

DOI: https://doi.org/10.48009/1_iis_2026_122

A Triple-A pedagogical framework for AI-Era digital literacy education: Awareness, ability, and accountability

Jing Hua, *La Roche University*, jing.hua@laroche.edu

Wenli Wang, *Robert Morris University*, wangw@rmu.edu

Abstract

Recent advances in generative artificial intelligence (GenAI) have changed how digital content is produced, circulated, and evaluated, creating new challenges for digital literacy education. Rather than treating GenAI mainly as a threat to academic integrity, this paper presents a redesign of an introductory digital literacy course that uses GenAI as an instructional entry point for student engagement and critical analysis. The teaching module focuses on four dimensions of AI-era digital literacy: content authenticity evaluation, privacy and security reasoning, digital infrastructure awareness, and responsible communication. Through project-based, student-centered activities, students examine AI-generated images, discuss deepfakes, analyze phishing emails, reflect on privacy-related decision-making, and communicate responsible AI use. Across these activities, the design follows a Triple-A pedagogical logic: Awareness, Ability, and Accountability. This pedagogy guides students to explore AI tools and uses, develop responsible evaluative and technical practices, and understand the ethical and social consequences of AI-mediated digital participation. The paper offers practical guidance for strengthening students' foundational competencies in understanding GenAI capabilities, authenticity evaluation, cybersecurity awareness, infrastructure reasoning, and responsible technology use.

Keywords: Digital literacy, generative AI, Triple-A pedagogical framework, AI-era competency development, privacy literacy, phishing detection, deepfakes, cybersecurity education, digital authenticity, project-based learning

Introduction

Following the public release of generative artificial intelligence (GenAI) tools such as ChatGPT in 2022, college students quickly emerged as early adopters, integrating these technologies into everyday learning and problem-solving practices. This rapid adoption intensified educators' concerns about authorship, authentic learning, and academic integrity. At the same time, GenAI raises a broader instructional question: how should digital literacy education respond to a digital environment in which content is increasingly synthetic, persuasive, and difficult to verify? Rather than prohibiting AI use or focusing on its detection, this paper proposes using GenAI as an instructional catalyst in digital literacy education. Specifically, it treats AI systems and AI-generated outputs as objects of inquiry through which students can examine authenticity, privacy, security, and digital infrastructure.

Introductory digital literacy instruction often faces a related challenge: foundational topics such as privacy, security, and digital infrastructure are essential, but students may perceive them as abstract or disconnected from their everyday digital experiences. At the same time, students are already highly aware of AI-generated media, deepfakes, and AI-assisted online communication. This creates an opportunity to use familiar and visible AI-related phenomena as bridges to deeper digital literacy learning.

In this paper, digital literacy is defined not simply as the ability to use digital tools, but as the capacity to interpret, evaluate, and act responsibly within digital environments. In the context of generative AI, this includes four interrelated competencies: (1) recognizing the capabilities and limitations of generative AI in producing convincing digital content; (2) reasoning about AI-related privacy and security risks; (3) understanding basic digital infrastructure such as domains, URLs, and email structures; and (4) communicating responsibly about technology use. This framing is especially important because generative AI does not merely introduce new tools; it changes how users encounter, judge, and respond to digital content. Accordingly, this teaching module uses AI-generated images, deepfakes, and phishing not as isolated topics, but as connected instructional entry points into AI-era digital literacy.

In addition, the teaching module is grounded in project-based and student-centered learning with four interrelated instructional goals:

1. Increase student engagement through real-world AI phenomena that students already encounter in social, academic, and workplace contexts.
2. Develop awareness of generative AI's ability to produce convincing digital content by examining synthetic media and recognizing the limitations of intuitive or visual judgment.
3. Strengthen applied privacy, security, and digital infrastructure reasoning through phishing analysis and evidence-based verification practices.
4. Support responsible communication by asking students to translate technical and ethical insights into audience-appropriate digital artifacts.

