

Theory-Grounded Cybersecurity Escape Rooms for Secondary Education: Three Student-Designed Prototypes

Luisa Jansen
University of Bern

Lara Jäggi
University of Bern

Noa Rohner
University of Bern

Annika Wenzl
PH Bern

Malte Elson
University of Bern

Abstract

As young people increasingly navigate complex digital environments, schools face growing pressure to provide effective cybersecurity education. However, cybersecurity education in secondary school remains limited, leading to gaps in digital literacy and confidence in dealing with online risks.

This paper presents three interactive, theory-grounded escape room prototypes for secondary education (grades 7–9) designed to support early cybersecurity learning. The designs were developed in an interdisciplinary seminar and are informed by problem-based learning and self-efficacy theory to promote active engagement, collaboration, and confidence in dealing with digital threats. The prototypes address competencies regarding (1) digital identity and online behavior, (2) cybergrooming prevention, and (3) detection of social engineering attacks. All three escape rooms are embedded in a shared narrative to increase engagement and continuity.

The prototypes aim to bridge the gap between motivational game-based learning approaches and pedagogical grounding. We propose plans for an evaluation study.

1 Introduction

Although young people are frequent users of the Internet, cybersecurity education remains unevenly distributed: younger students receive less exposure to cybersecurity content than older peers [7, 10]. Yet even where training is accessible, it does not prevent disproportionately high rates of cybercrime victimization rates among younger users [2]. Traditional curricula add to the problem, leaving significant gaps in students'

cybersecurity knowledge by emphasizing programming skills rather than holistic digital literacy [11]. As a result, young people often show signs of "cyber resignation", assuming security breaches are inevitable [15]. Against these trends, pupils require continuous, practical, and behavior-focused learning programs embedded in school education, focusing not only on technical instructions, but also on fostering their self-efficacy [15, 16].

In recent years, escape rooms for cybersecurity education have emerged as a promising tool for engaging student. Escape rooms are interactive, game-based learning environments in which participants collaboratively solve interconnected puzzles and challenges under time constraints to achieve a specific goal [22]. First empirical evaluations of escape rooms in university contexts show their potential for engaging and cooperative learning [22], effects on motivation [14], and indicators for improvements in so-called 21st century skills [20]. In a meta-analysis, [13] report substantial learning gains of escape rooms in education across age groups and contexts. However, a key challenge lies in aligning game mechanics with pedagogical goals [21]. Systematic reviews reinforce this design imperative and emphasize the pedagogical potential of escape rooms when integrated thoughtfully [14, 22].

Research addressing escape rooms specifically in cybersecurity education remains limited. Existing implementations are largely situated in higher education, but show improvements in understanding of cybersecurity concepts for university students [8, 19]. Secondary school students are underrepresented in this body of literature [3, 20]. Nonetheless, other game-based approaches have already demonstrated positive outcomes in school settings [12].

Building on this, we developed three escape room prototypes for early cybersecurity education within school curricula. To improve the alignment between pedagogical goals and contents, we use two established learning theories, problem-based learning and self-efficacy theory:

In **Problem-Based Learning (PBL)**, students actively solve real problems by researching information, creating solutions, and thinking about their results, instead of just memo-

izing facts [6]. Next to declarative knowledge, this approach also teaches important skills such as responsibility, teamwork, and reflection [6].

Self-efficacy refers to an individual's belief in their ability to successfully manage challenging or threatening situations [4]. It is an important, consistent predictor of intentions and behaviors in cybersecurity [9]. **Self-Efficacy Theory** identifies four sources of self-efficacy: mastery experience (the strongest), vicarious experience, persuasion, and affective states [4]. Self-efficacy is a relevant variable in many influential theories explaining behavior, e.g., Bandura's own Socio-Cognitive Theory [5], Rogers' Protection Motivation Theory [18], and Ajzen's Theory of Planned Behavior [1].

2 Escape Room Prototypes

Development Process. In an interdisciplinary university seminar, we developed three escape room prototypes for students in grades 7 to 9 to improve key competencies in the digital space. Psychology and pedagogy students developed content based on the aforementioned learning theories. Throughout the seminar, students interacted with cybersecurity domain experts and practitioners with experience in building escape rooms to achieve sound learning tools and accurate content.

