National College of Ireland

Enhancing Information Security through Gamification towards oblivious online users in Ireland, Malaysia and Singapore

MSc Research Project
Programme Name

Haezvine Deepak Singh
Student ID: x22200941

School of Computing
National College of Ireland

Supervisor: Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Haezvine Deepak Singh
Student ID:	X22200941
Programme:	Masters In Cybersecurity **Year:** One
Module:	Msc Research Project/Internship
Supervisor:	Rohit Verma
Submission Due Date:	15 December 2023
Project Title:	Enhancing Information Security through Gamification towards oblivious online users in Ireland, Malaysia and Singapore
Word Count:	5948 **Page Count** 21

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: Haezvine Deepak Singh

Date: 14/12/2023

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):	

Enhancing Information Security through Gamification towards oblivious online users in Ireland, Malaysia and Singapore

Haezvine Deepak Singh
22200941

Abstract

Numerous organisations and companies have undergone significant transitions into the digital realm following the onset of Covid in late 2019, resulting in an increase in cybercrimes. Many current generations may be unaware that their personal information is occasionally vulnerable, making them susceptible to hackers. Several researchers have developed strategies to address this problem by employing gamification techniques to enhance the security of information and privacy for both students and working professionals. Nevertheless, not all individuals from the current generations are actively involved in the solutions, meaning they may be excluded or struggle to comprehend the intricacies of the terms and security features being discussed. This paper aims to present a straightforward and precise understanding of an interactive novel tool that can enhance individuals' knowledge of information security while browsing the internet on multiple devices. The target audience for this tool is individuals above the age of seventeen in the present generation. The respondents' high level of awareness and concern over the possible drawbacks of online information is evident. Over half of the respondents, specifically 52%, possess knowledge of all the stated information security features signifying a potential inclination to pay more attention to online communications, potentially motivated by an increased awareness of cybersecurity.

Keywords: Cybersecurity, information security, gamification, interactive novel

1 Introduction

Games have impacted the world with game-like characteristics in a number of areas, such as marketing and health. Gamification are also utilized to enhance businesses, and products. For example, advertisers have implemented into marketing to sell their goods and services through the usage of adverse games. Gamification is an attempt to take use of games' motivational potential and apply it to real-world issues, such students' motivational struggles

in the classroom. Gamification holds significant potential to maintain learners' engagement with the pertinent subject. When the learning environment aligns well with the learners, they can achieve a state of flow, which is characterised by complete immersion and intense focus on the task at hand (Kapp, 2012b, p.71).

The integration of computer-based and inquiry-based learning has become increasingly popular in recent years, particularly in online laboratory environments (Brewer et al., 2013; Zacharia et al., 2015). In context to that, having ability to teach people where they would approach the gamifications method and understand certain content definitely helps to boost their morale and making sure that they would get hooked to it. This allows them to continue spending time and learn more by doing so they gradually gain the knowledge bit by bit. Learners should be encouraged to investigate content, take risks with their decision making, and be exposed to correct answer or lessons for making a bad or incorrect decision.

In an earlier study, Quayyum, F. (2020) identified two strategies that can be used to include instructional components in user gaming experiences. Gamification and serious games have been highlighted as two strategies for using gaming categories for educational goals, especially for users and youngsters (Quayyum, F., 2020). This study focuses on all people over the age of seventeen in the current generation since it is crucial to give them easily accessible and understandable cyber security education using gamification and simplified teaching techniques.

Páez-Quinde et al. (2023) argue that training the younger generation is a beneficial and efficient strategy for enhancing internet security and privacy. This technique allows them to gain knowledge quickly and efficiently. However, it is crucial for all persons to be equally knowledgeable about the latest technologies and techniques for improving their online privacy.

Individuals of all age groups, regardless of their young or older age, have the ability to understand a situation or gain significant knowledge. However, it is essential to recognise the importance of implementing this knowledge to individuals, as various age groups may interpret it in distinct ways. An excellent strategy to increase folks' understanding of the importance of privacy is to implement an interactive educational solution that successfully

captures their attention. The conversion of the content into an interactive and narrative format has the capacity to profoundly change the strategies used to captivate the audience, as emphasised in a distinct study conducted by Qusa and Tarazi (2021).

Research Question: Does gamification enhance information security towards oblivious online users in Ireland, Malaysia and Singapore?

With the research question about, it is will be tailored to the objectives listed below:

The Objectives of the study:

A) To find out the awareness of people about online threats

B) To identify that through gamification people will increase their awareness

C) To find out whether people will take considerations into securing their information stronger.

The research topic pertains to individuals in the current generation who are above the age of seventeen and may be unaware that their personal information is inadequately protected. An interactive novel would serve as the primary instrument, enabling people to engage with the story while incorporating certain security measures. A survey will be conducted to assess individuals' knowledge of information confidentiality, followed by a feedback form to see if participants have improved their awareness of online information security. The advantage of this result is that all voluntarily individuals would have acquired new or supplementary information that would enable them to exercise greater caution while browsing the internet.

The document will consist of several sections that will elucidate prior research conducted by other scholars, as well as introduce a novel methodology. Demographic information of participants is mandatory in Section A. Section B will specifically examine the concept of gamification and its relevance to this research. In this section, I will explain the rationale behind the utilisation of gamification methods and provide an overview of the approaches employed in prior research. The subsequent section, labelled as C, will delineate the research methodology and proposed remedy for addressing the circumstance and addressing the deficiency that was overlooked in prior studies. Each segment represents distinct tasks that are interconnected in order to comprehensively assess participants' satisfaction during the whole research process.

2 Related Work

The extensive historical background and diverse methods of integrating game-like interactions into educational settings have resulted in different terms being used to describe this approach, such as serious games, edugames or games for education, game-based learning, and more recently, gamification (Landers, 2014). Researchers in the field of gamification have utilised several methodologies to carry out their investigations, resulting in a range of solutions to the challenges that arise.

The advent of game-based learning (GBL) has brought about significant and transformative advances in pedagogy. GBL stands for game-based learning, which involves the integration of games into educational practices to facilitate teaching and learning. Games can be utilised to teach and engage in courses and assessments, hence enhancing traditional learning activities. Designing an educational game offers an enjoyable and engaging learning experience, while also enabling individuals to manage their learning and activities at their own speed and in their preferred environment (Nagalingam & Ibrahim, 2015).

