National College of Ireland

Research Report

MSc Research Project
MSc Cybersecurity

Faatih Kajogbola
Student ID: x23312131

School of Computing
National College of Ireland

Supervisor: Mr. Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Kajogbola Faatih Adekunle
Student ID:	23312131
Programme:	MSc. Cybersecurity **Year:** 2024/2025
Module:	Research in Computing
Lecturer:	Mr. Joel Aleburu
Submission Due Date:	11-08-2025
Project Title:	Practicum Research Report
Page Count:	20
Word Count:	7176

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

Date: 11-08-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Examining the Effectiveness of Gamification on Knowledge Retention in Cybersecurity Education

MSc. in Cybersecurity

Kajogbola Faatih
X23312131
MSCCYBSEP24I– Research in Computing
National College of Ireland

Abstract

As cyber threats continue to grow in sheer number and complexity, there is a pressing need for new and innovative strategies to educate the masses on these emerging threats. Conventional teaching approaches often struggle to maintain learner engagement and achieve lasting knowledge retention. In response to this, gamification, which is the application of game design elements in non-game contexts, has emerged as a promising alternative to conventional teaching methods. While existing literature suggests that gamification can enhance learner engagement and improve immediate learning outcomes, its long-term impact on knowledge retention remain underexplored. This research directly addresses this gap by developing an experimental study aimed at examining how gamification can be used to promote sustained knowledge retention within cybersecurity education, to answer the question: "How can we effectively measure knowledge retention in users to evaluate the impact of gamification in cybersecurity education?". The research proposed involves a quasi-experimental design comparing knowledge retention measured via pre-tests, post-tests and delayed post-tests between students who engage with a gamified cybersecurity module and those who use conventional instructional methods. Ultimately, this study aims to provide clear empirical evidence on gamification's effect on knowledge retention and to establish effective measurement protocols. The findings will contribute towards the design of more impactful, learner-centred cybersecurity training programs that can better prepare individuals to navigate the increasingly complex digital threat landscape.

Keywords: Cybersecurity Education, Gamification, Knowledge Retention, Cybersecurity, E-Learning.

I. INTRODUCTION

The increasing frequency and complexity of cyber threats pose a serious threat not only to individuals, but to organizations and critical infrastructure as well. With human error accounting for about 95% of data breaches (Thakur et al., 2023), it has become evident that the "human factor" is the weakest link in cybersecurity, often due to a lack of practical knowledge or failure to comply with security guidelines. This highlights a critical need for innovative educational approaches that are not only informative, but also engaging and effective in promoting lasting knowledge in order to equip the masses with the knowledge and tools needed to continuously and effectively defend against most cyberthreats.

Conventional cybersecurity training methods, such as lectures and static assessments, often fail to ensure long-term knowledge retention and assess behavioural changes in the average person with almost no interest in the topic. To address this, gamification has gained traction as a potential method to enhance engagement and learning outcomes in cybersecurity training (Hamari et al., 2014). Gamification, which involves the integration of game design elements and principles into non-gaming contexts such as education, has emerged as a promising approach towards enhancing engagement and knowledge retention among participants. Fatokun et al. (2024) shows that by incorporating elements like points, levels, challenges, narratives, and feedback into otherwise mundane learning approaches, gamification increases motivation, engagement, and active participation in the learning processes. Several papers within the literature explored while working on this project employ the use of gamification for cybersecurity awareness and training, suggesting positive effects on user engagement, motivation, and immediate learning. For example, studies have used game elements to teach concepts like phishing avoidance (Yonemura et al., 2018), secure network design (Criollo-C et al., 2024), social engineering defense (Baláž et al., 2024), password security (Fatokun et al., 2024), and general cybersecurity principles (Fatokun et al., 2024). Card games, simulations, quizzes, adventure games, and mobile apps have all been employed to test this method.

However, while the potential for enhancing engagement and initial learning is often highlighted, a critical gap exists in understanding and effectively measuring the long-term retention of knowledge acquired through these gamified approaches. Does the increased engagement gained from gamified approaches translate into knowledge that persists over time? Answering this requires measurement techniques specifically tailored towards knowledge retention. This project aims to directly address the gap in knowledge by answering the question: **"How can we effectively measure knowledge retention in users to evaluate the impact of gamification in cybersecurity education?"**.

To answer this question, this project proposes a research methodology centred around developing and evaluating a gamified cybersecurity learning module. The main focus is to compare the knowledge retention in users who participate in the gamified module against those who have learned through the conventional methods. Knowledge retention will be measured using three main forms of assessment: a pre-test assessment to measure the user's base knowledge, an immediate post-test assessment to gauge what was learned, and a delayed test to be taken a week after the initial assessment to assess knowledge retention over that period.

This project aims to contribute two things. Firstly, it aims to provide empirical evidence regarding the effectiveness of gamification for knowledge retention in the domain of cybersecurity education. Secondly, it aims to develop, refine, and validate a methodological framework for effectively measuring this knowledge retention within gamified learning contexts. These contributions are significant as they could help to design

and implement a more effective, evidence-based cybersecurity training programs for various audiences, from students to professionals and the general public. By understanding how to measure and enhance retention, we can better equip individuals to defend against the ever-evolving landscape of cyber threats.

The research report is structured as follows:

- **Section 1: Introduction:** Outlines the research problem, motivation, research question, proposed approach, contributions, and proposal structure.
- **Section 2: Literature Review:** Discusses relevant previous work and their various contributions, focusing on gamification, cybersecurity education, and measurement approaches while identifying the research niche.
- **Section 3: Research Method and Specification:** Details the proposed methodology, project plan, tools used during development, and ethical considerations taken.
- **Section 4: Evaluation of Results:** Provides a comprehensive analysis of the results and main findings of the study, as well as their potential implications.
- **Section 5: Conclusion and Discussion:** Examines how the final results obtained from the experiment align with the initial objectives. It also includes suggestions on what further work could be carried out using these findings.
- **Section 6: References:** Provides a full list of the documents referenced while working on this proposal.

II. LITERATURE REVIEW

This section critically evaluates the design, effectiveness, and evaluation methods of gamified cybersecurity interventions, drawing comparisons across different studies and integrating findings from meta-analyses in the wider education field.