Scope of Escape Rooms. The escape rooms focus on different relevant topics (i.e., cybergrooming, social engineering, digital citizenship), but are connected by an overarching story and setting: They follow the character Edwin, an alien, who discovers the digital world and encounters various challenges. Students support him in identifying risky situations and responding appropriately, thereby linking the contents of the individual escape rooms. The escape rooms are designed for students in grades 7 to 9 who are about 11 to 15 years old. They work on the escape rooms in small groups within a class period of approximately 45 to 60 minutes.

Escape Room I: Digital Identity. The first developed escape room prototype aims to foster students' competencies in managing their digital identity. The overall objective is to strengthen their ability to recognize risks and act responsibly in digital environments. The educational concept comprises four interconnected puzzles based on the STEP model (STOP, THINK, EMPATHIZE, PRIVACY) [17], focusing on recognizing risky situations, reflective decision-making, perspective-taking, and the conscious handling of privacy. Throughout the activities, students engage in tasks such as classifying chat messages and making appropriate decisions in digital interaction scenarios.

Escape Room II: Cybergrooming. The second prototype addresses cybergrooming prevention and aims to enhance students' self-efficacy in recognizing and countering grooming tactics. The objective is to equip students with the knowledge and confidence to recognize grooming tactics and act decisively in risky digital situations. The educational concept consists of three interconnected puzzles grounded in self-efficacy

theory and protection motivation theory, progressing from threat recognition to coping strategy selection and risk evaluation. A distinguishing feature is the emphasis on mastery experiences: students solve puzzles independently and build confidence in responding to manipulative online interactions.

Escape Room III: Social Engineering. The third prototype addresses social engineering prevention, focusing on phishing via different attack vectors. The overall objective is to inform about everyday phishing risks and train students to recognize and resist manipulative messages in their digital lives. The educational concept comprises three puzzles grounded in creating mastery experience in accordance with self-efficacy theory. The puzzles cover three phishing variants: social media phishing, SMiShing, and chain-phishing.

3 Discussion and Planned Evaluation

We present three prototypes of escape rooms for cybersecurity education in grade 7 to 9. The prototypes are grounded in established learning theories, bridging the gap between promising first results of escape rooms and their lacking pedagogical conception. We hope to contribute to the development of digital skills for the especially vulnerable and understudied group of 11- to 15-year-olds.

However, we acknowledge several limitations: Most centrally, we did not conduct any empirical evaluations on the effectiveness or enjoyability of our concepts. Also, we understand that escape rooms are usually one-off, short interventions that cannot, on their own, bridge the existing skill gaps. While we see value in a positive, fun-based introduction to cybersecurity learning, escape rooms need to be embedded in a curriculum that teaches the necessary competencies.

In the future, we plan to implement the escape rooms and evaluate them over several stages: In the first stage, we will have the escape rooms reviewed by experts in cybersecurity, who will assess the technical accuracy and relevance of the content, and by experts in pedagogy, who will evaluate the instructional design and age-appropriateness. We will also involve practicing teachers, whose feedback addresses curricular fit and feasibility. This feedback will be gathered through questionnaires and interviews, then synthesized to identify improvements. In the second stage, we will conduct walk-throughs with students from the target population to observe how they engage with the rooms. These sessions will reveal usability issues, puzzle difficulty, and engagement gaps that experts might not anticipate. After each stage, we will undertake iterative improvements, addressing identified issues before moving on. Finally, upon their first implementations in schools, we will use a pre-post design to measure the intended gains in students' knowledge, skills, and attitudes.

In conclusion, this paper proposes three theory-based escape room prototypes for cybersecurity education in secondary schools, designed to offer a positive, self-efficacy-enhancing first encounter with the topic.

Ethics

As we did not conduct any human-subjects research in this project, we have no ethical considerations to report.

