Expanding Pedagogical AI Scaffolding to IT and Cybersecurity Education: A Call for Multi-Institutional Validation

Anonymous Author(s)

Abstract

While large language models have rapidly infiltrated technical education, evidence suggests their pedagogical impact depends critically on how they are structured and integrated into learning workflows. We present *[Anonymized*, a framework for embedding metacognitive scaffolding and Feynman Technique-inspired prompts into AI assistants. In preliminary studies within Data Structures courses, students using our pedagogically-structured tool significantly outperformed peers using unstructured ChatGPT (mean scores: 92.7 vs. 74.3, $p < 0.001$), with greatest gains in conceptual reasoning and documentation quality. We now seek collaborators to validate and extend this framework to IT and cybersecurity education contexts, where structured reasoning about system vulnerabilities, threat modeling, and security trade-offs demands similar metacognitive awareness. This lightning talk will demonstrate the *[Anonymized]* platform, share our scaffolding design patterns, and invite institutions to participate in multi-site validation studies exploring how pedagogical AI design impacts learning outcomes in security analysis, network troubleshooting, and incident response scenarios.

CCS Concepts

• **Applied computing** → **Education**; *Collaborative learning*; • **Human-centered computing** → *Collaborative interaction*; • **Computing methodologies** → Natural language processing.

Keywords

Pedagogical AI Design, Metacognitive Scaffolding, Technical Education, Feynman Technique, AI-Assisted Learning

ACM Reference Format:
Anonymous Author(s). 2025. Expanding Pedagogical AI Scaffolding to IT and Cybersecurity Education: A Call for Multi-Institutional Validation. In *Proceedings of (SIGCITE '25).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Description

1.1 The Problem Space

Recent surveys indicate that 79% of computing students regularly use AI tools for technical tasks, yet unstructured interactions often lead to surface-level engagement and reduced problem-solving skills [1, 2]. This challenge becomes particularly acute in IT and cybersecurity education, where students must develop critical thinking about system behaviors, security vulnerabilities, and defensive strategies—skills that cannot be cultivated through passive consumption of AI-generated solutions.

Our preliminary work in Data Structures courses revealed a striking pattern: identical language models produce dramatically different learning outcomes depending on their pedagogical framing. Students using our structured tool demonstrated superior performance not just in implementation tasks, but particularly in areas requiring abstraction, explanation, and justification—precisely the metacognitive skills essential for cybersecurity professionals who must articulate threat models, justify security controls, and reason about complex attack vectors.

1.2 The *[Anonymized]* Framework

The *[Anonymized]* platform operationalizes learning science principles through conversational AI design. Rather than providing direct answers, our framework embeds three key pedagogical mechanisms:

Feynman-Inspired Explanation Prompts: Students must articulate problems in their own words before receiving guidance, forcing conceptual engagement before solution-seeking.

Predictive Reasoning Checkpoints: The system requires learners to predict outcomes and explain expected behaviors, developing the hypothesis-testing mindset crucial for security analysis.

Metacognitive Reflection Loops: After each design decision or problem-solving step, students justify their reasoning and consider alternatives, building the reflective practice essential for incident response and threat assessment.

1.3 Demonstrated Impact and Validation Needs

Our quasi-experimental study (N=36) showed effect sizes exceeding Cohen's d=2.14, with structured tool users achieving higher mean scores and lower performance variance—suggesting potential equity benefits. However, these results emerge from a single institutional context in traditional CS coursework. Validating the framework's transferability to IT and cybersecurity education requires diverse institutional partnerships and domain-specific adaptations.

1.4 Collaboration Opportunities

We invite institutions to join a multi-site validation study exploring *[Anonymized]*'s impact across technical computing disciplines. Participating institutions would:

- Integrate *[Anonymized]* into existing IT/cybersecurity courses for Spring and Fall 2026 terms
- Contribute domain-specific scaffolding patterns (e.g., threat modeling templates, incident response workflows)
- Collect comparative performance data using standardized assessment rubrics

SIGCITE '25,

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

- Co-author publications on pedagogical AI design in technical education

The platform architecture supports rapid customization—instructors can modify prompting patterns, add course-specific checkpoints, and tailor metacognitive scaffolds to their learning objectives without programming expertise. We provide deployment support, IRB templates, and assessment instruments validated in our preliminary studies.

1.5 Lightning Talk Demonstration

This presentation will include:

1. Live demonstration of student interactions with *[Anonymized]* versus unstructured ChatGPT (5 minutes)
2. Walkthrough of the instructor customization interface for creating domain-specific scaffolds (3 minutes)
3. Preliminary results showing differential impact on conceptual reasoning tasks (3 minutes)
4. Open discussion on adapting the framework for security education contexts (4 minutes)

We particularly seek feedback on extending our scaffolding patterns to support critical cybersecurity competencies: vulnerability assessment workflows, security control justification, incident timeline reconstruction, and threat intelligence analysis. How might structured AI interactions help students develop the skeptical, analytical mindset required for security work while avoiding over-reliance on AI-generated solutions?

References

[1] J. Finnie-Ansley et al. 2025. Patterns of Student Use and Perceptions of Generative AI in Advanced Computing Courses. In *Proceedings of SIGCSE '25*. ACM, 123–131.

[2] N. Kosmyna et al. 2025. Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant. *arXiv:2506.08872*.

[3] J. Prather et al. 2023. Metacodenition: Scaffolding the Problem-Solving Process for Novice Programmers. In *Proceedings of ACE '23*. ACM, 30–39.