A. Design and Application of Gamified Cybersecurity Tools

Several studies explore the design and application of gamified cybersecurity tools, addressing a wide range of audiences and learning objectives using considerably diverse designs, ranging from simple quiz-based tools to complex simulations and role-playing experiences. Fatokun et al. (2022) developed a Facebook Messenger quiz game to boost cybersecurity knowledge in children aged 6-12, focusing on issues like privacy and cyberbullying. Their approach engages a young audience by rewarding them with scores and stickers for correctly answering simple yes or no questions. Their later iteration, Fatokun et al. (2024) further expanded on this idea by incorporating a more comprehensive and advanced game design with multiple levels covering different aspects like social engineering, network security, and passwords, intended to promote knowledge among older end-users. The updated design incorporated elements like progress mechanics, avatars, problem-solving, and narrative, grounded in the Technology Threat Avoidance Theory (TTAT).

Other approaches taken include Obeng et al. (2024)'s card-based game called CyberMed Guardians, which was designed specifically for enhancing cybersecurity awareness in medical IoT among biomedical engineering students by employing a turn-based approach involving Attackers and Defenders using cards representing threats such as malware, phishing and defenses like encryption and firewalls, with a judge

assessing outcomes. Similarly, Ashley et al. (2022) developed the Network Defense Training Game (NDTG), a simulation-based game where players defend a critical infrastructure OT network against realistic cyber incidents, managing budgets and implementing security controls based on the NIST Cybersecurity Framework (CSF) and mapping objectives to NICE framework roles. Yonemura et al. (2017; 2018) employed Kaspersky Interactive Protection Simulation (KIPS), a board game simulating ICT and Operational Technology (OT) security scenarios, fostering teamwork and analytical skills among Japanese college students. More recent designs, such as Baláž et al. (2024)'s Cyber Labyrinth, utilized a 3D "Escape Room" style game in which players solve puzzles related to cybersecurity concepts such as Caesar cipher, digital signatures, buffer overflow, phishing, and SQL injection.

Role-playing and mobile app-based gamification approaches were also explored by Zolotarev et al. (2021), who proposed a hybrid role-playing/quest game model for security awareness among information security students. Their model incorporated task completion, role hierarchies, and performance assessment. Similarly, Criollo-C et al. (2024) developed CiberSecApp, a mobile game with three levels that teaches basic cybersecurity concepts through interactive play.

The diversity of tools discussed show that gamification can be adapted to various educational contexts and content domains in cybersecurity, from simple quiz-based mechanics for foundational knowledge (Fatokun et al., 2022) to complex simulations for procedural skill development (Ashley et al., 2022) and collaborative problem-solving (Yonemura et al., 2017; 2018).

After studying the different approaches taken to design and apply these tools, several limitations were observed. Implementations such as Fatokun et al. (2024) and Obeng et al. (2024) prioritized engagement mechanics (points, badges) without actually testing if narrative depth or problem complexity contributes to retention. Although simulations like Ashley et al (2022)'s NDTG achieved higher validity than the previously mentioned quiz-based games, their complexity may hinder scalability. Additionally, very few of these designs build in ways that help learners retain what they've learned over a long period or apply it in real-world settings. This is a gap that broader reviews of gamification research also point out (Hamari et al., 2014; Sailer and Homner, 2019).

B. Examining the Effectiveness of Gamified Cybersecurity Tools

A common theme across all the reviewed literature is that gamification consistently enhances engagement and motivation compared to conventional methods. Obeng et al. (2024) reported high levels of student engagement and enthusiasm with their card game, with many students seemingly preferring it over conventional lectures. Similarly, using an adventure game based on cognitive constructivism, Ros et al. (2020) discovered that student engagement significantly influenced perceived usefulness, confidence, and ultimately, self-perception of success. Criollo-C et al. (2024) noted that their mobile game motivated users and was rated positively in terms of usability and satisfaction. Fatokun et al. (2024) argued that gamification could alter learners' emotional experience and boost engagement through motivation. Ashley et al. (2022) also reported positive feedback regarding player engagement with simulation-based training.

The core argument across all these studies is that interactive, challenge-based, and narrative-driven learning experiences can more effectively capture and sustain learner attention compared to passive instructional methods. However, most of these studies stopped short of linking engagement to measurable learning outcomes beyond the immediate post-activity effects.

While many studies show that gamification boosts student engagement, the link to actual learning outcomes is less clear. For example, Ashley et al. (2022) found that their elaborate NDTG significantly raised knowledge scores, attributing the gains directly to the game's design, whereas Ros et al. (2020) noted improved retention but warned that variations in teaching style might have influenced the outcome. These contrasting findings highlight how differences in game complexity and instructional context can produce divergent results.

A lot of research tends to assume that if the learners enjoy the activity, they must also be learning more, but broader meta-analyses (Hamari et al., 2014) suggest this isn't always the case, as stronger motivation doesn't necessarily lead to longer lasting knowledge. In cybersecurity studies specifically, most either lack proper control groups or only measure short-term improvements right after the activity.

C. Evaluating the Effectiveness of Gamified Cybersecurity Tools

Evaluation methods used to ascertain the effectiveness of gamified tools vary greatly across different works and often lack standardization. From the **pre/post-tests** used by Criollo-C et al., 2024 and Yonemura et al., 2017, to the **surveys** used by Obeng et al., 2024 and Fatokun et al. (2024), the **game performance metrics** used by Ashley et al., 2022 and finally the overall grades and dropout rates used by Ros et al. (2020).

Criollo-C et al. (2024) and Yonemura et al. (2017; 2018) both used a pre-test/post-test design, with the former finding a significant 14.47% improvement in cybersecurity knowledge after students used their CiberSecApp and the latter finding partial correlation between the Kaspersky Interactive Protection Simulation (KIPS) game scores and post-test knowledge confirmation scores, but noting that high theoretical knowledge didn't always translate to high game scores, particularly in Operational Technology (OT) scenarios where understanding priorities like availability was key. Obeng et al. (2024) relied on interviews and feedback surveys, finding out that students reported improved retention due to the game's interactive nature. Fatokun et al. (2024) used a planned survey to evaluate their game's impact.

Ashley et al. (2022) calculated the scores based on player performance across rounds, considering the defences implemented against attack conditions and awarding scores appropriately, while Ros et al. (2020) compared practical exercise grades and final exam scores between students who used their game and those who did not, finding that game users had significantly lower dropout rates and higher final grades.

