AI-Augmented Public Security Interfaces: Advancing Cybersecurity Awareness through Adaptive Learning

Doruntina Murtezaj
doruntina.murtezaj@unibw.de
University of the Bundeswehr Munich
Munich, Germany
LMU Munich
Munich, Germany

Viktorija Paneva
viktorija.paneva@ifi.lmu.de
LMU Munich
Munich, Germany

Florian Alt
florian.alt@ifi.lmu.de
LMU Munich
Munich, Germany
University of the Bundeswehr Munich
Munich, Germany

Abstract

Public displays are widely used for various applications, including advertising, transportation, and public service announcements. However, their potential in the security domain remains largely untapped. Public Security Interfaces (PSIs) play a crucial role in cybersecurity education by providing interactive and accessible learning experiences [12]. Nevertheless, traditional PSIs lack adaptability, personalized feedback, and emotional awareness, which can limit user engagement and learning effectiveness. This position paper explores how AI-powered enhancements can improve PSIs, based on the use case of *Roby's Password Mission*, a public display quiz designed to promote password manager adoption. We propose integrating adaptive learning mechanisms, sentiment-aware feedback, and AI-driven gamification to provide a tailored user experience. These AI-driven improvements enable PSIs to dynamically adjust difficulty, personalize feedback based on user interactions, and create a more supportive learning environment. We outline future research directions and discuss how AI can enhance PSIs in fostering secure behavior.

Keywords

Public Security Interfaces (PSIs), AI-driven learning, cybersecurity education, adaptive interfaces, emotion-aware AI, gamification, intelligent public displays, personalized security awareness, behavior change, AI-powered feedback systems

1 Introduction

Public Security Interfaces (PSIs) are interactive public displays designed to educate and engage users on cybersecurity topics [12]. Given the increasing threats in digital security, raising awareness and fostering secure behavior through public education has become essential. Traditional approaches, such as security awareness posters or static digital screens, often fail to captivate users or adapt to individual learning needs [11, 14].

We conceptualized and developed a gamified public display quiz aimed at increasing awareness about password managers. While effective at engaging users, its static feedback system and uniform difficulty level limit personalized learning experiences. AI integration can address these limitations by dynamically adjusting content based on user performance, providing sentiment-aware responses, and leveraging gamification elements to sustain engagement.

This position paper explores how AI can enhance PSIs by focusing on three key areas: adaptive learning and personalized feedback, emotion recognition and sentiment-aware feedback, and AI-driven gamification for engagement. The conclusion includes future research directions and the broader implications of AI-driven PSIs for cybersecurity education.

2 Workshop Info

The need for AI in education is becoming more urgent due to the increasing diversity in student needs, learning styles, and socioeconomic backgrounds. Traditional teaching approaches that rely on standardized curricula and manual feedback are no longer sufficient to meet these varied demands. AI technologies, especially those powered by large language models (LLMs), offer a solution by enabling tailored feedback at scale and providing personalized learning experiences across a range of disciplines, from writing and debate to project-based activities. Additionally, AI's ability to process large amounts of data from student interactions enables real-time insights, allowing teachers to focus on high-impact tasks such as nurturing creativity, critical thinking, and problem-solving.

3 Motivation

AI is transforming education by offering personalized learning experiences, real-time feedback, and content that adjusts to individual needs [18]. Tools like intelligent tutoring systems and adaptive learning platforms can customize instruction, boosting engagement and improving knowledge retention [4]. Studies indicate that AI-driven approaches enhance learning outcomes by making educational content more interactive and aligned with each learner's progress [1, 15]. However, in areas like security education, where interest and engagement are often lacking, AI has the potential to make learning more compelling and impactful [3]. By integrating innovative methods and tailoring experiences to individual preferences, AI can address the challenge of disengagement and foster a deeper understanding of critical topics. Despite its potential, the wider implications of AI in education, such as its impact on teaching methods, accessibility and ethical considerations, need to be further explored to ensure its full benefits are realised.

