

A PROPOSAL OF ROLE-PLAYING GAMIFICATION BASED E-LEARNING TO LEARN CYBER SECURITY FOR SAUDI STUDENTS

Njoud Alsubaiheen*, Kazuhiko Sato, Kento Suzuki

Graduate School of Engineering, 27-1 Mizumoto-cho, Muroran, Hokkaido 050-8585, Japan

Abstract

This proposed research aims to create an e-Learning prototype as a game that teaches topics on cyber security in a Gamification format by creating a role-playing game. By using a survey with a quantitative method and multiple-choice questions, numerical results are expected in regards to what Saudi middle school students prefer when it comes to learning Cyber Security terms, the proposed prototype or their school text book as an evaluation method another objective is to see what their current background in Cyber Security terms. Secondly and most importantly, this research aims for to have a positive impact on middle school students regarding learning cyber security terms, what they do and how to approach them in a working environment or on a daily basis.

Keywords: Gamification, Role-play, Cyber Security, Phishing, Baiting, Vishing, Social engineering

1. INTRODUCTION

The computer literacy in the modern age is key especially for Cyber Security knowledge, it is often sought after in Corporation and in day to day basis whilst using technology. Students would often lack basic knowledge in security awareness in systems or would want to expand their knowledge in Cyber Security but would be intimidated by the amount of information online or lack the desire to learn.

On the other hand, understanding of computer literacy is proportional to how important it is in the education of the country in which the subject lives. In Saudi, computer literacy is not yet widespread for many people. Cyber security is particularly noticeable.

Gamification [1]-[3] is the act of combining both education and game mechanics to make the learning process on any topic more engaging “Gamification is about taking something that is not a game and applying game mechanics to increase user engagement, happiness and loyalty!” [4]. We aim to develop the e-learning to learn Cyber security for Saudi students by using role-playing gamification. The concept and effect of a role-playing game but with a purpose of motivating Saudi students to learn basic knowledge in Cyber security is what this research investigates.

2. VISION

This research aims to create an E-learning prototype as a game that teaches topics on cyber security in a Gamification format by creating a role-playing game. In this game, the player (student) can choose their character, name them and play through 5 cyber security tasks whilst increasing or decreasing their score point's in-game if they successfully or unsuccessfully completed the tasks. To motivate students, the points can be used to either buy clothes or buy furniture for their in-game house or character.

Secondarily and most importantly, the research compares if middle school students prefer studying by using the game prototype or by an educational book (as an evaluating method). A preliminary experiment will be conducted with university students who are different from the original target users.

By using a survey with a quantitative method and multiple-choice questions, numerical results are expected in regards to what Saudi middle school students prefer and what their current background in Cyber Security knowledge.

One of the main goals this research aims for is to have a positive impact on middle school students regarding some main cyber security terms, what they do and how to approach them in a working environment or on a daily basis. By using the prototype, having Saudi middle school students to be aware of the terms and how to deal with them would shed light on how aware or knowledgeable Saudi middle school students are regarding cyber security, the bigger the percentage on how this prototype is more engaging than reading about the terms on a middle school information and communication technology (ICT) textbook.

3. E-LEARNING PROTOTYPE

3.1. Programs

There are two ways to create an e-learning game, one is to code completely new [5]-[7] and the other is to use an existing game platform [8]. We adopted the latter method. Currently a prototype is being created by using RPG maker game engine [9], the engine is for creating role-playing games specifically with flexibility in the development by scripting in JavaScript separately or by developing within the game itself.

Surveys will be created by Survey Monkey [10] an online software for creating surveys which an analysis tool that allows the user to analyze the data gathered from the survey and visualize it by using different types of charts.