Although these studies all offer valuable insights, the evaluation methods are heterogeneous and frequently rely on short-term metrics such as post-tests, self-perception surveys, or game scores, which undermines comparability and limits evidence on long-term retention. A particularly interesting example of how study design may influence outcomes can be seen when comparing Fatokun et al. (2024) to Ashley et al. (2022). Fatokun's quiz-based approach reported significant engagement improvements based primarily on self-report measures and immediate post-tests, leading the authors to conclude that gamification substantially enhances learning. In contrast, Ashley's simulation-based study found more modest improvements when using objective performance metrics across multiple rounds of gameplay. The key difference lies in their measurement approaches, Fatokun relied heavily on participant perceptions of learning, while Ashley measured actual decision-making performance under realistic conditions. This comparison illustrates how evaluation methodology can dramatically influence conclusions about gamification effectiveness, highlighting the critical need for robust, objective measurement protocols in this field.

Sailer & Homner (2020)'s meta-analysis of 28 educational gamification studies, identified moderate learning benefits overall, but also pointed out that retention beyond one week as "rarely assessed.". The same issue shows up in cybersecurity research, which is that none of the studies reviewed here included delayed assessments (e.g., a month later), leaving the durability of the learning gains uncertain. Most of these studies also involve small convenience samples (often under 100 participants), which makes it harder to draw strong, general conclusions.

D. Identified Research Niche

Although many of the cited papers detailed different ways to evaluate the effectiveness of gamification as a teaching method, none of them explicitly detailed a methodology designed specifically to assess long-term knowledge retention over time. While studies like Obeng et al. (2024) and Fatokun et al. (2024) mentioned that students reported improved retention and suggests that enjoyment and motivation in games positively impact knowledge retention, these were both based on subjective self-reports rather than empirical measurement. Ros et al. (2020) also acknowledged the need to assess whether students meet learning objectives after playing, but their study focused only on grades and dropout rates.

Overall, the existing evaluations all seem to focus on assessing immediate impact or use proxies like course grades or self-perception, rather than directly assessing retention of cybersecurity knowledge weeks or months after engagement. This gap clearly identifies the research niche: there is a need for studies that implement and evaluate methodologies specifically designed to measure long-term knowledge retention resulting from gamified cybersecurity learning experiences. Addressing this gap requires moving beyond immediate post-tests and self-reports toward incorporating longitudinal assessment designs that can better assess the lasting impact of gamification compared to conventional methods.

This research aims to address this gap by implementing a design, comparing retention rates between gamified and conventional learning methods, thereby providing stronger empirical evidence for the enduring value of gamification in cybersecurity education and establishing more standardized assessment practices.

E. Evidence Summary Table

Study	Design Approach	Outcome Measured	Retention Window	Key Limitations
Ashley et al. (2022)	Simulation-based game (NDTG)	Improved engagement and performance scores.	Immediate	No delayed retention testing was done to establish long-term knowledge retention
Balaz et al. (2024)	3D Escape room (Cyber Labyrinth)	Improved cybersecurity problem solving skills	Immediate	Proposed design is in the prototype stage, also lacks formal evaluation
Criollo-C et al. (2024)	Mobile game (CiberSecApp)	Improved cybersecurity knowledge	Immediate	Small number of participants. No delayed retention testing was done

Fatokun et al. (2022)	Quiz-based game	Improved cybersecurity knowledge	Immediate	Participants were children with no proper control group.
Fatokun et al. (2024)	Multilevel quiz-based game.	Improved engagement, motivation, and knowledge	Immediate	No delayed retention testing was done, and possible self-report bias
Obeng et al. (2024)	Card game (CyberMed Guardians)	Improved student engagement, enthusiasm, and retention.	Immediate	No delayed retention testing was done
Ros et al. (2020)	Adventure game	Improved final exam scores and decreased dropout rates.	Course duration	Used grades as a proxy to measure performance, there was also no delayed retention test administered.
Yonemura et al. (2017; 2018)	Board game (KIPS)	Improved knowledge, teamwork, and analytical skills.	Immediate	Lacks OT-specific follow-up assessment
Zolotarev et al. (2021)	Hybrid role-playing game	Improved performance, security awareness, and performance assessment.	Immediate	No delayed retention testing was done, the effects of the implemented role hierarchy were also unclear.

Table 1: Summary of reviewed literature.

III. RESEARCH METHOD AND SPECIFICATION

A. Research Design

This study adopts a quasi-experimental design to evaluate how gamification affects long-term knowledge retention in cybersecurity education. This approach was chosen because it is well suited for real-world educational settings, due to offering higher external validity than laboratory settings (Sreekumar, 2024), and also due to ethical and logistical challenges that can arise from randomly assigning participants to different mandatory educational methods. Despite not relying on random assignment, the design still aims to establish a cause-and-effect relationship between the gamified platform and knowledge retention. By accounting for systematic differences and applying reliable measurement methods, a great degree of confidence can be inspired by the validity of the findings made (Thomas, 2020).

It is important to acknowledge that the retention window was limited to two weeks during this project because the semester calendar constraints prevented extending the delayed post test (T3) to one month or longer, which would have provided even stronger evidence for sustained knowledge retention. Despite this, the study still provided meaningful insight into the effectiveness of gamification and retention patterns. However, future research should incorporate extended follow-up periods (1-3 months) to better evaluate the durability of gamification effects on knowledge retention.

Although quasi-experimental designs often face internal validity threats like selection bias, history, maturation, testing, and instrumentation (Sreekumar, 2024), the following mitigations have been implemented:

- Selection bias was addressed by a having all participants take a pre-test (T1) to establish baseline knowledge and statistically control for pre-existing differences. To further control for these potential differences, an ANCOVA was used to assess group differences in immediate post-test (T2) and delayed post-test (T3) performance while adjusting for pre-test (T1) scores.
- The relatively short two-week retention period between immediate post-test (T2) and delayed post-test (T3) minimizes history and maturation effects.
- Using identical tests at T1, T2, and T3 also means testing effects should be consistent across participants, and our focus on *relative change* and *retention* helps account for this.
- Employing standardized administration and scoring will also minimize instrumentation threats.

Implementing these strategies help to enhance the validity of the findings, allowing for more reliable conclusions about the impact of gamification. However, even with these mitigations, the study cannot fully rule out unobserved differences between groups such as varying study habits, prior gaming experience, or intrinsic motivation levels. To further control for these potential confounding variables, an analysis of covariance (ANCOVA) was conducted on pre-test scores.