The main goal is to ensure that participants understand the need of protecting their privacy from potential internet attackers. I would also clarify the research groups that have been the object of previous research and provide a rationale for choosing to concentrate on individuals aged seventeen and older in the present cohort. Acquiring up-to-date data would be beneficial in understanding the extent of persons' awareness regarding information security in the digital era.

Computer-based learning is a prevalent method for hands-on learning. The COVID-19 epidemic has underscored the significance of computer and internet connectivity in education, as highlighted by recent advancements (Walters, 2020). Currently, there exists a diverse array of gaming methodologies that can be utilised by game designers, developers, researchers, and practitioners to initiate the process of designing and developing games. Designing a user interface (UI) is one of the essential approaches. The user interface (UI) is crucial in directing the user's attention towards the intended item and subject in any programme or game. This is particularly important when developing a product that adheres to specified requirements.

In his work, Kapp (2012a) outlines four game elements that have been found to be successful: (1) allowing students the freedom to make mistakes, which promotes experimentation and risk-taking for the purpose of learning, (2) utilising an interest curve to sustain engagement by strategically organising the progression and sequence of events, (3) integrating storytelling, as students tend to grasp information more effectively when it is presented within a narrative context, and (4) providing regular and specific feedback. Advanced level components include progression (organised training), teamwork, and competitiveness.

Malone and Lepper identified multiple elements that have a significant impact on the intrinsic motivation of learners. The six key variables that contribute to increasing intrinsic motivation in learning are challenge, curiosity, fantasy, cooperation, competition, and recognition (Malone & Lepper, 2021). Participants are more likely to be intrinsically motivated when these six elements are present in a learning setting. Through the examination of intrinsic and extrinsic motivational aspects in gamification, one can discern the impact of including game-based components on learners' performance.

As to Sitzmann's (2011) findings, computer-based learning does not solely yield favourable results in terms of procedural and declarative knowledge. Nevertheless, there is a strong correlation between game-based learning and confidence. Learners who incorporated game-based components into their learning process had approximately 20% higher levels of confidence compared to those who engaged in standard computer-less learning. Often, learners are driven by external factors to enhance their performance by obtaining feedback on their progress and comparing it with that of others. Nevertheless, incentive systems can also foster intrinsic motivation when the drive to enhance performance is assisted by internal variables, such as personal performance expectations (Kapp, 2012b).

Utilising technology can provide additional opportunities to inspire students and enhance their educational achievements. Given that a significant number of higher education students are already familiar with gamification, it is anticipated that the learners will readily embrace its application (Ortiz et al., 2016). Toda et al. (2019a) argue that the wide variety of gamification tools poses a challenge for designers in accurately evaluating and forecasting the outcomes of these tools. Previous studies have identified the necessity of a taxonomy system

to categorise the various components of gamification, resulting in the following classifications: performance, ecological, social, personal, and fictional.

Implementing time constraints might heighten the level of pressure experienced by participants. The presence of a running clock leads to disengagement among the participants due to external pressure (Toda, 2019b). The author must possess a comprehensive understanding of the probabilities and potential drawbacks associated with gamification aspects. By incorporating appropriate gamification aspects into the learning materials and presenting participants with a challenging task, it is highly probable that learners' acquisition of knowledge and motivation will be enhanced.

2.1 Significance of Gamification

2.1.1 Increasing engagement with the topic

Gamification is known in education since it helps to increase students' involvement in understanding a topic. The primary goal in game development is to create a game that is both enjoyable and engaging, allowing players to be challenged and apply their skills. Additionally, the game should provide aesthetically pleasing experiences, support social interaction, and allow players to identify with the game (Forlizzi & Battarbee, 2004). Point systems and incentives are examples of gamified components that appeal to people's innate drive for success and advancement. Gamification draws students' attention and holds it throughout the learning process by establishing a dynamic and interactive learning environment.

Landers et al. (2018) suggest that gamification can be incorporated into current learning settings to implement a learning method that incorporates game elements. The efficacy of the current learning environment must be established prior to implementing gamification, as gamification is intended to enhance instruction rather than replace it. Research on gamification has been conducted across multiple disciplines, including computer science, social sciences, language arts, math, physics, and biology (Chang et al., 2008; Kapp, 2012b; Ortiz et al., 2016; Tsai, 2017).

2.1.2 Enhancing the ability to learn efficiently

Gamification proponents contend that it improves learning outcomes and goes beyond simple participation. In a gamified learning environment, students are frequently expected to solve issues, make choices, and use critical thinking abilities. These exercises improve students' capacity to apply information to real-world contexts by simulating real-world experiences. In recent years, there has been a growing interest in inquiry-based learning (IBL). IBL is an educational method that emphasises problem-solving and gradual discovery learning. According to Pedaste et al. (2015, p. 48), Inquiry-Based Learning (IBL) seeks to offer an "authentic scientific discovery process." Active participation and self-directed responsibility are required from learners in order to engage in the learning process. Furthermore, learners who are well acquainted with the inquiry process acquire a greater amount of knowledge during different scientific procedures compared to learners who lack a suitable introduction (Zacharia et al., 2015).

3 Research Methodology

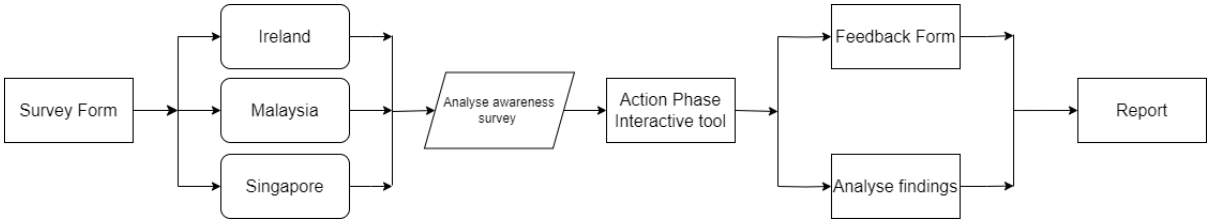

Figure 1: Research Project Flowchart.

In the Google form, the initial status before allowing any participant to move forward is to get their consent. Once they accept the consent, they will move on to the survey which have different sections resulting different parts of the survey. Each sections are tailored based on the situation of the participants are currently in. As mention previous in the research methodology, there will be the awareness phase which will ask participants about their awareness of their current understanding of the security aspects that is being used. This provides information that will help to understand how much the prototype training tool will help after the participants have gone through it. There will be 15 questions for the awareness phase which will ask about the participants understanding.

