Journal of Applied Engineering and Technological Science
Vol 7(1) 2025:539-549

ASSESSMENT OF CYBER SECURITY AWARENESS USING DEVELOPED GAME FROM H5P ON USERS AGED AT ELEMENTARY AND FIRST SECONDARY SCHOOL IN MADIUN CITY

Andria[1], Ridam Dwi Laksono[2], Kelik Sussolaikah[3*], Mazura Binti Mat Din[4], Shaifizat Mansor[5], Siti Rafidah Muhamat Dawam[6]
Universitas PGRI Madiun, Indonesia[123]
UiTM Cawangan Kedah, Malaysia[456]
andria@unipma.ac.id[1], ridam.dl@unipma.ac.id[2], kelik@unipma.ac.id[3],
mazuramd@uitm.edu.my[4], shaifizat@uitm.edu.my[5], srafidah192@uitm.edu.my[6]

Received: 05 December 2024, Revised: 07 May 2025, Accepted: 25 August 2025
**Corresponding Author*

ABSTRACT
The increasing cyber threats among children using digital devices without supervision highlight the importance of early cybersecurity awareness. This study aims to develop and evaluate an H5P-based educational game to enhance cybersecurity awareness among elementary and junior high school students in Madiun City. Using a Research and Development (R&D) approach, the game was developed through four stages: needs analysis, design and development, expert validation, and limited field testing. The game incorporates gamification elements such as points, badges, and instant feedback to engage students in learning topics such as password management, data protection, and phishing recognition. The results indicate that 70% of 68 elementary students and 74% of 92 junior high school students showed improved awareness after playing the game. These findings suggest that interactive educational games can effectively enhance cybersecurity awareness among children. The study recommends broader implementation of gamified approaches in educational curricula to foster safe online behavior from an early age.
Keywords: *Assessment, Cyber Security, Gamification.*

1. Introduction

The digital revolution, often referred to as "cyber civilization," has significantly altered how humans interact in various aspects of life, including communication, business, and access to information (Admass et al., 2024). This rapid technological development has made digitalization an essential component of daily life for individuals and organizations alike (Catanese et al., 2012; Serpa et al., 2020). However, this progress also introduces critical challenges, particularly cybersecurity threats that increasingly target vulnerable users, such as children. As children are spending more time using digital devices, they are exposed to significant online risks, especially when unsupervised (Akter et al., 2022). The potential consequences of these threats are dire, as they can compromise the confidentiality, integrity, and availability of sensitive data and online services (Xu et al., 2023).

The growing usage of gadgets among students, particularly after the COVID-19 pandemic, further exacerbates these vulnerabilities (Eshetu et al., 2024). This situation is critical in developing countries like Indonesia, where a significant gap remains in policymakers' understanding of cybersecurity and the lack of robust, nationwide cybersecurity policies (Chaudhary et al., 2023; Da Veiga et al., 2023). To address these risks, preventive measures must be implemented at both the individual and group levels (Ayyash et al., 2024). Moreover, cybersecurity education campaigns are essential for building knowledge and fostering safe digital habits from an early age (Admass et al., 2024; Kuraku et al., 2023).

A key aspect of these efforts is the use of gamified learning tools that can engage young learners effectively. One innovative approach is the use of H5P, a platform designed to create interactive content such as videos and games (Rahmi et al., 2024). H5P has proven effective in boosting user engagement and can be integrated with Moodle, a learning management system, to create educational games that promote cybersecurity awareness (Hayati & Guspatni, 2023). While H5P has primarily been used for blended and online learning, its potential to develop interactive games for measuring cybersecurity awareness has been largely unexplored (Serpa et al., 2020).

The increasing complexity of cyber threats has highlighted the urgent need for comprehensive cybersecurity education. It is no longer just a concern for technology professionals but also a critical issue for general internet users, including children (Guo & Tinmaz, 2023; Shaikh & Siponen, 2024). Understanding privacy, trust, and the risks associated with online activities is fundamental in shaping users' attitudes and behaviors toward cybersecurity (Alfalah, 2023; Hong et al., 2023). However, children, especially in Indonesia, often lack awareness of these risks, particularly when accessing the internet without adult supervision (Ayanwale et al., 2024).

