

Hossain MD Saiful Hoque

# **GAMIFICATION OF CYBERSECURITY TRAINING TO IMPROVE AWARENESS**

Master's Thesis  
Faculty of Information Technology and Communication Sciences  
Tiina Schafeitel-Tähtinen  
Marko Helenius  
June 2025

# ABSTRACT

Author : Hossain MD Saiful Hoque  
Title : Gamification of cybersecurity training to improve awareness  
Master's Thesis  
Tampere University  
Master of Science (Technology), Information Technology  
June 2025

---

In this digital world, cybersecurity education has become one of the essential requirements for safe online practice. Effective cybersecurity training is important for providing the necessary knowledge and skills. To examine the effectiveness of gamified cybersecurity education, a game-based training tool called CyberBee was developed. The aim of this thesis is to assess the impact of the gamified cybersecurity training on participants' knowledge, confidence, skills, attitude, and competence in managing cybersecurity threats, with a specific focus on phishing and password security.

This thesis was completed using mixed methods such as pre- and post-training surveys, non-parametric analysis (Wilcoxon Signed-Rank test, Mann-Whitney U test), and thematic feedback analysis. The study includes 15 participants, a mix of university students and employees from an organization.

After playing the game confidence level increased directionally and showed strong reliability metrics. Although, the changes narrowly missed statistical significance, the effect size ( $|r| = 0.49$ ) indicates meaningful improvement in confidence. Knowledge and skills did not show statistically significant improvement due to the ceiling effect, but item-level analysis revealed a meaningful gain in specific areas such as using a password manager (knowledge improved by 13.3%) and managing phishing email (skills improved by 13.3%).

Awareness has demonstrated a statistically significant improvement with a large effect size  $|r| = 0.62$ . Attitude and competence remained stable and suggests a ceiling effect. Evaluation of the gamified training experience emphasized excellent engagement (median = 4.33), ease of use (median = 5.00), and positive learning motivation, though suggestions for more complex content and additional modules were noted.

Findings in this study indicate that gamification of cybersecurity training is an effective way to improve awareness, but they also indicate the areas where training design and scope could be better. Future research could explore larger sample sizes, extended data collection periods, and more diverse training modules.

Keywords: Gamification, Cybersecurity, Awareness Training

The originality of this thesis has been verified using the Turnitin Originality Check service.

# USE OF AI IN THESIS

I have utilized AI tools in my thesis:

- No
- Yes

The AI tools utilised in my thesis and their purposes are described below:

Names and versions of AI tools: QuillBot v23.8.1, ChatGPT-4-turbo

Purpose of using AI tools: QuillBot was used mainly for grammar check and paraphrasing lines in a more academic format. ChatGPT to find different kinds of data analysis methods that can be conducted on the collected data.

Sections where AI tools were used: QuillBot was used to rephrase lines in Introduction, Literature Review, Methodology, and Conclusion. ChatGPT in the Result section.

I acknowledge that I am fully responsible for the entire content of my thesis, including the parts generated by AI, and I accept accountability for any violations of ethical standards in publications.

## PREFACE

This study was completed as a part of my master's studies at Tampere University in the Information Technology program. The study explores the impact of gamified cybersecurity training on improving awareness. This topic reflects both my academic interest and growing need for practical cybersecurity education.

I like to express my sincere gratitude to my thesis supervisors, Tiina Schafeitel-Tähtinen and Marko Helenius, for their continuous support, valuable feedback, and guidance throughout the process. I also thank the participants' who participated in the study voluntarily, as their involvement made this research possible.

I extend my appreciation to the faculty and staff of the Information Technology and Communication Sciences for providing a supportive learning environment. Special thanks to my family and friends for their encouragement and patience during this journey.

Tampere, 03 June 2025

Hossain MD Saiful Hoque

# CONTENTS

LIST OF FIGURES.....	V
LIST OF TABLES.....	VI
1.INTRODUCTION .....	1
2.LITERATURE REVIEW.....	3
3.METHODOLOGY.....	6
3.1 Research design and procedure.....	6
3.2 Variables and measurement.....	11
3.2.1 Summary of variables and items.....	11
3.2.2 Confidence.....	15
3.2.3 Knowledge.....	16
3.2.4 Skills.....	16
3.2.5 Awareness, attitude, and competence.....	16
3.2.6 Gamified training evaluation.....	17
3.3 Data processing activity.....	17
3.4 Data analysis.....	18
4.RESULTS.....	20
4.1 Confidence in identifying and managing cyber threats.....	20
4.2 Knowledge of phishing & password security.....	21
4.3 Practical cybersecurity skills.....	22
4.4 General cybersecurity awareness, attitude and competence.....	25
4.5 Gamified training evaluation.....	26
4.6 Feedback analysis.....	27
5.DISCUSSION.....	29
6.LIMITATIONS.....	33
7.CONCLUSIONS.....	34
REFERENCES.....	35

## LIST OF FIGURES

<b>Figure 1.</b>	<i>Cyber Bee welcome page.</i>	7
<b>Figure 2.</b>	<i>Phishing tutorial for participants.</i>	7
<b>Figure 3.</b>	<i>Phishing level 7 simulated phishing email.</i>	8
<b>Figure 4.</b>	<i>Password Security level 1 multiple-choice questions.</i>	8
<b>Figure 5.</b>	<i>Immediate feedback to reinforce the learning.</i>	9
<b>Figure 6.</b>	<i>Pre-training survey at the beginning of the game.</i>	10
<b>Figure 7.</b>	<i>Post-training survey at end of the game.</i>	10
<b>Figure 8.</b>	<i>Wilcoxon Signed Rank Test for knowledge.</i>	22
<b>Figure 9.</b>	<i>Wilcoxon Signed Rank Test for skills.</i>	23
<b>Figure 10.</b>	<i>Cross-tab analysis of pre training skills.</i>	24
<b>Figure 11.</b>	<i>Cross-tab analysis of post training skills.</i>	24

## LIST OF TABLES

<b>Table 1.</b> Variables and pre-post training items.....	11
<b>Table 2.</b> Variables descriptive statistics and reliability values.....	20
<b>Table 3.</b> Variables descriptive statistics of confidence.....	21
<b>Table 4.</b> Knowledge item level analysis.....	22
<b>Table 5.</b> Skills scenario level analysis.....	23
<b>Table 6.</b> Descriptive analysis of awareness, attitude, and competence.....	25
<b>Table 7.</b> Frequency analysis of awareness, attitude, and competence.....	25
<b>Table 8.</b> Composite evaluation of training evaluation.....	26
<b>Table 9.</b> Effective features.....	27
<b>Table 10.</b> Suggested improvements.....	28

## LIST OF SYMBOLS AND ABBREVIATIONS

C	Confidence
K	Knowledge
S	Skills
AW	Awareness
AT	Attitude
CM	Competence
EG	Engagement
EU	Ease of Use
SA	Satisfaction
GS	Game support
FM	Future motivation
BG	Background
https	HyperText Transfer Protocol Secure

$n$	sample size
$p$	probability
$r$	effect size
$U$	Mann-Whitney U test
$v$	version
$Z$	Z-score
$\alpha$	Cronbach's alpha

# 1. INTRODUCTION

Our daily life standard is directly influenced by the internet. A few clicks or touches make our usual daily tasks simple and complete. However, these same few clicks or touches that make our lives easier, they can also make our lives miserable if we lack awareness. Cybersecurity threats in our digitalized world are rising at an alarming pace [1]. Threats like phishing and password security continue to escalate along with other threats, targeting individuals and organizations. Solutions based on technology are not enough to provide complete protection. Cybersecurity awareness plays a vital role in protecting against such threats. Despite extensive awareness training, studies indicate users make the wrong choice and put themselves at risk due to gaps in applied knowledge, skills, and confidence [2][3]. Traditional cybersecurity training is not effective at encouraging good security practices and normally does not engage participants [4]. In addition, traditional training methods such as lecture-based instructions or e-learning modules have limited capability to keep people engaged and modify their behaviour for the long term [5]. Furthermore, traditional methods are typically passive, depend on memorization, and often lack context like real-world scenarios [5][6]. According to Parsons et al., such traditional methods may increase awareness temporarily, but they often fail to translate into improved security behaviour [7]. Another problem with traditional training method is that they lack quick feedback and active learning, both of which are important for building skills and self-efficacy [5]. Bada et al. indicate that traditional training has low retention and engagement rates; hence, participants often lose interest and face difficulties in applying learned content [8].

In response to these shortcomings in traditional approaches, gamified training approaches have been introduced where game-like features are integrated into non-game contexts. Studies suggest that gamification of cybersecurity training can enhance knowledge, motivation, and behavioural intents [5][9]. However, the results of the real-world studies still vary, particularly regarding the impact of gamification on constructs such as confidence, knowledge, skills, and behavioural intents across different cybersecurity areas[5][9].

The objective of this thesis was to assess the impact of gamified cybersecurity training in improving participants ability to identify phishing threats and manage password security.

This study used a multi-dimensional assessment to analyse the effectiveness of gamified training focusing on phishing and password security. The training's purpose was to improve participants knowledge, confidence, skills, awareness, attitude, and competence. Additionally, user experience metrics such as engagement, ease of use, and satisfaction were collected. The aim was to provide insight into how gamification can support enhancing cybersecurity education.

The central research questions guiding this study were:

- RQ1.** Does gamified cybersecurity training increase participants' confidence in identifying and managing cyber threats (phishing & password security)?
- RQ2.** Does gamified cybersecurity training improve participants' actual knowledge of phishing and password security?
- RQ3.** How effectively does gamified cybersecurity training develop participants' practical skills in identifying phishing threats and strengthening password security?
- RQ4.** Does previous or current experience (such as prior training experience or experience with gamified training) influence participants' improvement in knowledge and confidence after training?
- RQ5.** How do participants evaluate the gamified training in terms of engagement, effectiveness, and ease of use?

