

In this issue:

- 4. Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy**
Gary Yu Zhao, Northwest Missouri State University
Cindy Zhiling Tu, Northwest Missouri State University
Joni Adkins, Northwest Missouri State University
- 17. Excessive Equating: An Exploration of Knowledge Unit (KU) Curricular Load for CAE-CD Program Design and Evaluation**
Kasey Miller, University of North Carolina Wilmington
Kevin Matthews, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
- 41. Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education**
Paul Wagner, University of Arizona
Robert Honomichl, University of Arizona
Crystal Beasley, University of Arizona
Thomas Reid, University of Arizona
Logan Bradford, University of Arizona
Alexandra Urbaszewski, University of Arizona
- 52. Linking Security Self-Efficacy and Communication Networks to Perceived Success in Cybersecurity Tabletop Exercises**
Shawn F. Close, University of Montana
Theresa Floyd, University of Montana
Ryan T. Wright, University of Virginia
Patricia Akello, University of Montana
Reda Haddouch, University of Montana
- 79. Semantic Technologies for Cybersecurity Education Competencies: JSON-LD Implementation of Distributed Learning Analytics**
Ryan Straight, University of Arizona
Aaron Escamilla, University of Arizona
- 104. Enhancing Cybersecurity Awareness in Business Students through Gamified Learning**
Mubashrah Saddiqa, University of Southern Denmark
Marie Louise Haagenen, Business Academy Dania
Niels Østergaard, Business Academy Dania

The **Cybersecurity Pedagogy and Practice Journal (CPPJ)** is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (<https://cppj.info>). Our sister publication, the proceedings of the ISCAP Conference (<https://proc.iscap.info>) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at <https://iscap.us/papers>. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2026 ISCAP Board of Directors

Amy Connolly
James Madison University
President

Michael Smith
Georgia Institute of Technology
Vice President

Jeff Cummings
Univ of NC Wilmington
Past President

David Firth
University of Montana
Director

Mark Frydenberg
Bentley University
Director/Secretary

Leigh Mutchler
James Madison University
Director

RJ Podeschi
Millikin University
Director/Treasurer

Bryan Reinicke
Rochester Institute of
Technology / Director

Jeffry Babb
West Texas A&M University
Director/Curricular Matters

Eric Breimer
Siena University
Director/2026 Conf Chair

Tom Janicki
Univ of NC Wilmington
Director/Meeting Planner

Xihui "Paul" Zhang
University of North Alabama
Director/JISE Editor

Copyright ©2025 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Jeffrey Cummings
Co-Editor
University of North Carolina
Wilmington

Anthony Serapiglia
Co-Editor
Saint Vincent College

Thomas Janicki
Publisher
University of North Carolina
Wilmington

2026 Review Board

Brandon Brown
Coastline College

Jamie Pinchot
Robert Morris University

Kevin Slonka
Saint Francis University

Shawn Clouse
University of Montana

Samuel Sambasivam
Woodbury University

Geoff Stoker
Univ of NC Wilmington

Jeff Landry
Univ of South Alabama

Shwadhin Sharma
California State University
Monterey Bay

Paul Wagner
University of Arizona

Li-Jen Lester
Sam Houston State Univ

Sushma Mishra
Robert Morris University

Paul Witman
California Lutheran
University

Enhancing Cybersecurity Awareness in Business Students through Gamified Learning

Mubashrah Saddiqa
msad@mmmi.sdu.dk
University of Southern Denmark
5230 Odense M, Denmark

Marie Louise Haagensen
maha@eadania.dk
Business Academy Dania
8960 Randers, Denmark