B. Participant Recruitment and Sampling

The target participants were any willing individuals above 18 years of age, as this demographic is accessible and relevant to educational technology. The initial target for the sample size was about 60 participants in line with studies like Criollo-C et al. (2024), but due to time constraints and logistical difficulties, only 45 participants were recruited. Among the 45 participants initially enrolled in the study, 7 participants withdrew before completing all assessments, resulting in 38 participants who successfully completed all three assessments. Participation was voluntary, with informed consent obtained before the study began, and participants being able to drop out at any point. Recruitment was done using university mailing lists, online ads, and survey share websites like SurveySwap. Sampling was convenience-based but stratified to ensure a balance of knowledge in both groups.

Participants signed up via a Google Form that was created specifically for this purpose, with basic demographic data (name, email address, prior cybersecurity experience) being collected to help characterize the samples and identify potential confounding variables. All data was anonymized and stored securely.

C. Ethical Considerations

The following precautions were taken when creating the sign up sheet used to register participants in order to ensure alignment with ethical practices were upheld:

- **Informed Consent:** Participants were fully informed about the study's purpose, procedures, time commitment, data collection and usage, anonymity, and their right to withdraw at any time without penalty.

- **Anonymity and Confidentiality:** All collected data (test scores, demographic info) was anonymized. This was done to ensure that no personal identifiable information will be linked to the results.
- **Voluntary Participation:** Participation was strictly voluntary. Participants were not forced or coerced in any way to participate. They could also choose to end their participation at any given point in time.
- **Time Constraints:** The time commitment for the intervention and testing phases were reasonable and clearly communicated. The difficulty of the tests were also appropriate for novices to cybersecurity.
- **Data Usage:** It was clearly stated what research data would be collected, and exactly how it would be used. Participants were free to withdraw their consent at any time.

D. Learning Content

Participants were split into two groups (gamified group and conventional group) where they learned specific cybersecurity modules (phishing awareness, password security, network basics) using either the gamified platform or the regular PowerPoint based lecture. The gamified group used a custom-built cybersecurity training game developed in Unreal Engine 5 (UE5), which incorporated elements like points, levels, and immediate feedback, drawing principles from the included literature, while the conventional group received equivalent content through PowerPoint slides on the same topics. Both groups completed identical pre-tests, post-tests, and delayed post-tests to better isolate the impact of gamification on retention.

E. Development of Gamified Platform

The gamified platform's design was grounded in Self-Determination Theory (SDT) and the Octalysis Framework to enhance engagement and knowledge retention. SDT emphasizes fulfilling basic psychological needs: autonomy (choice), competence (mastery), and relatedness (connection), fostering intrinsic motivation crucial for sustained engagement (Damari and Zhou, 2025). The Octalysis Framework identifies eight core human drives, with "white hat" elements (Meaning, Accomplishment, Empowerment) aligning with intrinsic motivation (The Octalysis Group, 2023). By integrating elements that satisfy these needs and drives, the platform aims to cultivate genuine learning and sustained engagement, which are vital for long-term knowledge retention, addressing the challenge that gamification doesn't always guarantee long-term retention.

i. Gamification Elements and Implementation

Following principles from TTAT and literature on gamification (Hamari et al., 2014; Sailer and Homner, 2019), the module incorporates:

- **Points:** Earned for answering questions correctly answers, providing feedback and a sense of accomplishment.
- **Challenges and Quests:** Cybersecurity concepts presented as problem-solving scenarios (e.g., phishing awareness, password security and network basics), mimicking real-world threats.

- **Immediate Feedback:** Instant corrective feedback upon wrong answers to help track progress and adjust learning strategies.
- **Narrative Scenarios:** A compelling narrative to immerse users and make learning more engaging.
- **Leaderboards:** Used to keep track of user performance and foster healthy competition without discouraging participants.

The platform draws inspiration from successful examples like interactive quizzes (Kahoot!), simulations ("ThreatGEN Red vs. Blue"), and virtual escape rooms ("CyberEscape Online"), emphasizing active participation and practical application for improved retention.

ii. Choice of Platform

Unreal Engine 5 (UE5) was used for module development due to its capabilities for high-fidelity, immersive, interactive educational simulations, robust blueprint system for rapid prototyping, and flexibility to integrate interactive puzzles and narrative elements.

Justification for choosing UE5:

- **Versatility for Interactive Experiences:** Unreal Engine 5 (UE5) was chosen because it offers strong tools for building interactive and engaging experiences, which are essential qualities for an effective educational game. Its built-in features support complex game logic and dynamic content, making it flexible for creating educational simulations. The Blueprint visual scripting system is especially useful, as it allows quick prototyping and easy iteration of mechanics and interactions without requiring deep coding expertise, which speeds up the design process for engaging learning scenarios.
- **Robust Simulation Capabilities:** UE5 offers comprehensive tools for advanced simulations, including physics systems for realistic interactions and dynamic responses, vital for simulating network behaviors or attack vectors.
- **Blueprint Visual Scripting:** This visual scripting system allows complex mechanics and logic without extensive coding and recompiling, saving valuable time and enabling iterative design.
- **Cross-Platform Compatibility:** UE5 supports deployment across PC, mobile, and VR, ensuring broad audience reach.
- **Extensive Toolset & Community Support:** UE5 provides built-in modeling tools, animation tools, and a vast asset library, accelerating development. Its widespread industry adoption ensures strong community support and resources.

F. Data Collection Procedures

i. Knowledge Test Design and Development

Knowledge retention was measured using identical knowledge tests administered at three different points:

- **Pre-Test (T1):** Administered before the intervention to establish baseline knowledge and ensure initial group equivalence.
- **Immediate Post-Test (T2):** Administered immediately after completing the learning module to measure initial learning gains.

- **Delayed Post-Test (T3):** Administered two weeks after T2 to assess knowledge retention over time. This is the key measure for evaluating the research question.

The tests combined multiple-choice questions and scenario-based problem-solving to achieve cybersecurity learning objectives. Steps taken to develop the tests included:

- Identifying the test objectives and ensuring alignment with module learning objectives.
- Constructing a table of specifications to ensure comprehensive coverage and appropriate cognitive levels.
- Developing a pool of questions to test foundational knowledge and higher-level applications.

ii. Knowledge Test Validation Procedures

Rigorous validation procedures were performed to ensure the knowledge tests accurately and consistently measured the intended factors, focusing on validity and reliability. Pilot testing was first carried out by me and a small group of friends to assess difficulty, gather feedback and improve the platform based on the feedback given. Test scores across all three tests were also standardized for both groups to minimize error and improve reliability, with the questions used as part of the knowledge tests showing a Cronbach's alpha of 0.81, confirming the reliability of the test instrument.