Chapter 2 reviews the existing literature on cybersecurity training and gamification. Chapter 3 explains the research methodology, game design, variables and measurements, items, data analysis, and data processing. The results of the thesis are presented in Chapter 4. Chapter 5 offers a detailed discussion of the findings in relation to the research questions. Chapter 6 outlines the limitations confronted during the research and recommendations for future work. Chapter 7 concludes the thesis by summarizing the key results and contribution.

## 2. LITERATURE REVIEW

In a rapidly growing digitalized world, cybersecurity threats such as phishing, password theft, ransomware, and social engineering continue to escalate. While defensive technology has improved in several aspects, human behaviour is still a significant vulnerability. Verizon's data breach investigation in 2021 found that 85% of data breaches involved a human mistake, including actions influenced by social engineering [10]. Since then, the percentage of data breaches caused by human mistakes has dropped over the past few years: 82% in 2022, 74% in 2023, and 68% in 2024 [10]. Finding such concerning statistics, organizations have invested in training programs for cybersecurity awareness. Without cybersecurity awareness training, any organization will be vulnerable to cybersecurity threats. Organizations select various training models according to their needs, the threats they encounter, and the model's design. In general, traditional training models rely on pre-built systems with fixed curricula, which makes the system less flexible because it trains the user with the concept of “-one for all” [6]. Users often find conventional training models, such as lectures, static modules, and small general tests, to be repetitive, challenging, and unengaging [8][7]. As a result, traditional security awareness training does not always change behaviour but helps recognize the threat [8]. Furthermore, several security awareness programs rely on outdated methods that prioritize knowledge over action [7].

An effective and strong training program should be behaviour-driven, adaptive, and personalized to reduce the cyber threat. To address the limitations of traditional training methods, alternative approaches such as gamified learning have been explored in recent studies. For instance, Gjertsen et al. imply that gamified cybersecurity training resulted in 15% improvements in learning outcomes compared to static modules [11]. A similar study by Scholefield and Shepherd observed that participants exposed to interactive game-based modules showed significant threat recognition accuracy and reported a higher satisfaction level (mean engagement 4.2/5) than those in the lecture-based group [12]. According to Keepnet Labs systematic review, organizations implementing gamified training tools have observed a significant improvement in employee engagement and more accuracy in phishing detection [13].

Gamification refers to the application of game design elements, such as point scoring, competition rules, feedback, and rewards, implemented in non-game contexts to enhance user engagement and motivation [14]. In the study by Khoshnoodifar et al., authors found that the implementation of gamified learning in a statistics course for health school students significantly improved both learning outcomes and student attitudes compared to traditional teaching methods [14]. The gamification of learning is effective because studies have shown that gamification has a positive impact on cognitive, motivational, and behavioural learning outcomes [15][16].

The study by Zeng and McEneaney suggests that adding competitive components to learning can help certain participants stay motivated and engaged [17]. However, this study also noted that competition may negatively affect participants who experience stress or performance anxiety, indicating its usefulness relies on the participant and the situation [17]. Moreover, they also found that when designed appropriately, competition can serve as an effective educational tool to increase engagement and motivation [17]. Games always carry several such motivational elements. According to a TalentLMS survey on gamification techniques, points, tracking, badges, and leaderboards help users' engagement and reinforce knowledge [15].

In the field of cybersecurity training, gamification has shown capability in changing the traditional training program into a more engaging experience, where ThreatGEN Red vs. Blue is a practical example of it [18]. Red vs. Blue is a cybersecurity simulation game where players can be on either the offensive (red team) or defensive (blue team) side. In this simulation game, real world-based threat scenarios make it more engaging by encouraging critical thinking, decision making and active learning [18]. Real-world simulations and quizzes inspired by real-world situations can promote active participation in gamification training modules. Leading platforms for cybersecurity awareness training, like Hoxhunt, Infosec IQ, and ThreatGEN are now using gamification methods in cybersecurity training [19][20][21]. Usually "gamification" typically connotes entertainment or fun; its primary objective is to engage participants in the process of learning about cybersecurity and equip them with substantial knowledge. This will enable participants to recognize and protect themselves against cyber threats [22]. Furthermore, this research implies that gamification in cybersecurity is only effective if it's properly implemented, such as keeping the training relevant, ensuring that it aligns with real-world threats, and its effectiveness is continuously measured [22].

Despite several studies highlighting the benefits of gamification of cybersecurity training [22][23], there is still a shortage of comprehensive studies examining the gamification impact on participants confidence, knowledge, and practical skills simultaneously. Many studies, like Scholefield and Shepherd, Idierukevbe and Addo, primarily focus on measuring the immediate knowledge gained from gamification training, where it can enhance a short-term learning outcome, but often overlook critical factors such as self-efficacy and practical skills [12][24]. Moreover, a single-point assessment of participants after training usually results in information about the changes related to the gamified training but does not provide insights into participants' knowledge and confidence before training. Although gamification in cybersecurity training is often theoretically well-established by highlighting principles such as points, badges, and leaderboards that can motivate learning, few studies explicitly link these elements to behavioural changes alongside knowledge and confidence [11][25]. Gjertsen et al. observed that even though gamified training improved immediate knowledge acquisition, it did not significantly influence participants' attitudes or intentions regarding security compliance [11]. In the study conducted by Capatina et al., results indicated that implementing gamified elements in training significantly enhanced employee's ability to retain knowledge, confidence, and skills [25].

A pilot study conducted by Mason et al. assessed the gamification intelligent cyber aptitude and skills training (GICAST) program using a pre- and post-experimental design [9]. Where a total 43 students participated, significant improvement in knowledge, attitude, and behaviour was observed. Quantitative data from the Human Aspects of Information Security Questionnaire (HAIS-Q) supported the findings [9]. Similarly, Abu-Amara et al. implemented a gamified training model including pre- and post-game phishing simulation [26]. The result indicated 84.72% improvement in awareness and 77.78% reduction in phishing exposure [26]. Alnajim et al. found that a pre- and post-assessment using a Likert-scale measure showed statistically significant increases in confidence [6].

This thesis points out the gaps in gamification of cybersecurity research, specifically the lack of thorough evaluation of participants confidence, knowledge, skills, and behavioural intentions by implementing pre- and post-training assessments. Furthermore, this study will help to analyse participants experiences and engagement levels along with behavioural perspectives. This approach aims to provide a broader understandings of how gamified cybersecurity training can improve awareness among the users.

## 3. METHODOLOGY

This chapter explains the methodological structure for this thesis. First, the research design and procedure are explained, followed by the development of the gamified training tool Cyber Bee. Furthermore, the game structure, learning elements and assessment process used to evaluate participants cybersecurity awareness are explained too.

### 3.1 Research design and procedure

In this study, a quasi-experimental pre- and post-survey design [27] was implemented to measure the impact of Cyber Bee, a web-based gamified cybersecurity training tool developed for this thesis. Cyber Bee focuses on two of the most common threats encountered by users today: phishing and password security. The aim was to assess the gamification's impact on participants cybersecurity knowledge, confidence, awareness, skills, and behavioural intentions. This design helps to compare the outcome of pre- and post-training without the use of a control group, which is suitable for small-scale exploratory educational research [5].

Cyber Bee was developed using the open-source platform GDevelop (v5) and designed to teach participants about two important cybersecurity threats: phishing and password security. Figure 1 presents the welcoming screen of Cyber Bee. The game is structured in two phases: the learning phase and the assessment phase. In the learning phase, participants are presented with cybersecurity concepts through interactive tutorials. At the beginning of the game, participants are given the option to select a learning tutorial. Currently Cyber Bee has two tutorials: phishing and password security. Each tutorial helps participants to understand the topic and real-world scenarios. It also includes guidance to distinguish between threat and non-threat elements. Figure 2 presents the phishing tutorial page. Later in the assessment phase, participants will navigate scenario- and quiz-based challenges that will test their ability to recognize threats and implement safe actions.



*Figure 1. Cyber Bee welcome page.*



*Figure 2. Phishing tutorial for participants.*

This gamified training tool includes several elements designed to guide and assess participants performance, such as point-based rewards, penalties, and immediate feedback. Participants who could identify and report the simulated phishing emails or right practice of password security were rewarded with +15 points. Failing to do so got a penalty of -10 points. Figure 3 is a simulated phishing email in game stage 7, and Figure 4 shows the multiple-choice question for password security stage 1. Upon an incorrect answer the instant feedback pops up. Figure 5 shows the instant feedback.

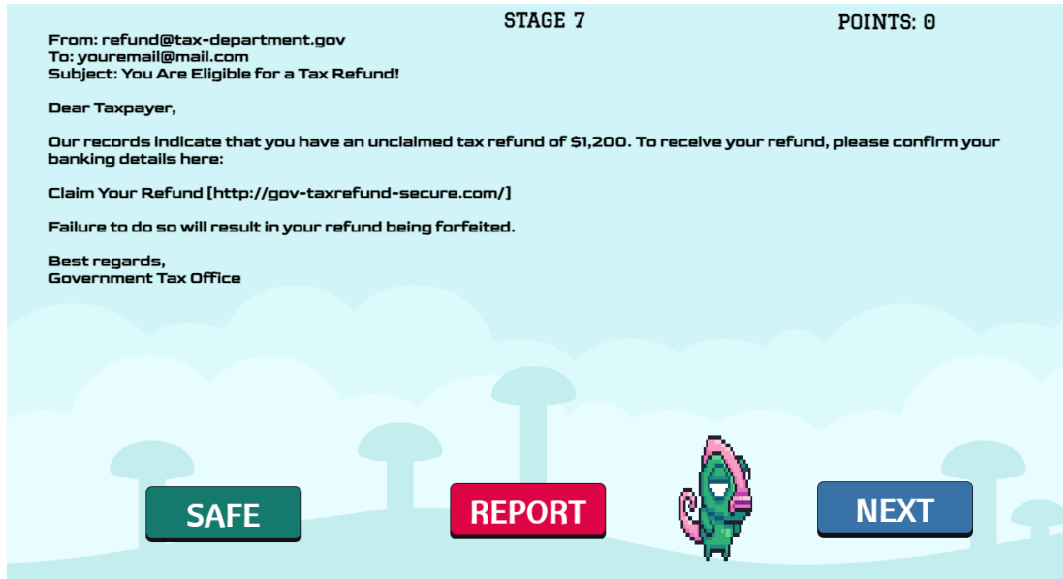


Figure 3. Phishing level 7 simulated phishing email.