The second part will be referred to as the "action phase" or the phase of teaching and educating. During this phase, I will be replicating the methodology used by the previous

researcher, which involves creating an interactive module/game with a unique element. The previous research utilised a tool called Serious Game Design Assessment Framework (SGDA) to develop a game concept (Matovu et al., 2022; Ros et al., 2020; Xiao et al., 2023). The tool primarily focused on attack tactics employed by hackers, security systems, Intruder Detection Systems (IDSs), and other technical aspects. This content is particularly impactful for younger individuals and working professionals.

Participants will then be brought to the final section which is the feedback phase that will ask some similar questions to see whether participants now understand the importance of information security and will make changes and improve their actions towards securing their information now than previously during the awareness phase. There will be 15 questions which are segregated to 5 different security aspects. Based on the evaluation recorded below, the results drastically improved a lot.

4 Design Specification

The prototype tool that is implemented for this research survey is used for giving a game for the participants to learn about simple 5 security aspects that are most common but often overlooked. The game training model is created from a software called “Visual Novel Maker” (Visual Novel Maker, 2017) which is available from a gaming platform known as “**STEAM**” (Steam, 2003). The software was purchased in order to use the tools and model characters which are available in the game. The game framework consists the Menu Screen, five chapters that is specifically created for each 5 security aspects that are separated through the story.

There are multiple features in the prototype game such as interactions with the characters, quizzes, animations and story lore. In each chapters there are 3 sub-chapters which are different methods to secure the security aspect based on the main title of the chapter. Each chapter there will be one character that will guide the participant step by step on how to understand the security aspect. There will be some topics where participant will interact with the game to provide the immersive feeling of playing through the game instead of general reading through the content provided within.

Participants will have to click on certain places to activate the interaction between the characters and the surrounding of the environment. Some chapters, participants will receive some items as a gift by the some characters which is obtainable by playing certain sub-chapters. There will be examples provided to show the mistakes that some people that overlook small details of information security. Each examples there will be explanation and methods on how to tackle the situation should it arise. For every method, there will be a short quiz to ensure that the participant remember what they have just learn couple of seconds ago. There is also point-based system for each quizzes answered correctly. The point-based system implemented is to ensure that participants have a goal to achieve at the end of the training.

5 Implementation

The development process begin with the prototype training tool which is explained in detail in design specifications. During this process, having users that are oblivious to information security I need to ensure that the security aspects are commonly used in day to day activities and simple but often times overlook by people. These security aspects are password strengthening, Email Scam Detection, Backup Data, Anti-virus protection and WI-FI Protection Connectivity. Each of the security aspects are listed in separate chapters allowing the participants to understand a single chapters initially before moving on to the next.

In the game, I have implemented several aspects and functions of what is required for the tool to be a gaming experience. First off, having a story line in the game there is a story line surrounding the characters and the participants engaging with it. However the storyline is rather short and more precisely focused on the topics of which resolves around the security aspects of the training. Next, is the functions of each sections, every chapters there is a link between different chapters which will take the participants into different places and surrounding that makes it look as if participants are immersing into another reality within the game.

As for the point-based system, I have implemented a common-event which is known to calculate the points gathered within the game when a participant correctly answers a quiz given by the characters of each chapters. The point will then accumulate to the very end of the training and will then provide the fully accumulated result for the participant to look back

and see how much they have gotten from their training. Next, the interactions between the game and participants. Participants will need to do certain that will activate some key points during the training and will be given items or helping the characters.

A bonus to that is certain chapters there will be some characters giving away gifts to participants to show the interaction between the characters and participants. Lastly, to ensure that participants understands each security aspects, each one of the chapters have sub-chapters which discusses different methods of securing their information based on the chapters that it focuses on.

6 Evaluation

6.1 Case Study 1: Password Strengthening

6.1.1 Awareness Phase

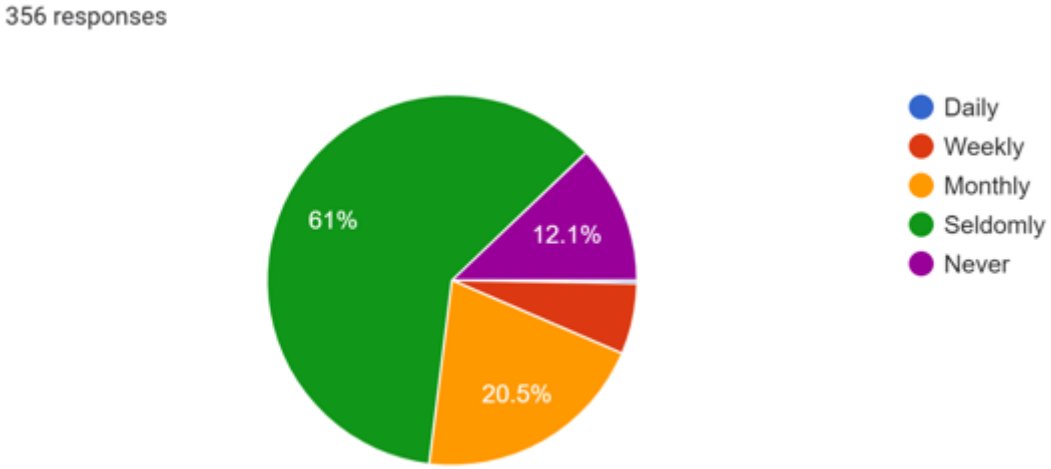

Figure 2: Pie Chart percentage of participants resetting password before training

Figure 2: The majority of respondents, at 61%, seldom update, reset, or change their passwords. Monthly updates are practiced by 20.5%, while a smaller percentage, 6.2%, does so weekly. Daily updates are extremely rare, with only 0.3% engaging in this frequency. The remaining 12.1% admit to never updating their passwords. These results underscore that a significant portion of the surveyed population may not be adopting frequent password updates, which is a crucial aspect of maintaining robust cybersecurity.