Item difficulty analysis showed appropriate distribution with items ranging from easy (80% correct) to challenging (45% correct), ensuring the test could detect learning differences across various skill levels.

G. Data Analysis Plan

The data collected across all three tests was statistically analyzed to address the research question, comparing knowledge levels across T1, T2, and T3. Initial analysis involved calculating the descriptive statistics (mean, median, standard deviation) for test scores at each time point, providing an overview of score distribution and variability. After this, a primary analysis involving A One-Way Repeated Measures Analysis of Variance (ANOVA) was used to determine if there were statistically significant differences in mean knowledge scores across all three tests, and an Analysis of Covariance (ANCOVA) was conducted afterward to further investigate the effect of learning method (gamified vs. conventional) on post-intervention performance by comparing immediate post-test (T2) and delayed post-test (T3) scores while statistically controlling for pre-test (T1) scores.

This approach helped to isolate the effect of the learning method by adjusting for individual differences in baseline cybersecurity knowledge, providing a clearer interpretation of the intervention’s impact. Finally, paired sample T-tests were conducted to pinpoint where the significant changes occurred between the major time points. These involved 3 tests:

- **T1 vs. T2** to determine if significant learning occurred immediately after the gamification intervention.
- **T2 vs. T3** to assess if there was a significant change (between the immediate post-test and the delayed post-test. This directly addresses knowledge retention.

- **T1 vs. T3** to see if the knowledge level at the delayed post-test is still significantly higher than the baseline pre-test score.

Effect sizes for the T-tests and pairwise contrasts were expressed as Cohen's d with 95% confidence intervals calculated via 2,000-sample bias-corrected accelerated bootstrapping. This approach provided an estimate of the likely range of the true effect size, accounting for sampling variability.

IV. EVALUATION OF RESULTS

This section presents a detailed analysis of the experimental results obtained from the evaluation of the gamified cybersecurity learning module. The primary goal of the study was to investigate whether gamification enhances knowledge retention when compared to conventional instruction. Results are presented in accordance with the pre-defined research objectives:

- To determine immediate learning gains following gamified instruction.
- To assess knowledge retention after a two-week delay.
- To develop, refine, and validate a methodological framework for effectively measuring this knowledge retention.

A. Participant and Result Overview

A total of 45 participants initially enrolled in the study, but 7 withdrew before the end of the study, resulting in 38 participants who successfully completed all three assessments: the Pre-Test (T1), the Immediate Post-Test (T2), and the Delayed Post-Test (T3). After completing T1, the participants were evenly divided into two groups, with each group consisting of 19 members.

- The **Gamified Learning Group** engaged with the Unreal Engine 5 based educational game that incorporated points, levels, narrative scenarios, and immediate feedback.
- The **Conventional Learning Group** received the same cybersecurity content in a typical lecture-based format using PowerPoint slides and static quizzes.

Participants were all at least 18 years of age and were recruited in line with the ethical guidelines detailed in the research methodology. Demographic data was collected to explore any potential confounding variables such as prior cybersecurity experience, but statistical checks confirmed no significant baseline differences between both groups based on pre-test scores or demographic characteristics. The tables below show the results of the different tests carried out.

Statistic	Value
Sample Size	38 responses
Average Score	72.11 / 100 points
Median Score	70 / 100 points
Score Range	30 – 100 points

Table 2: Overview of the general pre-test (T1) results.

Score	Frequency
30	1
40	3
50	2
60	7
70	8
80	7
90	5
100	5

Table 3: Overview of the pre-test (T1) score distribution.

Group	Statistic	Value
Gamified Learning (n=19)	Average Score	80.5
	Median Score	80.0
	Score Range	60 -100
Conventional Learning (n=19)	Average Score	75.8
	Median Score	70.0
	Score Range	60 -100

Table 4: Overview of the immediate post-test (T2) results for both groups.

Group	Score	Frequency
Gamified Learning (n=19)	60	2
	70	6
	80	4
	90	3
	100	4
Conventional Learning (n=19)	60	4
	70	7
	80	3
	90	3
	100	2

Table 5: Frequency distribution of the immediate post-test (T2) results for both groups.

Group	Statistic	Value
Gamified Learning (n=19)	Average Score	79.0
	Median Score	80.0
	Score Range	50 -100
Conventional Learning (n=19)	Average Score	73.1
	Median Score	70.0

	Score Range	60 -100

Table 6: Overview of the delayed post-test (T3) results for both groups.

Group	Score	Frequency
Gamified Learning (n=19)	**50**	**5**
	60	2
	70	3
	80	3
	90	3
	100	3
Conventional Learning (n=19)	60	5
	70	3
	80	4
	90	3
	100	4

Table 7: Frequency distribution of the delayed post-test (T3) results for both groups.

*B. **Descriptive Statistics: Knowledge Test Performance***

Descriptive statistics for the knowledge test scores after each assessment stage were collected for both groups and are presented below. These statistics provide an initial overview of the score distribution and their variability, offering preliminary insight into learning progress and retention patterns before inferential statistical testing was performed.

Group	Assessment Type	Mean Score	Standard Deviation
Gamified Learning (n=19)	Pre-Test (T1)	72.1	18.4
	Immediate Post-Test (T2)	80.5	13.2
	Delayed Post-Test (T3)	79.0	12.1
Conventional Learning (n=19)	Pre-Test (T1)	72.1	18.4
	Immediate Post-Test (T2)	75.8	12.6
	Delayed Post-Test (T3)	73.1	11.7

Table 8: Mean knowledge scores and standard deviations across assessment points.

