Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 3, 1282-1294
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i3.364

Raising Employee Cybersecurity Awareness Through Octalysis-Based Gamification: A Pre-Post Assessment Using HAIS-Q at the Ministry of Public Works and Public Housing

Ramadhan Papua Putra*
Universitas Bina Nusantara, Indonesia

Abba Suganda Girsang
Universitas Bina Nusantara, Indonesia

***Corresponding author:**
Ramadhan Papua Putra, Universitas Bina Nusantara, Indonesia.
✉ramadhan.putra@binus.ac.id

Article Info:

Article history:
Received: May 25, 2026
Revised: June 29, 2026
Accepted: July 13, 2026
Available Online: August 26, 2026

Keywords:
Cybersecurity; Cybersecurity Awareness; Gamification; The Human Aspect of Information Security Questionnaire (HAIS-Q); Game-Based Learning.

Abstract

Background: Rapid digital transformation has increased cybersecurity threats, while employee awareness remains a critical vulnerability in many organizations, including government institutions. Strengthening cybersecurity awareness is essential to reduce human-related security risks.

Objective: This study aims to assess employee cybersecurity awareness at the Ministry of Public Works and Housing (*Kementerian Pekerjaan Umum dan Perumahan Rakyat* [Ministry of PUPR]) using the Human Aspects of Information Security Questionnaire (HAIS-Q) and to evaluate the effectiveness of an *Octalysis*-based gamification intervention in improving awareness across knowledge, attitude, and behavior dimensions.

Methods: A pre-post quasi-experimental design was applied involving 146 employees. Data were collected using the validated HAIS-Q instrument before and after a four-week web-based gamification intervention. The gamification design implemented two *Octalysis* core drives: Development & Accomplishment and Empowerment of Creativity & Feedback, through leaderboard, badge, and instant feedback features.

Results: The findings show that overall cybersecurity awareness increased from 75.85% (medium level) to 83.69% (good level), indicating a 10.33% improvement. All seven HAIS-Q focus areas improved, with the most significant gain observed in internet use (58.22% to 69.79%).

Conclusion: The *Octalysis*-based gamification approach effectively enhanced employee cybersecurity awareness. Integrating gamification with HAIS-Q provides a structured and evidence-based method for improving cybersecurity behavior in government organizations.

To cite this article: Putra, R. P., & Girsang, A. S. (2026). Raising Employee Cybersecurity Awareness Through Octalysis-Based Gamification: A Pre-Post Assessment Using HAIS-Q at the Ministry of Public Works and Public Housing. *Equivalent: Jurnal Ilmiah Sosial Teknik*, *8*(3), 1282-1294. https://doi.org/10.59261/jequi.v8i3.364

INTRODUCTION

The rapid development of information technology has greatly contributed to societal and economic progress, as well as improved productivity (Budi et al., 2021; Septasari, 2023). Information technology development is utilized by various organizations, including private, nonprofit, and government organizations such as the Ministry of Public Works and Housing (PUPR), to support organizational activities and business processes. However, the advancement of information technology has also increased the cyber threats faced by organizations. According to the 2022 annual report from the National Cyber and Encryption Agency, Indonesia recorded 976,429,996 traffic anomalies, highlighting the critical role of cybersecurity.

There are three pillars of cybersecurity: people, processes, and technology. Among these pillars, people are considered the weakest link and often become the entry point for cyberattacks that can harm organizations. This vulnerability occurs because exploiting human weaknesses is relatively easy, requires minimal investment beyond communication costs, and carries low risk for attackers (Mitnick & Simon, 2003; Yang et al., 2025). The interconnectedness of these cybersecurity pillars is intended to achieve the fundamental objectives of information security: maintaining confidentiality, integrity, and availability. The people and process pillars are responsible for preserving confidentiality, while the people and technology pillars contribute to maintaining integrity. Similar to other organizations, the Ministry of Public Works and Housing (PUPR) has predominantly focused its cybersecurity incident mitigation efforts on technological aspects while paying less attention to people and process aspects. Therefore, efforts are required to raise employee cybersecurity awareness and improve cybersecurity-related behaviors (Qusa & Tarazi, 2021; Wijanarko & Erlansari, 2025).

Cybersecurity awareness is a combination of continuous vigilance and actions that comply with security standards and guidelines established by an organization (Islam et al., 2026; Kemper, 2019). Therefore, employee cybersecurity awareness is closely related to individual knowledge and organizational work culture. It is essential for organizations to continuously develop a cybersecurity culture. The primary objective of cybersecurity awareness is to ensure that employees understand the risks associated with technology use and comply with established security regulations and procedures (Iskandar et al., 2026; Parsons et al., 2017). Individuals with cybersecurity knowledge tend to demonstrate higher cybersecurity awareness and adopt preventive measures against cyberattacks by utilizing common and user-friendly tools or applications (Pryhodii & Radkevych, 2026). Furthermore, cybersecurity knowledge and internet usage are associated with cybersecurity-related activities, indicating a relationship between cybersecurity awareness, cybersecurity knowledge, and cybersecurity behavior.