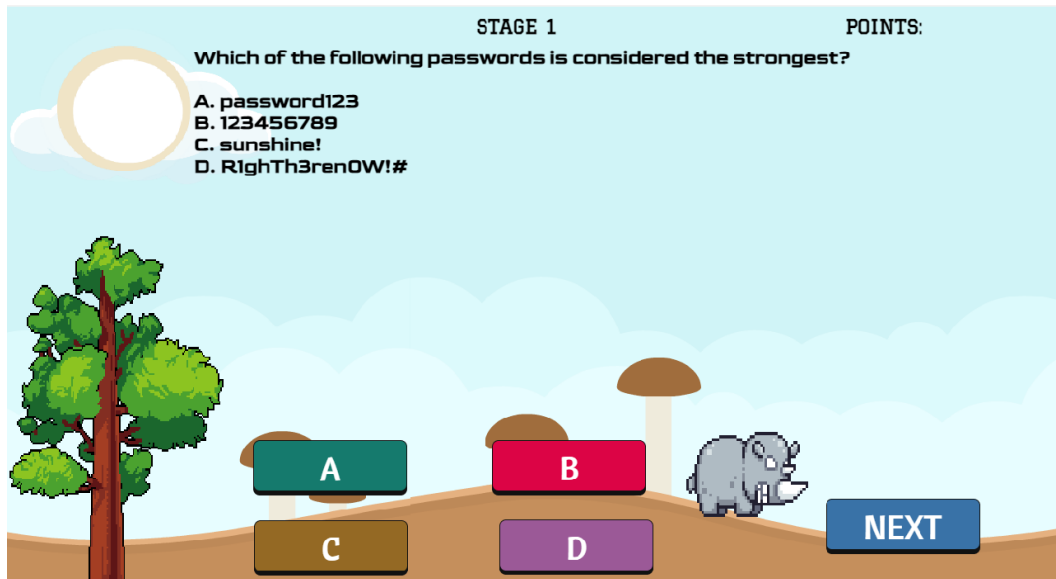
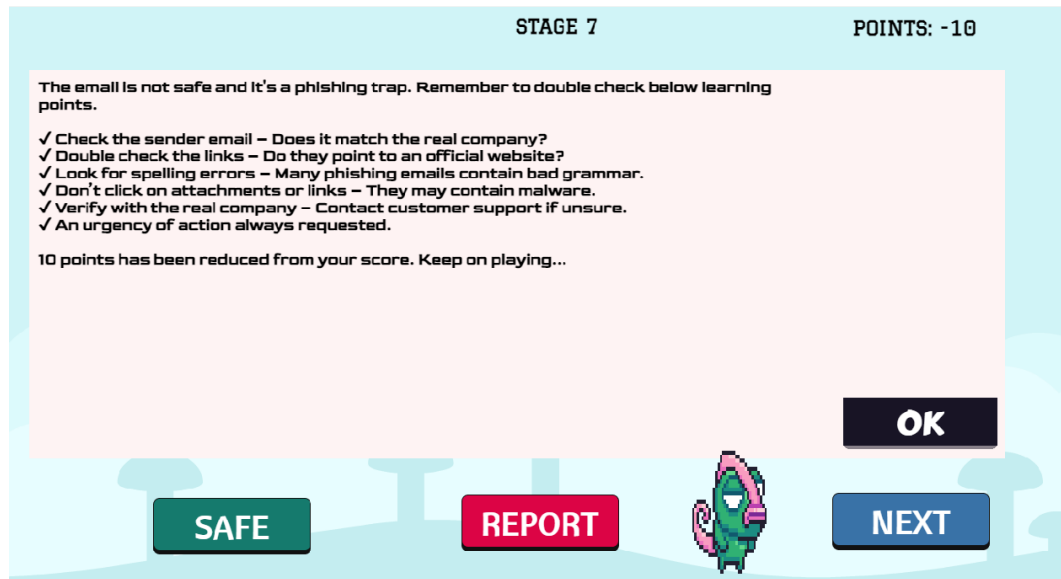


Figure 4. Password Security level 1 multiple-choice questions.



*Figure 5. Immediate feedback to reinforce the learning.*

Participants were recruited on a voluntary basis. A call for participations was sent out to university students and research participants through emails, instant messaging group chat, etc. Upon accessing the game link, participants were asked to fill out the pre-training survey, where the privacy notice and consent form were presented in line with ethical research practice. Participation was anonymous, and no personally identifiable data was required, ensuring compliance with GDPR and university research ethics procedures. The training experience was entirely delivered through a single web-based link.

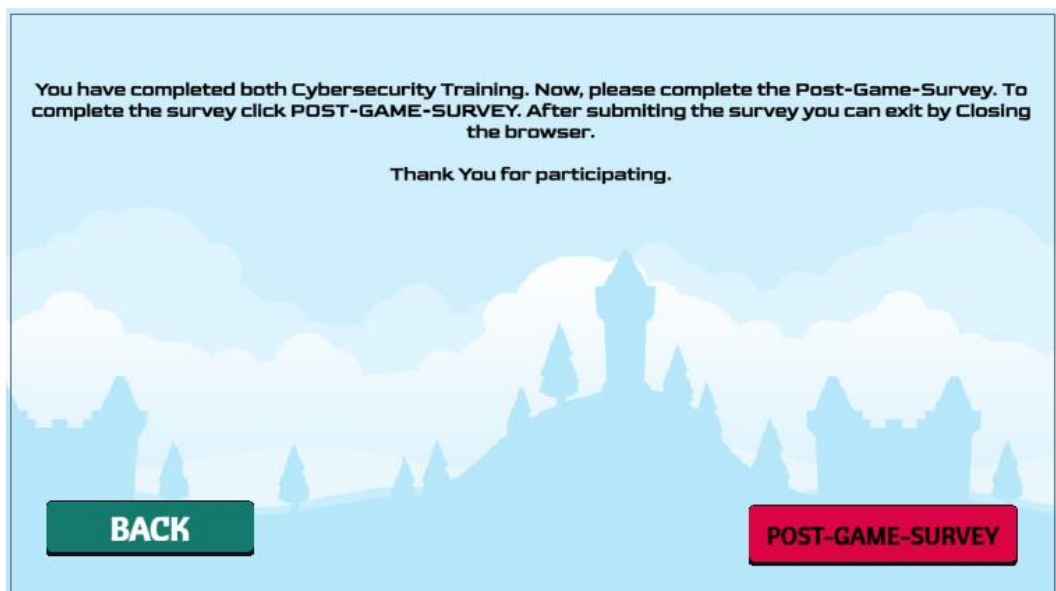
The training procedure was conducted according to below sequence:

1. **Pre-Training Survey:** Participants complete a structured questionnaire that assesses their baseline in cybersecurity knowledge, skills, awareness, and behavioural intentions. Figure 6 shows the presentations of pre-survey link at the game beginning. There is a mix of Likert-scale items and objective multiple-choice questions.



*Figure 6. Pre-training survey at the beginning of the game.*

2. **Game-Based Training:** Participants start with the Cyber Bee game, which includes learning modules and scenario-based challenges.
3. **Post-Training Survey:** Immediately after completing either the phishing game or password security or both, participants complete another identical survey to measure the changes for targeted variables. Figure 7 shows the representations of the post-survey link at the game ending.



*Figure 7. Post-training survey at end of the game.*

Based on real-world phishing and password-related scenarios simulated emails, SMS, and correct/incorrect multiple-choice questions were designed to assess participants actual understanding.

## 3.2 Variables and measurement

A set of variables was developed by the author drawing from relevant literature and research studies to evaluate the impact of gamified cybersecurity training. This section describes each variable and its measurements.

### 3.2.1 Summary of variables and items

To ensure methodological transparency and theoretical validity, a detailed overview of the variables and survey items used in pre- and post-training assessments are provided in Table 1.

**Table 1.** Variables and pre-post training items.

Variables	Pre Training Items	Post Training Items
Confidence	<p>C1. I can accurately recognize suspicious email or SMS.</p> <p>C2. I understand the importance of strong and unique password.</p> <p>C3. I can identify key signs of phishing attempts (Ex: checking if a link is legitimate or if the URL starts with 'https' or verify with original address).</p>	<p>C1. I can accurately recognize suspicious email or SMS.</p> <p>C2. I understand the importance of strong and unique password.</p> <p>C3. I can identify key signs of phishing attempts (Ex: checking if a link is legitimate or if the URL starts with 'https' or verify with original address).</p> <p>C4. I feel more confident in my ability to recognize and respond to cyber threats after playing the game.</p>
Knowledge	K1. It is safe to click links in the email from a known or unknown person without verifying.	K1. It is safe to click links in the email from a known or unknown person without verifying.