6.1.2 Feedback Phase

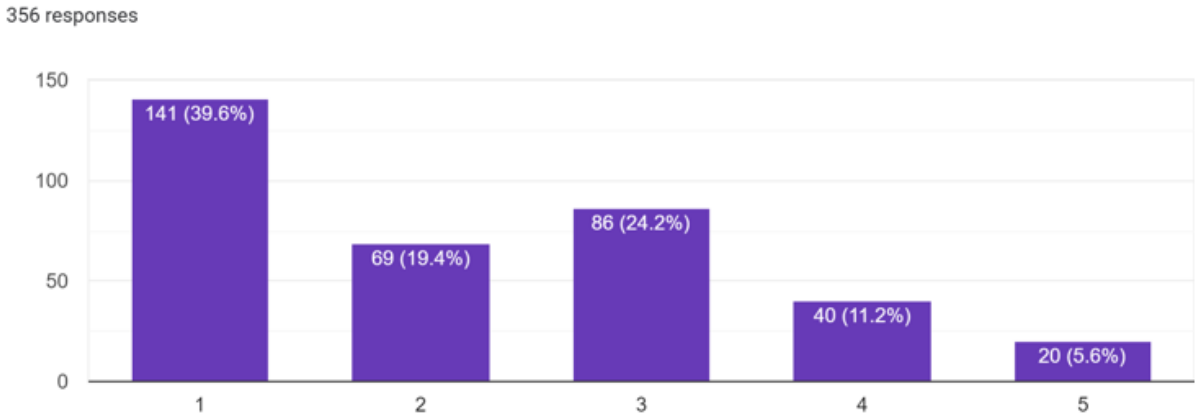

Figure 3: Bar Chart of likeliness of participants resetting password after training

Figure 3: A significant portion of respondents, at 39.6%, express a high likelihood of updating, resetting, or changing their passwords. Additionally, 19.4% find it likely to do so. On the other hand, 11.2% are not likely, 5.6% are least likely, and 24.2% are uncertain about updating their passwords. The positive inclination of a significant portion towards updating passwords is encouraging for maintaining strong online security. However, the uncertainty and lower likelihood among a notable percentage suggest potential areas for awareness and education regarding the importance of regular password updates.

6.2 Case Study 2: Email Scam Detection

6.2.1 Awareness Phase

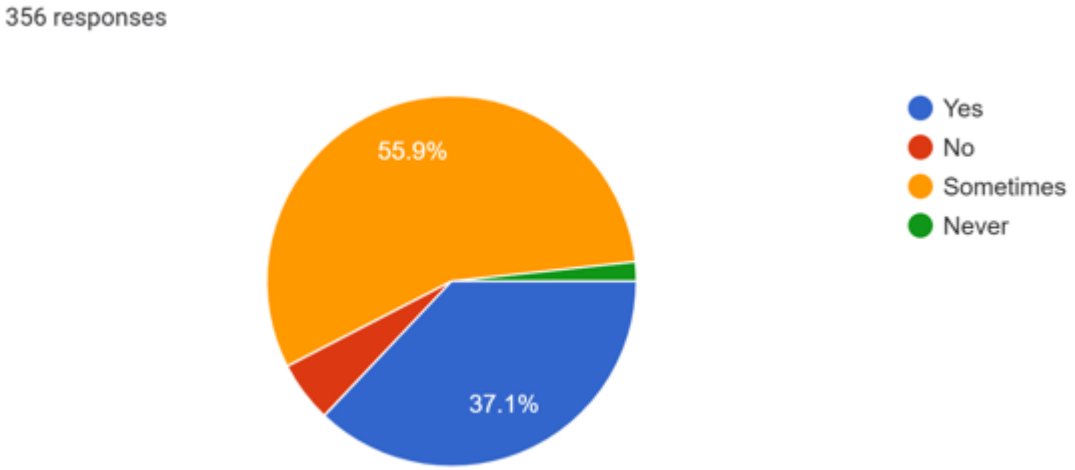

Figure 4: Pie Chart percentage of participants reading emails carefully before training

Figure 4: A vast majority of respondents, at 55.9%, admit to sometimes reading emails carefully, while 37.1% claim to read all emails sent to them carefully. A smaller percentage, 5.3%, explicitly states not reading all emails carefully, and 1.7% confess to never reading them carefully. These results suggest that a significant portion of the surveyed population

takes a selective approach to email reading, possibly depending on factors like the sender or the content of the email.

6.2.2 Feedback Phase

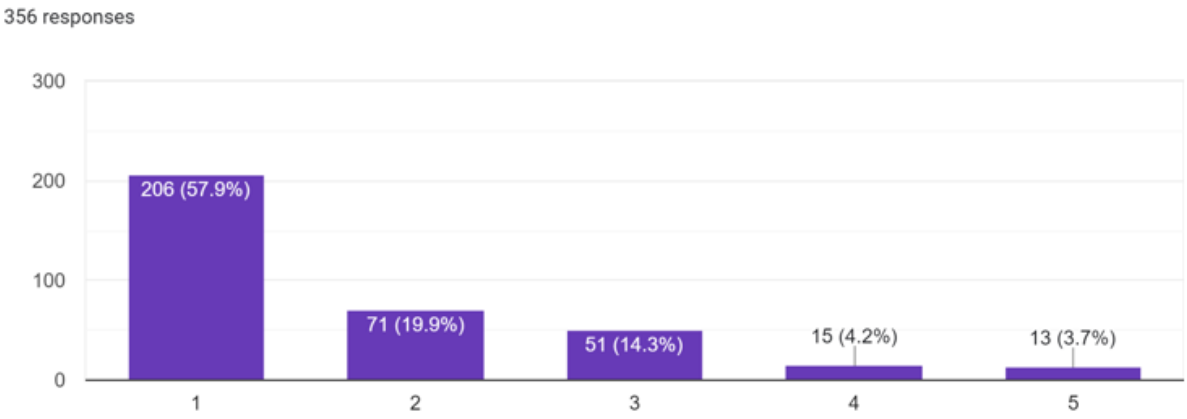

Figure 5: Bar Chart of likeliness of participants reading emails carefully after training

Figure 5: The majority of respondents, at 57.9%, express a high likelihood of reading their emails carefully from now on. An additional 19.9% find it likely to do so. A smaller percentage, 14.3%, is unsure about their future email-reading habits, while 4.2% are not likely and 3.7% are least likely to read their emails carefully. The positive inclination of a significant portion towards improving their email-reading habits is promising. It suggests a potential willingness to be more attentive to online communications, possibly driven by a heightened awareness of cybersecurity.