Currently, the efforts implemented by the Ministry of PUPR to raise employee cybersecurity awareness remain suboptimal. These efforts primarily focus on current cybersecurity issues and use conventional methods, such as disseminating information through emails, social media, and infographics. Additionally, no assessment has been conducted to evaluate employees' cybersecurity awareness and determine their current awareness levels. This assessment can be performed using several methods, one of which is the Human Aspect of Information Security Questionnaire (HAIS-Q). The HAIS-Q consists of seven categories: password management, email use, internet use, social media use, mobile device use, information handling, and incident reporting (Iskandar et al., 2026; Parsons et al., 2017). The results of cybersecurity awareness assessments are categorized into three levels: Good, Medium, and Bad (Iskandar et al., 2026; Kruger & Kearney, 2006). After determining the current state of employee cybersecurity awareness, organizations can design and implement programs to improve cybersecurity awareness effectively and efficiently.

Several methods can be employed to enhance employee cybersecurity awareness, including gamification (Qusa & Tarazi, 2021; Wijanarko & Erlansari, 2025). This approach applies game elements and mechanisms in non-game contexts to increase engagement, motivation, and participation in activities, thereby creating a more enjoyable learning experience (Deterding et al., 2011; Landers & Sanchez, 2022). Gamification can improve understanding and encourage secure technology usage behaviors by incorporating elements such as challenges, points, rewards, and competition (Kusuma et al., 2021; Setiawan & Yatim, 2026). The advantages of gamification include making the learning process more enjoyable, helping users focus and better understand learning materials, and providing opportunities for exploratio (Kusuma et al., 2021; Setiawan & Yatim, 2026).

One of the gamification frameworks is the Octalysis Framework. The Octalysis Framework applies core behavioral drives that motivate users to complete tasks effectively through interactive experiences (Marisa et al., 2020; Rahman et al., 2025). As shown in Figure 1 (Octalysis Framework), there are eight core drives in the Octalysis Framework: epic meaning and calling, development and accomplishment, empowerment of creativity and feedback, ownership and possession, social influence and relatedness, scarcity and impatience, unpredictability and curiosity, and loss and avoidance (Chou, 2015; Inano, 2024).

Gamification has proven to be an effective approach for improving employee cybersecurity awareness because it enables cybersecurity training content to be tailored to specific learning needs. (Gjertsen et al., 2017) conducted an empirical study to examine the effectiveness of gamification in Scandinavian businesses (Pahlavanpour & Gao, 2024). The researchers introduced an interactive prototype game to employees, and the results demonstrated that employees became more motivated and willing to follow cybersecurity procedures, thereby improving their cybersecurity awareness. Several gamification implementations have been developed to enhance cybersecurity awareness, including attack simulation laboratories (Chou, 2020; Khan et al., 2022), Capture the Flag (CTF) platforms (Ortiz-Garces et al., 2023), card games (Hart et al., 2020), Augmented Reality-based games (Alqahtani & Kavakli-Thorne, 2020), and the Cyber-Hero game (Aslam et al., 2025; Qusa & Tarazi, 2021). It is important to note that gamification methods for enhancing employee cybersecurity awareness should be simple, easy to use, time-efficient, and focused on relevant training materials (Aldawood & Skinner, 2019; Aslam et al., 2025).

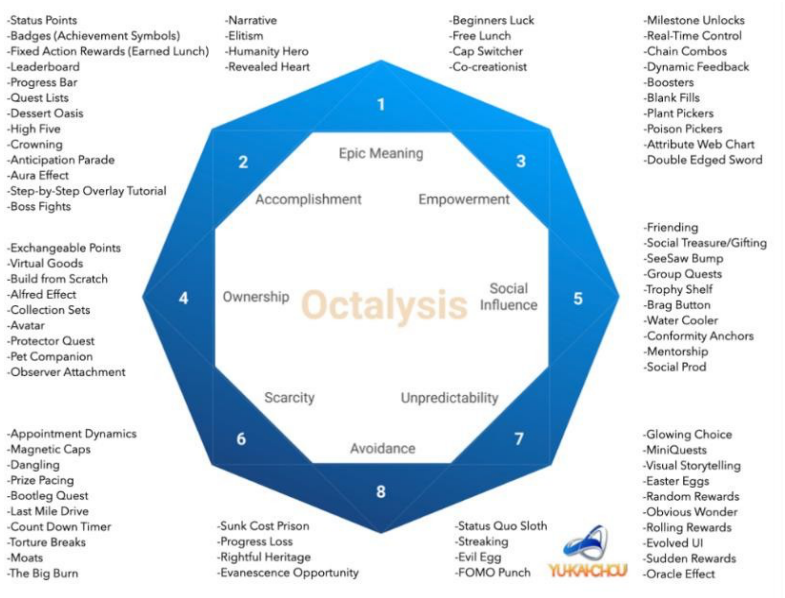

Figure 1. Octalysis Framework

Cybersecurity awareness refers to individuals' understanding of cyber threats and their ability to behave securely in accordance with organizational policies. Recent studies indicate that most cybersecurity incidents are caused by human-related factors rather than technical vulnerabilities. Therefore, improving employee awareness is essential for reducing organizational cyber risks.