This paper contributes to information systems education research in three ways. First, it offers a pedagogical design model for integrating GenAI into digital literacy education without solely regarding AI as a prohibited tool that jeopardizes academic integrity. Second, it connects emerging concerns about GenAI privacy, synthetic content, and AI-enabled deception to foundational digital literacy competencies, especially regarding infrastructure reasoning and applied risk evaluation. Third, it presents an assessment structure that allows students to demonstrate learning through phishing detection, evidence-based analysis or public-facing cybersecurity communication. Importantly, this paper is positioned as a design-oriented pedagogical contribution rather than an empirical evaluation study. Its purpose is to demonstrate how GenAI related technologies, benefits, risks, privacy concerns, cybersecurity issues, and responsible communications can be integrated into one coherent digital literacy learning experience.

Generative AI Challenges and Pedagogical Design

Generative AI creates new challenges for digital literacy education while also offering meaningful opportunities for instructional design. This section focuses on student engagement as a central challenge in introductory digital literacy courses and explains how real-world, project-based learning can help students connect abstract concepts to concrete digital experiences. The redesign of digital literacy education aims to leverage students' interest in GenAI while strengthening their competencies in AI-generated content awareness, privacy and security reasoning, digital infrastructure understanding, and responsible technology use.

The Engagement Challenge in AI-Era Digital Literacy Education

Prior research suggests that digital distraction and media multitasking can undermine sustained attention and academic performance in technology-mediated environments (Ophir et al., 2009; Rosen et al., 2013; Ward et al., 2017). These concerns are especially relevant in introductory digital literacy courses, where foundational topics such as privacy, security, and digital infrastructure may appear abstract unless they are connected to visible and meaningful real-world contexts.

In the context of GenAI, this engagement challenge is particularly significant. Students are often highly interested in AI-generated images, deepfakes, chatbots, and AI-enabled scams, yet they may not fully understand the privacy, security, infrastructure, and ethical issues connected to these technologies. This gap creates an instructional opportunity: GenAI can be used not only as a topic of concern, but also as an entry point for helping students examine how digital content is produced, circulated, evaluated, and acted upon.

Pedagogy Design: Engagement through Real-world Project-based Learning

Educational research suggests that student engagement increases when instruction connects directly to authentic, real-world contexts (Kuh, 2008). Project-based and experiential learning approaches have also been associated with higher motivation, deeper knowledge retention, and improved critical thinking (Kolb, 1984; Prince, 2004). Consistent with these perspectives, the module is designed around authentic AI-era digital platforms that students are likely to encounter in academic, workplace, and everyday settings. Rather than presenting AI literacy, cybersecurity awareness, privacy reasoning, and responsible communication as separate topics, the model connects them through applied activities that require students to observe, analyze, evaluate, and communicate about GenAI-related digital risks.

Because students regularly encounter AI-generated media, deepfakes, suspicious messages, and phishing attempts in their daily digital lives, these phenomena provide natural entry points for digital literacy learning. The pedagogical design is intentionally cumulative: students begin with familiar and visible AI-related examples and then move towards more abstract concepts, including authorship, authenticity, copyright, privacy, security, digital infrastructure, and responsible AI use. In this way, GenAI serves both as course content and as a pedagogical bridge for helping students understand why foundational digital literacy competencies matter in real-world digital environments.

The teaching module translates these concerns into concrete student activities. AI-generated images and deepfakes help students recognize the capabilities and limitations of synthetic media; phishing analysis and instructor-guided simulations strengthen privacy, security, and infrastructure reasoning; and the cybersecurity awareness campaign asks students to communicate AI-era digital risks to a broader audience. Together, these activities connect engagement, authenticity evaluation, risk analysis, infrastructure awareness, and responsible digital participation within a coherent learning sequence.

Learning Module: Digital Literacy with Generative AI

This section presents the teaching module design that integrates generative AI into digital literacy education. The module includes student learning objectives, teaching materials and activities, and assessment strategies.

Learning Objectives

After completing this learning module, students should be able to:

- A. Critical AI and authenticity literacy

- A.1 Explain what artificial intelligence is; discuss examples of AI-generated media and recognize the role of humans in AI content creation.
- A.2 Evaluate the limits of visual authenticity judgments in the context of AI-generated media and explain why contextual verification matters.
- A.3 Describe real-world applications, benefits, and risks of AI-generated images and deepfake technologies.
- B. Privacy, security, and infrastructure reasoning
 - B.1 Differentiate between security and privacy in digital environments, explaining how security mechanisms enforce privacy decisions.
 - B.2 Identify common tactics used in phishing emails, including AI-enhanced personalization, domain spoofing, and social engineering strategies.
 - B.3 Explain basic digital infrastructure concepts, including domain names, URLs, and email headers, and their relevance to online authenticity and data practices.
 - B.4 Apply privacy-protective reasoning by analyzing suspicious communications and evaluating digital risk scenarios.
- C. Responsible communication and production
 - C.1 Create a digital awareness artifact (poster or campaign) using office or creative software tools to communicate responsible technology use.