	<p>K2. According to you which of the following is the secure way to create a password?</p> <p>K3. Phishing email/SMS usually contains urgent or persuasive language which pressure you to act immediately. (e.g. clicking the link, opening the attachment).</p> <p>K4. A website with https:// in the URL is always safe to enter personal information's.</p> <p>K5. Using same password for multiple accounts is safe as long as it's complex.</p> <p>K6. Two-factor authentication provides an extra layer of beyond just a password.</p> <p>K7. Using password manager is recommended to generate and store strong, unique password for each account.</p>	<p>K2. According to you which of the following is the secure way to create a password?</p> <p>K3. Phishing email/SMS usually contains urgent or persuasive language which pressure you to act immediately. (e.g. clicking the link, opening the attachment).</p> <p>K4. A website with https:// in the URL is always safe to enter personal information's.</p> <p>K5. Using same password for multiple accounts is safe as long as it's complex.</p> <p>K6. Two-factor authentication provides an extra layer of beyond just a password.</p> <p>K7. Using password manager is recommended to generate and store strong, unique password for each account.</p>
--	---	---

Skills	<p>S1. If a friend or known person sends you an unexpected email with link/attachment, it's safe to open it because you trust them.</p> <p>S2. You receive an email from "security@amazon-update.com" asking you to reset your password by clicking a link. What should you do?</p> <p>S3. You receive a text message from an unknown number stating: "Your online banking password has been compromised! Click this link to reset it now." What should you do?</p> <p>S4. Your web browser suggests saving your passwords for convenience. What should you do?</p>	<p>S1. If a friend or known person sends you an unexpected email with link/attachment, it's safe to open it because you trust them.</p> <p>S2. You receive an email from "security@amazon-update.com" asking you to reset your password by clicking a link. What should you do?</p> <p>S3. You receive a text message from an unknown number stating: "Your online banking password has been compromised! Click this link to reset it now." What should you do?</p> <p>S4. Your web browser suggests saving your passwords for convenience. What should you do?</p>
Awareness	AW1. I am aware how to identify and manage potentials cyber security threats.	AW1. I am aware how to identify and manage potentials cyber security threats.
Attitude	AT1. For my daily online activities, I believe it's important to be knowledgeable about Cyber Security.	AT1. For my daily online activities, I believe it's important to be knowledgeable about Cyber Security.

Competence	CM1. I have sufficient knowledge and skills to protect myself from cyber threats	CM1. I have sufficient knowledge and skills to protect myself from cyber threats
Engagement	EG1. Do you believe that gamified training is an interesting way to learn about cybersecurity threats?	EG1. Do you believe that gamified training is an interesting way to learn about cybersecurity threats?  EG2. The competitive elements (e.g., points, stages) in the game motivated me to learn more about cybersecurity threats.  EG3. Playing the game was fun and enjoyable.
Ease of Use		EU1. Game was easy to navigate, and the instructions was clear.
Satisfaction		SA1. How likely are you to recommend such gamified cybersecurity training to a friend or colleague?
Game support		GS1. Immediate feedback during my mistake, helped me to understand better.
Future motivation		FM1. After completing the game, I intend to adopt more secure online practices.

Background	<p>BG1. Did you participate in any gamified cybersecurity awareness training before?</p> <p>BG2. If yes, what kind of training have you participated before?</p> <p>BG3. How frequently do you engage in digital games or interactive applications?</p>	
------------	---	--

Variables with multiple items were tested for reliability using Cronbach's Alphas where appropriate. Data analysis involved descriptive statistics, reliability analysis, the Wilcoxon Signed-Rank test, the Mann-Whitney U test and item-level analysis.

### 3.2.2 Confidence

Confidence in the context of cybersecurity refers to participants self-perceived assurance in their ability to recognize and effectively respond to cyber threats, such as phishing attempts and password-related vulnerabilities. This subjective measure of participants own judgement, and awareness is captured through Likert scale statements evaluating their confidence in pre- and post-training. Self-confidence in cybersecurity has been found to significantly influence participants behaviour, which is sometimes even more than actual knowledge in cybersecurity [28]. Research has shown that often cybersecurity behaviour is driven more by self-confidence than actual knowledge [29]. In this study, confidence was measured using a Likert scale in pre- and post-training. The items in pre-training C1-C3 and post training C1-C4 designed to reflect the core cybersecurity task (Table 1 subchapter 3.2.1). The items used in the confidence variable reflect the core cybersecurity task such as identifying phishing emails/SMS and understanding password security, which aligns with the validated approach to measuring self confidence in the digital context study [29].

### 3.2.3 Knowledge

Knowledge in cybersecurity is the information and understanding of participants about the principles, including threat identification, safe online practice and protective measures. Items in this variable assess the depth and accuracy of participants cybersecurity-based information. According to Victor Bolbot's article on the Internet of Things, cybersecurity knowledge is the domain-specific information gathered and articulated using formal methods to support the creation of rules for cybersecurity systems [31]. The items for knowledge were developed independently by the author, but the concept was adopted from the Kruger & Kearney of cybersecurity awareness model [32]. The model emphasizes assessing the awareness through the domains of knowledge, attitude and behaviour. For example, the item, "*A website using https:// is always safe*" reflects a knowledge-based misunderstanding that training aimed to correct.

### 3.2.4 Skills

Participants' ability to apply cybersecurity knowledge properly in real-life situations is known as skill. Skill usually includes decision-making in response to cyber threats such as phishing email/SMS, safe online practice etc. This thesis used multiple-choice questions based on real-world scenarios to test participants skill. For example, participants were presented with a fake email and asked if it's safe or needs to be reported. The test items were designed to simulate real-life scenarios, aligning with the NIST NICE framework, which defines cybersecurity skills usually involve the application of knowledge to perform tasks that protect systems [33].

### 3.2.5 Awareness, attitude, and competence

In cybersecurity, awareness is described as the continuous understanding and recognition of cyber threats and the proactive action to mitigate such threats. It's an ongoing process of educating individuals about threats in the cyber world and acting accordingly, which emphasizes proactive security behaviour [34]. AW1 item from Table 1 subchapter 3.2.1 is used to measure the awareness of participants. It aligns with the ability to recognize the threats and understand the action required to resolve it.

Attitude displays a participant's mindset towards cybersecurity practice including his/her motivation to engage in safe behaviour and the value of cybersecurity in daily activities. Attitudes about cybersecurity have a major impact on the will to follow security policies

and the probability of participating in protective activities [35]. AT1 in the Table 1, subchapter 3.2.1 represents the attitude that exhibits the purpose as well as the importance of engaging in secure online practice.

In cybersecurity, competence generally refers to an individual's capability to implement both knowledge and skill to protect a system [33]. But in this study, competence was measured using self-assessment item CM1 in Table 1, Subchapter 3.2.1, which is focused on participants perceived ability to protect themselves from cyber threats. It indicates readiness and proficiency to manage cybersecurity challenges. From Table 1 Subchapter 3.2.1 the items AW1, AT1, and CM1 were designed to assess three closely related constructs: cybersecurity awareness, attitude towards safe online behaviour and competence.

### **3.2.6 Gamified training evaluation**

The gamified training evaluation was conducted using four conceptual subscales: engagement, ease of use, satisfaction, game support, and future motivation. Each structure was based on responses to 5-point Likert-type items. From Table 1 subchapter 3.2.1, engagement items are represented by pre-training item EG1 and post-training items EG1-EG3. Ease of use, satisfaction, game support, and future motivation are represented by post-training item EU1, SA1, GS1, and FM1 respectively, from Table 1 subchapter 3.2.1. Engagement items evaluated how enjoyable the training was and participants attentiveness. EU1 was used to measure if the training general instructions were clear to participants. SA1 measured if participant were willing to recommend similar gamified cybersecurity training to their friends or colleagues. GS1 was used to measure if the immediate feedback during the mistake helped participants understand better. Participants willingness to apply secure online practice after completing the training was measured by FM1.

## **3.3 Data processing activity**

Data collections were conducted using LimeSurvey (v 6.13.0), an open-source online survey platform. It helped to structure the pre- and post-training survey questionnaires. For data analysis, the responses were exported from LimeSurvey and imported into IBM SPSS Statistics (v 29.0.2.0).

The purpose of collecting personal data was to evaluate the effectiveness of the gamified cybersecurity training to improve the participants awareness. It also helped to assess participants confidence, knowledge, and skills related to phishing and password security.

The data was also used to determine if gamification training improves participants knowledge gap. The collected data specifically contributed to answering the research questions mentioned in Chapter 1.

In this research a minimum amount of personal data was required. Only data that are essential for the evaluation of the training effectiveness were collected. This includes scores, responses to pre- and post-surveys, and additional feedback. Demographic information such as age range, educational background, and prior experience with cybersecurity training and digital games was collected too. No sensitive data such as name, email, phone number, or other personally identifiable information was collected.

The pre-survey was used to gather demographic information, baseline cybersecurity knowledge, confidence, and previous training experience. The post-survey was used to collect data on changes in knowledge, confidence, and skills. Also to obtain participants evaluation of the gamified training in terms of engagement, effectiveness, and ease of use.

Collected data were securely stored in an encrypted file on password-protected laptop. Backup files were stored in the encrypted Tuni cloud. The participants' data was linked with a unique participant ID instead of a personal identifier. To protect participants privacy, data analysis was conducted using these anonymous IDs. Only the researcher had access to the raw data.

Personal data were retained only for the duration necessary to complete the research and analyse the results. After submission of the thesis, data will be retained for a maximum of 3 months to address any follow-up requirements, revisions, or questions from participants. After the retention period, all personal data will be permanently deleted from the laptop and backup system using secure deletion tools to ensure it cannot be recovered.