Cybersecurity awareness encompasses not only technical knowledge but also attitudes and behaviors. Employees with sufficient knowledge may still engage in risky practices if awareness programs fail to influence behavioral aspects (Alshaikh, 2020; Sutton & Tompson, 2025). Hence, effective awareness initiatives must address knowledge, attitude, and behavior simultaneously.

Human Factors in Information Security: Information security relies on people, processes, and technology, with the human factor being the most vulnerable component . Human errors, such as susceptibility to phishing attacks and non-compliance with security policies, remain dominant causes of security incidents despite technological advancements.

Employees' security behavior is influenced by organizational culture, perceived responsibility, and motivation (Ifinedo, 2013; Park et al., 2026). Without sufficient awareness and motivation, compliance with security policies remains low, emphasizing the importance of human-centered security approaches.

Cybersecurity Awareness Measurement Using HAIS-Q: The Human Aspect of Information Security Questionnaire (HAIS-Q) is a validated instrument used to measure cybersecurity awareness across knowledge, attitude, and behavior dimensions (Iskandar et al., 2026; Parsons

et al., 2017). The HAIS-Q covers multiple security focus areas, including password management, email usage, and incident reporting.

Previous studies confirm that the HAIS-Q demonstrates high reliability and validity in evaluating awareness levels and assessing the effectiveness of security training programs. Consequently, the HAIS-Q is widely adopted in cybersecurity awareness research.

Gamification applies game design elements to non-game contexts to increase engagement and motivation (Deterding et al., 2011; Landers & Sanchez, 2022). In training environments, gamification has been shown to improve learning outcomes and knowledge retention compared with traditional approaches (Sarsa, 2013; Triantafyllou et al., 2025).

Recent studies report that gamified cybersecurity awareness training enhances employee engagement and improves the ability to recognize cyber threats. Interactive learning mechanisms and immediate feedback provided through gamification contribute to improved security behavior.

Octalysis Framework and Research Gap: The Octalysis Framework is a human-centered gamification framework that addresses eight core motivational drivers influencing behavior]. By emphasizing intrinsic and extrinsic motivation, the Octalysis Framework provides a structured approach for designing effective gamified learning systems.

Although gamification has demonstrated positive outcomes in cybersecurity awareness initiatives, many existing programs lack a comprehensive motivational framework. Additionally, limited studies have integrated gamification with validated measurement tools such as the HAIS-Q. Therefore, this study addresses the research gap by combining the Octalysis Framework with the HAIS-Q instrument to develop and evaluate a structured cybersecurity awareness intervention.

This study aims to achieve three objectives: (1) to assess the current cybersecurity awareness level of Ministry of PUPR employees using HAIS-Q across the knowledge, attitude, and behavior dimensions; (2) to design and implement a gamification-based awareness program grounded in the Octalysis Framework; and (3) to evaluate the effectiveness of the gamification intervention by comparing pre- and post-implementation HAIS-Q scores. Unlike previous studies that employ gamification without validated measurement instruments, this research integrates the Octalysis motivational framework with the HAIS-Q assessment tool, providing a systematic and evidence-based approach to improving cybersecurity awareness within a government organization context

METHOD

There are four processes in this research that focused on the proposed gamification framework used to raise employee cybersecurity awareness, as illustrated in Figure 2: cybersecurity awareness assessment, creating gamification design, gamification implementation, and evaluation.

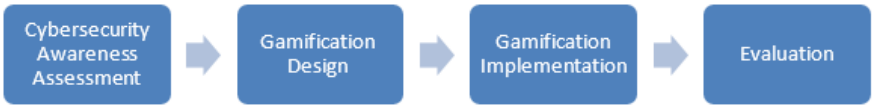

Figure 2. Research Stages

Cybersecurity Awareness Assessment

Cybersecurity awareness assessment use the Human Aspect of Information Security Questionnaire (HAIS-Q) method, which is commonly used to evaluate cybersecurity awareness. HAIS-Q has 63 questions and encompasses seven focus area: password management, email use, internet use, social media use, mobile device usage, information handling, and incident reporting. These sections are classified into three dimensions: Knowledge, Attitude, and Behavior (KAB). Answers are given using the likert scale 1-5 where 1 is strongly agree and 5 is strongly agree. The results of this assessment provide an overall cybersecurity awareness level and detailed awareness levels for each section, categorized into three levels: Good, Medium, and Bad (Iskandar et al., 2026; Kruger & Kearney, 2006).