Public displays are effective tools for education, offering spontaneous engagement without requiring users to install apps or seek out information [10]. This is particularly beneficial for cybersecurity awareness, where users often overlook security best practices until directly confronted with risks. Prior research has shown that interactive public displays enhance knowledge retention and behavior change by making learning more engaging and accessible [13, 17]. Gamified public displays have been found to improve user participation and motivation [7, 8], making them a suitable medium for security-related topics.

Unlike static awareness campaigns, public displays can use interactivity, visual cues, and AI-driven personalization to dynamically adapt content, provide tailored feedback, and adjust difficulty levels to accommodate different users. Furthermore, public displays create opportunities for social learning [6]. When users interact with a display in a public or semi-public space, bystanders may also take notice and join the activity, sparking conversations on the topic. This social aspect of learning has been shown to reinforce knowledge retention and encourage community-wide adoption of security practices [9]. A promising area to explore is how AI can enhance PSIs by addressing challenges such as adaptability, technical feasibility, and ethical considerations, with the goal of making security learning more effective and inclusive.

4 Use Case: Adoption of a Password Manager

The main purpose of this use case is to promote awareness about cybersecurity, specifically password managers, through PSIs. The quiz-based application aims to educate users on the importance of secure password behavior, the general functionality of a password manager and motivate them to integrate password managers into their daily lives. As the interface is designed for a public display, its primary goal is to capture user attention.

The welcome screen (see Figure 1-a) includes the quiz's name, a short description, and an indicator that the screen is interactive, featuring a touch icon. To enhance user engagement, the quiz features animations and a jumping robot avatar that guides users through their journey. The robot presents cybersecurity facts through speech bubbles, designed to further capture the user's attention. The robot is designed to appear friendly and inviting. The quiz name, *Roby's Password Mission* and the touch-screen indicator, conveys that the display is interactive and related to passwords. During the quiz, users get to know Roby's story and assist him with password-related challenges.

The quiz comprises six questions. An example question is: *"Roby has collected a few ideas for his new password. Help him choose the best one."* (see Figure 1-b). After each question, the user receives feedback on their chosen option (see Figure 1-c). This encourages them to reflect on their own secure behavior and realize that some methods they use may not be as secure as they previously believed. The feedback includes a description, an updated mood for Roby's avatar, and a visual or animation aligned with the feedback. For instance, Roby may display a smiling face when the most secure option is selected, while a sad or worried face appears for less secure choices. Visuals include animated clocks showing how quickly different passwords can be cracked. For the most secure answers, celebratory confetti is displayed to provide positive and rewarding feedback. After completing all the questions, the final screen thanks the user for helping Roby and shows a final score (see Figure 1-d). Additionally, a QR code is used to trigger the action of downloading the Bitwarden[1] password manager.

After some design iterations, we plan to deploy the application on public displays across the university campus as part of a field study to evaluate its effectiveness in a real-world setting. This deployment aligns with a broader campaign to promote secure password practices, and we have chosen to recommend this specific password manager as it supports an ongoing initiative to introduce it to university employees. The in-the-wild deployment will enable us to observe user engagement, gather feedback, and refine our approach based on real-world interactions outside of a controlled lab environment.

5 AI-Augmented Enhancements

While traditional public user interfaces serve as effective tools for raising awareness on cybersecurity topics, they often rely on one-size-fits-all approaches. This limits their ability to adapt to individual users, provide tailored learning experiences, and sustain engagement over time. AI-powered enhancements can address these limitations by making these interfaces more responsive, personalized, and interactive.

Adaptive Learning and Personalized Feedback. AI-driven PSIs can analyze user responses to dynamically adjust difficulty and personalize feedback. If a user struggles with certain concepts, the system can simplify questions and provide additional explanations. For more advanced users, complex security scenarios can be introduced to maintain engagement and challenge their knowledge. AI-powered content adaptation ensures that users receive educational material suited to their knowledge level, enhancing learning outcomes and preventing disengagement due to overly simplistic or overly complex content [5].