### **3.4 Data analysis**

Data collected through pre- and post-training surveys were analysed systematically using both quantitative and qualitative methods. For quantitative data analysis, descriptive and inferential statistical tests were conducted using IBM SPSS Statistics (v 29.0.2.0) software. Descriptive statistical analysis includes means, medians, standard deviations,

and ranges that were calculated to summarize the central tendencies and dispersions for all the variables. Cronbach's alpha  $\alpha$  was calculated to assess the reliability for the variables with multiple items in the survey. Reliability values above the threshold of 0.7 were considered acceptable, with values above 0.9 suggesting excellent reliability. As the sample size is small ( $n = 15$ ) and data was collected using Likert-type scales, non-parametric statistical test Wilcoxon Signed-Rank and Mann-Whitney U were conducted. The Wilcoxon Signed-Rank test was conducted to assess the items difference between pre- and post-training responses for confidence, knowledge, skills, awareness, attitude, and competence. Mann-Whitney U was used to evaluate the impact of the prior training experience on participants improvement in awareness, attitude, and competence. The effect size was calculated using a standard non-parametric formula.

$$r = \frac{Z}{\sqrt{n}} \quad (1)$$

where  $r$  denotes the effect size,  $Z$  denotes the Z-score or standard score in a Z-test and  $n$  is the sample size.

Also, as the evaluation data was collected using ordinal Likert scales, medians were used to represent the central tendencies without assuming equal intervals between the response categories. This approach aligns with non-parametric best practice and provides a more accurate reflection of participants experiences.

In the post-training survey, open-ended feedback was collected from participants, which was analysed using thematic analysis. This process involved

- Reviewing participants feedback several times.
- Grouping each response to find patterns related to topics.
- Grouping the feedback into positive feedback and constructive feedback.

Themes were selected based on the frequency of the mentions. This systematic, mixed-method analysis helped to assess and understand both quantitative results and qualitative user experience. Additionally, this study provided insight on the impact of gamified cybersecurity training.

## 4. RESULTS

This chapter represents the results acquired from the assessment of gamified cybersecurity training on participants confidence, knowledge, skills, awareness, attitude, and competence. Descriptive statistics for all variables in Table 1, subchapter 3.2.1, and Cronbach's alpha for confidence, knowledge, and engagement variables are summarized in Table 2.

**Table 2.** Variables descriptive statistics and reliability values.

Variables	Sum Variable	Cronbach's $\alpha$	Mean	Median	Standard Deviation	Binary Recoded
Confidence Pre Training	True	0.907	3.91	4	0.77	No
Confidence Post Training	True	0.967	4.22	4.25	0.78	No
Knowledge Pre Training	True	N/A	6.6	7	0.49	Yes
Knowledge Post Training	True	N/A	6.67	7	0.49	Yes
Skills Pre Training	True	N/A	3.1	3.25	0.43	Yes
Skills Post Training	True	N/A	3.27	3.5	0.33	Yes
Awareness	False	N/A	3.20	3.00	1.08	No
Attitude	False	N/A	4.73	5.00	0.46	No
Competence	False	N/A	3.73	4.00	0.88	No
Engagement Pre Training	False	N/A	4.02	4.00	1.1	No
Engagement Post Training	True	0.901	4.07	4.0	0.3	No
Game support	False	N/A	4.00	4.00	1.25	No
Future motivation	False	N/A	4.13	4.00	0.74	No

### 4.1 Confidence in identifying and managing cyber threats

To measure internal consistency of the variable confidence items, Cronbach's alpha ( $\alpha$ ) test was conducted on pre- and post-training items. The pre-training confidence scale yielded an  $\alpha = 0.907$  with items C1, C2, and C3 (Table 1 subchapter 3.2.1), indicating excellent reliability. Corrected item-total correlations ranged from 0.744 to 0.915, suggesting each item had a strong correlation between the items and total scale. Furthermore, Cronbach's alpha decreased, indicating if any single item was removed, supporting the contribution of each item to the reliability of the scale.

The reliability scale for post-training confidence yielded even further,  $\alpha = 0.967$  for the item C1 to C4 (Table 1 subchapter 3.2.1). The corrected item-total correlations were above 0.89, and removing any item reduces the overall reliability, which indicates the strong contribution to scale. The result demonstrates high internal consistency and suggests that the additional item C4 integrated well with the existing structure.

To measure the changes in confidence following gamified training, the median composite score was calculated based on the participants responses to Likert-type questions.

**Table 3.** Variables descriptive statistics of confidence.

Measure	Pre Training	Post Training
Total Number	15	15
Mean	3.8	4.2
Median	4.0	4.0
Standard Deviation	0.86	0.77
Min-Max Range	2.0 – 5.0	3.0 – 5.0

Descriptive statistics of confidence in Table 3 show an increase in the mean confidence score from 3.8 in pre-training to 4.2 post-training. The median remained at 4.0, the range of the response narrowed from 2.0-5.0 to 3.0-5.0. To assess if the change between pre-training and post-training for confidence is statistically significant, the Wilcoxon Signed-Rank test was conducted. The test produced  $Z = -1.89$   $p = 0.059$ , narrowly missing the conventional threshold of statistical significance  $p = 0.050$ . The effect size was calculated using equation (1), and  $|r| = 0.49$ , indicating a medium-size effect according to Cohen's benchmark [36], despite the non-significant p-value.

## 4.2 Knowledge of phishing & password security

A Wilcoxon Signed-Rank Test was conducted comparing pre- and post-training results to assess changes in participants knowledge. Item K1 – K7 from Table 1, subchapter 3.2.1 represented the knowledge variable for pre- and post-training. The test yielded  $Z = 0.302$ ,  $p = 0.763$  presented in Figure 8. Using the equation (1), effect size was measured  $|r| = 0.075$  ( $n=15$ ), which is a negligible range according to Cohen's benchmark [36].

Descriptive statistics in Table 2 for the knowledge variable indicate the pre-training mean slightly increased from 6.6 to 6.7 in the post-training, where the median, standard deviation remained constant.

**Related-Samples Wilcoxon Signed Rank  
Test Summary**

Total N	15
Test Statistic	20.000
Standard Error	6.633
Standardized Test Statistic	.302
Asymptotic Sig.(2-sided test)	.763

**Figure 8.** Wilcoxon Signed Rank Test for knowledge.

In addition, an item-level analysis was conducted for knowledge variable to examine the performance in pre-training and post-training. The correct response percentages for each item are presented in Table 4.

**Table 4.** Knowledge item level analysis

Survey Question Focus	Pre-Training Correct %	Post-Training Correct %	Changes %
Knowledge of verifying links before clicking (from known or unknown senders)	100%	100%	0%
Recognizing secure password creation methods	93%	100%	+ 6.7%
Understanding urgency as a phishing tactic	100%	93.3%	- 6.7%
Misconception that https:// always a safe website	86.7%	86.7%	0%
Belief that complex passwords are safe even if reused across accounts.	100%	93.3%	- 6.7%
Understanding the role of 2FA authentication.	100%	100%	0%
Understanding and use of password managers for strong, unique passwords.	80%	93.3%	+ 13.3%

For the knowledge variable comparing pre and post-training response of 3 items showed no change in the correct response. Two items showed an increase in correct response rate: secure password creation + 6.7% and use of password manager + 13.3%. Two items, urgency as tactics and reuse of complex passwords decreased by – 6.7%.

### 4.3 Practical cybersecurity skills

For evaluating the skills of participants pre- and post-training a non-parametric Wilcoxon Signed-Rank test was conducted, using the responses from items S1 to S4 from the Table 1 subchapter 3.2.1, skills variable. The Wilcoxon Signed-Rank test resulted in  $Z =$

0.979,  $p = 0.327$  presented in Figure 9. However, the effect size calculated by equation (1) resulted in  $|r| = 0.253$ , which represents a small to approaching medium effect, according to Cohen's benchmark [36]. According to Table 2, pre-training mean and median slightly increased in post-training, but standard deviation decreased.

**Related-Samples Wilcoxon Signed Rank Test Summary**

Total N	15
Test Statistic	30.500
Standard Error	8.170
Standardized Test Statistic	.979
Asymptotic Sig. (2-sided test)	.327

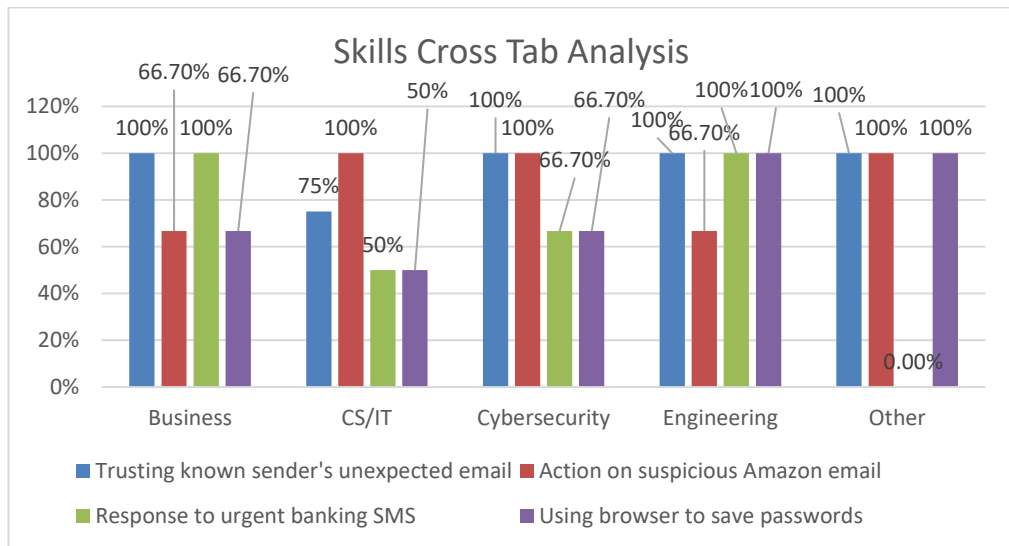
**Figure 9.** Wilcoxon Signed Rank Test for skills.