References

- [1] Icek Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, December 1991.
- [2] National Cybersecurity Alliance. *STUDY: 37% Intimidated, 39% Frustrated with Online Security Highlighting Digital Anxiety*. October 2023.
- [3] Mostafa Hussam Mostafa Altarawneh, Ahmad Althunibat, Mohammad Husien Almajali, Naif Alzriqat, and Seif Alazzam. Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. *International Journal of Innovative Research and Scientific Studies*, 8(1):1516–1529, February 2025.
- [4] Albert Bandura. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2):191–215, 1977.
- [5] Albert Bandura. On the Functional Properties of Perceived Self-Efficacy Revisited. *Journal of Management*, 38(1):9–44, January 2012.
- [6] John Barell. *Problem-Based Learning: An Inquiry Approach*. SAGE Publications, 2007.
- [7] EdWeek Research Center. *The State of Cybersecurity Education in K-12 Schools*. June 2020.
- [8] Sam Collins, Adithya Phanish, Diya Modi, Jacob Mayne, Matt Tabraham, Trinity Barson, Viacheslav Radiukov, Yusuf Hegazy, Yike Fang, Luca Arnaboldi, Marius Muench, and Todd Waugh Ambridge. HackRoom: A Pop Up Cyber Security Escape Room for Interactive Learning. In Phil Legg, Natalie Coull, Charles Clarke, Harjinder Lallie, and Hany Atlam, editors, *Advances in Teaching and Learning for Cyber Security Education*, volume 1791, pages 1–33. Springer Nature Switzerland, Cham, 2026.
- [9] ENISA. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Publications Office, LU, 2018.
- [10] Michelle Faverio and Olivia Sidoti. *Teens, Social Media and Technology 2024*. Pew Research Center, December 2024.
- [11] Said Gulyamov, Jahongir Babaev, and Uktam Rakhmatov. Building Cybersecurity Culture in Education as Imperative for Youth to Thrive in Digital Society. *Uzbek Journal of Law and Digital Policy*, 2(5):1–10, October 2024.
- [12] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)*, 12(1):150–158, February 2018.
- [13] Sonsoles López-Pernas. Educational Escape Rooms Are Effective Learning Activities Across Educational Levels and Contexts: A Meta-Analysis. *IEEE Transactions on Learning Technologies*, 17:711–724, 2024.
- [14] Agoritsa Makri, Dimitrios Vlachopoulos, and Richard A. Martina. Digital Escape Rooms as Innovative Pedagogical Tools in Education: A Systematic Literature Review. *Sustainability*, 13(8):4587, April 2021.
- [15] James Nicholson, Julia Terry, Helen Beckett, and Pardeep Kumar. Understanding Young People’s Experiences of Cybersecurity. In *Proceedings of the 2021 European Symposium on Usable Security*, pages 200–210, Karlsruhe Germany, October 2021. ACM.
- [16] Dana Ondrušková and Richard Pospíšil. The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology*, 15(3):ep435, July 2023.
- [17] Michelle O’Reilly, Nikki Kiyimba, and Diane Levine. Promoting a digital ethics of care: A digital cognitive interruption to facilitate U.K. adolescents’ empathy in online spaces. *Journal of Children and Media*, 19(2):307–326, April 2025.
- [18] Ronald W. Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change¹. *The Journal of Psychology*, 91(1):93–114, September 1975.
- [19] Thitima Srivatanakul. Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning. *Journal of Cybersecurity Education, Research and Practice*, 2024(1), September 2024.
- [20] Lene Hayden Taraldsen, Frode Olav Haara, Mari Skjerdal Lysne, Pernille Reitan Jensen, and Eirik S. Jenssen. A review on use of escape rooms in education – touching the void. *Education Inquiry*, 13(2):169–184, April 2022.
- [21] Alice Veldkamp, Sigrid Merx, and Jasper Van Winden. Educational Escape Rooms: Challenges in Aligning Game and Education, October 2020.

- [22] Alice Veldkamp, Liesbeth van de Grint, Marie-Christine P. J. Knippels, and Wouter R. van Joolingen. Escape education: A systematic review on escape rooms in education. *Educational Research Review*, 31:100364, November 2020.