6.3 Case Study 3: Backup Data

6.3.1 Awareness Phase

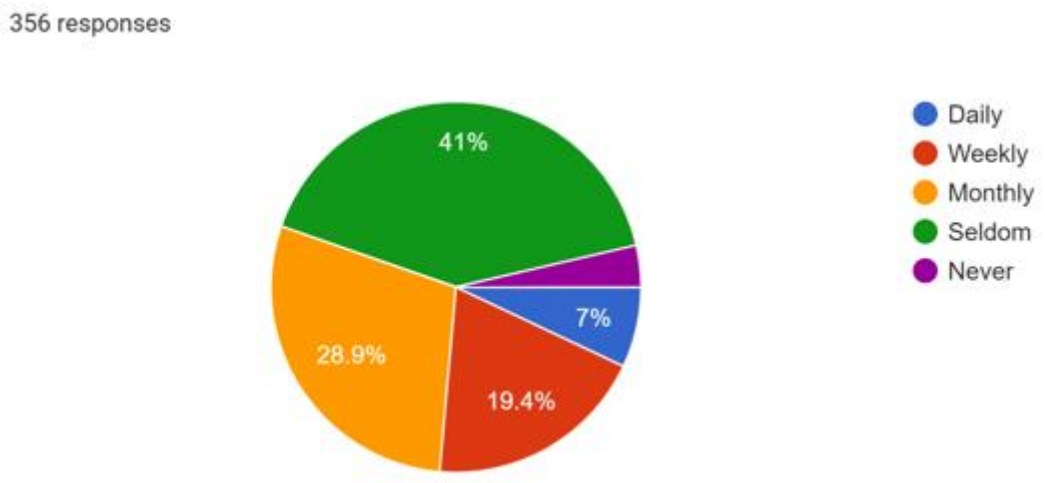

Figure 6: Pie Chart percentage of participants backing up data before training

Figure 6: A significant portion of respondents, at 41%, seldom backup their information, while 28.9% do so on a monthly basis. Weekly backups are practiced by 19.4%, and daily backups are conducted by 7%. A small percentage, 3.7%, admits to never backing up their information. These results highlight that while a considerable number of respondents engage in regular backup practices, there is also a notable portion that does so less frequently or not at all. Regular backups are a key aspect of data security and recovery in case of unexpected events.

6.3.2 Feedback Phase

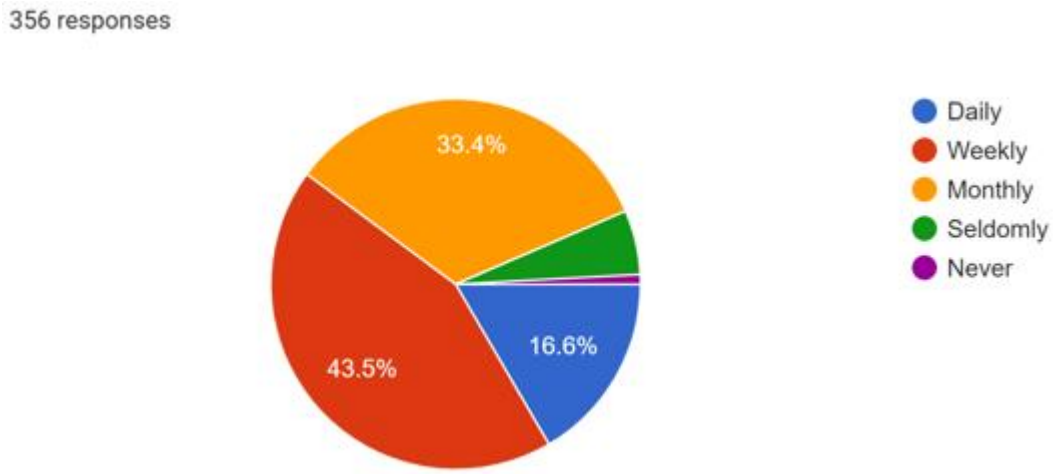

Figure 7: Pie Chart percentage of participants backing up data after training

Figure 7: The reported frequencies of data backup indicate that a substantial portion of respondents is actively engaged in regular backup practices. Specifically, 43.5% would back up their data weekly, and an additional 33.4% would do so monthly. Daily backups are conducted by 16.6%, and only a small percentage, 5.6%, seldom backs up their data. A mere 0.8% admit to never backing up their data. These results suggest a positive trend towards regular data backup practices, which is crucial for data security and recovery in the event of unexpected incidents.

6.4 Case Study 4: Anti-Virus Protection

6.4.1 Awareness Phase

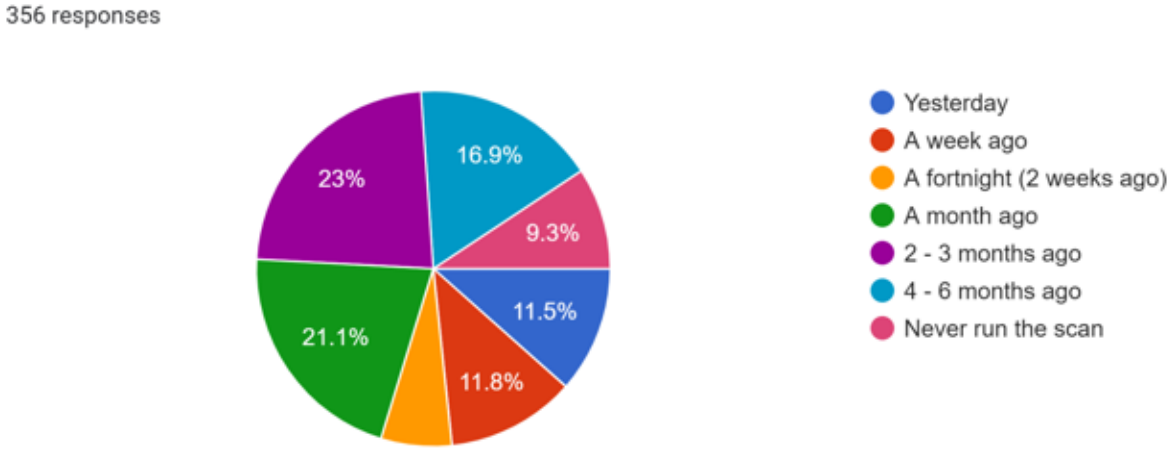

Figure 8: Pie Chart percentage of participants scan using anti-virus protection before training

Figure 8: The reported frequencies of the last antivirus scan indicate that a significant portion of respondents has run a scan relatively recently. Specifically, 11.5% ran a scan yesterday, and 11.8% did so a week ago. A combined 28.5% have conducted scans within the last two weeks. A substantial portion, 21.1%, performed a scan a month ago, and an additional 23% did so within the last 2-3 months. The 4-6 months' timeframe accounts for 16.9%, while 9.3% admit to never running an antivirus scan. These results suggest that a considerable number of respondents are actively running antivirus scans, especially within the last month, which is positive for maintaining cybersecurity.