Niels Østergaard
nios@eadania.dk
Business Academy Dania
8800 Viborg, Denmark

Abstract

Business students often lack cybersecurity awareness, leaving them vulnerable to social engineering and weak authentication practices. This study presents two gamified cybersecurity modules—Social Engineering and Authentication—designed for non-technical business students. The modules were developed collaboratively across three campuses of Business Academy Dania and hosted on the SmartLearning platform, combining storytelling, hands-on exercises, and the “Go Phishing” card game to support practical, scenario-based learning. The paper describes the design, development, and curricular integration of the modules, showing how they were embedded into existing business programs and adapted to diverse student groups. The modules were evaluated with undergraduate business students in two learning modules: Social Engineering (n = 44) and Authentication (n = 42). Pre- and post-assessment results showed substantial learning gains, with average quiz scores increasing from 41% to 78% for the Social Engineering module and from 45% to 82% for the Authentication module. Paired-sample t-tests confirmed significant improvements with large effect sizes (Cohen’s $d = 6.03$ and $d = 6.51$). Moreover, qualitative feedback indicated strong student engagement and perceived practical relevance of the gamified learning activities. By providing a structured and transferable pedagogical approach, this study offers a model for enhancing cybersecurity awareness among non-technical learners in higher education.

Keywords: Cybersecurity Education, Gamification, Business Students, Social Engineering, Authentication, Experiential Learning.

Recommended Citation: Saddiqa, M., Haagensen, M., Østergaard, N., (2025). Enhancing Cybersecurity Awareness in Business Students through Gamified Learning. *Cybersecurity Pedagogy and Practice Journal*; v5(n1) pp 104-113. DOI#: <https://doi.org/10.62273/WOBZ8483>

Enhancing Cybersecurity Awareness in Business Students through Gamified Learning

Mubashrah Saddiqa, Marie Louise Haagensen and Niels Østergaard

1. INTRODUCTION

In today's digital world, cybersecurity is essential across all sectors (Mallick & Nath, 2024; Blažič, 2022). While traditionally associated with IT professionals, cybersecurity awareness is crucial for all employees, including business roles, to protect sensitive data and organizational assets (Furnell, 2021; Abrahams et al., 2024; Crumpler et al., 2022). Business students often lack technical training yet will operate in environments vulnerable to phishing, social engineering, and weak authentication practices (Trumbach et al., 2022; Wiechetek et al., 2022; Bhusal, 2021; Desolda et al., 2021; Tirfe et al., 2022). For example, a marketing manager might unknowingly click on a phishing email disguised as a client message, or a finance officer might fall victim to social engineering tactics that trick them into transferring funds to fraudulent accounts. Despite these risks, business programs often overlook essential cybersecurity topics, leaving students vulnerable to threats that could impact operations, reputation, and profitability. This knowledge gap emphasizes the importance of cybersecurity awareness training specifically designed for business students, ensuring they can recognize, prevent, and respond to digital threats in real-world business settings (AlDaajeh et al., 2022).

This study addresses this gap by presenting the design, development, and curricular integration of gamified cybersecurity modules for non-technical business students. The modules were developed across three campuses of Business Academy Dania and are hosted on the SmartLearning platform. SmartLearning (<https://www.smartlearning.dk/>) is a national Danish e-learning platform used across eight academies. It provides interactive modules, multimedia content, and assessment tools. The modules developed in this study focus on social engineering and authentication. They combine interactive storytelling, hands-on exercises, and the "Go Phishing" card game for practical, scenario-based learning. The design and activities are grounded in research on gamified learning for cybersecurity concepts (Gwenhure & Rahayu, 2024; Saddiqa et al., 2021; Williams et al., 2024).

The study is part of the Sikkerhed på Spil (Security through Gaming) project, which seeks to enhance cybersecurity education through engaging, hands-on learning (Sikkerhed på Spil, 2023). The study is guided by the following research questions:

RQ1. *How can gamified cybersecurity modules be designed to effectively engage non-technical business students?*

RQ2. *How can these modules be integrated into existing business curricula to enhance cybersecurity awareness?*

This study presents an instructional design and implementation approach for developing gamified cybersecurity modules tailored to non-technical business students. Through multi-campus integration and the use of storytelling, interactive exercises, and gamified activities, the work demonstrates how accessible, scenario-based cybersecurity learning can be embedded into existing curricula and scaled through the SmartLearning platform.

The paper is structured as follows: Section 2 provides background; Section 3 outlines methodology; Sections 4–5 describe development and testing; Section 6 presents results; Section 7 discusses limitations; and Section 8 concludes the paper.