In response to this gap, this study aims to develop an innovative tool that assesses and improves cybersecurity awareness among elementary and junior high school students, aged 6–14 years, using an H5P-based educational game. The game will incorporate gamification elements like points and badges to engage students and help them learn about key cybersecurity topics such as password management, data protection, and phishing recognition.

2. Literature Review

Cybersecurity awareness among children has become a critical concern due to the increasing threats targeting young users online. The rise of phishing, online scams, and the broader issue of digital footprints significantly impact children's digital safety. Research shows that children, especially those unsupervised, are more vulnerable to cyber threats due to their limited understanding of digital security practices (Alfalah, 2023; Ayanwale et al., 2024; Alrobaian et al., 2023). The increasing dependency on gadgets, particularly among elementary and junior high school students, heightens this risk, especially post-pandemic, as online learning and social media usage have surged (Eshetu et al., 2024). Addressing these threats requires early interventions to shape children’s attitudes towards safe online behavior.

Cybersecurity Awareness in Education

The importance of early cybersecurity education has been well-documented. Studies indicate that children who receive education on digital safety from a young age are better equipped to handle online risks (Kianpour & Raza, 2024; Alyami et al., 2023). This intervention helps to foster a culture of cybersecurity awareness that can extend into their adulthood (Kuraku et al., 2023). Recent research by Mat Din et al. (2023) focused on an H5P-based Moodle learning platform to enhance cybersecurity awareness among elementary and middle school students in Madiun, Indonesia. Their findings showed that interactive platforms like these could make cybersecurity education more engaging and effective, particularly in overcoming gaps in students’ cybersecurity knowledge. This aligns with research by Hayati and Guspatni (2023), who found that interactive learning using H5P significantly improved students’ engagement in chemistry classes.

Furthermore, research by Diaz-Rodas (2024) demonstrated the effectiveness of H5P for teacher training in digital content creation. By using a hands-on approach, teachers developed better digital content creation skills, which indirectly support the integration of cybersecurity education tools. These findings highlight the potential of H5P as a versatile tool not just for content creation but also for enhancing digital literacy in various domains, including cybersecurity.

Gamification in Cybersecurity Education

Gamification is increasingly recognized as an effective pedagogical tool, particularly for enhancing student engagement and learning outcomes in digital environments. According to Cassano et al. (2018) and Pirta-Dreimane et al. (2024), incorporating game design elements such as points, badges, and leaderboards into educational contexts helps motivate students and enhances their participation. This approach has been successfully applied in various educational settings, including cybersecurity education. In a study by De Santos-Berbel et al. (2024), an H5P-based matching game was used to teach structural analysis to engineering students. The study found that students who participated in the game demonstrated higher levels of motivation, engagement, and performance compared to traditional learning methods. This suggests that gamification elements, when applied correctly, can improve learning outcomes and make cybersecurity education more interactive and enjoyable.

Moreover, the use of H5P to create gamified content provides several advantages. H5P allows the creation of rich, interactive multimedia content that can be integrated seamlessly with Learning Management Systems (LMS) such as Moodle. This integration enhances the learning experience by providing immediate feedback, which is crucial for fostering cybersecurity awareness (Rahmi et al., 2024). In a cybersecurity context, immediate feedback helps students understand why certain actions are unsafe and provides corrective measures, which strengthens their ability to recognize and avoid cyber threats (Deborah & Sugihartanto, 2024).

Assessment in Cybersecurity Education

Assessment plays a vital role in the effectiveness of cybersecurity education, particularly in game-based learning environments. Gamified assessments offer real-time evaluation and immediate feedback, which not only keeps students engaged but also helps them internalize key cybersecurity concepts (Checa et al., 2023). According to Alahmari et al. (2023), such assessments allow educators to evaluate whether students can effectively identify cybersecurity threats, apply preventive measures, and practice secure online behaviors. This is especially important in the context of cybersecurity, where knowledge retention and practical application are crucial for long-term behavior change.