To identify more about skills improvement based on the data, a scenario-level analysis was conducted to assess which specific skill improved most in post-training. Binary coded responses were analysed to calculate the correct answer for pre- and post-training aggregated by field of study.

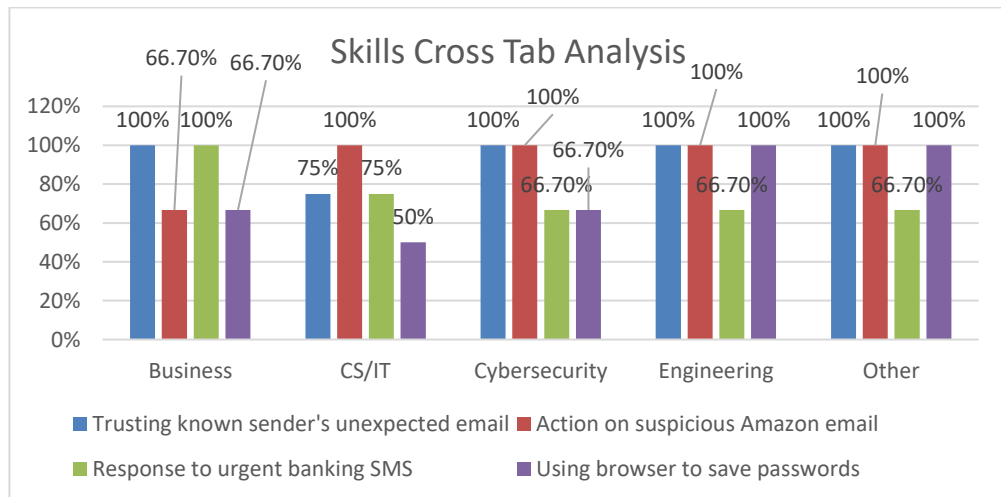
**Table 5.** Skills scenario level analysis

Survey Question Focus	Field of Study	Group Size	Pre-Training Correct %	Post-Training Correct %	Changes %	Interpretation
Trusting known sender's unexpected email.	Business & Management	3	93.3%	93.3%	0%	No change. The baseline trust and threat recognition were retained highly.
	Computer Science & IT	4	93.3%	93.3%	0%	
	Cybersecurity	3	93.3%	93.3%	0%	
	Engineering	3	93.3%	93.3%	0%	
	Other	2	93.3%	93.3%	0%	
Action on suspicious email.	Business & Management	3	86.7%	100%	13.3%	Improved through gamification learning. Accurate answer in post-training.
	Computer Science & IT	4	86.7%	100%	13.3%	
	Cybersecurity	3	86.7%	100%	13.3%	
	Engineering	3	86.7%	100%	13.3%	
	Other	2	86.7%	100%	13.3%	
Response to urgent banking SMS.	Business & Management	3	66.7%	66.7%	0%	No changes but needs more improvements.
	Computer Science & IT	4	66.7%	66.7%	0%	
	Cybersecurity	3	66.7%	66.7%	0%	
	Engineering	3	66.7%	66.7%	0%	
	Other	2	66.7%	66.7%	0%	
Using browser to save passwords	Business & Management	3	60%	80%	20%	Improved significantly, but still improvement is needed.
	Computer Science & IT	4	60%	80%	20%	
	Cybersecurity	3	60%	80%	20%	
	Engineering	3	60%	80%	20%	
	Other	2	60%	80%	20%	

In the Table 5, the item trusting unexpected emails showed no changes in pre- and post-training retaining the accuracy at 93.3%. In action regarding suspicious email changes was 13.3%, reaching 100% accuracy in post-training. There was no change in response to urgent messages as response accuracy remained the same 66.7%, in pre-training and post-training. Using a browser to save password items had a 20% increase in post-training accuracy.



**Figure 10.** Cross-tab analysis of pre training skills.



**Figure 11.** Cross-tab analysis of post training skills.

In Figure 10 and Figure 11, the crosstab analysis for the skills variable indicates that across all fields of study, recognizing unexpected email remained consistently high, with most groups scoring 100%. Accuracy in handling suspicious email ranged from 50% to 100%, where urgent SMS phishing scenarios and browser-based passwords had a quite varied percentage, ranging from 50% to 100%.

## 4.4 General cybersecurity awareness, attitude and competence

For analysing the awareness, attitude, and competence variables descriptive analysis, and Wilcoxon Signed-Rank test was conducted using the items AW1, AT1 and CM1 from pre- and post-training in Table 1 subchapter 3.2.1. From Table 6, awareness variable median stayed almost the same, but the mean changed from 3.20 of pre-training to 3.93 post-training. Attitude towards cybersecurity was already extremely high in pre-training indicating a ceiling effect, where the median stayed the same in 5 for pre- and post-training. In competence median stays the same and the mean changes from 3.73 to 3.93, which is a modest improvement.

**Table 6.** Descriptive analysis of awareness, attitude, and competence.

Variable	Mean (Pre)	Median (Pre)	Mean (Post)	Median (Post)	Mean Change	Median Change	Standard Deviation Change	Min-Max Change
Awareness	3.20	3.00	3.93	4.00	0.73	0.00	0.96	0 to 3
Attitude	4.73	5.00	4.67	5.00	-0.07	0.00	0.26	-1 to 0
Competence	3.72	4.00	3.93	4.00	0.20	0.00	0.77	-1 to 2

**Table 7.** Frequency analysis of awareness, attitude, and competence.

Change Category	Awareness %	Attitude %	Competence %
Declined	0%	6.7%	13.3%
No changes	53.3%	93.3%	60.0%
Improved (+1)	26.7%	0%	20.0%
Improved (+2 or +3)	20.0%	0%	6.7%

For awareness, with sample size  $n = 15$  the Wilcoxon Signed-Rank test resulted in  $Z = 2.41$ ,  $p = 0.016$ ,  $|r| = 0.62$ , suggesting a large effect of gamified cybersecurity training. For attitude ( $Z = -1.00$ ,  $p = 0.317$ ,  $|r| = 0.26$ ) and competence ( $Z = 1.00$ ,  $p = 0.317$ ,  $|r| = 0.26$ ) there were no significant changes, but for both variables, effect size indicates a small to medium effect [36]. Table 7 summarizes that 46.7% of participants awareness improved and 53.3% had no changes. Attitude remained unchanged at 93.3%, with a 6.7% decline. In competence, 26.7% of participants improved, 60% had no changes, and 13.3% declined.

To examine if prior gamified training experience influenced improvements in cybersecurity awareness, attitude, and competence, a Mann-Whitney U test was performed. Along with the awareness, attitude, and competence variable, background variable items of

pre-training BG1 and BG2 were used. Among 15 participants, 8 had no prior experience whereas 7 had prior experience. These were compared against the change scores in the variable's awareness, attitude, and competence. Although the difference in competence gain was not statistically significant ( $U = 15.5$ ,  $Z = -1.641$ ,  $p = 0.152$ ), the effect size  $|r| = 0.42$  indicates a moderate practical difference [36]. For the awareness test, yields  $Z = -0.445$ ,  $p = 0.694$ , and effect size  $|r| = 0.11$ , indicating a small effect size [36]. Attitude scores showed  $Z = 0.935$ ,  $p = 0.694$ , and effect size  $|r| = 0.24$ , suggesting a small effect size [36].

## 4.5 Gamified training evaluation

For measuring engagement, participants' sense of immersion, attention, and active involvement during training were considered, which are represented with EG1 in the pre-training and the post-training items EG1, EG2, and EG3 in Table 1 subchapter 3.2.1. Reliability was tested for post-training engagement, and Cronbach's  $\alpha$  resulted in 0.901, which is excellent reliability. Ease of use was represented by EU1, and satisfaction was represented by SA1 in post-training item in Table 1 subchapter 3.2.1. For representing game support and future motivation items GS1 and FM1 in Table 1 subchapter 3.2.1. A composite evaluation score was computed by averaging the participants responses across the 7 items in Table 8. These measurements were helpful to understand participants perception of gamified cybersecurity training.

**Table 8.** Composite evaluation of training evaluation.

Category	Mean	Median	Standard Deviation	Interpretation
Engagement Pre-training	4.02	4.00	1.1	Participants were engaged and motivated to learn
Engagement Post-training	4.07	4.00	0.3	
Ease of Use	4.4	5.00	0.82	Navigation was easy.
Satisfaction	3.86	5.00	1.41	Participants likely to recommend the training.
Game support	4.00	4.00	1.25	Provided feedback during mistake was helpful to learn.
Future motivation	4.13	4.00	0.74	Participants intend to apply the security practice which was learned through game.

From Table 8, participants reported a high level of engagement with a median composite of 4.00. The interface and instruction were very intuitive, with a full median score of 5. The satisfaction median scored 5, suggesting that at least half of the participants' were highly satisfied, where the mean score of 3.68 and high standard deviation of 1.41 indicates that some of the participants were not satisfied.

## 4.6 Feedback analysis

Open-ended feedback was collected from the participants for the quantitative evaluation of the gamified cybersecurity training to gain more insight into areas of improvement. Based on thematic analysis, comments were categorized as effective features in Table 9 and suggested improvements in Table 10.