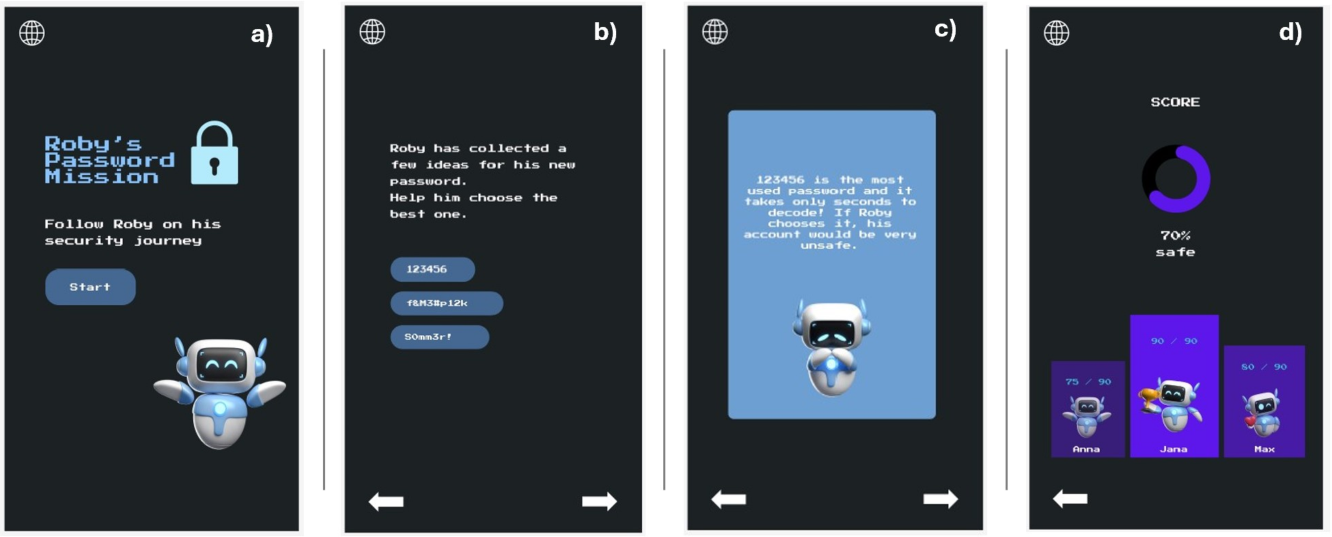
Emotion Recognition and Sentiment-Aware Feedback. AI can improve user experience by detecting emotions and adjusting responses accordingly. Facial expression analysis and tracking interaction speed can help identify when a user is frustrated or disengaged [2]. If the system detects hesitation or signs of confusion, it can offer supportive encouragement or suggest helpful hints. Personalized feedback responses, such as reinforcing correct answers with positive reinforcement or guiding struggling users with clearer explanations, help maintain motivation. By adapting the quiz's tone in real-time, PSIs can create a less intimidating learning environment.

AI-Driven Gamification for Engagement. Gamification elements can be enhanced using AI to keep users motivated [16]. AI-generated hints can provide context-sensitive guidance when users struggle with a task, allowing them to learn without feeling discouraged. Progress-based rewards, such as animations, point accumulation, and interactive visual effects, reinforce positive behavior and sustain engagement. Dynamic difficulty scaling ensures that users remain challenged but not overwhelmed, allowing for a more enjoyable learning experience.

6 Key Challenges and Open Questions

While AI-enhanced PSIs present promising opportunities, several key challenges and open questions remain. Addressing these questions is key to refining the design and deployment of intelligent

[1] https://bitwarden.com (Last accessed: 26.02.2025)



Follow Roby on his security journey

Roby has collected a few ideas for his new password.
Help him choose the best one.

123456 is the most used password and it takes only seconds to decode! If Roby chooses it, his account would be very unsafe.

Figure 1: Screenshots of *Roby's Password Mission* illustrating the main stages of user interaction. (a) The welcome screen, which introduces the quiz and invites users to participate. (b) An example quiz question, where users assess a password-related scenario. (c) The feedback screen, providing immediate textual and visual feedback on the user's response using color-coded indicators. (d) The final screen, displaying the user's total score and encouraging further engagement with password managers.