Data was collected using a questionnaire distributed trough an online form and the target employees in Ministry of PUPR with final sample size consisted of 146 participants. The index value is obtained by dividing the total score by the maximum Likert scale value (Y) multiplied by 100% as in Equation (1).

$$\text{Index} = \frac{\text{Total Score}}{\text{Y}} \ 100\% \qquad (1)$$

Based on the collected index values, the next step is to calculate the mean values for each dimension. The evaluation of the degree of information security awareness follows from this. Three categories have been established by Kruger and Kearney (2006) for information security awareness levels: Good (80–100 %), Medium (60–79.99 %) (Iskandar et al., 2026), and Bad (59.99 %) as illustrated in Table 1.

Table 1
Cybersecurity Awareness Classification

Awareness Level	Value (%)
Good	80 – 100
Medium	60 – 79.99
Bad	≤ 59.99

The results of this cybersecurity awareness assessment then analyzed and used as the basis for determining the objectives and requirements of the gamification to be developed. This analysis also helps to describe the current state of the users, allowing for the identification of the core drives to be used in the Octalysis framework.

Gamification Design

The gamification design is based on the results of the previous stage, where the overall and detailed cybersecurity awareness levels of employees are obtained to identify areas that need improvement. The gamification design utilizes the Octalysis framework and will be in the form of a quiz game and web-based, considering simplicity, user-friendliness, and minimal time requirement (Hart et al., 2020; Li et al., 2025). Based on Figure 1, Octalysis has eight core drives and each of them has purpose that will be benefit in raising awareness process. Epic Meaning and Calling centers on how gamification can inspire individuals to contribute to the greater good, even in the absence of immediate rewards. This concept is rooted in the intrinsic motivation to engage in meaningful activities that transcend personal gain. Development and Accomplishment pertains to the innate drive for self-improvement and the commitment to increasing one's capabilities for a greater cause. Empowerment of Creativity and Feedback emphasizes the importance of engaging in creative processes and receiving feedback to enhance outcomes continuously. Ownership and Possession relates to the sense of belonging and control over one's assets, which fuels the desire to manage and protect what one owns. Social Influence and Relatedness highlights the motivational power of social interactions and connections. Scarcity and Impatience addresses the human tendency to covet scarce resources, often leading to a sense of urgency and impatience to acquire something perceived as difficult to obtain. Unpredictability and Curiosity tap into people's interest in future events and the unknown, driven by varying patterns. Finally, Loss and Avoidance involve the motivation to prevent negative outcomes, often fueled by the fear of loss. The design and implementation itself will not take all core drives in the gamified system, but only Development and Accomplishment and Empowerment of Creativity and Feedback core drives. Through these two core drives, employees are expected to experience a more engaging and competitive cybersecurity awareness learning experience through a series of gamification elements. The highlighted elements from the system are leaderboard, badge and instant feedback.

Gamification Implementation

The presence of a leaderboard allows employees to track their progress in completing tasks provided within the system. Furthermore, the implementation of this element is expected to foster competitiveness among employees as they learn about cybersecurity. The implementation of the Empowerment of Creativity & Feedback in this study can be seen in the Instant Feedback element. This element provides various explanations based on the quizzes completed by employees during their cybersecurity learning. This gamification element enables employees to identify areas that need improvement. In addition to corrections, employees can view the final results of the quizzes in the form of scores. Through these two core drives, employees are expected to experience a more engaging and competitive cybersecurity awareness learning experience through a series of gamification elements. The highlighted elements from the system are leaderboard, badge and instant feedback. The presence of a leaderboard and badge allows employees to track their progress in completing tasks provided within the system and the implementation of leaderboard and badge are shown in Figure 3, where leaderboard and badge in Dashboard. Furthermore, the implementation of this element is expected to foster competitiveness among employees as they learn about cybersecurity. The application of the Empowerment of Creativity & Feedback in this study can be seen in the Instant Feedback element. This element provides various explanations based on the quizzes completed by employees during their cybersecurity learning. This gamification element enables employees to identify areas that need improvement. In addition to corrections, employees can view the final results of the quizzes in the form of scores. The implementation drives are shown in Figure 4 and Figure 5 where instant feedback in Quiz Questions page and Quiz Results page.

