

Grace, I'm tied up in a sensitive negotiation this morning. I cannot access my official email or phone, so I'm using a private channel. **Please join me on a secure video call at 10:00 AM** via the link below. Urgent matter. A confidential payment for your eyes only.

Zoom Meeting Link: <u>Join Meeting</u> (Meeting ID: 912 3456 7890, Passcode: X7Fg)

Do not involve others yet. I'll explain everything on the call. This is critical and time sensitive.

Thank you for your absolute discretion.
-Michael

Exhibit 1. Phishing Email Transcript

Grace felt uneasy. A confidential payment tied to negotiations? PATL had been exploring a Southeast Asia investment, so the request didn't seem out of place. The tone sounded like Michael and she knew he was traveling that week. Using a personal email was unusual, but executives occasionally did so when abroad. Wanting to be dependable and mindful of confidentiality, Grace chose to follow the instructions.

At 9:58 AM, Grace clicked the Zoom link and entered the passcode. Her laptop camera activated, and soon a video window opened. The face that appeared caused Grace to exhale in relief. It was Michael Chan. The video quality appeared grainy due to a poor connection, and Michael's face was partially shadowed. Still, she recognized the salt-and-pepper hair and thin-rimmed glasses. He was wearing what looked like his favorite deep navy suit jacket that he frequently wore during board meetings. His voice was nearly

identical to Michael's, with only a slight echo that Grace attributed to a poor connection. She had no reason to suspect the image or voice, as both appeared entirely consistent with a routine video call from a traveling executive.

Michael greeted her with a strained smile. "Grace, thank you for joining on short notice," he said. "I'm in a bit of a bind. We have an opportunity to secure a strategic partnership earlier than expected, but we need to move funds immediately." He explained that a foreign partner was offering an early buy-in to a lucrative project, but a security deposit of $250,000 had to be wired within the next hour to finalize the deal. Because he was in transit and dealing with delicate negotiations, he needed Grace to execute the transfer on his behalf. He emphasized the confidentiality: "No one else is looped in. Not even the CEO. This is extremely sensitive. Once the transfer is done, I'll handle the paperwork. For now, I just need you to trust me and do this quietly."

Grace felt both anxious and determined. Handling a quarter million dollar transfer alone was not routine. Typically, any large fund transfer required at least two approvers (often the CFO and another executive). But extraordinary situations had occurred before. Michael's on-screen demeanor was urgent yet reassuring. Grace assumed this explained why he had reached out privately. She hesitated and asked a verifying question: "This is for the joint venture we discussed last month, right?" The deepfake Michael nodded. "Yes, exactly. The one in Malaysia. I'll brief everyone properly later, but right now, we could lose the opportunity if we don't act. I knew I could count on your discretion."

Any remaining doubt in Grace's mind dissolved. The mention of Malaysia aligned with an actual project the company had been considering. It was something Michael would be involved in. The attackers had gathered this detail from press releases and compromised emails. Grace agreed to arrange the transfer. The fake Michael quickly provided the beneficiary details via the Zoom chat. Michael stated that the provided account number was for his partner's lawyer's escrow account in Singapore. He added, "After you send it, email me the confirmation. Use my personal email for now. I'll be in meetings and can't pick up calls."

By 10:20 AM, the video call ended with Grace promising, "I'll get it done immediately." She felt a surge of responsibility and pride at being trusted with this mission. Grace immediately drafted an internal email to a back-office colleague who handled wire transfers (Exhibit 2).

Grace marked the email as high priority and attached a payment authorization form, on which she forged a quick e-signature for Michael Chan (a practice she would never normally consider, but she believed he had given verbal approval). In the email she wrote that CFO Michael Chan had personally instructed this urgent transfer and that formal paperwork would follow. She then called the bank's corporate liaison to initiate the $250,000 wire transfer using her authorized signatory privileges. The bank, recognizing Grace's position and the urgency conveyed, processed the transfer request.