PSIs, ensuring they are effective, ethical, and impactful in promoting cybersecurity awareness.

- A central question is how to evaluate the real-world effectiveness of AI-driven PSIs. *How can we measure improvements in cybersecurity awareness and assess whether these systems lead to sustained behavior change rather than short-term engagement?* Identifying appropriate metrics and designing longitudinal studies will be crucial to understanding their long-term impact.
- Ethical concerns, particularly regarding AI-powered emotion recognition and user privacy, also require attention. *How do we balance personalization with privacy in public settings? What safeguards are necessary to prevent misuse of emotion detection technologies?* Additionally, ensuring transparency and user consent in AI-driven PSIs is essential to fostering trust and encouraging engagement.
- Another discussion point is the role of AI-driven gamification and adaptive feedback in reinforcing secure behavior. *Can these techniques effectively motivate users beyond initial interactions? How can PSIs encourage long-term habit formation rather than fleeting engagement?* Exploring strategies that integrate social dynamics and collaborative interactions may offer new insights into their effectiveness.
- A challenge unique to PSIs is addressing group interactions. Public displays are often viewed by multiple users at once, potentially leading to collaborative learning or conflicting interactions. *How should PSIs adapt when multiple people engage simultaneously? Should content be tailored based on the group composition, and how can AI mediate interactions to ensure inclusive and productive engagement?*
- Finally, scalability and technical feasibility is an important consideration. *What are the technical constraints of deploying AI-enhanced PSIs in real-world environments, and how can they be overcome?*

7 Conclusion

This position paper highlights how AI can enhance PSIs by integrating adaptive learning, sentiment-aware responses, and gamification elements. These advancements personalize the learning experience, improve user engagement, and foster secure behaviors. Future research should focus on refining AI-driven techniques, ensuring ethical considerations, and expanding PSIs to cover broader security topics. By leveraging AI, PSIs can become more intelligent and effective tools for cybersecurity education in public spaces.

Acknowledgments

This research is part of the *Voice of Wisdom* project and received funding from dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

References

[1] Amy Adair. 2023. Teaching and Learning with AI: How Artificial Intelligence is Transforming the Future of Education. *XRDS* 29, 3 (April 2023), 7–9. doi:10.1145/3589252

[2] Ajwa Aslam, Allah Bux Sargano, and Zulfiqar Habib. 2023. Attention-based multimodal sentiment analysis and emotion recognition using deep neural networks. *Appl. Soft Comput.* 144, C (Sept. 2023), 16 pages. doi:10.1016/j.asoc.2023.110494

[3] Karla Carter. 2023. "I, ChatBot": Co-Teaching Cybersecurity Courses With Generative AI. *J. Comput. Sci. Coll.* 39, 3 (Oct. 2023), 27–28.

[4] Mahmoud Elkhodr and Ergun Gide. 2025. Integrating Generative AI in Cybersecurity Education: Case Study Insights on Pedagogical Strategies, Critical Thinking, and Responsible AI Use. arXiv:2502.15357 [cs.CY] https://arxiv.org/abs/2502.15357

[5] Ilie Gligorea, Marius Cioca, Romana Oancea, Andra-Teodora Gorski, Hortensia Gorski, and Paul Tudorache. 2023. Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review. *Education Sciences* 13, 12 (2023). doi:10.3390/educsci13121216

[6] Simo Hosio, Andy Alorwu, Niels van Berkel, Miguel Bordallo López, Mahalakshmy Seetharaman, Jonas Oppenlaender, and Jorge Goncalves. 2019. Fueling AI with public displays? a feasibility study of collecting biometrically tagged consensual data on a university campus. In *Proceedings of the 8th ACM International Symposium on Pervasive Displays* (Palermo, Italy) *(PerDis '19)*. Association for Computing Machinery, New York, NY, USA, Article 14, 7 pages. doi:10.1145/3321335.3324943