2. BACKGROUND

Cybersecurity is increasingly vital across all sectors due to growing digital threats (Safitra et al., 2023). While IT professionals receive extensive technical training, many business students and professionals lack the knowledge to identify and mitigate risks, leaving organizations vulnerable (Sussman, 2021; Afenyo et al., 2023). Business programs often overlook cybersecurity topics, particularly social engineering and authentication, despite these being common sources of organizational breaches (Trumbach et al., 2022; Wiechetek et al., 2022; Bhusal, 2021; Desolda et al., 2021; Tirfe et al., 2022; Shilair et al., 2023; Triplett, 2023). This gap highlights the need for accessible, engaging training tailored to non-technical learners.

Research shows that gamification can enhance learning and engagement, particularly for complex subjects like cybersecurity (Deterding et al., 2011; Subhash & Cudney, 2018; Alshaikh, 2020; Abu-Amara et al., 2021; Gwenhure & Rahayu, 2024). When combined with experiential and constructivist learning approaches, gamified modules contextualize threats in realistic scenarios, promoting active problem-solving and applied knowledge (Lander, 2014; Zaric et al., 2021; Mouheb et al., 2019; Saddiqa et al., 2023a; Saddiqa et al., 2023b). Storytelling, multimedia content, and interactive exercises further support retention and understanding. However, few studies focus specifically on non-technical business students, creating a gap in both research and practice.

The Sikkerhed på Spil (Security through Gaming) project was developed to address this need by providing interactive, gamified cybersecurity modules for business students (Sikkerhed på Spil, 2023). By integrating storytelling, hands-on exercises, and scenario-based activities, these modules aim to equip students with foundational cybersecurity awareness while remaining accessible to learners without technical backgrounds. This study presents the design, development, and integration of these modules into business curricula, offering a pedagogical model for other institutions.

3. METHODOLOGY

The development of the gamified cybersecurity modules followed a structured process aimed at engaging non-technical business students and integrating seamlessly into existing curricula. Three campuses of Business Academy Dania—Viborg, Skive, and Grenaa—collaborated to ensure relevance across diverse programs, including Multimedia Design, Marketing, and Economics.

Local business representatives were consulted to identify the most pressing cybersecurity challenges, while instructors from the participating programs provided guidance on curricular alignment and practical applicability. This input informed the selection of two modules: Social Engineering, focusing on psychological manipulation tactics such as phishing and pretexting, and Authentication, emphasizing secure password practices, multi-factor authentication, and account protection.

The modules were designed for accessibility and engagement, grounded in constructivist learning

theory (Zajda, 2021), and delivered through short, focused segments incorporating interactive storytelling, quizzes, and simulations (Clark & Mayer, 2023; Mayer, 2014). Gamification elements, including point scoring and the “Go Phishing” card game, reinforced active learning and motivation (Deterding et al., 2011; Subhash & Cudney, 2018; Gwenhure & Rahayu, 2024; Zaric et al., 2021), while scenario-based exercises contextualized concepts in realistic business environments (Yang & Wu, 2012; Palioura & Dimoulas, 2022). Optional challenge-based platforms such as TryHackMe provided students with hands-on opportunities to practice cybersecurity in controlled settings (TryHackMe, 2025).

Students piloted the modules in iterative testing cycles, providing feedback on clarity, engagement, and usability, which guided subsequent refinements. Pre- and post-module quizzes were used to assess learning gains, complemented by qualitative feedback from both students and instructors.

Qualitative data from open-ended survey responses and focus group discussions were analyzed using thematic analysis following the framework proposed by (Braun & Clarke, 2006). Two researchers independently reviewed the qualitative responses and conducted initial open coding to identify recurring concepts related to engagement, usability, and perceived learning outcomes. The researchers then compared codes and grouped them into broader themes through iterative discussion and refinement. Themes were included if they appeared in at least 20% of responses or were strongly emphasized during the focus group discussion. To enhance validity, preliminary findings were discussed with five student participants during debrief sessions (member checking) to confirm that the interpretations reflected their experiences. The qualitative themes were subsequently triangulated with quantitative survey results to identify consistent patterns across the findings. Table 1 shows the participants' overview.