3.2. Outline

In my current progress, after the students starts the prototype, they are directed to character creation once they have chosen their gender, appearance (hair color) and name they are redirected to the first map the player can interact with which is the players house. As you can see in Fig 1, the first map is the player's house, the player starts off after character creation with 5 coins in his/her inventory that can decrease/increase once they start doing the Cyber Security related tasks (quests) later on, in the house the player will be able to use the bed to start a new day and be able to use the computer to start the email phishing quest. The phishing quest is scheduled to be the last quest the player is able to do, once the player interacts with the computer, a replica of two emails starting with the first one as a screen pop up the player will be able to read the email and judge if its phishing or not [11] by choosing from two choices, failing to do so the player will lose 5 coins and the screen will show a screen pop up that explains why their answer was wrong in order for the student to learn their mistake. Once the player leaves the house, they are redirected to the main neighborhood map shown as Fig 2. On the map, mark 1 is the player's house as previously explained. Mark 2 is the store where the player will be able to use their points earned from completing the tasks to buy new clothes or furniture for the house, and lastly, mark 3 is the academy where 3 of the quests will take place two password quests and the baiting quest. The first quest would be the first password quest the player will do, the player will be asked to go to the system room via the quest log (which will explain where is it in the academy) as after interacting with the system in the room the system in the room will start asking the player to choose the right password for the player's system in the academy, the player will be presented with multiple choices of random choices ranging from strong to medium and to weak passwords, failing to choose the right answers the screen will show a screen pop up that explains why their answer was wrong in order for the student to learn their mistake, the player will lose 5 or 3 coins depending on the level of weakness of the password, if it's extremely weak the player will lose 5 coins, the player can also choose a password with a medium level and earn only 3 coins instead of 5 and will be presented with a screen pop up explaining how their choice was not the safest one which included tips on how to choose a strong password. The 2nd password quests as seen in figure 3 depicts a scene from the quest, where the player will be informed via the quest log to go to the meeting room to talk to their colleague regarding their project. The colleague will ask the player about choosing the best fitted password for their project from a security perspective. The 2nd password follows the same outline as the 1st password quest.

The 3rd quest in the academy will take place on the 2nd floor in the office room, the quest is about baiting. The quest starts when a non-playable character interacts with the player and they will ask the

player if they know the owner of a USB memory found in the office [12], the screen will show a pop up of how the USB look like and the quest will follow a similar outline of the previous quests presenting the player with multiple choice answers and each answer will present further answers for further investigating the scenario. Failing to choose the right choice the player will lose either 5 coins, the screen will show a screen pop up that explains why their answer was wrong in order for the student to learn their mistake as well as earning 5 coins if the player chooses the right answer.

The main map is where the 4th quest is scheduled to take place which is about another type of social engineering called vishing (voice phishing) [13], the quest will ask the player to go back to his/her house and on their way to the house their personal phone would ring automatically interacting with the player, the player will receive a call from an anonymous person pretending to work in the academy asking for personal information. The quest will follow the same outline like the previous quests.

All quests include:

- Multiple choice answers
- Explanation of cyber security words.
- Explanation of why the chosen answer is correct/incorrect.
- Increasing/decreasing points.



Fig. 1. Players House. Screenshot by the author and created in the RPG maker software.

Source: Njoud Alsubaiheen, RPG maker, (June 2020).



Fig. 2. Main Map. Screenshot by the author and created in the RPG maker software.

Source: Njoud Alsubaiheen, RPG maker, (June 2020).



Fig. 3. 2nd password quest. Screenshot by the author and created in the RPG maker software.

Source: Njoud Alsubaiheen, RPG maker, (June 2020).

3.3. Functions for Survey

The main and non-playable characters, maps and 3 cyber security related tasks have been created which the player must choose their character and complete the tasks. Once the game prototype is playable, the goal of this research is to test it on 100 Saudi middle school students focusing on 5 public, private and international schools with a survey to be created with closed ended questions and distributed to get the final results.

During the Survey phase, the research aims to reach one of two outcomes either middle school students would prefer learning about cyber security basics through playing the game prototype or a large percentage would prefer learning about the cyber security basics through their Information and communications technology academic books as most private, international and public schools have a section regarding cyber security in them.

The survey won't be limited to only one main question if middle school students prefer the game prototype or not, it will have question regarding the percentages of how many males or females have tried the prototype, how many students had previous knowledge in cyber security and last but not least the percentages of which type of cyber security term included in the game students had previous knowledge about.

The sample survey questions would look something like as Fig 4. In this figure, the student is able to choose how much did they enjoy the game prototype by scaling and choosing from 0 (low on enjoyment) to 5 (high on enjoyment) or keeping it at neutral.

1. On a scale of 0 to 5, How much did you enjoy the game prototype ?

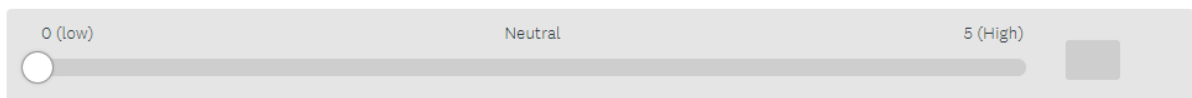


Fig. 4. 0 to 5 Scale question. Created by Survey Monkey.

Source: Njoud Alsubaiheen, Survey Monkey, (November 2020).

In Fig 5 we can see that the student has a multiple-choice type of question in order to choose between which was more enjoyable, their school textbook or the game prototype they just tried. This question will be one of the most fundamentals questions in this research as it unlocks the main result this research aims to discover.

* 2. Which is more enjoyable to use for learning Cyber security ?

- ☐ School's ICT (Information and communication technology) book
- ☐ This gaming prototype

Fig. 5. Prototype vs. school textbook question. Created by Survey Monkey

Source: Njoud Alsubaiheen, Survey Monkey, (November 2020).