By 11:15 AM, Grace received a standard confirmation from the bank. The funds were on their way. She forwarded the confirmation receipt to Michael's personal Gmail, as instructed, with a brief note: "Transfer done. Confirmation attached. Will brief you when you're free. Grace." With the task completed, she waited for acknowledgment from Michael. None came. She assumed Michael was still tied up.

At 2:30 PM on Monday, Grace ran into Angela, the CFO's executive assistant. Angela mentioned, "Michael just texted that his flight back from Singapore is delayed until tomorrow." Grace paused. Why would Michael be flying if he was supposedly in meetings for a negotiation? And why hadn't he sent a thank you reply about the transfer? A sense of doubt emerged. Grace decided to send Michael a quick text message on his known work mobile number to confirm if he received the confirmation. A few minutes later, her phone buzzed. It was Michael calling. Grace answered, expecting a quick thanks. Instead, she was greeted by a very confused Michael Chan.

"Grace," the real Michael said, "I'm looking at your text. What transfer are you talking about? I have no idea what you mean." Her face dropped. Grace explained the morning's email and video call, struggling to maintain composure. Michael's stunned silence was followed by urgent insistence: "I did not send any email or video call you today. I've been on a plane for the past two hours without internet!" The realization hit Grace. She had been duped. The person on the video call was not Michael. She recognized the urgency of the situation and acted quickly. Grace stammered an apology and immediately hung up to escalate the

issue. She understood that she had been deceived by a highly convincing impersonation. How would she explain that she, a trusted finance professional, had wired a quarter million dollars to a fraudster?

Within minutes, Grace contacted the head of IT security, David Park, and the finance director. She forwarded everything. The suspicious email, the Zoom link, the wire details. She spent the evening reviewing the sequence of events to identify points where the interaction seemed unusual. There was the off-tone voice echo, the dimly lit room, the strangely static facial expressions on the call, and the pressure to bypass standard procedures.

Despite these clues, the deepfake had been convincing enough under the urgent circumstances. Exhausted and distraught, Grace could only hope the company's security team would unravel what happened and that this expensive lesson would not cost Grace her job or reputation. She braced herself for the internal investigation to come, knowing that tomorrow, every detail of her actions on Monday would be under scrutiny.

***From*:** Grace Lee <grace.lee@patl.co>
***To*:** Operations Treasury Team <wire.transfers@patl.co>
***Date*:** January 8, 2024, 10:27 AM
***Subject*: URGENT:** Executive Authorization for Immediate Wire Transfer

Dear Treasury Team,

Please process an **urgent wire transfer** today as follows:

- **Amount:** $250,000.00 USD
- **Debit Account:** PATL Operating Account #**HK001-7745**
- **Beneficiary Name:** *Redacted Law Associates* (Escrow)
- **Beneficiary Bank:** UOB Singapore
- **Beneficiary A/C:** ******1098
- **Reference:** "Project Phoenix Deposit"

I certify that **CFO Michael Chan has authorized this transfer** verbally due to extreme time sensitivity. I have attached a scanned approval form signed on his behalf to expedite processing. Michael will countersign the physical document upon his return.

This transaction is highly confidential and related to a strategic investment. **Please prioritize and confirm once sent.**

Thank you,
Grace Lee
Senior Finance Officer, PATL
(Attachment: PATL_FundsTransferAuth.pdf)

Exhibit 2. Internal Transfer Request Email

2.2 The Security Manager: David Park

On Monday at 3:00 PM, David Park was wrapping up a server installation when he received the flurry of messages. As PATL's IT Security Manager, David was no stranger to urgent incidents. However, nothing like this had crossed his desk before. He received an email marked "HIGH PRIORITY: Fraud Incident." Attached were copies of a perplexing email thread from Grace and a forwarded Zoom invite. David reviewed Grace's summary of the events. The CFO's identity had apparently been impersonated over a

video call, and $250,000 was now wired to an unknown bank account. David immediately convened an emergency call with Grace, the real Michael Chan, and the finance director to triage the situation.