[7] Tuuli Keskinen, Jaakko Hakulinen, Tomi Heimonen, Markku Turunen, Sumita Sharma, Toni Miettinen, and Matti Luhtala. 2013. Evaluating the experiential user

experience of public display applications in the wild. In *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia* (Luleå, Sweden) *(MUM '13)*. Association for Computing Machinery, New York, NY, USA, Article 7, 10 pages. doi:10.1145/2541831.2541840

[8] Ioannis Leftheriotis, Michail Giannakos, and Letizia Jaccheri. 2017. Gamifying informal learning activities using interactive displays: an empirical investigation of students' learning and engagement. *Smart Learning Environments* 4 (05 2017). doi:10.1186/s40561-017-0041-y

[9] Nemanja Memarovic, Marc Langheinrich, Florian Alt, Ivan Elhart, Simo Hosio, and Elisa Rubegni. 2012. Using public displays to stimulate passive engagement, active engagement, and discovery in public spaces. In *Proceedings of the Media Architecture Biennale Conference: Participation* (Aarhus, Denmark) *(MAB '12)*. Association for Computing Machinery, New York, NY, USA, 55–64. doi:10.1145/2421076.2421086

[10] Mateusz Mikusz, Peter Shaw, Nigel Davies, Petteri Nurmi, Sarah Clinch, Ludwig Trotter, Ivan Elhart, Marc Langheinrich, and Adrian Friday. 2021. A Longitudinal Study of Pervasive Display Personalisation. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 2 (Jan. 2021), 45 pages. doi:10.1145/3418352

[11] Jörg Müller, Florian Alt, Daniel Michelis, and Albrecht Schmidt. 2010. Requirements and design space for interactive public displays. In *Proceedings of the 18th ACM International Conference on Multimedia* (Firenze, Italy) *(MM '10)*. Association for Computing Machinery, New York, NY, USA, 1285–1294. doi:10.1145/1873951.1874203

[12] Doruntina Murtezaj, Viktorija Paneva, Verena Distler, and Florian Alt. 2025. Public Security User Interfaces: Supporting Spontaneous Engagement with IT Security. In *Proceedings of the New Security Paradigms Workshop (NSPW '24)*. Association for Computing Machinery, New York, NY, USA, 56–70. doi:10.1145/3703465.3703470

[13] Jörg Müller, Florian Alt, Albrecht Schmidt, and Daniel Michelis. 2012. Looking Glass: A Field Study on Noticing Interactivity of a Shop Window. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 297–306. doi:10.1145/2207676.2207719

[14] Callum Parker, Martin Tomitsch, and Judy Kay. 2018. Does the Public Still Look at Public Displays? A Field Observation of Public Displays in the Wild. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 73 (July 2018), 24 pages. doi:10.1145/3214276

[15] Shaila Rana and Rhonda Chicone. 2025. *Gamification and Immersive Learning with AI*. Springer Nature Switzerland, Cham, 51–75. doi:10.1007/978-3-031-81780-9_3

[16] Z. Cliffe Schreuders and Emlyn Butterfield. 2016. Gamification for Teaching and Learning Computer Security in Higher Education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders

[17] Marcus Winter. 2021. Display Placement and Design: Impact on Engagement with Social Object Labels in a Gallery Environment. In *Computer-Human Interaction Research and Applications*, Maria Jose Escalona, Andres Jimenez Ramirez, Hugo Plácido Silva, Larry Constantine, Markus Helfert, and Andreas Holzinger (Eds.). Springer International Publishing, Cham, 1–24.

[18] Husam Yaseen, Abdelaziz Saleh Mohammad, Najwa Ashal, Hesham Abusaimeh, Ahmad Ali, and Abdel-Aziz Ahmad Sharabati. 2025. The Impact of Adaptive Learning Technologies, Personalized Feedback, and Interactive AI Tools on Student Engagement: The Moderating Role of Digital Literacy. *Sustainability* 17, 3 (2025). doi:10.3390/su17031133