6.4.2 Feedback Phase

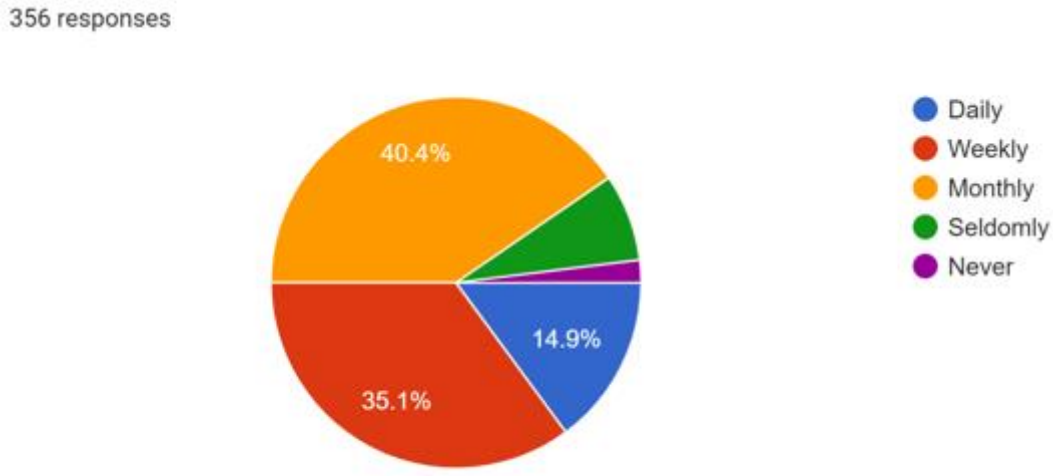

Figure 9: Pie Chart percentage of participants scan using anti-virus protection after training

Figure 9: The reported frequencies of running antivirus scans indicate that a substantial portion of respondents is actively engaged in regular scanning practices. Specifically, 40.4% would run antivirus scans monthly, and an additional 35.1% would do so weekly. Daily scans are conducted by 14.9%, and only a small percentage, 7.6%, seldom runs antivirus scans. A mere 2% admit to never running antivirus scans. These results suggest a positive trend towards regular antivirus scanning practices, which is crucial for detecting and preventing potential security threats.

6.5 Case Study 6: WI-FI Protection Connectivity

6.5.1 Awareness Phase

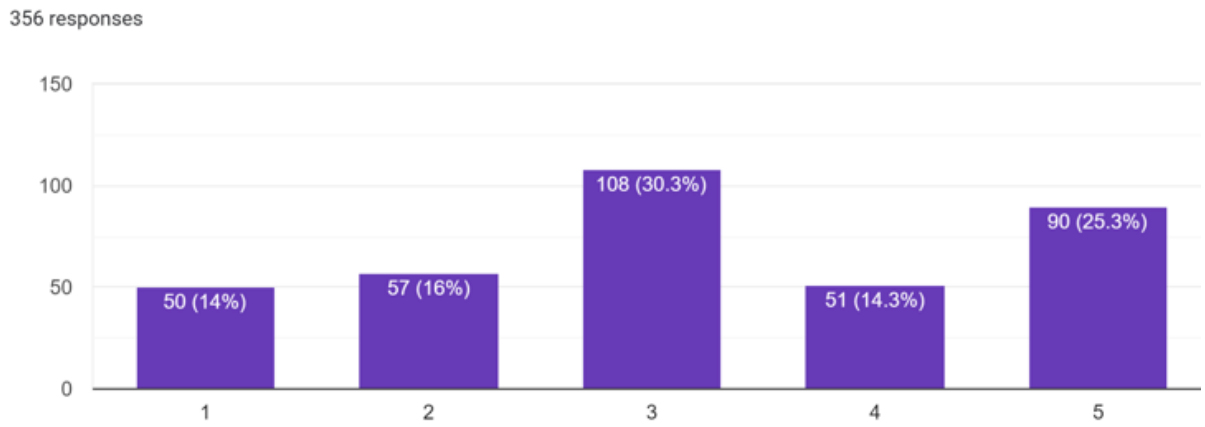

Figure 10: Bar Chart percentage of participant's likeliness to connect to public WI-FI before training

Figure 10: The distribution of responses indicates a varied stance on connecting to public Wi-Fi. A relatively small percentage, 14%, is most likely to connect, and an additional 16% find it likely. On the other hand, 25.3% are least likely to connect, and 14.3% find it not likely. A notable portion, at 30.3%, is uncertain about connecting to public Wi-Fi. These results reflect a range of attitudes towards the security risks associated with public Wi-Fi. The uncertainty among a significant portion of respondents suggests a cautious approach when it comes to connecting to these networks.

6.5.2 Feedback Phase

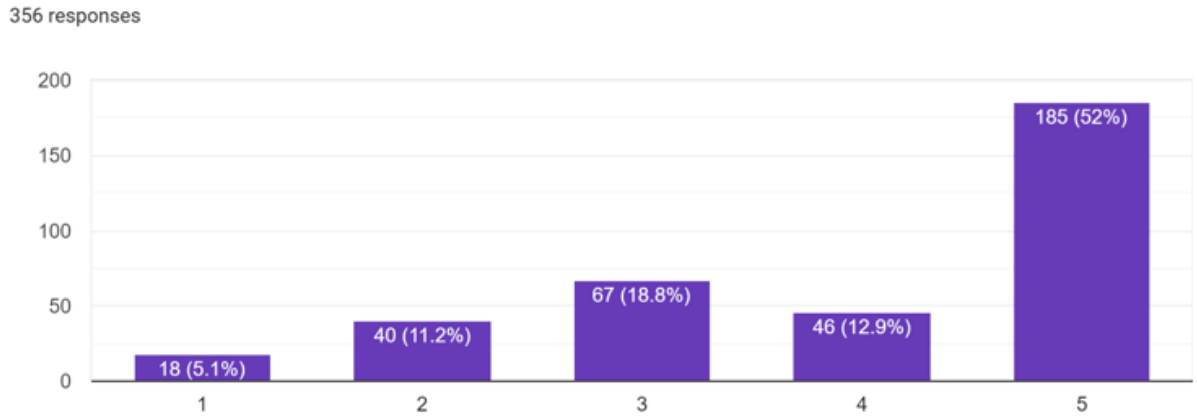

Figure 11: Bar Chart percentage of participant's likeliness to connect to public WI-FI after training

Figure 11: A majority of respondents, at 52%, express a strong inclination to avoid connecting to public Wi-Fi, marking themselves as least likely to do so. Additionally, 18.8% are unsure about their likelihood, 12.9% find it not likely, and a smaller percentage, 11.2%, is likely to connect. Only a very small percentage, 5.1%, is most likely to connect to public Wi-Fi. These results highlight a cautious approach among a significant portion of the surveyed population when it comes to using public Wi-Fi, recognizing the potential security risks associated with these networks.