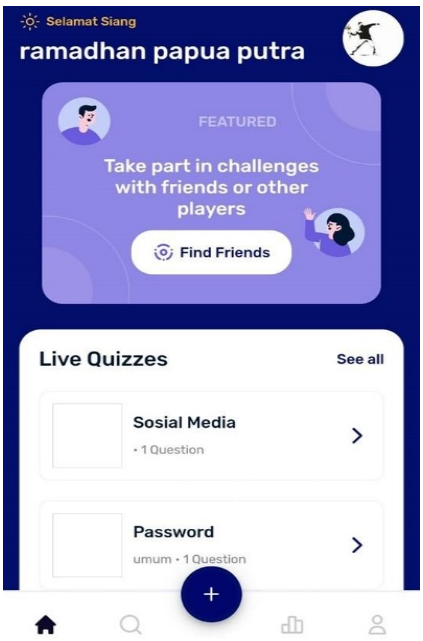

Figure 3. Gamification Dashboard

Figure 4. Quiz Questions

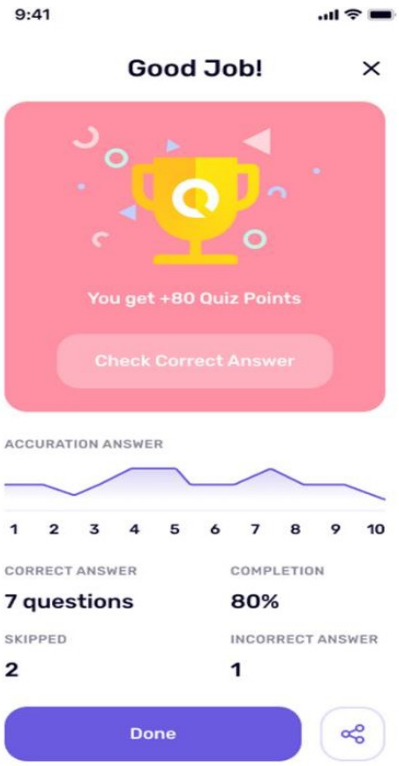

Figure 5. Quiz Result

Evaluation

This study employed a pre-post quasi-experimental design without a control group. The evaluation was conducted using a quantitative method, where the data evaluated was the cybersecurity awareness level based on HAIS-Q results. The HAIS-Q instrument was administered to the same cohort of 146 employees both before and after the gamification intervention. Pre-implementation scores established the baseline awareness level, while post-implementation scores measured changes following a four-week gamification period. The effectiveness of the gamification method was evaluated by comparing mean awareness scores across all seven HAIS-Q focus areas and three KAB dimensions. Percentage improvement was calculated for each focus

area to identify domains with the greatest and least improvement. The classification thresholds established by Kruger and Kearney (2006) were applied to categorize awareness levels as Good (80–100%) (Iskandar et al., 2026), Medium (60–79.99%), or Bad (≤59.99%).

RESULTS AND DISCUSSION

Results

This section explained about cybersecurity awareness assessment using HAIS-Q to determine the current state of the employee cybersecurity awareness level, the implementation of gamification to raise employee cybersecurity awareness and post assessment to evaluate the implementation of gamification.

Cybersecurity awareness assessments distributed through online form and the target employees in ministry of PUPR with final sample size consisted of 146 participants. Table 2 presented the findings of cybersecurity awareness level at Ministry of PUPR and this result became the pre-implementation gamification level that will be compared to after implementation. Ministry of PUPR employee cybersecurity awareness level were in Medium level (75.15).

Focus area that met Good level were information handling and incident reporting. Password management, email use, social media use, and mobile devices are the focus area that met the Medium Category. Otherwise focus area that need attention was internet use because in Bad category.

Table 2
Cybersecurity Awareness Level

Password management	73.28	75.29	81.61	77.84
Email use	61.21	78.16	77.30	72.64
Internet use	49.14	61.49	62.36	58.22
Social media use	66.38	79.31	79.60	75.57
Mobile devices	71.26	82.76	84.20	80.03
Information handling	81.61	84.48	88.51	85.63
Incident reporting	80.75	76.44	83.05	81.03
Total Awareness	69.09	76.85	79.52	75.85

After knowing the value of cybersecurity awareness of employees of the Ministry of PUPR, the design and implementation of gamification based on the octalysis framework can be carried out to increase employee cybersecurity awareness.

Discussion

Design and Implementation

The Octalysis Framework applies core behavioral drives that motivate users to efficiently complete tasks through interactive experiences (Marisa et al., 2020; Rahman et al., 2025). In this research, the design and implementation of the gamified system do not incorporate all core drives; instead, they focus only on the Development and Accomplishment and Empowerment of Creativity and Feedback core drives. Through these two core drives, employees are expected to experience a more engaging and competitive cybersecurity awareness learning experience through a series of gamification elements. The highlighted elements implemented in the system are the leaderboard, badges, and instant feedback. The presence of a leaderboard allows employees to track their progress in completing tasks provided within the system. Furthermore, implementing this element is expected to foster competitiveness among employees as they learn about cybersecurity. The implementation of the Empowerment of Creativity and Feedback core drive in this study can be observed through the Instant Feedback element. This element provides various explanations based on the quizzes completed by employees during their cybersecurity learning process. This gamification element enables employees to identify areas that require improvement. In addition to receiving corrections, employees can view their final quiz results in the form of scores. Through these two core drives, employees are expected to experience a more engaging and competitive cybersecurity awareness learning experience through a series of

gamification elements. This research focuses only on email use, internet use, and social media use because these areas received the lowest scores in the Ministry of PUPR.