Teaching Materials and Student Activities

Building on this pedagogical rationale, the instructional sequence moves from AI-generated images, to deepfakes, and then to phishing-related activities. The module begins with AI-generated images to introduce questions of authorship, originality, authenticity, copyright, and the limitations of intuitive visual judgment. It then extends to deepfakes to connect synthetic media with issues of privacy, impersonation, consent, and personal data exposure. Finally, the module moves to phishing-related activities, with two possible options depending on students' prior knowledge, disciplinary background, learning needs, and engagement levels. In one option, students compare phishing emails with legitimate emails and develop infrastructure-based reasoning by analyzing domains, sender identities, URLs, email structures, and social engineering tactics. In the second option, students use GenAI in a controlled, instructor-guided simulation to generate sample phishing messages for educational analysis. This activity is not designed to teach phishing, but to help students understand how AI can intensify social engineering through personalization, persuasive language, urgency, and imitation of legitimate communication. Students then critique the generated examples by identifying warning signs, examining ethical risks, and discussing prevention strategies.

AI-generated Images, Authorship, and Authenticity

The lesson begins with an interactive visual exercise in which students are shown four artworks, two created by humans and two generated by AI. Students are asked to make an initial judgment about whether each image appears human-created or AI-generated. The purpose is not to evaluate students' detection accuracy or to suggest that authorship can be reliably inferred from visual appearance. Rather, the activity demonstrates the limitations of intuitive visual judgment and creates an entry point for introducing artificial intelligence, GenAI, and, where appropriate, related concepts such as the Turing test. The activity then expands into a class discussion of the real-world applications, benefits, and risks of AI-generated images. Students often identify potential benefits such as time savings, reduced production costs, creative experimentation, accessibility, and increased productivity. The instructor then guides discussion toward potential risks, including misinformation, fraudulent use, algorithmic bias, and labor disruption in creative industries. Depending on the course emphasis and students' background, the activity may also be extended to introduce copyright uncertainty and digital rights management, both of which are important components of digital literacy in AI-mediated environments.

As an opening activity, this exercise functions as an engagement catalyst while introducing foundational digital literacy themes, including authorship, authenticity, and critical evaluation of digital content.

Copyright and Digital Rights Management

Copyright and digital rights management are important components of digital literacy because they shape how digital content is created, reused, attributed, accessed, and governed. Questions of authorship in the AI-generated image activity can therefore open discussion of ownership, platform governance, and digital rights in AI-mediated environments. Depending on the course emphasis, students' disciplinary backgrounds, the instructor may extend the activity into a brief discussion of copyright in digital content, including current debates about AI-generated works, the use of copyrighted materials in GenAI training data, and the ways digital platforms use technical mechanisms to regulate access, copying, and reuse.

This extension can be especially relevant for students in fields such as journalism, communication, marketing, design, education, and other areas where content creation, attribution, and public communication are central professional practices. Rather than presenting copyright as a purely legal topic, the discussion encourages students to think critically about how digital content is produced, reused, monetized, and governed in platform-based environments.

Deepfake Technologies, Privacy, and Security

To shift from questions of authorship and content ownership to more personal forms of digital risk, the module next introduces deepfake technology. While students may initially view AI-generated images as interesting or creative rather than personally relevant, deepfake examples help them recognize how synthetic media can affect identity, privacy, reputation, and safety. The instructor begins with a short demonstration or case example showing how a single facial image and a brief audio sample can be used to generate a realistic talking-head video. For example, Microsoft's VASA-1 research demonstration illustrates how AI systems can animate a still image using an audio track, producing synchronized facial movement, lip motion, and head movement. During viewing, students are asked to observe facial movement, lip synchronization, realism, and any remaining visual or audio irregularities.