Additionally, assessments in cybersecurity games help to validate the learning experience, ensuring that these tools are both effective and credible as educational resources. Gao (2024) and Calvano et al. (2023) highlight that structured assessments increase the reliability of game-based learning tools, making them more likely to be accepted by educational institutions, cybersecurity organizations, and other stakeholders. In this regard, tools like H5P offer a scalable solution for integrating assessments into interactive learning experiences.

Gap in Existing Research

Despite the growing body of literature on cybersecurity education, a critical gap remains in the availability of age-appropriate, engaging assessment tools for younger students. Most existing studies focus on adult populations or do not tailor their tools to the cognitive and developmental stages of children (Alfalah, 2023; Ayanwale et al., 2024). This study addresses this gap by introducing a customizable H5P-based educational game designed specifically for elementary and junior high school students in Indonesia. The tool not only measures cybersecurity awareness but also provides an engaging, gamified experience that fosters better retention and practical application of cybersecurity knowledge.

Conclusion

In conclusion, gamification and the use of interactive tools such as H5P offer promising avenues for improving cybersecurity awareness among young learners. By incorporating game design elements and providing immediate feedback, these tools can significantly enhance students' engagement and understanding of cybersecurity concepts. However, further research is needed to assess the long-term effectiveness of such tools and to create more standardized, age-appropriate assessment tools for cybersecurity education.

3. Research Methods

This study uses the Research and Development (RnD) method, which is commonly applied in educational technology development, especially for cybersecurity awareness assessments. The RnD approach is chosen because it allows for the development of a product (in this case, an educational game) and its evaluation in a real-world context. The method is carried out in four stages, adapted from Borg & Gall (1983), which are:

1. Tech-shifting from academic results to dream products

In this stage, the theoretical findings from prior studies are translated into a tangible educational product, in this case, an interactive cybersecurity awareness game developed using H5P integrated with Moodle.

2. Product Manufacturing

This phase involves the design and development of the educational game. The game is developed with interactive elements, such as quizzes, badges, and feedback mechanisms, to engage students in learning about cybersecurity practices.

3. Product User Testing

After the game is created, it undergoes user testing with elementary and junior high school students. This phase aims to evaluate how well the game engages users and measures their cybersecurity awareness through specific indicators.

4. Test Result Correction and Retesting

Based on feedback from users, the game is refined and improved, and another round of testing is conducted to assess whether the revisions have enhanced the game's effectiveness in improving cybersecurity awareness.

The educational game developed in this study measures students' cybersecurity awareness and aims to improve their skills in areas such as password security, phishing recognition, and safe online behavior (Alrobaian et al., 2023).

Participants

The participants of this study are students from elementary and junior high schools in Madiun, Indonesia. A total of 68 elementary school students and 92 junior high school students were selected as participants. These students were chosen through random sampling from several schools to ensure a representative sample of the population. The age range of the participants is from 6 to 14 years old, which corresponds to the typical age group for elementary and junior high school students.

Ethical considerations were taken into account, with informed consent obtained from both the students and their parents/guardians prior to participation in the study. This ensured that the participants were fully aware of the research's purpose and how their data would be used.

Instruments and Data Collection

To measure cybersecurity awareness, this study uses a pre-test and post-test design. The pre-test is administered before the students play the educational game, while the post-test is administered after the game to assess any changes in their cybersecurity knowledge.

The assessment includes 16 game models available on the platform sicermat.web.id. These models address five key cybersecurity indicators, including:

1. Security in using email and gadgets
2. Password strength and security
3. How to interact safely on social media
4. Interacting in digital markets and using digital banking
5. Personal data security

The students' cybersecurity awareness is measured through these models using quizzes, scenario-based questions, and instant feedback provided within the game. The game's design aims to test students' ability to apply cybersecurity knowledge in real-world scenarios.

Next, the product usage test is measured, and the test results are improved. From these five indicators, students are given 16 game models available on sicermat.web.id. to be tested on users. The testing flow follows the RnD method (Cheng & Chang, 2019).