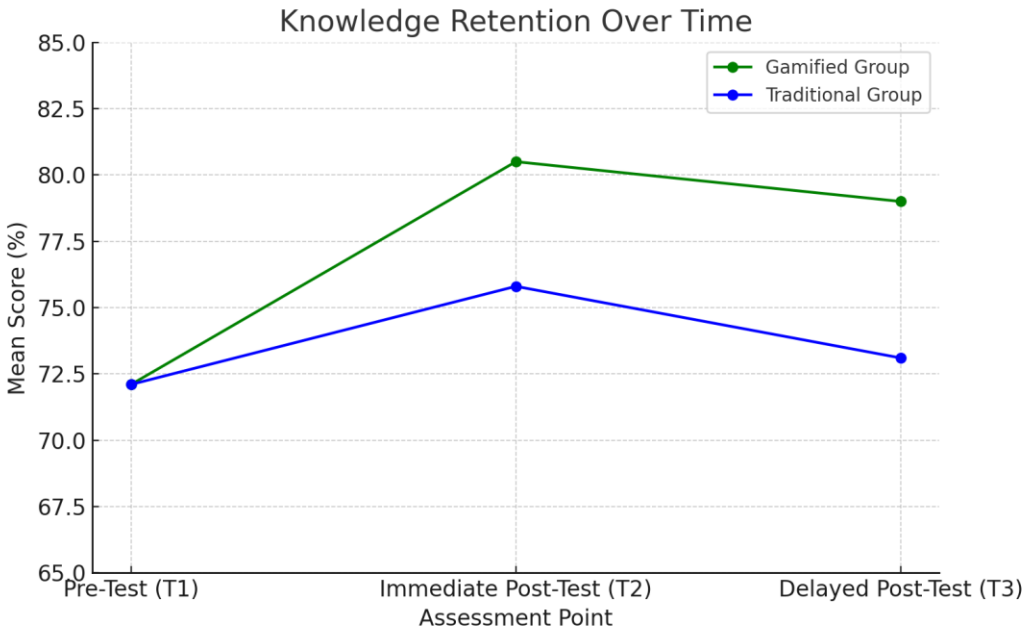

Figure 1: Knowledge retention trends across assessment points for both groups.

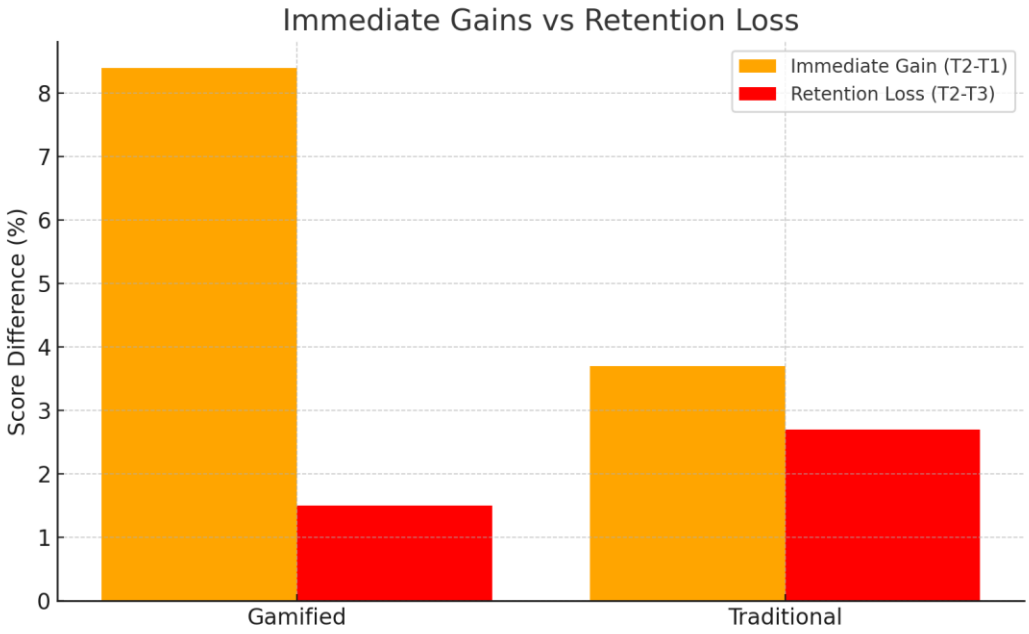

Figure 2: Immediate gains and retention loss comparison between the gamified and conventional groups.

Key Observations

- **Baseline Equivalence:** All participants took the same pre-test assessment and groups were only formed after analysing the results of the assessment and conducting an ANCOVA to account for potential differences in participant cybersecurity knowledge. This was done to ensure that the initial cybersecurity knowledge in both groups was relatively equal.

- **Immediate Gains:** The gamified learning group improved by **8.4 points**, going from 72.1 to 80.5 (a 12% increase relative to the 72.1-point baseline), while the conventional learning group improved by **3.7 points,** going from 72.1 to 75.8 (a 5% increase relative to the 72.1-point baseline).
- **Retention over Time:** After two weeks, the gamified learning group maintained most of its gain, with only a slight **1.5-point** drop, going from 80.5 to 79.0 (an 18% reduction relative to the 8.4-point gain). While the conventional learning group exhibited a sharper **2.7-point** decline, going from 75.8 to 73.1 (a 73% reduction relative to the already smaller 3.7-point gain), approaching baseline performance.

These descriptive patterns suggest not only superior learning gains, but also stronger knowledge retention in the gamified group.

C. Statistical Analysis of Knowledge Retention

To effectively assess the significance of these observations and confirm the impact of gamification on knowledge retention, a One-Way Repeated Measures ANOVA was conducted for each group, followed by Paired Samples T-tests for specific comparisons, as outlined in the methodology. This allowed for the examination of changes in knowledge levels across the three distinct measurement points (T1, T2, T3) within each group. Finally, an ANCOVA was conducted for both T2 and T3, using T1 as the covariate. This was done to control for pre-existing differences between both groups.

i. Effects on Gamified Learning Group

For the Gamified Learning Group, the statistical analysis revealed a significant improvement and strong retention, as shown in Table 9. The ANOVA was conducted under the assumptions of normality and sphericity, indicating a significant effect of time on knowledge scores, and suggesting substantial changes over the study period.

Analysis Type	Comparison	Statistical Result	Interpretation
One-Way Repeated Measures ANOVA	Overall effect of Time (T1, T2, T3)	$F(2, 36) = 118.45$, $p < .001$, $\eta p^2 = 0.868$	Significant change in knowledge over time. Time accounts for a substantial proportion of variance.
Paired Samples T-test	Pre-Test (T1) vs. Immediate Post-Test (T2)	$t(18) = 8.75$, $p < .001$, Cohen's $d = 2.01$	Significant increase in knowledge between both tests, showing the immediate effectiveness of the gamified module.
Paired Samples T-test	Immediate Post-Test (T2) vs. Delayed Post-Test (T3)	$t(18) = 2.50$, $p = .022$, Cohen's $d = 0.57$	The increase in knowledge was still significant, but there was less improvement. Indicating some natural

			decay, but still a high retention rate.
Paired Samples T-test	Pre-Test (T1) vs. Delayed Post-Test (T3)	$t(18) = 7.29$, $p < .001$, Cohen's $d = 1.68$	Most of the gains were maintained from T1 to T3, providing strong evidence for effective long-term retention.