The discussion that follows explores both beneficial and harmful applications of deepfake and synthetic media technologies. Possible beneficial uses include film production, accessibility, language translation, education, marketing, and creative storytelling. Potential harms include impersonation scams, misinformation, reputational damage, nonconsensual image use, and fraud. To make these risks more concrete, the instructor then presents a short news video or case report about an AI-enabled virtual kidnapping scam. This case illustrates how publicly available online media, including profile photos, short videos, and voice recordings, can be repurposed in ways individuals did not intend. The discussion reinforces the connection between privacy and security by showing how everyday sharing practices can create future risks in AI-mediated environments.

This activity also introduces an important conceptual distinction between privacy and security. Students are prompted to reflect on whether they have actively adjusted privacy settings on their social media platforms. Privacy refers to individuals' decisions about what personal information is shared, with whom, and under what conditions. Security, by contrast, refers to the technical mechanisms, such as encryption, authentication, and access controls, that enforce those privacy preferences. Students are encouraged to recognize that without deliberate privacy choices, security mechanisms alone cannot fully protect personal data.

By explicitly linking personal decision-making, synthetic media risks, and technical safeguards, this activity strengthens students' understanding of how digital infrastructure supports, or sometimes fails to support, privacy intentions. It also prepares students for the following phishing activity, where similar issues of impersonation, urgency, and social engineering appear in message-based deception.

Phishing and AI-Enabled Social Engineering

As the final hands-on component of the module, instructors may choose one of two instructional options before assigning the Security Awareness Campaign Project. The first option emphasizes phishing detection and infrastructure analysis, while the second option emphasizes instructor-guided GenAI phishing simulation. Both options prepare students for the final project by helping them identify phishing tactics, evaluate suspicious digital communication, and communicate prevention strategies to a non-expert audience.

Option 1: Phishing Detection and Infrastructure Analysis

In this option, students are presented with a series of instructor-provided emails, including both legitimate and phishing examples. Working collaboratively, they analyze each message, determine its authenticity, and justify their reasoning with specific evidence. Through guided discussion, students examine indicators such as the sender display name versus the actual email address, domain structure, URL previews, hyperlink mismatches, tone, urgency, and common social engineering techniques. This activity introduces foundational digital infrastructure concepts, including how domain names function, how email addresses are structured, how DNS connects domains to IP addresses, and how spoofing and impersonation occur.

The instructor emphasizes that effective phishing detection requires more than surface-level cues. In AI-assisted environments, traditional warning signs such as grammatical errors or awkward phrasing are no longer reliable indicators of fraud. Instead, students are encouraged to apply structured evaluation strategies grounded in digital infrastructure literacy and contextual reasoning.

Option 2: Instructor-Guided GenAI Phishing Simulation: "Can You Outsmart AI-Enabled Scams?"

In this option, students participate in a supervised class activity titled "Can You Outsmart AI-Enabled Scams?" In the activity, students use generative AI tools to produce simulated phishing-style messages, such as fake banking alerts, job offers, or account verification requests. The activity is conducted within clear ethical boundaries and is designed for educational analysis rather than real-world use. This activity allows students to observe how AI can generate persuasive and linguistically polished scam content. Students then analyze the generated messages by identifying tactics such as urgency, impersonation, emotional manipulation, personalization, and misleading or spoofed links. The purpose is not to teach students how to conduct phishing, but to help them critically examine how GenAI can amplify social engineering tactics and why structured verification strategies are necessary in AI-mediated communication environments.

Through discussion and reflection, students evaluate the ethical implications of AI-generated deception and consider how awareness of such techniques can strengthen responsible digital participation. This option may be especially useful for students in information systems, cybersecurity, information technology, digital media, or related programs where understanding AI-enabled threat scenarios is relevant to professional practice.

Across both options, the module incorporates elements of in-class collaborative learning. Students develop analyses, discuss reasoning processes, and present their conclusions during class. This structure helps make students' thinking visible and reinforces active engagement with the materials.

Assignment: Security Awareness Campaign Project

Following either instructional option, students complete the Security Awareness Campaign Project. This assignment asks students to create a poster, short presentation, infographic, or awareness campaign focused

on phishing prevention, AI-enabled scams, deepfake risks, or responsible digital verification. If the GenAI phishing simulation option is used, students may incorporate a sanitized excerpt from the AI-generated phishing example created during class. If the phishing detection option is used, students may instead incorporate an instructor-provided phishing example or a fictionalized example based on the class activity.