On the call, Grace was audibly shaken as she recounted the morning's events. Michael confirmed he had been completely offline during the time in question. The implication was clear. An external attacker had successfully tricked an employee via a deepfake video call and convinced her to violate financial controls. David recognized that the company needed to begin incident response. His role was immediately defined. Contain the damage (attempt to recover funds, involve law enforcement as needed) and investigate the breach (how the attacker infiltrated and what could be learned).

By 3:30 PM, David had alerted the company's bank to flag the transfer as fraudulent. Unfortunately, initial feedback was not hopeful. Due to the urgent transfer, the money had already landed in the recipient's account in Singapore. More concerning, the money had likely already been split and forwarded to additional accounts (a common tactic by attackers to evade detection). David contacted Hong Kong law enforcement's cybercrime unit to file an official report, knowing that international cooperation would be required to trace the money. Meanwhile, he pulled in his small security team to start forensic analysis.

They began by examining the phishing email Grace had received (Exhibit 1). Although it displayed the name "Michael Chan," the sender's address (michael.chan.patl@gmail.com) was not Michael's corporate email (michael.chan@patl.co). It was a cleverly crafted look-alike. David searched the company's email logs and found no sign of the email on the corporate server, meaning it likely went directly to Grace's inbox via her public-facing email address. Grace's email was listed on the company website for vendor contacts. The attacker must have scraped that information and emailed her from a dummy Gmail account.

Why hadn't this raised alarms for Grace? David surmised that the attacker anticipated suspicion about the odd email and preemptively gave a plausible excuse in the message. Michael claimed he was using a private channel due to being in a sensitive situation. This social engineering tactic exploited Grace's trust and the context of Michael's travel. David then investigated the Zoom meeting link. The invite was a standard-looking Zoom URL, but it did not match the company's official Zoom domain. It appeared the attacker had set up a basic Zoom meeting using a throwaway account. Upon contacting Zoom's security team, David learned that the meeting was created that very morning from an IP address in another country (later traced to a VPN exit node, making the attacker hard to pinpoint). There was no waiting room enabled. The attacker likely timed it so that Grace would join to find "Michael" already on the call.

Next, David's team interviewed Grace to gather more details about the video call itself. Grace described the video quality and how Michael's image looked grainy with occasional stutters. She also noted that Michael's mouth movements appeared slightly out of sync, which she attributed to network lag at the time of the call. David realized this was a hallmark sign of deepfake video. The slight visual irregularities that a non-expert might not catch under pressure. The voice, Grace said, was "exactly like Michael's, though perhaps a tad robotic at times." David knew AI-based voice cloning had become advanced. He knew that only a few minutes of recorded speech could enable a highly realistic impersonation. He surmised that the attackers gathered video and audio of Michael from earnings calls or presentations posted online. Michael admitted that several of his past conference talks were on YouTube. Anyone could easily download them. Similarly, several high-resolution photos of Michael from LinkedIn and press releases could be downloaded and used to train an AI to create a life-like talking head for the video.

Next, an unsettling question arose. Had the attacker gained internal information as well? Grace mentioned the fake Michael knew about a potential Malaysia joint venture project. Michael confirmed that project was real but still confidential, known only to a few senior leaders. How did the fraudsters know to mention it? David dug into email system logs and found, to his alarm, that Michael's corporate email account had suspicious login activity late last week. There were two login attempts from an IP in Hong Kong that were flagged as unusual (Michael was traveling in Singapore at that time).

One login was successful. It appears that the attackers might have hacked the CFO's email account days before the video call. They could have read through his emails or documents to pick up insider details like the Malaysia joint venture discussions and his travel schedule. Michael, embarrassed, admitted that he hadn't changed his password in two years and he had not enabled two-factor authentication on his email.

The phishing email to Grace might have been just one piece of a larger breach. By Monday evening, David's team pieced together a timeline (Exhibit 3).