6.6 Case Study 6: Action Phase

6.6.1 Point Based system

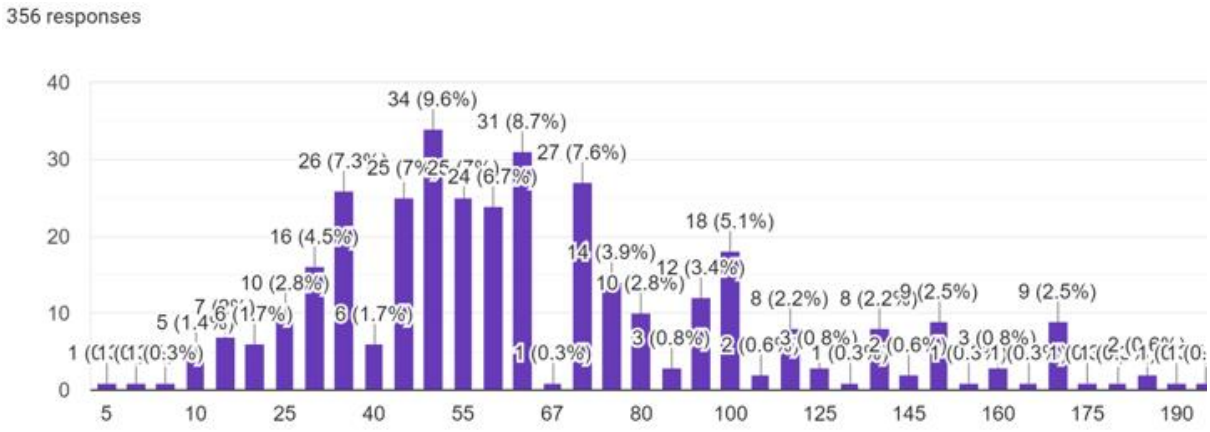

Figure 12: Bar Chart percentage of overall points scored after completing the training

Figure 12: The distribution of scores at the end of the training indicates a relatively balanced performance among the respondents. A significant portion, at 46.3%, scored in the range of 55-100 points. The next most common score range is 1-50 points, with 38.8% of respondents falling into this category. A smaller percentage, 9.3%, scored in the range of 105-150 points, and an even smaller percentage, 5.6%, achieved scores between 155-190 points. These results

suggest that a majority of respondents performed reasonably well in the training, with a substantial portion achieving scores within the mid-range.

6.7 Case Study 7: User Satisfaction with Prototype Training Tool

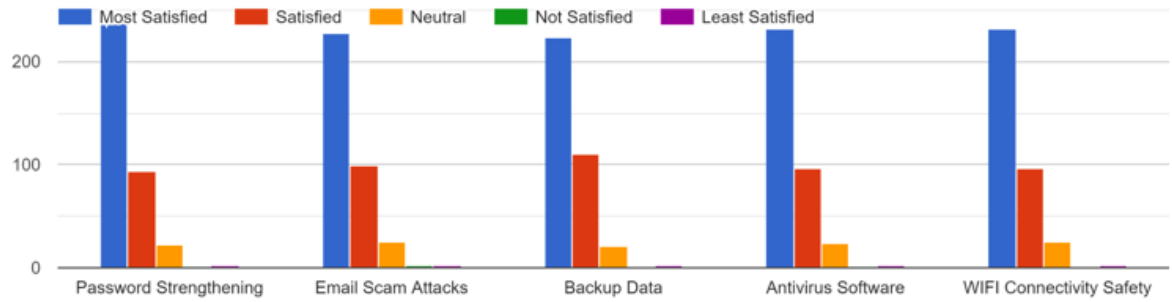

Figure 13: Bar Chart percentage of participant's satisfaction after training

Figure 13: The satisfaction levels with different chapters of the game prototype are consistently high among the respondents: "Password Strengthening" has the highest satisfaction level, with 66.6% of respondents being most satisfied. "Anti-Virus Software" and "Wi-Fi Connectivity Safety" chapters both have a satisfaction level of 65.2%, with most respondents being highly satisfied. "Email Scam Attacks" and "Backup Data" chapters also received positive responses, with 64% and 62.6% of respondents, respectively, being most satisfied. These results suggest that the game prototype effectively resonates with users across various cybersecurity topics, receiving favourable feedback for its different chapters.

The results suggest that the game prototype effectively resonates with users across various cybersecurity topics and receiving favorable feedback from respondents. The following are partial comments on the interactive prototype visual novel game.

"An eye opening gamification video

Fantastic video guide

Excellent Guide gamification video

Facts and Fun. Valuable knowledge.

An Amazing Video Guide to Cyber Security

Insightful knowledge of cyber security

Lift up the mood to learn new things because of the interesting visual and content

Very helpful and interesting to play for everyone

It was fun and very educational. More of that it also good education for everyone to learn

Interesting and fun, understandable and a new way to interact with student

The game is really enjoying while the information is easily understood
Interesting and fun, understandable and a new way to interact to student”

6.8 Discussion

Based on the results provided in the case studies, each case study shows the Awareness Phase and the Feedback Phase where clearly shows signs in significant improvements among participants after undergoing the training using the prototype game training tool. This goes to show that participants are beginning to understand that they are in need of improvements towards simple security aspects that could cause severe damage to their information and to themselves. It also noted that, the results from the point based system shows that majority of the participants score between 30 – 100 points of the main cluster of results. This shows that participants manage to improve their understanding of the security aspects while in training. As for the final case study, it shows the level of satisfaction which indicates that participants are happy and satisfied with the training tool and solidifying the point that the prototype tool indeed has help them improve their understanding while providing some comments listed just below the graph.

7 Conclusion and Future Work

In conclusion, does gamification enhance information security towards oblivious online users in Ireland, Malaysia and Singapore? Yes it does. With the results accumulated from the findings and the evaluations made it is safe to say that the objectives of the research has also been achieved which are 1) To find out the awareness of people about online threats; 2) To identify that through gamification people will increase their awareness; 3) To find out whether people will take considerations into securing their information stronger.