The Security Awareness Campaign Project is presented as an example of how instructors can extend in-class analysis into project-based assessment and responsible public communication.

Assessment

Activity and Assessment Alignment

This learning module's topics, activity formats, targeted competencies, learning objectives and assessment methods are summarized in Table 1. It demonstrates the instructional strategies that support AI-era digital literacy competencies and emphasizes the alignment among the different aspects. Because the module is designed to be adaptable, instructors may modify the activities and assessment methods based on course level, student background, program requirements, and available instructional time.

Table 1. Alignment of Topics, Activities, Competencies, Learning Objectives, and Assessment Methods

Topics	Activity Formats	Targeted Competencies	Learning Objectives	Assessment Methods
AI-generated images	In-class visual exercise and discussion	AI-generated content awareness; authenticity evaluation	Explain generative AI's ability to produce realistic digital content and recognize the limits of relying on visual judgment alone	Class discussion, short reflection, or connection to campaign artifact
Copyright and digital rights management	Instructor-led discussion or optional extension	Authorship and digital rights awareness	Explain how authorship, ownership, copyright, and platform governance shape digital content creation and reuse	Class discussion or short reflection
Deepfakes, privacy, and security	Video case, discussion, and reflection	Synthetic media awareness; privacy and security reasoning	Describe potential risks of deepfakes and reflect on personal data exposure in AI-mediated environments	Short reflection, discussion response, or campaign artifact
Phishing and AI-enabled scams	Phishing detection activity or instructor-guided generative AI phishing simulation	Privacy, security, and digital infrastructure reasoning	Identify phishing tactics and explain how domains, URLs, sender information, spoofing, and social engineering contribute to cybersecurity risk	Phishing Detection Activity or class analysis
Assignment: Security Awareness Campaign Project	Project	Responsible communication and applied digital production	Communicate AI-related digital risks to a target audience using accurate, accessible, and responsible messaging	Poster, presentation, infographic, or campaign artifact

Following the instructional activities, instructors may assess student learning through one of two adaptable assignment options. The Phishing Detection Activity evaluates students' ability to analyze suspicious digital content using evidence-based reasoning, including domain authenticity, sender information, URL indicators, spoofing, and social engineering tactics. The Cybersecurity Awareness Campaign evaluates students' ability to translate technical and ethical concepts into clear, audience-appropriate communication about phishing prevention, AI-enabled scams, deepfake risks, or responsible digital verification. Together,

these assessment options reinforce the module's broader goal of helping students connect GenAI-related phenomena to foundational digital literacy competencies.

Rubrics

To support assessment, instructors may use a rubric aligned with the module's learning objectives. The rubric evaluates students' ability to identify AI-enabled phishing tactics, explain privacy and security risks, apply infrastructure-based reasoning, and communicate prevention strategies to a non-expert audience. The assignment may use a 10-point scale that assesses inclusion of the simulated phishing example, quality of tactic analysis, accuracy and relevance of poster content, clarity of visual design, and timely submission.

Table 2. Assessment Rubrics for the Security Awareness Campaign Project

Criterion	Points	Alignment
Simulated phishing example included	2	AI-enabled scam awareness
Tactic analysis	2	Social engineering and phishing detection
Accuracy and relevance of poster content	3	Privacy, security, and infrastructure reasoning
Visual clarity and audience-appropriate communication	2	Responsible communication and digital production
Timely submission	1	Course participation and completion

This rubric can be adapted depending on whether instructors emphasize phishing detection, cybersecurity communication, or broader AI-era digital literacy. Instructors may also modify the point values to align with local course policies and assignment expectations.

Discussion

This paper illustrates how generative AI can be incorporated into digital literacy instruction as a pedagogical bridge rather than treated primarily as a threat to academic integrity. By organizing instruction around authenticity evaluation, privacy and security reasoning, digital infrastructure awareness, and responsible communication, the module connects familiar AI-related phenomena to foundational digital literacy competencies in a visible and applied way.