Participant	Number	Role in Study
Local Business	10	Identified key cybersecurity challenges
Instructors	3	Advised on curriculum alignment
Students	86	Pilot testing and feedback

Table 1. Participants Overview

The study ran from January 2023 to December 2024, encompassing the development, testing, and revision of the cybersecurity modules. Interviews with local businesses and educators were conducted in early 2023 to identify key cybersecurity challenges. The Social Engineering module was developed and tested in late 2023, and the Authentication module was developed and tested in the second half of 2024. Revisions based on iterative feedback were implemented by December 2024. Data from pre- and post-module assessments, student surveys, and focus groups were analyzed in the first half of 2025 to evaluate learning gains and student engagement.

While this study does not use industry-standard programs such as Cisco Networking Academy or Palo Alto Networks courses, it follows European Union Agency for Cybersecurity (ENISA, 2022) and National Institute of Standards and Technology (NIST, 2021) recommendations for simulation-based and gamified learning. The modules aim to equip non-technical business students with practical cybersecurity skills to act securely and responsibly in professional contexts.

The methodology focuses on replicability and scalability, and demonstrates how gamified, scenario-based cybersecurity education can be designed, integrated, and evaluated for non-technical business students.

4. MODULE DEVELOPMENT

The development of the cybersecurity modules was an iterative and collaborative effort, incorporating input from local businesses, educators, and students. Ten companies from the Viborg region provided insights into real-world cybersecurity challenges, emphasizing the importance of employee training in areas such as phishing, social engineering, and authentication. Educators from the Multimedia Design, Marketing, and Economics programs also contributed, ensuring the modules would be feasible and relevant for non-technical business students.

One business owner said, *“Employees are the weakest link in our cybersecurity strategy. They are often tricked by phishing emails or phone calls, and we see a growing need for awareness training in this area.”*

Another commented, *“We invest in technology, but we are realizing that human error is often the biggest vulnerability.”*

Regarding authentication, a business owner emphasized,

“If employees are reusing passwords or not using MFA, that’s a huge risk. We need people who are aware of how to secure their accounts.”

Educators from the Multimedia Design, Marketing, and Economics programs also contributed, ensuring the modules would be feasible and relevant for non-technical business students.

One instructor stated, *“Teaching cybersecurity awareness is no longer optional—it’s essential. Our students need to understand how social engineering tactics work so they can protect both themselves and the businesses they will work for.”*

Module	Key Topics	Optional Activities
Social Eng.	Introduction to social engineering concepts (phishing, baiting, pretexting) Storytelling-based phishing scenarios Interactive quizzes to reinforce learning Ransomware simulation	TryHackMe exercises Teacher-guided discussions or group exercises
Auth.	Password security and multi-factor authentication Biometric and certificate-based methods Gamified password strength game Quizzes and case studies	Use of “Have I Been Pwned?” (Hunt, 2025) Optional teacher-led discussion activities
Go Phishing (Game)	Identification of phishing indicators in emails Collaborative problem-solving in small groups	Printed classroom activity Self-paced /Teacher-guided

Table 2. Key Activities and Optional Components in the Cybersecurity Modules

Based on this feedback, two modules were developed: Social Engineering and Authentication. The development process focused

on creating engaging, interactive content that allows students to understand and apply cybersecurity concepts in practical scenarios.

Both modules are integrated into the SmartLearning platform and designed primarily for self-paced learning. However, optional teacher guides support instructors who wish to facilitate discussions or group exercises, enabling classroom integration when desired.

The modules combine interactive storytelling, hands-on exercises, quizzes, and scenario-based activities to reinforce practical cybersecurity skills. Optional activities encourage deeper engagement and exploration.

A summary of the modules and their key components is presented in Table 2.

a. Social Engineering Module

The Social Engineering module introduces students to the psychological tactics used by cybercriminals to manipulate individuals into revealing confidential information or performing unsafe actions. The module employs storytelling, interactive quizzes, and scenario-based ransomware simulations to provide students with experiential learning opportunities.