**Table 9. Effective features**

Theme	Mentions	Example Response
Gamification/Motivations	4	"The points because I wanted to get a good score!', 'A good starting point for a basic security training and awareness. Within a quick interactive tutorial, you could teach someone how to recognize threats. Works much better than Hoxhunt."
Interactive/Engagement	5	"It was interactive way to learn', 'I thought it was fun and engaging and provided a lot of accurate examples of phishing mails."
Realistic Scenario/Practical Example	9	'Good examples in learning sections', 'Multiple and detailed examples.', 'Examples of what to do and not to do.', 'Instant information on mistakes was really helpful'
Content Quality/Clarity	3	"The introduction provided before starting the game was both informative and easy to understand, which enable me to participate confidently and perform effectively. The survey questions were also well-structured and relevant. Overall, this study has significantly enhanced my understanding of cybersecurity."

**Table 10. Suggested improvements**

Theme	Mentions	Example Response
Improved Onboarding/ Clear Instructions	2	"I was a little bit disappointed at the start where I have to read through the material when I thought the game would start. Maybe the game could just start, and people could play another round if they feel like they could do better after the first one."
Content Expansion/Advanced Topics	3	'i guess you could add some other modules too like malware.', 'I think if we add more graphical character, that could be a great addition for the gamified training.'
Difficulty /Personalization	Adjustments 4	'For cyber-aware people there should be more difficulty. Too easy to get full score.', 'I believe more difficult scenarios can add some extra improvements.'

In the category of effective features, participants highlighted several strengths related to motivation, engagement, real-life scenarios, and clarity of content. Participants also appreciated the detailed examples, clear instructions, and feedback on mistakes. This also aligns with the findings from Gjertsen et al. that realistic simulations in gamified training enhance understanding of the topic and retention [11]. The participants also appreciated gamification and motivational elements such as a points scoring system.

In the improvement suggestion, cyber-aware participants suggested more complex challenges. Furthermore, adding more modules such as malware and ransomware, social engineering, etc., was recommended.

## 5. DISCUSSION

In this chapter, a detailed discussion is presented of the findings from the study in relation to the research questions, which evaluate the impact of gamified cybersecurity training in improving participants confidence, knowledge, skills, awareness, and behavioural intents. Cyber Bee is a gamified training tool that was used to provide the training, and participants can assess their learning through playing the game.

**RQ1.** Does gamified cybersecurity training increase participants' confidence in identifying and managing cyber threats (phishing & password security)?

A directional improvement in participants' confidence was observed in the analysis following the gamified training. Although the median remained constant, it suggested an already high baseline of confidence in pre-training. The increase in mean from 3.8 to 4.2 (Table 3 subchapter 4.1) accompanied by a narrowing of the standard deviation range, indicates more consistent confidence across participants. Given the small sample size ( $n = 15$ ), descriptive statistics point toward a meaningful improvement but not a statistically significant one. However, the result was not statistically significant, but the positive trend towards confidence aligns with the study conducted by Misra et al., indicating gamification enhances participants' confidence in mitigating cyber threats [37]. Using a similar design with a Likert-type assessment, Misra et al. observed a statistically significant increase in confidence levels attributed to gamification training. In the context of cybersecurity, it is found that perceived confidence often predicts secure behaviour more effectively than objective knowledge [29]. By providing clear feedback loops, the structured scenario-based game may have helped reinforce participants trust in their own judgement. The Wilcoxon Signed-Rank test yielded a  $p = 0.059$ , slightly crossing the threshold of 0.05, and then the medium effect size indicates a meaningful improvement in confidence. However, as the sample size is small, a careful interpretation is required. As this thesis found a medium effect size and meaningful improvements in descriptive statistics, this suggest that gamification could be a good way to improve participants confidence in cybersecurity education. Despite narrowly missing statistical significance, the result supports the idea that it could have a real-world effect.

**RQ2.** Does gamified cybersecurity training improves participants' actual knowledge on phishing and password security?

The thesis reveals minimum gains in post-training knowledge scores due to a ceiling effect. Participants entered the study with a high baseline of knowledge, limiting the opportunity to calculate the measurable gains. The Wilcoxon Signed-Rank test further confirmed no statistical significance with a negligible effect size. According to earlier research, gamified training environments are more effective at reinforcing existing knowledge than introducing complex new concepts [38]. Moreover, item-level descriptive analysis indicates a refined improvement. There was a 13.3% improvement in knowledge of password manager benefits and a 6.7% gain in identifying secure password creation (Table 4 subchapter 4.2). The observed knowledge improvements in password security align closely with findings by Mason et al., who noted that gamified training led to improvements in cybersecurity knowledge, although the gains were more observed in practical knowledge areas such as password management [9]. Training with Cyber Bee effectively reinforces best practices in password security. On the other hand, misunderstandings around HTTP and urgency-based phishing language indicate that future builds of the game should include more complex scenarios based on these areas. As Hamari et al. suggested, complex or multi-layered cybersecurity topics may require more interactive and scenario-based gaming elements to improve conceptual clarity [38].

**RQ3.** How effectively does gamified cybersecurity training develop participants' practical skills in identifying phishing threats and strengthening password security?

The improvements in participants' skills were not statistically significant, but scenario-based assessments showed measurable gains in specific competencies, such as correctly handling phishing emails with links and password management. Use of browser for saving passwords had 20% improvement, and identification of phishing emails increased by 13.3%, indicating an effective learning outcome from the training (Table 5 subchapter 4.3). These findings are consistent with previous studies on the impact of gamified training on cybersecurity skills [9]. Mason et al. indicated that gamified training in cybersecurity programs is specifically effective at improving skills such as email threat detection and password management [9].

Moreover, lower standard deviations in post-training suggest a convergence of participants' performance, indicating the training may have contributed to a more identical level

of practical understanding across the group. Crosstab analysis across different fields of study revealed no discipline outperformed others, showing that the training method is effective for a wide range of people of different backgrounds (Figure 9, Figure 10 subchapter 4.3).

**RQ4.** Does previous or current experience (such as prior training experience, experience with gamified training) influence participants improvement in knowledge and confidence after training?

For awareness Wilcoxon Signed-Rank test data ( $p = 0.016$ ,  $|r| = 0.62$ ) indicates that gamified training effectively increases participants' ability to identify and manage cyber threats. The large effect size suggests the training had a strong influence, even though the sample size was small ( $n = 15$ ). For attitude, there were no statistically significant changes. The median of pre-training marked at 5, which stayed the same in post-training, which suggests a ceiling effect, where participants' held positive attitudes towards cybersecurity. The improvement in competence is not statistically significant, even though a positive trend was observed. The stable median score of 4 suggests consistent response among participants', while the rise in the mean indicates participants' may have reassessed their ability more positively, likely by the clarity and immediate feedback during training (Table 6 subchapter 4.4). Even though the results for attitude and competence are not statistically significant, both variables effect size was small to medium. Effect size suggests that participants' attitudes and competence may have changed slightly; that may be relevant in an educational context with limited sample sizes. But the ongoing prevalence of some myths, such as the belief that <https://> is always safe or complex passwords can be reused securely, and the lack of change in SMS phishing response suggest that competence might be domain-specific instead of universal. The competence post-mean resulted in 3.93 (Table 6 subchapter 4.4); therefore, it seems to fit the general profile of a reasonably competent but still evolving cybersecurity-aware user.

The participants with prior experience have shown moderately larger gains in competence. This underlines the potential value of familiarity with the gamified training format, which enhances learning outcomes [14][23]. The competence gain also suggests that prior experience in such an interactive learning environment may serve as a method for deeper engagement and confidence development [37]. These findings may have a significant consequence for the design and organization of cybersecurity training modules, where introductory gamified modules can be strategically used to prepare learners for more advanced content.

**RQ5.** How do participants evaluate the gamified training in terms of engagement, effectiveness and ease of use?

Feedback from participants indicated great satisfaction with the training. Engagement, ease of use, and future motivation result in a highly supportive notion that gamified training can enhance learning through fun and immediate feedback. These findings correlate with another study that concludes gamification enhances both engagement and knowledge retention [38]. During training intuitive interface, timely feedback, and a competitive structure most likely contributed to the positive experience from participants. Feedback during mistakes was helpful for learning, was reported by 73% participants. However, there was qualitative feedback from participants that highlights the need for access to the game by skipping the learning materials, increasing the challenging , etc. Further, it appears training was effective in increasing behavioural intent towards safe cybersecurity practice. Feedback also suggests that training helped motivate participants' to applying the knowledge in real-world scenario. Like this thesis, Gjertsen et al. study on gamification of information security awareness and training indicates that gamification potentially increases motivation and learning outcomes [11].

In conclusion, the results suggest that gamification of cybersecurity training holds considerable promise for enhancing both awareness and participants' self-confidence. Even though the current result is based on a limited sample size ( $n = 15$ ), it is still encouraging. In future research with a larger sample size, a more diverse group, and challenging content design may provide a more concrete result on the current analysis. It will also help to provide deeper insights into the scalability of the gamification approach with cybersecurity education and behaviour change.

## 6. LIMITATIONS

Despite the valuable insights this thesis provides about the impact of gamified cybersecurity training, it's subject to several methodological and contextual limitations that should be acknowledged.

The sample size was relatively small ( $n = 15$ ), consisting of university students and research participants. This limited sample size reduced the statistical power of the analysis and limited the application to larger groups, such as non-academic or professional users. Additionally, the post-training survey was conducted immediately; hence, this study cannot provide evidence regarding long-term knowledge retention, behavioural changes, or prolonged motivation. Future studies can benefit from introducing delayed post-training surveys to evaluate training stability over time. Another limitation concerns participants' demonstration of high-level knowledge in the pre-training survey, which resulted in less evidence of improvement in the post-training survey. This ceiling effect suggests that the training tool contents were simpler for cyber-aware participants. The use of single-item measurement for competence and attitude limited the robustness of those assessments. Moreover, the training tool's narrow focus on phishing and password security restricts the comprehensiveness of the training and educational scope. By adding more challenging scenario-based content, critical cybersecurity topics will help validate some of the results this study was unable to. Also, introducing an adaptive difficulty scale in Cyber Bee could help optimize learning outcomes across varying proficiency groups. Enhancing the user interface to allow participants to interact with the scenario outcome could improve the learning experience.