This design also suggests a practical structure for AI-era digital literacy instruction organized around a Triple-A framework: Awareness, Ability, and Accountability. The Triple-A framework is proposed as a pedagogical organizing logic rather than as a fully validated theoretical model. It is intended to help instructors sequence learning activities from initial awareness of GenAI-mediated digital practices, to applied evaluative and technical capabilities, and finally to responsible AI use and accountable digital participation. Awareness refers to students' guided exploration of AI tools, AI uses, and AI-mediated digital practices across everyday, academic, workplace, and social contexts. It includes understanding what GenAI tools can do, how they are used, and how they reshape digital content production, communication, authenticity, privacy, and risk. Ability refers to students' capacity to apply responsible and critical practices in AI-mediated environments, including evaluating AI outputs, checking contextual and infrastructure cues, identifying phishing and impersonation tactics, and making privacy- and security-conscious decisions. Accountability refers to students' responsibility to consider the ethical, social, legal, and communicative consequences of AI use, including authorship, copyright, data exposure, bias, deception, and audience impact.

Together, these three dimensions provide an educational guide for integrating GenAI into digital literacy instruction without reducing AI literacy to tool use, prompt engineering, or academic-integrity compliance. This approach reframes AI use as a means of learning and reflection rather than as an external threat to assessment integrity. By making AI use visible in the classroom, students are encouraged to articulate their reasoning, examine AI's limitations, and reflect on ethical and practical implications instead of relying on AI as an invisible shortcut.

Conclusion

As generative AI technologies continue to evolve, digital literacy education must expand beyond basic tool proficiency to include authenticity evaluation, privacy and security reasoning, digital infrastructure awareness, and responsible technology use. This paper presented a redesign of an introductory digital literacy course that uses AI-generated images, deepfakes, phishing analysis, and AI-assisted phishing simulations as pedagogical materials to increase student engagement and support applied digital literacy learning.

By connecting students' interest in AI to foundational concepts in authorship, copyright, data practices, domain authenticity, privacy-related decision-making, and responsible communication, the module positions GenAI as a catalyst for instructional innovation. The instructional sequence helps students move from visible media phenomena to deeper forms of evaluation and reasoning about digital environments. More broadly, the paper contributes a design-oriented model for integrating generative AI into project-based digital literacy instruction. The proposed Triple-A framework, Awareness, Ability, and Accountability, offers a practical guide for helping students explore AI tools and uses, develop responsible evaluative and technical practices, and reflect on the ethical and social consequences of AI-mediated communication.

While the module offers a practical framework for educators seeking to incorporate generative AI into digital literacy teaching in a transparent, critical, and student-centered manner, this paper does not present systematic empirical evidence of student learning outcomes. Future research should evaluate the module through classroom implementation, student feedback, reflective responses, rubric-based analysis of student artifacts, and pre/post assessment of digital literacy and AI-era competency development. Such work would help assess how effectively the module supports student engagement, authenticity evaluation, privacy and security reasoning, infrastructure awareness, responsible AI use, and accountable digital participation.

References

- Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M., Al-Busaidi, K., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., ... Wright, R. (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>

- Elsen-Rooney, M. (2023, January 3). *NYC education department blocks ChatGPT on school devices, networks*. <https://www.chalkbeat.org/newyork/2023/1/3/23537987/nyc-schools-ban-chatgpt-writing-artificial-intelligence/>
- Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdinger, F., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., ... Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, 102274. <https://doi.org/10.1016/j.lindif.2023.102274>
- Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice Hall.
- Kuh, G. D. (2008). *High-impact educational practices*. Association of American Colleges and Universities.
- Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. *Proceedings of the National Academy of Sciences*, 106(37), 15583–15587. <https://doi.org/10.1073/pnas.0903620106>
- Panjehfouladgaran, H., Stavropoulou, F., & Teimouri, M. (2025). How has the COVID-19 pandemic affected students' online social presence? *INFORMS Transactions on Education*, 25(2), 106–121. <https://doi.org/10.1287/ited.2022.0054>
- Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, 93(3), 223–231.
- Rosen, L. D., Lim, A. F., Carrier, L. M., & Cheever, N. A. (2013). An empirical examination of the educational impact of text message-induced task switching in the classroom. *Educational Psychology*, 33(3), 323–345.
- Wheelwright, T. (2026, January 1). *Cell phone usage stats 2026: Americans check their phones 186 times a day*. Reviews.org. <https://www.reviews.org/mobile/cell-phone-addiction/>
- Ward, A. F., Duke, K., Gneezy, A., & Bos, M. W. (2017). Brain drain: The mere presence of one's own smartphone reduces available cognitive capacity. *Journal of the Association for Consumer Research*, 2(2), 140–154.