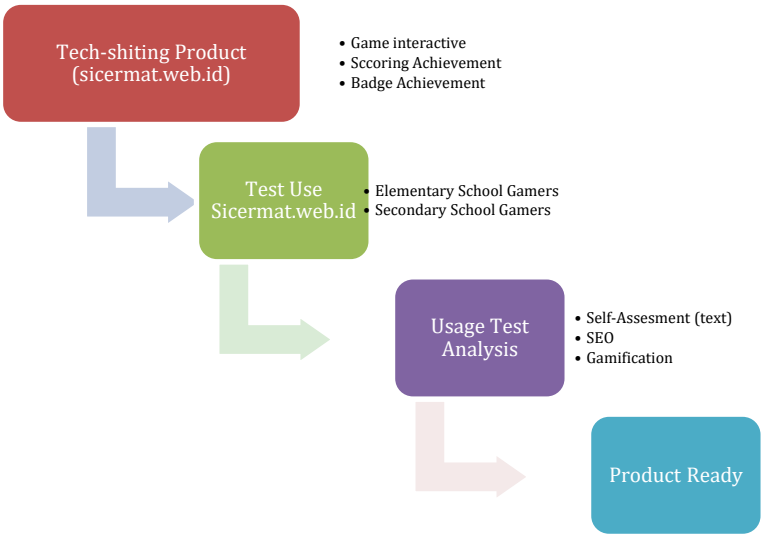

Fig. 1. Testing Flow According to RnD Method

Data Analysis Techniques

The data collected from the pre-test and post-test assessments will be analyzed using quantitative methods. Specifically, the study will calculate the percentage change in students' cybersecurity awareness scores before and after playing the game. The analysis will include:

- Descriptive statistics to summarize the pre-test and post-test scores.
- Paired t-test or other relevant statistical tests to compare the mean scores before and after the game and determine if the differences are statistically significant.

The goal is to determine whether the educational game effectively increases students' awareness and understanding of cybersecurity concepts.

Additional Considerations

The R&D method in this study incorporates randomization in the assessment process to ensure unbiased results. For instance, the questions presented to the students during the game are randomized to prevent them from predicting the correct answers based on prior knowledge. This ensures that the students' responses reflect their true understanding of cybersecurity practices rather than memorization or external cues.

In addition, scenario-based assessments will be employed, where students are exposed to different cybersecurity challenges (e.g., phishing, password management). These scenarios are designed to assess students' spontaneous reactions and problem-solving skills in a controlled environment.

Finally, since the study involves minors, ensuring the privacy and confidentiality of student responses is paramount. All responses will be anonymized to protect the participants' identities and ensure that the data collected is used solely for the purposes of this research.

4. Results and Discussions

The results of the cybersecurity awareness assessment were analyzed to evaluate the effectiveness of the educational game in enhancing students' cybersecurity knowledge. The results provide a clear overview of the changes in students' cybersecurity awareness before and after participating in the game. The analysis is divided into two parts: the quantitative results and the qualitative insights from participants.

Quantitative Results

The data shows that a significant percentage of students exhibited an increase in cybersecurity awareness after engaging with the game. The results are summarized in the following tables:

Table 1 - Term & Indicator of Cyber Security Awareness

Term Indicator on Games	Interactive Games

Security Using Email and Gadgets	What is Electronic Mail?
	Google email
	Unlock Screen
	Gadget is?
	Gadget safety from Dr. Evil
Password/Password Security	What is the Preferred Email Password?
	Crossword Game "Password"
	Powerful Password
	Crossword Puzzle II Password
Social Media	People & Social Media
	Get to know fake/fraudulent WA chats.
	Social Media
Buying and Selling Online & Digital Banking	Application permissions
	Digital Market & e-Money
	OTP, what is it?
5. Personal Data Security	Personal Data

The test results were analysed using the self-assessment method for text and sentences. SEO describes the game's appearance so that the location, graphics deficiencies, and quality can be known. Meanwhile, a gamification model is compiled as score achievement or badge achievement to increase user involvement in this game. The percentage shown in the table above shows the change process after improvements to the game. After improvements are made, it is used to measure cybersecurity awareness. The following are the results of measuring the cybersecurity level based on the game users' backgrounds.