According to the use case diagram in Figure 6, the implementation of gamification includes four main features for employees: learning cybersecurity awareness materials, taking quizzes, viewing leaderboards, and viewing badges. The use case diagram provides an overview of the functionalities presented in the gamification application. For each feature offered, an activity diagram is provided to explain the flow of its usage. Through these diagrams, users can better understand how the features within the system operate. Figure 7 presents one of the features of the gamification application, namely the quiz feature, which can be accessed after employees complete the learning materials in the selected course. This quiz feature is used to evaluate employees' understanding of cybersecurity awareness materials. It represents the implementation of the Instant Feedback element within the Empowerment of Creativity and Feedback core drive. Another feature of this gamification application is the leaderboard, which displays employees' quiz results. This feature represents the Leaderboard element within the Development and Accomplishment core drive.

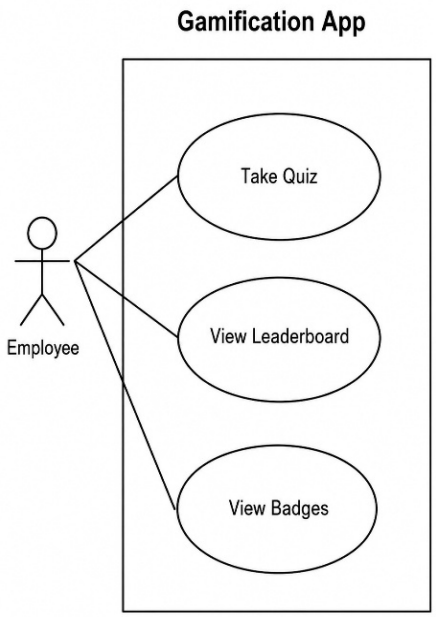

Figure 6. Gamification apps Use Case Diagram

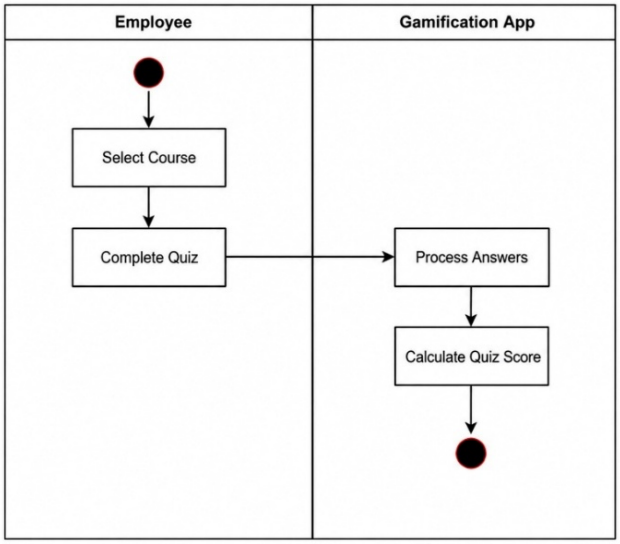

Figure 7. Quiz Activity Diagram

Evaluation

In this study, the evaluation procedure conducted to ensure the data and experiment factors are eligible to generate intended results. The evaluation of this study will be conducted using a quantitative method, where the data evaluated will be the cybersecurity awareness level based on HAIS-Q results. The evaluation plan for the effectiveness of the gamification method will involve questionnaire based on HAIS-Q and KAB model to assess respondent cybersecurity awareness level improvement. The analysis results of the HAIS-Q and KAB model questionnaire before implementation will be compared with the analysis results after gamification implementation to obtain the evaluation results of effectiveness of the gamification method in improving employee cybersecurity awareness.

Table 3 Post Implementation Gamification Cybersecurity Level. Based on Table 3, the implementation of gamification raised the overall employee cybersecurity awareness level from 75.85% (Medium) to 83.69% (Good), representing a 10.33% improvement. The most substantial improvements were observed in email use (72.64% to 81.66%, a 12.42% increase), social media use (75.57% to 84.17%, an 11.38% increase), and mobile devices (80.03% to 87.90%, a 9.83% increase). Internet use, the weakest area pre-intervention at 58.22% (Bad), improved to 69.79% (Medium), reflecting a 19.87% relative increase, the highest proportional gain among all focus areas. These results indicate that the gamified intervention was most effective in areas where baseline awareness was lowest, suggesting that gamification serves as a targeted remediation tool for cybersecurity knowledge gaps.