As we can see in Fig 6, the multiple-choice question allows the student to choose which Cyber Security terminology they previously had prior knowledge about. The aim of this question is to figure out which Cyber Security terminology presented in the game prototype Saudi middle school students had previous

understanding regarding it, this will help articulate the popularity of the some of the terminologies as well as which terminology had the most impact previously on students in their daily life

3. Which Cyber Security term you previously were knowledgeable about ?

- ☐ Password security
- ☐ Email Phishing
- ☐ Baiting
- ☐ Vishing (voice phishing)
- ☐ None of the above

Fig. 6. Previous Cyber Security knowledge question. Created by Survey Monkey

Source: Njoud Alsubaiheen, Survey Monkey, (November 2020).

4. JAPANESE GAMIFICATION

This section discusses one of the two most common types of Gamification found in Japan and how the results they had impacted the Japanese society and what this research aims to have as a result.

Commercial type:

- **Information Management in Gamification:** one of the most famous chain of convenience stores Seven Eleven has been using a tuning method to respond to customers' needs in Japan. By using the POS (Point of Sales) information system, the employees can predict the best items that fits customers based on their gender or age and by doing that items can be placed on a shelf in a way that fits the customer's needs. *"tuning," in the context of social games to ensure an optimal performance, is also being exercised in the business practices of the convenience stores operated by Seven-Eleven Japan" [14].*
- **Freemium Model in Gamification:** Gatcha (ガチャ) a term used quite popularly in Japan as they are toys encapsulated in small packages and are found in toy dispenser around the streets, airport and even some department stores. What makes Gatchas possess the Gamification element is the fact that each encapsulated toy in one toy dispenser form a set which makes people want to come back to the same toy dispenser, dispensing more coins in order to fully complete ones set of toys. Similar to playing cards or sport cards where a player would negotiate with other players in order to earn the missing cards they do not own yet.
- **Kentucky Fried Chicken (KFC) game:** the famous fried chicken food chain branch in Japan has collaborated with a company called Gamify to create a phone game to increase customer awareness and to markets new items on the menu. The Player must defend the KFC castle in the game from the shrimp attacking it, the more you defend it the more points and vouchers you receive to be used at your nearest KFC branch. The game has proven to be successful with an overwhelming amount of sales particularly with the new shrimp menu items.

Non-Commercial type:

- **Information Exchange Platforms:** virtual community-based platforms like question and answer (Q&A) have used an element in Gamification. Popularly in Japan Oshiete! Goo (教えて! goo), OKWave and Yahoo! Answers (Yahoo!知恵袋) are information exchange platforms that allows users to answer each other's questions and ask any question regarding any topic. *"the reward policy that is being advocated differs per knowledge community service" [14].* In most cases users are

rewarded by receiving points for each answer they have written and sometimes even rewarded with points that can be exchanged for real money.

- **Serious Games:** the term Serious Games has appeared in 70's meaning a game that serves a specific purpose and goal and can be about topics such as education, cyber security or environment awareness and many more. Serious Games can use elements in Gamification for the purpose of engaging the user, one of the popular Serious Game in Japan called #denkimeter developed by Inoue Akito in 2011 which has a gamified looking user-interface, it was found after the Great East Japan Earthquake and Tsunami disaster. The concept of the game is based on competing with other users about energy consumption, each person records the 4 digits of their electricity meter and uploads it on the official website of the game resulting in the website generating a specific number to the user. The user can use this number to compete with other users on Twitter by using the hashtag #denkimeter as the higher the user consumes energy the more points they receive.

5. DISCUSSIONS

This chapter discusses some of the main and related literature review compiled for this research. The first review discusses the use of Gamification in security awareness and training programs [15]. Which discusses how unmotivated employees are when it comes to expanding their knowledge in Cyber security awareness and one of the primary ways of raising an employees' cyber security awareness based on this research is through programs and trainings set in companies but so many employees find it tedious and uninteresting.

A prototype of a gamified application was developed to help this research, the results found that having a gamified Cyber security awareness training had a positive effect on employees. What makes this research similar to the proposed research in this conference paper is that they both focus on security awareness Gamification while they differ one the scope and the concept is more of an interaction program rather than a game based on role-play.

The second review discusses using gaming technology for cyber security awareness [16]. The research focuses on technological crime when it comes to mobile use, in many undeveloped countries these technologies are new compared to developed regions. A previous research was made to test which cyber security awareness application was preferred; users preferred a mobile gaming application to address the issue of creating awareness.