Players' cybersecurity awareness levels were measured before and after the game.

a. Player engagement level elementary school-age

Table 2 - Elementary School Age Players

Number of Elementary School Age Player Participants	86
Game finish participants	68
The participant Did Not Finish the Game	18

b. Elementary school-age players who experience changes in understanding cyber security awareness

Table 3 - Changes in Understanding of Cyber Security Awareness SD

Participants who experienced an increase in understanding of Cyber Security Awareness	48
Participants who did not experience an increase (static) in their understanding of Cyber Security Awareness	20

c. The real condition of elementary school-age players that has not changed (static)

Table 4 - Conditions of Changes in Elementary School-Age Players

Static Ability	20
Low Initial Ability	10
High Initial Ability	10

d. Player engagement level junior high school age

Table 5 - Junior High School Age Players

Number of Junior High School Players	109

Finish Game Participants	92
The participant Did Not Finish the Game	17

e. Junior high school-age players who experience changes in understanding cyber security awareness

Table 6 - Changes in Understanding of Cyber Security Awareness in Middle Schools

Participants who experienced an increase in understanding of Cyber Security Awareness	68
Participants who did not experience an increase (static) in their understanding of Cyber Security Awareness	24

f. The real condition of junior high school-age players has not changed (static)

Table 7 - Conditions of Changes in Junior High School-Age Players

Static	24
Low Ability	10
High Ability	14

These results suggest that a significant percentage of both elementary and junior high school students showed improvements in their understanding of cybersecurity. Specifically, 56% of elementary school participants and 62% of junior high school participants experienced an increase in their awareness of cybersecurity after playing the game.

Statistical Analysis

To further assess the significance of these improvements, a paired t-test was conducted to compare the pre-test and post-test scores for both groups. The test results showed that the mean score for both groups significantly improved after playing the game, with p-values well below the 0.05 threshold, indicating that the observed improvements were statistically significant.

This analysis highlights that the educational game effectively enhanced students' cybersecurity awareness. The improvements were particularly notable in areas such as password security, safe online behavior, and understanding the risks of digital platforms.

Qualitative Insights

In addition to the quantitative results, feedback was collected from students and teachers. Over 80% of participants reported that they found the game engaging and helpful in understanding cybersecurity concepts. Many students mentioned that the interactive nature of the game, including quizzes and scenario-based questions, made learning more enjoyable and memorable.

Teachers also observed that the game was an effective tool for sparking discussions about cybersecurity topics that are often neglected in the formal curriculum. This suggests that game-based learning can bridge the gap in students' understanding of digital safety and complement traditional educational methods.

Discussion

The findings of this study are consistent with previous research, which suggests that game-based learning is effective in enhancing cybersecurity awareness among students (Deborah & Sugihartanto, 2024; Gao, 2024). The interactive nature of the game helps students actively engage with the material, making it easier for them to retain key cybersecurity concepts.

The significant improvements in cybersecurity awareness observed in both elementary and junior high school students highlight the potential of gamification in educating young learners. This aligns with the notion that interactive and engaging learning tools are effective in instilling important skills that are often overlooked in conventional education.

However, some students did not show significant improvements in their understanding of cybersecurity. 20% of elementary school students and 22% of junior high school students either showed no change or demonstrated a static ability. This could be due to several factors, such as prior knowledge of cybersecurity or lack of engagement with the game. Further research is needed to explore the reasons behind these findings.

Limitations and Future Research

One of the key limitations of this study is the sample size, which may not be representative of the broader student population. Additionally, the research was conducted only in Indonesia, and the results may not be generalizable to other cultural contexts. Future studies could involve a larger, more diverse sample to examine whether the findings hold across different regions.

Another limitation is that this study only involved a single session of gameplay. While the results indicate improvements in students' cybersecurity awareness, it is possible that the effects may diminish over time. Future research could explore the impact of repeated exposure to the game or the use of supplementary materials to reinforce the concepts learned.

5. Conclusion

The measurement of cybersecurity awareness through an interactive educational game has successfully demonstrated its ability to assess and improve students' cybersecurity literacy. Of the 68 elementary school students who completed the game, 48 students showed an increase in awareness. Similarly, among the 92 junior high school students who completed the game, 68 students experienced an improvement in their cybersecurity knowledge. The educational game, which integrates H5P with the Moodle platform, effectively enhanced students' understanding of various cybersecurity concepts in a fun and engaging manner. This approach not only helped students grasp theoretical knowledge but also provided practical experience in dealing with cyber threats.