As optional activities, students can practice phishing scenarios on the TryHackMe platform and participate in teacher-facilitated discussions if the module is used in a classroom setting.

b. Authentication Module

The Authentication module covers secure password practices, multi-factor and biometric authentication, and case studies of real-world authentication failures. Students engage in hands-on exercises such as password strength games and quizzes that reinforce best practices in cybersecurity.

As optional activities, students may explore additional exercises on TryHackMe, use the "Have I Been Pwned?" (Hunt, 2025) tool to evaluate compromised accounts and participate in

teacher-guided discussions when integrated into classroom instruction.

c. Go Phishing Card Game

To complement the Social Engineering module, the Go Phishing card game was developed to provide an interactive, scenario-based learning experience. Students work in small groups to identify phishing indicators in a variety of email scenarios, discussing their reasoning and learning from peers. Points are awarded for correct identifications, and immediate feedback reinforces learning. Teachers can use a facilitation guide with discussion prompts, debriefing questions, and guidance on connecting the game outcomes to workplace cybersecurity risks. This activity enhances engagement, critical thinking, and confidence in identifying phishing attempts in real-world contexts, supporting the experiential and gamified design of the modules.

5. TESTING PROCEDURE

The objective of the study was to evaluate the effectiveness of the gamified cybersecurity modules in increasing awareness and understanding of core cybersecurity concepts among non-technical business students. Understanding these concepts is crucial, as business students often enter professional environments in which phishing, social engineering, and weak authentication practices pose significant risks to organizational security.

In the second half of the study period, in-class testing sessions were conducted across the three campuses of Business Academy Dania (Viborg, Skive, and Grenaa), involving students from the Multimedia Design, Marketing, and Economics programs. Both first- and third-semester students participated, providing insights across various stages of their academic progression. First-semester students initially assessed the Social Engineering module, while third-semester students engaged with the revised Social Engineering module alongside the Authentication module.

Table 3. Overview of Module Testing Sessions

Module	Students	Activities	Duration	Campus/Programs
Social Eng.	44	Pre/post assessment, videos, quizzes, interactive exercises, qualitative survey, game testing	3-4 hours	Viborg, Skive, Grenaa/ Multimedia Design, Marketing, Economics
Authentication	42	Pre/post assessment, videos, quizzes, interactive exercises, qualitative survey	3-4 hours	Viborg, Skive, Grenaa/ Multimedia Design, Marketing, Economics

In the second half of the study period, in-class testing sessions were conducted across the three campuses of Business Academy Dania (Viborg, Skive, and Grenaa), involving students from the Multimedia Design, Marketing, and Economics programs. Both first- and third-semester students participated, providing insights across various stages of their academic progression. First-semester students initially assessed the Social Engineering module, while third-semester students engaged with the revised Social Engineering module alongside the Authentication module.

Each in-class session lasted approximately 3–4 hours. Students were first introduced to the project and completed a pre-module assessment, including a brief survey and quiz, to gauge their prior knowledge and familiarity with topics such as phishing, ransomware, and password security. Students then explored the modules independently, engaging with interactive elements including videos, quizzes, storytelling simulations, and the Go Phishing card game. Optional activities, such as TryHackMe exercises and the Have I Been Pwned? tools were available for students seeking additional hands-on practice.

Following the module exploration, students completed a post-module assessment and a qualitative survey. The survey collected open-ended feedback on the modules’ strengths, challenges, and suggestions for improvement. In addition, a focus group with five students was conducted to gather more in-depth feedback on usability and content clarity. Two instructors reviewed the modules to provide expert perspectives on pedagogical structure, accessibility, and instructional flow.

Given the exploratory nature of the study and the small sample size, qualitative responses were analyzed using thematic analysis, as described in the methodology section.

Informal member checking during debriefs ensured that the summarized findings accurately reflected the students’ experiences. The testing results informed revisions to module content, interactive elements, and instructional design, ensuring that both modules were accessible, engaging, and effective for non-technical learners. Table 3 presents an overview of the activities during the module testing session.