These limitations highlight the current study's experimental traits and provide guidance for future improvements. To strengthen future research, larger varied sample, longer assessment windows, and additional cybersecurity topics need to be addressed for enhancing the robustness and applicability of the findings.

## 7. CONCLUSIONS

The improvement of cybersecurity awareness is a continuous process as threats are evolving over time. To minimize the human factor as the weakest point in the cybersecurity chain, gamified cybersecurity training has shown better results as a tool to improve awareness than conventional training methods [39]. This thesis evaluated the impact of gamification in cybersecurity training on participants confidence, knowledge, skills, awareness, attitude, and behavioural intentions, focusing on phishing and password security. Data was collected using a quasi-experimental pre- and post-survey design. These data were analysed systematically using both quantitative and qualitative methods.

This thesis provided experimental evidence suggesting that gamification of cybersecurity training can increase awareness. Moreover, it indicates that gamification of cybersecurity training is particularly effective when it is integrated with both conceptual understanding and practical support. This combination appears to influence participants confidence and motivation to apply cybersecurity practices in real-world situations. This study also noted limitations in its design. The sample size was small, drawn from a specific demographic. Furthermore, participants indicated that the scenario lacked challenge and narrative depth.

In conclusion, this thesis shows the initial evidence that gamified cybersecurity training can improve awareness when properly designed. It also highlights the importance of gamification of cybersecurity training to support minimizing the human factor as the weakest point. Although the study is modest in scale, it contributes to a growing understanding of the impact of gamified training on cybersecurity education. Future work is required to examine how gamified cybersecurity training can improve knowledge and behaviour retention over time.

## REFERENCES

- [1] IMF [Internet]. 2024 [cited 2025 Jun 2]. Rising Cyber Threats Pose Serious Concerns for Financial Stability. Available from: <https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability>
- [2] Arachchilage NAG, Love S. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*. 2014 Sep 1;38:304–12.
- [3] Tsohou A, Kokolakis S, Karyda M, Kiountouzis E. Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*. 2008;17(5–6):207–27.
- [4] Brady C, M'manga A. Gamification of Cyber Security Training - EnsureSecure. In: 2022 IEEE International Conference on e-Business Engineering (ICEBE) [Internet]. 2022. p. 7–12. Available from: <https://ieeexplore.ieee.org/document/10035080>
- [5] Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 2012 Feb 1;31(1):83–95.
- [6] Alnajim AM, Habib S, Islam M, AlRawashdeh HS, Wasim M. Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*. 2023 Dec;15(12):2175.
- [7] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*. 2014 May 1;42:165–76.
- [8] Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv [Preprint]*. 2019 Jan 9. Available from: <https://arxiv.org/abs/1901.02672>
- [9] Mason O, Collman S, Kazamia S, Boureau I. Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training. *Journal of Cybersecurity Education, Research and Practice [Internet]*. 2023 Nov 29;2024(1). Available from: <https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/11>
- [10] From Awareness to Action: Transforming Cybersecurity with Human Risk Management [Internet]. *Cyber Defense Magazine*. 2025 [cited 2025 Apr 28]. Available from: <https://www.cyberdefensemagazine.com/from-awareness-to-action-transforming-cybersecurity-with-human-risk-management/>
- [11] Gjertsen EA, Gjørre EA, Bartnes M, Flores WR. Gamification of information security awareness and training. In: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*; 2017 Jan; p. 59–70. doi:10.5220/0006128500590070

- [12] Scholefield S, Shepherd LA. Gamification Techniques for Raising Cyber Security Awareness. In: Moallem A, editor. HCI for Cybersecurity, Privacy and Trust. Cham: Springer International Publishing; 2019. p. 191–203.
- [13] Keepnet Labs. Why Security Awareness Needs an Upgrade: Building a Behavior-Driven Security Culture [Internet]. [cited 2025 Apr 29]. Available from: <https://keepnetlabs.com/blog/security-awareness-isn-t-dead-but-it-s-not-enough>
- [14] Khoshnoodifar M, Ashouri A, Taheri M. Effectiveness of Gamification in Enhancing Learning and Attitudes: A Study of Statistics Education for Health School Students. J Adv Med Educ Prof. 2023 Oct;11(4):230–9.
- [15] McGuire L. How Gamification Boosts Engagement, Retention in Training [Internet]. LearnExperts. 2024 [cited 2025 Apr 29]. Available from: <https://learnexperts.ai/blog/gamification-in-learning-why-add-fun-to-your-courses/>
- [16] Caveney L. The Importance of Competition in Learning [Internet]. BuildEmpire. 2024 [cited 2025 May 1]. Available from: <https://buildempire.co.uk/competition-in-learning/>
- [17] Zeng Y, McEneaney J. Not All Competitions Are the Same: Digital Game-based Learning Environments That Incorporate Competition Facilitates Students' Learning Motivation. Journal of Research Initiatives [Internet]. 2022 Nov 3;7(1). Available from: <https://digitalcommons.uncfsu.edu/jri/vol7/iss1/2>
- [18] ThreatGEN. Cybersecurity Gamification [Internet]. [cited 2025 May 2]. Available from: <https://threatgen.com/red-vs-blue/>
- [19] Gamified Cyber Security Training: Everything You Need to Know - Hoxhunt [Internet]. [cited 2025 May 2]. Available from: <https://hoxhunt.com/blog/gamified-cyber-security-training>
- [20] Bui S. Gamified Cyber Security for Training: TOP 5 Best Examples to Watch in 2024 [Internet]. 2024 [cited 2025 May 2]. Available from: <https://flearningstudio.com/gamified-cyber-security/>
- [21] Security Compass. Gamified Cybersecurity Training [Internet]. [cited 2025 May 2]. Available from: <https://www.securitycompass.com/blog/gamified-cybersecurity-training/>
- [22] Fatokun Faith B, Long ZA, Hamid S. Promoting Cybersecurity Knowledge via Gamification: An Innovative Intervention Design. In: 2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC) [Internet]. 2024 [cited 2025 May 2]. p. 1–8. Available from: <https://ieeexplore.ieee.org/document/10454080>
- [23] Bitrián P, Buil I, Catalán S, Merli D. Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. Journal of Business Research. 2024 Jun 1;179:114685.
- [24] Idierukevbe IU, Addo A. Bridging the cybersecurity skills gap: A gamification model. Journal of Business Studies Quarterly. 2024;14(1):1–16
- [25] Capatina A, Juarez-Varon D, Micu A, Micu AE. Leveling up in corporate training: Unveiling the power of gamification to enhance knowledge retention, knowledge

- sharing, and job performance. *Journal of Innovation & Knowledge*. 2024 Jul 1;9(3):100530.
- [26] Abu-Amara F, Hosani RA, Tamimi HA, Hamdi BA. Spreading cybersecurity awareness via gamification: zero-day game. *Int J Inf Technol*. 2024 Jun 1;16(5):2945–53.
- [27] Creswell JW. *Research design: Qualitative, quantitative, and mixed methods approaches*. 4th ed. New Delhi: SAGE Publications, Inc; 2014. p. 168–70.
- [28] Sawaya Y, Sharif M, Christin N, Kubota A, Nakarai A, Yamada A. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* [Internet]. New York, NY, USA: Association for Computing Machinery; 2017 [cited 2025 May 10]. p. 2202–14. (CHI '17). Available from: <https://dl.acm.org/doi/10.1145/3025453.3025926>
- [29] Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*. 2009 Nov 1;28(8):816–26.
- [30] Compeau DR, Higgins CA. Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*. 1995;19(2):189–211.
- [31] Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*. 2022 Dec 1;39:100571.
- [32] Kruger HA, Kearney WD. A prototype for assessing information security awareness. *Computers & Security*. 2006 Jun 1;25(4):289–96.
- [33] National Institute of Standards and Technology. *Cybersecurity skills and workforce frameworks* [Internet]. 2024 May 3 [cited 2025 May 1]. Available from: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/cybersecurity-skills-and>
- [34] Spanning. *Cybersecurity Awareness: Definition, Importance & More* [Internet]. 2022 [cited 2025 May 2]. Available from: <https://www.spanning.com/blog/cyber-security-awareness/>
- [35] Toro-Jarrin MA, Pazos P, Padilla MA. It is not only about having good attitudes: factor exploration of the attitudes toward security recommendations. *Journal of Cybersecurity*. 2024 Jan 1;10(1):tyae011.
- [36] Cohen J. *Statistical power analysis for the behavioral sciences*. 2. ed., reprint. New York, NY: Psychology Press; 2009. 567 p.
- [37] Misra G, Arachchilage NAG, Berkovsky S. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks [Internet]. arXiv; 2017 [cited 2025 May 19]. Available from: <http://arxiv.org/abs/1710.06064>
- [38] Hamari J, Koivisto J, Sarsa H. Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. In: *2014 47th Hawaii International Conference on System Sciences* [Internet]. 2014 [cited 2025 May 19]. p. 3025–34. Available from: <https://ieeexplore.ieee.org/document/6758978>

- [39] Karzan HS, Siddeeq YA. A Review on Gamification for Information Security Training. In: 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI) [Internet]. 2021 [cited 2025 May 20]. p. 1–8. Available from: <https://ieeexplore.ieee.org/document/9664771>