The game’s effectiveness is attributed to its incorporation of gamification elements such as points, levels, and awards, which encourage active learning (Nordby et al., 2024). Compared to traditional educational methods such as lectures or reading modules, this interactive game proved to be more engaging, leading to better information retention. Additionally, the incorporation of practical, hands-on scenarios allows students to apply cybersecurity concepts, which enhances their real-world preparedness.

One key takeaway is that the game significantly improved students' cybersecurity awareness, with 48% of elementary school participants and 74% of junior high school participants showing measurable improvements. Notably, a portion of students who demonstrated high initial knowledge also participated in the game, further confirming that the tool is effective across varying levels of prior knowledge.

Implications and Recommendations

This educational game has significant practical implications. It can be easily scaled and adapted for use in other regions or educational systems, helping to bridge the gap in cybersecurity education. By incorporating such a tool into the school curriculum, educators can proactively address the growing need for cybersecurity awareness among students, potentially reducing the risks posed by cyber threats.

Furthermore, as the study indicates, the gamification approach to learning cybersecurity can be highly effective in engaging students and promoting long-term behavioral changes. This suggests that widespread adoption of such games could cultivate safer online habits in students, helping them to better protect themselves and their personal data in the digital age.

To enhance the reach and impact of this tool, it is recommended that the game be integrated into mobile applications or Learning Management Systems (LMS) for broader accessibility. Additionally, implementing this game across a wider range of schools could help standardize cybersecurity education, ensuring that all students are equipped with the necessary skills to navigate the digital world safely.

Future Work

For future studies, a longitudinal study is recommended to assess the retention of cybersecurity awareness over time. While the current study demonstrated significant improvements immediately following gameplay, further research could explore how well these improvements are retained and whether students continue to apply the knowledge in their daily digital interactions.

In conclusion, this cybersecurity awareness educational game offers a promising tool for enhancing students' understanding of digital safety. By integrating gamification into education, the game not only engages students but also provides them with practical, lasting skills to navigate the online world safely.

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*(October 2023), 100031. https://doi.org/10.1016/j.csa.2023.100031

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*. https://doi.org/10.1007/s10479-022-04844-8

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management*, 21(1), 123-158. Springer Berlin Heidelberg. https://doi.org/10.1007/s10257-022-00575-2

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences*, *10*(4), 136–144. https://doi.org/10.21833/ijaas.2023.04.017

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the TechnicaAl and Vocational Training Corporation. *Big Data and Cognitive Computing*, *7*(2). https://doi.org/10.3390/bdcc7020073

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model. *Information Technology and People*, *36*(8), 94–125. https://doi.org/10.1108/ITP-07-2022-0515

Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education. *Education and Information Technologies*, *29*(3), 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. *IEEE Access*, *12*, 86596–86617. https://doi.org/10.1109/ACCESS.2024.3416045

Calvano, M., Caruso, F., Curci, A., Piccinno, A., & Rossano, V. (2023). A Rapid Review on Serious Games for Cybersecurity Education: Are "Serious" and Gaming Aspects Well Balanced? *CEUR Workshop Proceedings*, *3408*.

Cassano, F., Piccinno, A., Roselli, T., & Rossano, V. (2018, June). Gamification and learning analytics to improve engagement in university courses. In *International Conference in Methodologies and intelligent Systems for Techhnology Enhanced Learning* (pp. 156-163). Cham: Springer International Publishing.

Catanese, S., De Meo, P., Ferrara, E., Fiumara, G., & Provetti, A. (2012). Extraction and analysis of Facebook friendship relations. In *Computational Social Networks: Mining and Visualization*. https://doi.org/10.1007/978-1-4471-4054-2_12

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, *50*, 100592. Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2023.100592

Checa, D., Miguel-Alonso, I., & Bustillo, A. (2023). Immersive virtual-reality computer-assembly serious game to enhance autonomous learning. *Virtual Reality*, *27*(4), 3301–3318. https://doi.org/10.1007/s10055-021-00607-1

Chen, J. C., & Chang, T. H. (2019, August). Modified PPO-RND method for solving sparse reward problem in *ViZDoom. In 2019 IEEE Conference on Games (CoG)* (pp. 1-4). IEEE. https://doi.org/10.1109/CIG.2019.8847999

Da Veiga, A., Loock, M., & Renaud, K. (2022). Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. *The Electronic Journal of Information Systems in Developing Countries, 88*(1), e12198.