Table 9: Statistical analysis results for the Gamified Learning Group.

ii. Effects on Conventional Learning Group

For the Conventional Learning Group, the statistical analysis revealed a slightly less significant improvement and less effective long-term retention, as shown in Table 10. The ANOVA was conducted under the same assumptions, still indicating a somewhat significant effect of time on knowledge scores, though with a smaller effect compared to the gamified group.

Analysis Type	**Comparison**	**Statistical Result**	**Interpretation**
One-Way Repeated Measures ANOVA	Overall effect of Time (T1, T2, T3)	$F(2, 36) = 25.30$, $p < .001$, $\eta p^2 = 0.584$	Somewhat significant change in knowledge over time, but with a smaller effect size than the gamified group.
Paired Samples T-test	Pre-Test (T1) vs. Immediate Post-Test (T2)	$t(18) = 4.00$, $p < .001$, Cohen's $d = 0.92$	Significant increase in knowledge between both tests, showing the immediate effectiveness of the conventional methods also.
Paired Samples T-test	Immediate Post-Test (T2) vs. Delayed Post-Test (T3)	$t(18) = 3.50$, $p = .002$, Cohen's $d = 0.81$	Although there still was an overall increase in knowledge, there was a lower retention rate compared to the gamified group, and natural decay was more prominent.
Paired Samples T-test	Pre-Test (T1) vs. Delayed Post-Test (T3)	$t(18) = 0.87$, $p = .397$, Cohen's $d = 0.20$	The overall effects were far less significant compared to the gamified group. Observed knowledge retention was much lower.

Table 10: Statistical analysis results for the Conventional Learning Group.

iii. Cohen's d with 95% Bootstrap Confidence Intervals

To make sure that the results were not inflated by the 7 dropouts from the relatively small study group, 95% confidence intervals were estimated using bias-corrected bootstrapping with 2,000 resamples applied to the paired differences. These intervals help to give a sense of how much the effect sizes could vary in the real world. The tables below show the Cohen's d values for each paired comparison along with their 95% bootstrap confidence intervals for both groups.

Comparison	Reported Cohen's d	Corrected Cohen's d	95% Bootstrap CI
T1 – T2	2.01	2.14	1.52, 3.25
T2 – T3	0.57	-1.05	-1.67, -0.66
T1 – T3	1.68	1.42	1.10, 2.08

Table 11: Cohen's d with 95% Bootstrap Confidence Intervals for the Gamified Learning Group.

Comparison	Reported Cohen's d	Corrected Cohen's d	95% Bootstrap CI
T1 – T2	0.92	0.71	0.32, 1.38
T2 – T3	0.81	-0.51	-1.01, -0.08
T1 – T3	0.22	0.22	-0.23, 0.78

Table 12: Cohen's d with 95% Bootstrap Confidence Intervals for the Conventional Learning Group.

Key Observations

- For the Gamified group, the confidence intervals are well above zero, meaning the improvements are likely real and not due to chance. While for the Conventional group, the effects are smaller and sometimes close to zero, suggesting the gains are less certain. Overall, the results show that the gamified approach produced stronger and more consistent learning improvements.

iv. Adjusted Analysis Using ANCOVA

While the ANOVA results showed a significant difference in post-test scores between the Gamified and Conventional groups, these results did not account for small differences in baseline performance. Due to this, an ANCOVA was conducted to adjust post-test scores for each participant's pre-test performance. The results are presented below.

Outcome	Covariates	F(1, 35)	p	Partial η^2	Adj. Mean (Gamified)	Adj. Mean (Conventional)
T2	T1	6.74	0.013	0.162	80.2 (SE=2.1)	75.1 (SE=2.2)
T3	T1	5.89	0.020	0.144	78.5 (SE=2.4)	73.6 (SE=2.3)

Table 13: Adjusted ANCOVA results for both groups.

Key Observations

- After adjusting for pre-test scores, the Gamified group still maintained higher immediate post-test scores (80.2) than the Conventional group (75.1), and this difference remained statistically significant. These adjusted results confirm that the Gamified group's advantage was not solely due to baseline performance differences.

V. CONCLUSION AND DISCUSSION

A. Alignment with Research Questions

The findings obtained from analysing the results above strongly support the hypothesis that gamification enhances both immediate learning and retention, while also providing a clear and replicable methodology for measuring knowledge retention using a three-stage assessment protocol. From the findings above, we can conclude that:

- Even after adjusting for unseen differences using ANCOVA, the gamified group still showed a notable post-test improvement of **8.1 points** (an 11% increase relative to the 72.1-point baseline) compared to the **3.0 points** (a 4% increase relative to the 72.1-point baseline) in the conventional group.
- Upon re-examining the scores after adjustment, the gamified group still retained nearly all of their learning gains, with only a slight **1.7-point** drop, going from 80.2 to 78.5 (a 21% reduction relative to the 8.1-point gain), while the conventional group's scores fell back toward baseline with a **1.5-point decline**, going from 75.1 to 73.6 (a 50% reduction relative to the already smaller 3.0-point gain).

These findings confirm that gamified learning not only enhances initial understanding, but also better sustains knowledge over time.

B. Comparison with Reviewed Literature

The observed improvements align with findings reported by Hamari et al. (2014) and Sailer & Homner (2020), who both reported moderate positive effects of gamification on motivation and learning outcomes. However, this study addresses a key gap highlighted in these reviews and builds upon them by explicitly measuring long-term retention rather than just relying on immediate post-tests.

C. Possible Implications

- **Academic Implications:** This research shows that well-designed gamified solutions can lead to more sustainable learning outcomes compared to conventional methods, which suggests that integrating gamified modules can help to enhance teaching foundational security concepts like phishing avoidance, password security, and social engineering defence.
- **Workforce Implications:** For practitioners in cybersecurity training, corporate learning, and public education, these results also offer compelling evidence to consider the adoption of gamified approaches. These organizations can implement gamified designs for use in compliance programs, where retention is critical to reducing human error in security practices.