Prior to January: Attackers conducted reconnaissance on PATL. Public info on executives (photos, videos, conference talks) is collected. Michael Chan (CFO) is identified as a high-value target. Attackers may have obtained Michael's email credentials (possibly via a leaked password or spear-phishing) and secretly accessed his email account, gathering intel (e.g., the Malaysia joint venture project and his travel schedule).

Monday, January 8, 2024, 8:47 AM: Grace receives a phishing email purportedly from Michael's personal account, requesting a private video meeting at 10:00 AM (Exhibit 1). Michael is traveling and offline.

10:00 AM: Grace joins the Zoom call (Exhibit 1). The attacker, using a deepfake video and AI-cloned voice of Michael, is already on the call. He instructs Grace to execute an urgent $250,000 transfer for a confidential deal, exploiting Grace's trust and knowledge of a real project.

10:15–10:30 AM: Grace prepares and authorizes the bank transfer, bypassing normal approval due to perceived direct CFO orders. She emails a colleague and the bank with instructions, attaching a forged approval (Exhibit 2). The bank processes the wire to the attacker's provided account.

Around 11:15 AM: Transfer confirmation is received by Grace. She forwards it to the fake Michael's email. Attacker likely withdraws or moves the funds quickly on the receiving end.

2:30 PM: Grace, now uneasy, contacts the real Michael via phone. Michael denies any knowledge of the meeting or transfer. Realization of the fraud sets in. Grace alerts IT Security (David) and senior management.

3:00–5:00 PM: Emergency response kicks off. The bank is notified to attempt freezing the funds, and law enforcement is informed. David's team starts investigating and collecting emails, meeting info, and system logs.

Next 1-2 Days: Internal investigation continues. Evidence of email compromise is found (unusual logins to Michael's account). David drafts a detailed post-mortem report with findings and recommendations (Exhibit 4). Management begins implementing immediate fixes (password resets, MFA, policy changes) and plans broader security improvements.

Exhibit 3. Attack Timeline

The attackers probably performed reconnaissance on PATL weeks in advance, identifying Michael and Grace on the corporate website or social media. They possibly obtained Michael's data via a password leak or targeted phishing, then accessed his email to gather intel. Armed with personal details and contextual knowledge, they set the trap. They spoofed Michael's identity in an email to Grace to lure her into a secure call. The deepfake video call was the final act of the scheme. The attacker was able to effectively bypass several security guardrails by exploiting human trust in a face-to-face interaction. In the days immediately following the incident, David led an exhaustive internal review. He drafted a post-mortem report (Exhibit 4) for the executive team and board.

(This is a portion of the incident report David Park prepared for PATL leadership, summarizing the event and recommendations. Only selected sections are shown.)

Incident Summary (Case #2024-01): On January 8, 2024, PATL experienced a targeted social engineering attack that resulted in an unauthorized wire transfer of $250,000. An attacker impersonated our CFO using a **deepfake video call** to deceive a finance employee into initiating the transfer. The attacker used a spoofed email and a realistic AI-generated likeness of the CFO's face and voice. The fraud was discovered within hours, but the funds had already left our account. Law enforcement has been notified and an investigation is ongoing.

Key Findings: The attacker obtained internal information (e.g., project code words) and likely accessed the CFO's email, indicating a possible credential compromise prior to the call. The finance employee followed what appeared to be a direct executive instruction, highlighting a breakdown of verification controls under pressure. The deepfake video and audio were sophisticated. Our employees were not trained to detect or challenge such impersonation in a live call. Standard phishing email cues were absent due to the use of real-time video, which our current training and protocols did not cover.

Impact: $250,000 (attempt to recover in progress, outcome uncertain). Internal confidence in security practices has been shaken. External disclosure is under consideration given the amount. We have placed a temporary freeze on large transactions until extra verification steps in place.

Immediate Actions Taken: We notified our bank and authorities to investigate and attempt fund recovery, implemented mandatory password reset and enabled multi-factor authentication for all executive accounts, and blocked the attacker's known email and Zoom details and scanned systems for any further indicators of compromise.