Table 3

Post Implementation Gamification Cybersecurity Level

Password management	77.63	81.51	88.81	82.65
Email use	71.46	85.62	87.90	81.66
Internet use	62.56	74.43	72.37	69.79
Social media use	76.71	87.21	88.58	84.17
Mobile devices	82.19	91.32	90.18	87.90
Information handling	88.81	90.87	93.38	90.95
Incident reporting	89.95	85.84	90.41	88.73
Total Awareness	78.47	85.26	87.36	83.69

Efficacy Analysis and Implications

The quantitative improvement from Medium (75.85%) to Good (83.69%) demonstrates that the Octalysis-based gamification intervention produced a measurable and meaningful improvement in employee cybersecurity awareness. This finding is consistent with Gjertsen et al. (2017), who reported increased motivation and procedural compliance following gamified security training in Scandinavian organizations (Pahlavanpour & Gao, 2024). Similarly, Qusa and Tarazi (2021) found that gamification-based approaches effectively improved cybersecurity awareness among students, supporting the applicability of game-based learning methods across diverse organizational contexts (Wijanarko & Erlansari, 2025).

The selection of Development & Accomplishment and Empowerment of Creativity & Feedback as the two active core drives proved effective. The use of leaderboard and badge features encouraged competitive engagement, while the instant feedback mechanism enabled participants to independently identify knowledge gaps. These findings align with Deterding et al. (2011), who emphasized that game mechanics, such as progress tracking and immediate rewards, enhance intrinsic motivation (Landers & Sanchez, 2022). However, the study acknowledges that only two of the eight Octalysis core drives were implemented, suggesting that incorporating additional drives, such as Social Influence & Relatedness, could further strengthen engagement and cybersecurity awareness outcomes in future implementations.

From a practical perspective, the gamification platform demonstrated that web-based, quiz-oriented learning can be effectively implemented in government organizations with minimal disruption to daily operations. Improvements across all three KAB dimensions (Knowledge: 69.09% to 78.47%; Attitude: 76.85% to 85.26%; Behavior: 79.52% to 87.36%) suggest that gamification supports not only cognitive understanding but also attitudinal and behavioral

changes related to cybersecurity, which are essential for establishing a sustainable organizational security culture (Alshaikh, 2020; Sutton & Tompson, 2025).

CONCLUSION

This study assessed the cybersecurity awareness of Ministry of PUPR employees using the HAIS-Q instrument and evaluated the effectiveness of a gamification-based intervention grounded in the Octalysis Framework. The pre-implementation assessment revealed an overall cybersecurity awareness level of 75.85% (Medium), with internet use identified as the weakest area at 58.22% (Bad). Following the implementation of a web-based gamified learning platform incorporating leaderboard, badge, and instant feedback features derived from the Development & Accomplishment and Empowerment of Creativity & Feedback core drives, the post-implementation assessment demonstrated a significant improvement to 83.69% (Good), representing a 10.33% overall increase. All seven HAIS-Q focus areas showed measurable improvements, with internet use exhibiting the highest proportional gain at 19.87%.

These findings confirm that Octalysis-based gamification can effectively enhance employee cybersecurity awareness, particularly when interventions are targeted at weak areas identified through validated pre-assessment instruments. The primary scientific contribution of this study lies in integrating the Octalysis motivational framework with the HAIS-Q measurement instrument within a government organizational context, providing an evidence-based approach to improving cybersecurity awareness. However, this study has several limitations. First, the absence of a control group limits the ability to attribute the observed improvements exclusively to the gamification intervention. Second, only two of the eight Octalysis core drives were implemented, which may have constrained the overall motivational impact. Third, the study was conducted within a single government ministry, potentially limiting the generalizability of the findings to other organizational contexts. Fourth, the post-assessment was administered immediately after the intervention; therefore, the long-term retention of cybersecurity awareness improvements was not evaluated. Future research should incorporate randomized controlled experimental designs, investigate the implementation of additional Octalysis core drives, extend evaluation periods to examine long-term retention effects, and replicate the study across diverse organizational settings to strengthen external validity.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Ministry of PUPR for granting access and support in conducting this study. Appreciation is also extended to all employees who participated in the survey and gamification program, as well as to colleagues and academic peers who provided valuable feedback during the development and implementation of this research. Their contributions were essential in ensuring the successful completion of this study.

AUTHOR CONTRIBUTION STATEMENT

Both authors contributed equally to this research. The contributions include conceptualization of the study, development of the HAIS-Q-based assessment framework, design of the Octalysis-based gamification system, data collection, analysis of pre- and post-intervention results, and manuscript preparation. All authors reviewed and approved the final version of the manuscript and are collectively responsible for the integrity and accuracy of the study.

REFERENCES

Aldawood, H., & Skinner, G. (2019). An academic review of current industrial and commercial cyber security social engineering solutions. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 110–115.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information*, *11*(2), 121.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003.