De Santos-Berbel, C., Hernando García, J. I., & Vázquez-Greciano, A. (2024). H5P-Based Matching Game for Training Graphs of Internal Forces in Structural Analysis. *Education Sciences*, *14*(4), 359. https://doi.org/10.3390/educsci14040359

Deborah, N., & Sugihartanto, M. F. (2024). Assessment of Sustainable Packaging Supply Chain Management Using the Life Cycle Assessment Method (Case Study: FMCG Company in Indonesia). *Procedia Computer Science*, *234*, 654–662. https://doi.org/10.1016/j.procs.2024.03.051

Diaz-Rodas, S. (2024). Implementation of the H5P laboratory to exercise the creation of digital content in university teachers. *Vivat Academia*, *157*, 1–24. http://doi.org/10.15178/va.2024.157.e1501

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data*, *11*(1), 118. https://doi.org/10.1186/s40537-024-00980-z

Gao, F. (2024). Advancing Gamification Research and Practice with Three Underexplored Ideas in Self-Determination Theory. *TechTrends*, *68*(4), 661–671. https://doi.org/10.1007/s11528-024-00968-9

Guo, H., & Tınmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. *Journal for the Education of Gifted Young Scientists, 11*(3), 351-367. https://doi.org/10.17478/jegys.1323423

Hayati, S., & Guspatni, G. (2023). Designing moodle-based learning media integrated with H5P interactive on chemical equilibrium topic. *Jurnal Pijar Mipa*, *18*(6), 851–860. https://doi.org/10.29303/jpm.v18i6.5621

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and information technologies*, *28*(1), 439-470. https://doi.org/10.1007/s10639-022-11121-5

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, *5*(1), 169–212. https://doi.org/10.1365/s43439-024-00111-7

Kuraku, S., Kalla, D., Smith, N., & Samaah, F. (2023). Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks. *International Journal of Computer Trends and Technology*, *71*(11), 74–79.

Mat Din, M. B., Mansor, S., Muhamat Dawam, S. R., Andria, A., Laksono, R. D., & Sussolaikah, K. (2023). The Implementation of H5P in Interactive Games for Cyber Security Awareness Learning Facilities for Elementary and Junior High School Students. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *9*(3), 596–605. https://doi.org/10.26555/jiteki.v9i3.26547

Nordby, A., Vibeto, H., Mobbs, S., & Sverdrup, H. U. (2024). System Thinking in Gamification. *SN Computer Science*, *5*(3). https://doi.org/10.1007/s42979-023-02579-2

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., & Bonders, M. (2024). Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach. *Technology, Knowledge and Learning*, *30*(3), 1577-1606.. https://doi.org/10.1007/s10758-024-09769-8

Rahmi, U., Fajri, B. R., & Azrul, A. (2024). Effectiveness of Interactive Content with H5P for Moodle-Learning Management System in Blended Learning. *Journal of Learning for Development*, *11*(1), 66–81. https://doi.org/10.56059/jl4d.v11i1.1135

Serpa, Y. R., Nogueira, M. B., Rocha, H., Macedo, D. V., & Rodrigues, M. A. F. (2020). An interactive simulation-based game of a manufacturing process in heavy industry. *Entertainment Computing*, *34*, 100343. https://doi.org/10.1016/j.entcom.2020.100343

Shaikh, F. A., & Siponen, M. (2024). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*, *26*(3), 1109–1120. https://doi.org/10.1007/s10796-023-10404-7

Xu, C., Qu, Y., Xiang, Y., & Gao, L. (2023). Asynchronous federated learning on heterogeneous devices: A survey. *Computer Science Review, 50*, 100595. Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2023.100595