Recommended Preventative Measures: First, any request to bypass normal financial controls must undergo a secondary verification. We must also train staff on the existence of AI-driven impersonation (voice and video). This should incorporate scenarios of CEO fraud and deepfakes in security awareness programs. We must emphasize a culture where employees are empowered to pause and verify identities without fear, even if the request is urgent or from high authority.

Second, we must enforce use of company communication channels for official requests. If executives must use personal emails or unfamiliar channels in emergencies, there should be pre-established codewords or shared secrets to confirm their identity. This should include investments in emerging solutions that assist in authenticating video calls (such as enterprise video conferencing tools with enhanced identity verification) or detect anomalies in audio/video.

Third, we will update the incident response plan to specifically address fraudulent payment scenarios and include legal, HR, and PR teams in planning. This will include reviewing and refining corporate policies around executive data exposure.

Finally, the organization will conduct a thorough audit of financial controls to ensure no single point of approval can move large funds without checks under any circumstance. We will then implement system-enforced approvals that cannot be bypassed by informal communication.
(End of report excerpt. The full report included a timeline of events and a more extensive analysis of IT forensics.)

Exhibit 4. Internal Post-Mortem Report Excerpt

The report outlined how the deepfake attack succeeded and identified several control failures and gaps:

- **Identity Verification Lapse**: Grace did not have a way to verify that the person on the call was truly Michael. The company lacked a policy for verifying instructions received over video or phone, especially from personal accounts. There was an implicit trust in familiar voices and faces that the attackers exploited.
- **Bypassed Payment Controls**: The requirement for dual approval on large transfers was effectively bypassed. The usual protocol was overwritten by social pressure from the fake CFO. This indicated a need to create and enforce controls that cannot be waived even by senior personnel without secondary verification.
- **Credential and Email Security Gaps**: The likely compromise of Michael's email pointed to weaknesses in password management on critical executive accounts. It also raised concerns about how quickly suspicious logins are detected and acted upon.
- **User Awareness**: Grace had never been trained to suspect that a video call could be fake. Security training at PATL covered phishing emails but never voice phishing or deepfake scenarios. This emerging threat wasn't on her radar and left her unprepared to spot the subtle anomalies.

3. CONCLUSION

The incident served as a wake-up call for PATL. In the days that followed, David Park's investigation documented how the attackers exploited gaps in identity verification, organizational communication norms, and trust in familiar channels. The findings prompted difficult conversations across the company about how such a convincing deception could have succeeded and what it revealed about PATL's broader cybersecurity posture and culture.

As leadership reviewed the incident, they emphasized the need to reassess long-held assumptions about what constitutes reliable proof of identity in an era where audio and video can be synthetically manipulated in real time. Grace's experience was treated as evidence of emerging threat complexity rather than individual negligence. Senior executives acknowledged that the organization lacked adequate preparation for AI-enabled social engineering.

Over the following months, PATL initiated a structured review of its controls for high-risk operations. The process led to debates about the balance between trust and verification, the appropriate role of employee discretion under time pressure, and the organization's tolerance for procedural friction in critical workflows. A follow-up audit later in the year indicated strengthened collaboration between finance, IT security, and executive leadership and a growing recognition that identity assurance is not solely a technical concern but a socio-technical one.

As the case concludes, PATL confronts questions that many organizations now face: How should identity be verified when appearances and voices can no longer be taken at face value? How can organizations preserve efficiency while defending against subtle but high-impact forms of deception? And what governance structures are needed to manage AI-enabled risks as they evolve? These open challenges frame the work that remains ahead for PATL and for any organization navigating the shifting boundaries of trust in a digital age.

4. DISCUSSION QUESTIONS

Students should be prepared to answer the following questions:

- What clues suggested that the video or voice might be a deepfake?
- Where did identity, authentication, and authorization fail?
- What governance updates would you require next quarter?
- What privacy choice increased cloning risk? What can realistically be changed?
- How would you design a minimal verification protocol for high-risk payments (see Table 1)?