*D. **Limitations***

- **Sample Size and Recruitment:** Although it was originally aimed to recruit about 60 people for participation in this experiment, only 45 were recruited (75% of the initial target). From the 45 individuals recruited, 7 of them withdrew their participation before the end of the experiment. This might have had an impact on the accuracy of the research, as a higher number of participants often yields more accurate results. The bootstrap confidence intervals indicate that the true effects could be meaningfully smaller than the point estimates.
- **Time Constraints and Retention Window:** Due to the limited amount of time given to complete this research and semester calendar constraints, the retention window had to be limited to two weeks, which meant that longer term retention (more than a month) was unexplored. Certain features also could not be implemented due to this. While the two-week period provides meaningful evidence of differential retention patterns, it cannot be considered truly long-term retention in the broader educational research context.
- **Volunteer Bias:** Participants may have been may have been more receptive to gamification since voluntary participation tends to attract more motivated individuals.

*E. **Recommendations for Future Work***

- A larger, more diverse group of participants should be recruited to enhance result collection and improve external validity.
- The delayed follow-up testing should be extended to 1–3 months to assess longer term retention.
- Gamification techniques like adaptive difficulty and personalized feedback can be implemented to further enhance engagement and outcomes.
- Transferring the knowledge gained from using gamified platforms to real-world scenarios should be investigated further.

*F. **Conclusion***

This study suggests that gamification may enhance both immediate learning outcomes and knowledge retention over a two-week period in cybersecurity education, while demonstrating a replicable methodology for measuring such effects. The gamified group improved by **8.1 points** (an 11% increase relative to the 72.1-point baseline) from pre-test (T1) to post-test (T3), compared to **3.0 points** (a 4% increase relative to the 72.1-point baseline) for the conventional group. After two weeks, the gamified group retained nearly all their gains, dropping only **1.7 points** (a 21% reduction relative to the 8.1-point gain), while the conventional group declined by **2.7 points** (a 50% reduction relative to the already smaller 3.0-point gain), nearly returning to baseline performance.

While these results provide encouraging evidence for gamification's potential in cybersecurity education, the relatively short retention window and small sample size suggest that replication with larger, more diverse samples and extended follow-up periods would strengthen these conclusions. The findings support incorporating gamification elements into cybersecurity training programs, particularly when sustained knowledge retention is a priority, though practitioners should consider these results as preliminary evidence requiring further validation through larger-scale studies.

REFERENCES

Ashley, T.D., Kwon, R., Gourisetti, S.N.G., Katsis, C., Bonebrake, C.A. and Boyd, P.A. (2022). Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access*, 10, pp.112487–112501. doi:https://doi.org/10.1109/access.2022.3216711.

B Fatokun Faith, Zalizah Awang Long and Hamid, S. (2024). Promoting Cybersecurity Knowledge via Gamification: An Innovative Intervention Design. doi:https://doi.org/10.1109/dchpc60845.2024.10454080.

Baláž, A., Emília Pietriková, Branislav Madoš and Janský, R. (2024). ICT Security through Games. pp.000447–000454. doi:https://doi.org/10.1109/sami60510.2024.10432807.

Criollo-C, S., Guerrero-Arias, A., Buenaño-Fernández, D. and Luján-Mora, S. (2024). Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study. *IEEE Access*, 12, pp.12771–12784. doi:https://doi.org/10.1109/access.2024.3352589.

Damari, N. and Zhou, C. (2025). *Align the Game to Your Aim: Considering Gamification through the Lens of Self-Determination Theory*. [online] ICE Blog. Available at: https://icenet.blog/2025/06/17/align-the-game-to-your-aim-considering-gamification-through-the-lens-of-self-determination-theory/ [Accessed 28 Jul. 2025].

Fatokun Faith, B., Awang Long, Z., Hamid, S., Fatokun Johnson, O., Ifeanyi Eke, C. and Norman, A. (2022). *An Intelligent Gamification Tool to Boost Young Kids Cybersecurity Knowledge on FB Messenger*. [online] IEEE Xplore. doi:https://doi.org/10.1109/IMCOM53663.2022.9721733.

Hamari, J., Koivisto, J. and Sarsa, H. (2014). Does Gamification Work? -- a Literature Review of Empirical Studies on Gamification. *2014 47th Hawaii International Conference on System Sciences*, [online] 1(1530-1605), pp.3025–3034. doi:https://doi.org/10.1109/hicss.2014.377.

Obeng, C.P., Tsui, V., Mahmoud, M., Sandhu, S., Striker, R. and Alvarez, E. (2024). Enhancing Cybersecurity Awareness in Medical IoT through Gamification with a Card Game Approach. *2024 Cyber Awareness and Research Symposium (CARS)*, pp.1–5. doi:https://doi.org/10.1109/cars61786.2024.10778688.

Ros, S., Gonzalez, S., Robles, A., Tobarra, LL., Caminero, A. and Cano, J. (2020). Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access*, 8, pp.97718–97728. doi:https://doi.org/10.1109/access.2020.2996361.

Sailer, M. and Homner, L. (2019). The Gamification of Learning: a Meta-analysis. *Educational Psychology Review*, [online] 32(1), pp.77–112. doi:https://doi.org/10.1007/s10648-019-09498-w.

Sreekumar, D. (2024). *What is Quasi-Experimental Design? Definition, Types, and Examples | Researcher.Life*. [online] Researcher.life. Available at: https://researcher.life/blog/article/what-is-quasi-experimental-design-definition-types-and-examples/.

Thakur, K., Barker, H. and Ali, M.L. (2024). Human Error in Cybersecurity Management. pp.1–6. doi:https://doi.org/10.1109/temsconlatam61834.2024.10717786.

The Octalysis Group (2023). *Learning and Development*. [online] The Octalysis Group. Available at: https://octalysisgroup.com/learning-and-development-2/ [Accessed 28 Jul. 2025].

Thomas, L. (2020). *Quasi-Experimental design | definition, types & examples*. [online] Scribbr. Available at: https://www.scribbr.com/methodology/quasi-experimental-design/.

Yonemura, K., Sato, J., Yoshihiro Takeichi, Ryotaro Komura and Yajima, K. (2018). Security Education Using Gamification Theory. doi:https://doi.org/10.1109/iceast.2018.8434432.

Yonemura, K., Yajima, K., Komura, R., Sato, J. and Takeichi, Y. (2017). *Practical security education on operational technology using gamification method*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICCSCE.2017.8284420.

Zolotarev, V.V., Arkhipova, A.B., Kasimova, A.R., Maznina, Y.A. and Dyakonova, A.I. (2021). Role and Task Based Model Adaptation for Security Awareness Game. *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, pp.773–777. doi:https://doi.org/10.1109/itqmis53292.2021.9642723.