6. RESULTS

Pre- and Post-Module Assessment Results

To evaluate learning gains, students completed pre- and post-module quizzes assessing core cybersecurity concepts.

Social Engineering Module (n = 44):

- 19 students had heard of phishing but were unaware of specific techniques like baiting or spear phishing.
- Most students were aware of ransomware but unfamiliar with its operational mechanisms.
- 40 students reported low confidence in protecting themselves against social engineering attacks.

Authentication Module (n = 42):

- 20 students believed they had strong, unique passwords.
- 18 reported prior use of password managers.
- None had used “Have I Been Pwned?” or the TryHackMe platform before.

Post-module assessment:

- In the Social Engineering module, average quiz scores increased from 41% to 78%.
- In the Authentication module, scores increased from 45% to 82%.
- Paired-sample t-tests confirmed significant gains: Social Engineering:

Theme	Positive Aspects	Challenges	Actions Taken
Engagement	Interactive storytelling, hands-on exercises (TryHackMe, Go Phishing, password game)	Some quizzes and interactive elements are confusing	Introduced guides, shorter video segments (3–5 min), and onboarding tutorials
Practical skills	Real-world scenarios like phishing and ransomware simulations	Platform onboarding difficulties, technical jargon	Added tutorials, simplified language, and included a glossary
Clarity & Structure	Moodle course layout, logical progression	Background colors, long text sections	Content restructuring, visual breaks, clear instructions
Teacher Support	Optional teacher guides for discussion or group activities	Not all teachers are familiar with cybersecurity concepts	Teacher guides revised with step-by-step facilitation tips

Table 4. Summary of Qualitative Feedback and Actions Taken

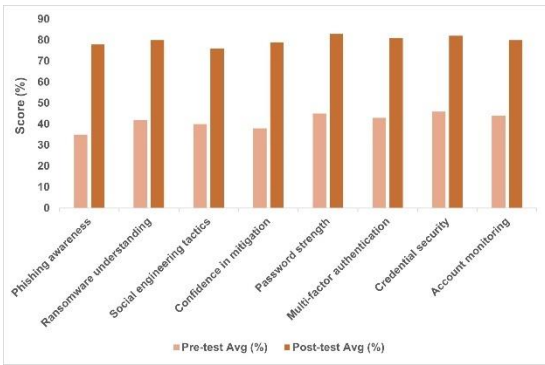


Figure 1. Pre- and Post-Module Quiz Scores for Social Engineering and Authentication Modules

$t(43) = 39.99, p < .001, \text{Cohen's } d = 6.03$; Authentication: $t(41) = 42.17, p < .001, \text{Cohen's } d = 6.51$. These results indicate substantial learning gains between pre- and post-assessments. The large effect sizes reflect the low baseline knowledge observed in pre-assessment, combined with the focused instructional content of the modules.

Student-reported outcomes:

- 40 of 44 students indicated learning practical skills applicable to daily tasks, such as verifying email senders and using stronger passwords
- 39 students enjoyed TryHackMe exercises, noting the real-life scenario experience.
- All students responded positively to the password game for assessing and improving password strength.

Figure 1 shows the overview of pre- and post-module quiz scores for the Social Engineering and Authentication modules.

Qualitative Feedback

Student feedback was collected through surveys, open-ended responses, and focus groups, and was categorized into positive aspects, challenges, and suggestions for improvement. Key results are presented in Table 4.

Student Focus Group Feedback:

- The Moodle platform was user-friendly, but some interactive elements required clearer navigation.
- Students suggested checklists at the end of modules and more localized case

studies relevant to Denmark; both were implemented.

- Students also requested additional preventive tips for personal cybersecurity, which were incorporated.

Teacher's Feedback:

- Instructors highlighted the importance of logical flow and accessible language.
- Technical jargon and video transitions need to be improved based on feedback.
- Quizzes need to be clear for intuitive navigation.

Following testing and refinement, both the Social Engineering and Authentication modules were revised based on student and instructor feedback and uploaded to the SmartLearning platform. Instructors across the eight Danish business academies can now provide students with access to self-paced learning, while optional classroom activities, such as discussions, group exercises, or the Go Phishing card game, allow teachers to reinforce practical cybersecurity skills collaboratively. This flexibility accommodates diverse teaching styles and learning contexts, ensuring consistent outcomes across Danish business academies and demonstrating the modules' effectiveness in engaging students and integrating with existing business programs.