Control Area	Control Name	Gap (i.e., what failed?)	Verification (i.e., proof)	Owner
Process (what rules do we follow)?	Dual Authorization	No fallback when dual sign-off was skipped	Trusted channel confirmation	CFO
People (how do we train employees?)	Awareness Training	Grace did not know deepfake calls existed	Targeted training programs	InfoSec
Technology (what should we install?)	MFA	Email password was easily bypassed	Second item (e.g., phone call)	InfoSec

Table 1. Minimal Verification Protocol Template

5. REFERENCES

He, W., Yuan, X., & Yang, L. (2013). Supporting Case-Based Learning in Information Security With Web-Based Technology. *Journal of Information Systems Education*, 24(1), 31-40.

Plachkinova, M., & Maurer, C. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education*, 29(1), 11-20.

Sipior, J. (2024). Deepfake at Star Isle Real Estate Group. *Communications of the Association for Information Systems*, 55(1), 327-335. https://doi.org/10.17705/1cais.05513

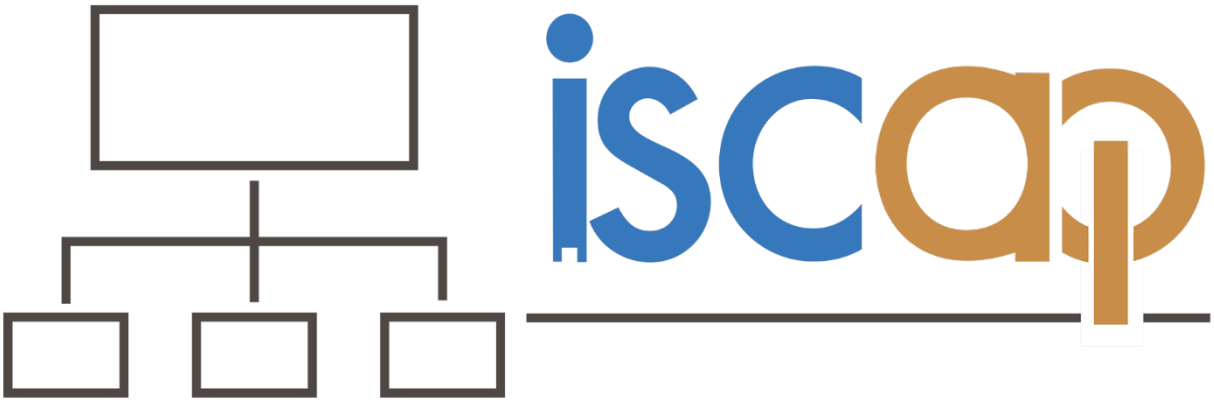
Vasist, P., & Krishnan, S. (2022). Deepfakes: An Integrative Review of the Literature and an Agenda for Future Research. *Communications of the Association for Information Systems*, 51(1), 590-636. https://doi.org/10.17705/1CAIS.05126

Young, J. A., & Farshadkhah, S. (2023). Teaching Tip: Hook, Line, and Sinker – The Development of a Phishing Exercise to Enhance Cybersecurity Awareness. *Journal of Information Systems Education*, 34(4), 347-359.

AUTHOR BIOGRAPHY

Benjamin M. Ampel is an Assistant Professor in the Department of Computer Information Systems at the J. Mack Robinson College of Business, Georgia State University. Benjamin received his Ph.D. from the Artificial Intelligence (AI) Lab at the University of Arizona. His research primarily focuses on AI-enabled Cybersecurity and has published peer reviewed articles that have appeared in journals such as *MIS Quarterly*, *Journal of Management Information Systems*, and *ACM Transactions on Management Information Systems* and in conferences such as *IEEE ISI*, *AMCIS*, and *ICIS*. He also serves as an Associate Editor for the journal *ACM Digital Threats: Research and Practice*. He has contributed to a variety of projects supported by the National Science Foundation (NSF) relating to secure and trustworthy computing (SaTC) and cybersecurity innovation for cyber-infrastructure (CICI).

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)