Aslam, M. M., Kalinaki, K., Tufail, A., Naim, A. G. H., Khan, M. Z., & Ali, S. (2025). Social Engineering

Attacks in Industrial Internet of Things and Smart Industry: Detection and Prevention. *Emerging Threats and Countermeasures in Cybersecurity*, 389–412.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia P-ISSN*, *2086*, 5805.Budi

Chou, T.-S. (2020). A Game-Based Multiplayer System for Cyber Security Training and Awareness. *2020 CIEC*.

Chou, Y. (2015). The octalysis framework for gamification & behavioral design. *URL: Https://Yukaichou. Com/Gamification-Examples/Octalysis-Complete-Gamification-Framework/[Accessed 2019-11-03]*.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining" gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9–15.

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of Information Security Awareness and Training. *ICISSP*, 59–70.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Ifinedo, P. (2013). Information systems security policy compliance: An. *Psychological Review*, *84*(2), 191–215.

Inano, M. (2024). *Using octalysis framework in the gamification process of a mobile application*.

Iskandar, A. S., Hilman, M., & Yazid, S. (2026). Information security awareness assessment for civil servant recruitment committee in Indonesia using HAIS-Q. *Information & Computer Security*, *34*(1), 86–103.

Islam, M. M., Bhuiyan, M. R. I., Islam, S. H., Tabassum, M. N., & Billah, M. (2026). Unlocking the Mediating and Moderating Role of Information Security in Information Systems: A Combined TAM, ISM, and HBM Model. *Human Behavior and Emerging Technologies*, *2026*(1), 5593002.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14.

Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. El. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, *27*(4), 5153–5177.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.

Kusuma, G. P., Suryapranata, L. K. P., Wigati, E. K., & Utomo, Y. (2021). Enhancing historical learning using role-playing game on mobile platform. *Procedia Computer Science*, *179*, 886–893.

Landers, R. N., & Sanchez, D. R. (2022). Game-based, gamified, and gamefully designed assessments for employee selection: Definitions, distinctions, design, and validation. *International Journal of Selection and Assessment*, *30*(1), 1–13.

Li, T., Dong, F., & Wen, C. (2025). The Security Awareness Adventure: A serious game for security awareness training utilizing a state transition system and a probabilistic model. *Computers & Security*, *156*, 104500.

Marisa, F., Ahmad, S. S. S., Yusoh, Z. I. M., Maukar, A. L., Marcus, R. D., & Widodo, A. A. (2020). Evaluation of student core drives on e-Learning during the covid-19 with octalysis gamification framework. *International Journal of Advance Computer Science and Application*, *11*(11), 104–116.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Ortiz-Garces, I., Gutierrez, R., Guerra, D., Sanchez-Viteri, S., & Villegas-Ch, W. (2023). RETRACTED: Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions. *Electronics*, *12*(7), 1753.

Pahlavanpour, O., & Gao, S. (2024). A systematic mapping study on gamification within information security awareness programs. *Heliyon*, *10*(19).

Park, J., Jeon, S., & Han, J. (2026). Motivating employees to engage in extra-role security behaviors:

the role of information security climate and leader–member exchange. *Journal of Enterprise Information Management*, 1–30.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40–51.

Pryhodii, M., & Radkevych, O. (2026). Intensification of vocational training for learners via SMART technologies. *Professional Pedagogics*, *1*(32), 3–17.

Qusa, H., & Tarazi, J. (2021). Cyber-hero: A gamification framework for cyber security awareness for high schools students. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 677–682.

Rahman, D. F., Tobing, F. A. T., & Hassolthine, C. R. (2025). Design and Evaluation of an AI-Driven Gamified Intelligent Tutoring System for Fundamental Programming Using the Octalysis Framework. *Ultimatics: Jurnal Teknik Informatika*, *17*(2), 221–230.

Sarsa, H. (2013). *Does Gamification Work? A Literature Review*.

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia: Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (AJIEE)*, *5*(2), 227–233.

Setiawan, P. R., & Yatim, M. H. M. (2026). Systematic Literature Review of HCI Principles in Role–Playing Game Design: Towards a Comprehensive Framework for Enhancing Programming Skills. *Sistemasi: Jurnal Sistem Informasi*, *15*(1), 33–48.

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, *148*, 104110.

Triantafyllou, S. A., Georgiadis, C., & Sapounidis, T. (2025). Gamification in education and training: A literature review: SA Triantafyllou et al. *International Review of Education*, *71*(3), 483–517.

Wijanarko, A., & Erlansari, A. (2025). Gamification on Cybersecurity Awareness Training for Adolescents: A Systematic Literature Review. *Indonesian Journal of Computer Science and Engineering*, *2*(02), 6–12.

Yang, Y. T., Ge, Y., & Zhu, Q. (2025). Human Risks and Cognition-Inspired Adaptive Cyber Deception. In *Foundations of Cyber Deception: Modeling, Analysis, Design, Human Factors, and Their Convergence* (pp. 181–200). Springer.