7. LIMITATIONS

Despite the findings, the study includes several limitations. First, the study used pre- and post-module assessments but relied on basic inferential statistics (paired t-tests) and descriptive feedback.

Second, the modules were tested in a specific educational and cultural context in Denmark, which may limit transferability to other settings. Finally, although the modules integrate third-party tools like TryHackMe and "Have I Been Pwned?" to provide hands-on learning, these resources are optional based on student interest. Reliance on external platforms may raise concerns about long-term accessibility or technical compatibility, which should be addressed in future scaling.

Despite these limitations, the study contributes valuable insights into designing accessible cybersecurity education for non-technical learners using gamification and experiential methods grounded in proven instructional approaches.

8. CONCLUSION AND FUTURE WORK

This study presented the development and evaluation of two interactive cybersecurity modules designed for non-technical business students. Grounded in experiential and constructivist learning theories, the modules leveraged gamified, scenario-based activities to increase student engagement, understanding, and practical application of cybersecurity concepts. Results demonstrated meaningful learning gains, heightened awareness, and self-reported improvements in security practices.

Instructor and student feedback affirmed the relevance, usability, and motivational aspects of the modules, while also highlighting areas for refinement, such as language simplification, multimedia clarity, and onboarding for optional tools. These insights were incorporated into updated versions. The modules are now accessible to students and instructors across eight Danish business academies via the SmartLearning platform, demonstrating a replicable and scalable approach that could be transferred to other educational contexts.

Future work will focus on developing additional modules and adding more interactive elements. Efforts will also aim to inform teachers about the existence of these modules and provide guidance on how to incorporate them effectively into their teaching, ensuring broader adoption and practical impact.

9. ACKNOWLEDGEMENTS

We thank Andreas Fjord Bonven for his ongoing support, Allan Schnoor for game development and testing, and the eight Danish business academies for their valuable collaboration.

10. REFERENCES

- Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, 13(6), 2371–2380. <https://doi.org/10.1007/s41870-021-00760-5>
- Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science and IT Research Journal*, 5(1), 100–119. <https://doi.org/10.51594/csitrj.v5i1.708>
- Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, 106493. <https://doi.org/10.1016/j.ocecoaman.2023.106493>
- AlDaajeh, S., Saleous, H., Alrabaaee, S., Barka, E., Breitingner, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. *Computers & Security*, 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Bhusal, C. S. (2021). Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security*, 12, 104–114. <https://doi.org/10.4236/jis.2021.121005>
- Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, 27(3), 3011–3036. <https://doi.org/10.1007/s10639-021-10704-y>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Clark, R. C., & Mayer, R. E. (2023). *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning** (5th ed.). Wiley.
- Crumpler, W., & Lewis, J. A. (2022). Cybersecurity workforce gap. Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/cybersecurity-workforce-gap>
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), 1–35. <https://doi.org/10.1145/3469886>

- Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification." In *Proceedings of the 15th International Academic MindTrek Conference, pp. 9–15. <https://doi.org/10.1145/2181037.2181040>
- European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
- Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, 102080. <https://doi.org/10.1016/j.cose.2020.102080>
- Gwenhure, A. K., & Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. *International Journal of Serious Games*, 11(1), 83–99. <https://doi.org/10.17083/ijsg.v11i1.719>
- Hunt, T. (2025, Last visited November 16). Have I Been Pwned – Check if your email has been compromised in a data breach. <https://haveibeenpwned.com/>
- Landers, R. N. (2014). Developing a theory of gamified learning: Linking serious games and gamification of learning. *Simulation & Gaming*, 45(6), 752–768. <https://doi.org/10.1177/1046878114563660>
- Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, 190(1), 1–69. <https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf>
- Mayer, R. E. (2014). Incorporating motivation into multimedia learning. *Learning and Instruction*, 29, 171–173. <https://doi.org/10.1016/j.learninstruc.2013.05.001>
- Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. In *Transactions on Edutainment XV*, 93–107. Springer. https://doi.org/10.1007/978-3-662-59351-6_9
- National Institute of Standards and Technology (NIST). (2021). Cybersecurity games: Building tomorrow's workforce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-220.pdf>
- Palioura, M., & Dimoulas, C. (2022). Digital storytelling in education: A transmedia integration approach for the non-developers. *Education Sciences*, 12(8), 559. <https://doi.org/10.3390/educsci12080559>
- Saddiqa, M., Larsen, K. H., Nielsen, R. N., & Pedersen, J. M. (2021). Digital innovation in education: Perspectives, opportunities and challenges of educational open data and sensor data. In *2021 Joint Business Informatics Research Workshops and Doctoral Consortium, BIR-WS 2021, CEUR Workshop Proceedings, Vol. 74, 74–83*. <https://ceur-ws.org/Vol-2991/paper07.pdf>
- Saddiqa, M., Larsen, K. H., Nielsen, R. N., & Pedersen, J. M. (2023a). Building a diverse cybersecurity workforce: A study on attracting learners with varied educational backgrounds. *Journal of Cybersecurity Education, Research & Practice*, 2024 (1). <https://doi.org/10.32727/8.2023.33>
- Saddiqa, M., Larsen, K. H., Nielsen, R. N., Sørensen, L. T., & Pedersen, J. M. (2023b). Privacy and security training platform for a diverse audience. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer Nature Singapore, 343–363. https://doi.org/10.1007/978-981-99-6974-6_19
- Safitra, M. F., Lubis, M., & Fakhurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), 13369. <https://doi.org/10.3390/su151813369>
- Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 102756. <https://doi.org/10.1016/j.cose.2022.102756>
- Sikkerhed på Spil. (2023). Sikkerhed på Spil 2. SmartLearning. Retrieved July 24, 2025, from <https://learninghub.smartlearning.dk/projekter/sikkerhed-pa-spil-2/>
- Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in Human*

- Behavior, 87, 192–206.
<https://doi.org/10.1016/j.chb.2018.01.003>
- Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, 3(1), 47–67.
<https://doi.org/10.52889/ijses.v3i1.132>
- Tirfe, D., & Anand, V. K. (2022). A survey on trends of two-factor authentication. In *Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020*, 285–296, Springer.
https://doi.org/10.1007/978-981-16-4244-9_23
- Trumbach, C. C., Payne, D. M., & Walsh, K. (2023). Cybersecurity in business education: The “how to” in incorporating education into practice. *Industry and Higher Education*, 37(1), 35–45.
<https://doi.org/10.1177/09504222221099389>
- TryHackMe. (Last visited 2025, November 19). TryHackMe – Learn cybersecurity, penetration testing, and ethical hacking.
<https://tryhackme.com/>
- Wiechetek, Ł., & Mędrek, M. (2022). Human factors in security–cybersecurity education and awareness of business students. *Annales Universitatis Mariae Curie-Skłodowska, Sectio H–Oeconomia*, 56(1), 119–142.
<https://doi.org/10.17951/h.2022.56.1.119-142>
- Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students. *Journal of The Colloquium for Information Systems Security Education*, 11(1), 8.
<https://doi.org/10.53735/cisse.v11i1.186>
- Yang, Y. T. C., & Wu, W. C. I. (2012). Digital storytelling for enhancing student academic achievement, critical thinking, and learning motivation: A year-long experimental study. *Computers & Education*, 59(2), 339–352.
<https://doi.org/10.1016/j.compedu.2012.02.003>
- Zajda, J. (2021). Constructivist learning theory and creating effective learning environments. In *Globalisation and Education Reforms: Creating Effective Learning Environments*, 35–50. Springer.
https://doi.org/10.1007/978-3-030-71575-5_3
- Zaric, N., Roepke, R., Lukarov, V., & Schroeder, U. (2021). Gamified learning theory: The moderating role of learners’ learning tendencies. *International Journal of Serious Games*, 8(3), 71–91.
<https://doi.org/10.17083/ijsg.v8i3.438>