My contributions towards this topic was to help people to understand that even the smallest of security feature is not be left reckon with it. Even though the five security aspects may seem too simple to be focused upon, people always take it for granted and often time overlook that aspect of security which leads to be a victim of a serious major of catastrophic event known as cybercrime that has been on the rise ever since a major proportion of the services shifted to online when COVID-19 hit back in 2019. All the work that took place ensured that there is an increase amount of participants understanding their safety of their data and ensuring they make certain extra steps to secure their information properly.

The limitations of the research is that it was a short research period which could have made the prototype training tool even more efficient in sense that it would have been created to personalized towards individuals learning capability. Although there were key aspects to a game and education concept however one key concept which is customization or personalization of content could have been implemented to have each participants have their own set of understanding.

This could be an imposed in a futures works by implementing personalization for each participants to have their own custom set training. Another futures work that could be implemented is by focusing specifically towards elderly people. Even though in this research there are some participants who are in the age of 55 – 60+. Since elderly people may have special attention towards some of their disabilities which was not able to be implemented in the prototype training tool. As mentioned above, the research was given a short period of time to assess and knowing that elderly people may need special attention and time focus on the topic it could not be focused much upon. This could be a futures work to help incorporate the assistance towards elderly people in learning it.

References

Brewer, R., Anthony, L., Brown, Q., Irwin, G., Nias, J., & Tate, B. (2013). Using gamification to motivate children to complete empirical studies in lab environments. Proceedings of the 12th International Conference on Interaction Design and Children. (pp. 388-391). Digital Library.

Chang, K.-E., Chen, Y.-L., Lin, H.-Y., & Sung, Y.-T. (2008). Effects of learning support in simulation-based physics learning. Computers & Education, Volume 51, Issue 4, (pp. 1486–1498).

Forlizzi, J., & Battarbee, K. (2004). Understanding experience in interactive systems. Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS ’04, (pp. 261 – 268). Digital Library.

Kapp, K. M., (2012a). Games, Gamification, and the quest for learner engagement. Training+Delopment, Volume 66, Issue 6, (pp 64-68).

Kapp, K. M., (2012b). The Gamification of Learning and Instruction: Gam-Based Methods and Strategies for Training and Education. San Francisco: Pfeiffer.

Landers, R. N. (2014). Developing a theory of gamified learning. Simulation & Gaming, Volume 45, Issue 6, (pp. 752–768). Sage Journals.

Landers, R. N., Auer, E. M., Collmus, A. B., & Armstrong, M. B. (2018). Gamification science, its history and future: Definitions and a research agenda. Simulation & Gaming, Volume 49, Issue 3, (pp. 315–337). Sage Journals.

Malone, T. W., & Lepper, M. R. (2021). Making learning fun: A taxonomy of intrinsic motivations for learning. In Aptitude, learning, and instruction (pp. 223-254). Routledge.

Matovu, R., Nwokeji, J.C., Holmes, T. and Rahman, T., (2022). 'Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges'. In 2022 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE.

Nagalingam, V., & Ibrahim, R. (2015). User Experience of Educational Games: A Review of the Elements. Procedia Computer Science, 72, (pp. 423–433). Science Direct.

Ortiz, M., Chiluiza, K., & Valcke, M. (2016). Gamification in higher education and STEM: A systematic review of literature. EDULEARN Proceedings. (pp. 6548 – 6558). iated Digital Library.

Páez-Quinde, C., Arroba-Freire, E., Espinosa-Jaramillo, M.T. and Silva, M.P., (2023). 'Gamification as collaborative learning resources in technological education'. In 2023 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-5). IEEE.

Pedaste, M., Mäeots, M., Siiman, L. A., de Jong, T., van Riesen, S. A. N., Kamp, E. T., Manoli, C. C., Zacharia, Z. C., & Tsourlidaki, E. (2015). Phases of inquiry-based learning: Definitions and the inquiry cycle. Educational Research Review, Volume 14, (pp. 47–61). Science Direct.

Quayyum, F., (2020) 'Cyber security education for children through gamification: research plan and perspectives'. In Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts (pp. 9-13).

Qusa, H. and Tarazi, J., (2021) 'Cyber-hero: A gamification framework for cyber security awareness for high schools students'. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0677-0682). IEEE.

Ros, S., Gonzalez, S., Robles, A., Tobarra, L.L., Caminero, A. and Cano, J., (2020). 'Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course'. IEEE Access, Volume 8, (pp. 97718-97728). IEEE.

Sitzmann, T. (2011). A meta-analytic examination of the instructional effectiveness of computer-based simulation games. Personnel Psychology, Volume 64, Issue2, (pp. 489–528). Wiley Online Library.

Toda, A. M., Klock, A. C., Oliveira, W., Palomino, P. T., Rodrigues, L., Shi, L., Bittencourt, I., Gasparini, I., Isotani, S., & Cristea, A. I. (2019a). Analysing gamification elements in educational environments using an existing gamification taxonomy. Smart Learning Environments, 6(1). Springer Open.

Toda, A. M., Oliveira, W., Shi, L., Bittencourt, I., Isotani, S., & Cristea, A. (2019b). Planning

Gamification strategies based on user characteristics and DM: A gender-based case study. In Proceedings of the Educational Data Mining 2019 conference (pp. 438–443). Montréal. Arxiv.

Tsai, F.-H. (2017). The development and evaluation of a computer-simulated science inquiry environment using gamified elements. Journal of Educational Computing Research, Volume 56, Issue 1, (pp. 3–22). Sage Journals.

Walters, A. (2020). Inequities in access to education: Lessons from the Covid-19 pandemic. The Brown University Child and Adolescent Behavior Letter, Volume 36, Issue 8, (pp. 8–8). Wiley Online Library.

Xiao, H., Wei, H., Liao, Q., Ye, Q., Cao, C. and Zhong, Y., (2023). 'Exploring the gamification of cybersecurity education in higher education institutions: An analytical study'. In SHS Web of Conferences (Vol. 166, p. 01036). EDP Sciences.

Zacharia, Z. C., Manoli, C., Xenofontos, N., de Jong, T., Pedaste, M., van Riesen, S. A., Kamp, E. T., Mäeots, M., Siiman, L., & Tsourlidaki, E. (2015). Identifying potential types of guidance for supporting student inquiry when using virtual and remote labs in Science: A literature review. Educational Technology Research and Development, Volume 63, Issue 2, (pp. 257–302). Springer Link.

Visual Novel Maker (2017). Available at: https://visualnovelmaker.com/ [Accessed 18 September 2023].

Steam (2003). Available at: https://store.steampowered.com/ [Accessed 18 September 2023].