The research focuses on technological crime when it comes to mobile use, in many undeveloped countries these technologies are new compared to developed regions. A previous research was made to test which cyber security awareness application was preferred; users preferred a mobile gaming application to address the issue of creating awareness. This research review focuses as well on security awareness in Gamification while researching gaming application that can help them raise awareness. The difference between it and the proposed research in this conference paper is that this research review focuses on mobile game applications only whilst their awareness concept is like a role-playing game.

The third review focuses on a developed role-playing phishing simulation game called What Hack [17]. Phishing attacks have always been a problem worldwide and it's not just corporates who suffer from them, politics have been hit hard for many times because of phishing attacks which leads to granting access to confidential information to unauthorized people. This happens because of the lack of awareness in cyber security particularly phishing and its what this research focuses on.

What. Hack is an engaging role-playing phishing Gamification that stimulates actual phishing attacks to encourage the player to practice protecting themselves. The research also showed how What. Hack made people more engaged as opposed to regular cyber security training with no game mechanics. What Hack is fairly similar to the role-playing prototype Gamification research the conference paper is proposing as they both follow a role-playing style and focuses on Gamification elements. They mainly differ on how What. Hack only focuses on one type of Cyber Security attacks as well as the study is not narrowed to any specific citizens, education or age group.

As for the fourth review the main focus here is a framework with a gamified e-learning concept and how accepted are they by Saudi students in Saudi Arabian universities [18]. The main idea is about the e-learning approach and how rapidly it has increased due to the development of recent technology. Nowadays many institutes are using e-learning to teach and deliver academic content to students. The main problem discussed in this research is the acceptance of e-learning by students as a teaching method and how many educational institutes are trying to find ways to increase the students' willingness to accept e learning, one of which is Gamification.

The paper also delves deeper about the benefits of Gamification in education and a review of e-learning systems. The research has a clear focus on introducing the concept of Gamification in the higher education system in

Saudi Arabia and testing framework on Saudi university students which is very similar to what this conference paper is proposing while they differ on the idea that this e-learning framework is not focused on Cyber Security but rather educational content in general.

The last review is fairly close to the proposal of this conference paper as it focuses on Gamification techniques to raise Cyber Security awareness [19]. The technique used in this paper is formed as a quiz in a role-playing 2D game that aims to educate users about Cyber Security awareness. It focuses on the importance for users to understand basic security measures in many sectors particularly about password security.

The role-playing quiz game was developed for android platforms, the resulted data from the role-playing quiz game showed that users enjoyed and benefited from learning about Cyber Security awareness whilst using the application. The difference between the last research review and the proposal in this conference paper is the interaction with the main character, in the proposal the student can create his/her own character and are able to walk and interact with other non-playable characters for the tasks to begin as well as it being 3D and not 2D as well as the study in this research review is not narrowed to any specific citizens or age group.

6. CONCLUSION

This research will focus on testing a role-playing Gamification concept that is focused to make the player learn concepts in Cyber Security in order to raise the awareness of middle school students varying from private, public and international schools in Saudi Arabia. In this day and age the cyber world has become a part of our present life and for the future as many things rely on the internet and as technologies advance cyber criminals advance in their tactics as well, there has been a large focus on Cyber Security awareness in Saudi Arabia particularly at educational institutes, companies, governments or even in their personal life's.

The main goal of this research beside raising awareness is to compare the middle school information and communication technology textbook with the role-playing Gamification based e-learning to see which one was more engaging when it comes to learning about some main Cyber Security concepts. The concept of the role-playing game surrounds a character that the students can create by choosing their name, hair color and gender. The player would start as a Cyber Security Academy student and have missions (tasks) to deal with Cyber Security related quests every once in a while, the player would be asked a What-If questions related to Cyber security such as password security, baiting and social engineering (phishing email and vishing) related scenarios. The player must complete the tasks correctly in order to level and gain special items (Coins to buy in-game items) failing to respond correctly would lead the player reading an on-screen pop up that explain the reason why the answer they choose was wrong and they would lose coins as the player already starts with 5 coins in the beginning of the game.

The research will be evaluated by surveys targeting Saudi Arabian middle school students to see if the concept is ideal or not. The game will be a prototype for now and hopefully will expand later into a full solution.

REFERENCES

- [1] Chou Y. Actionable gamification. Fremont: Octalysis Media; 2019. Burke B. Gamify.
- [2] Kim S, Song K, Lockee B, Burton J. Gamification in Learning and Education.
- [3] Acer for Education, “The benefits of Gaming in Education: The Build A World case - Acer for Education”, Available from: <<https://acerforeducation.acer.com/education-trends/gamification/the-benefits-of-gaming-in-education-the-build-a-world-case/>> [Accessed 22 March 2021].
- [4] CodinGame, “Coding Games and Programming Challenges to Code Better”, Available from: <<https://www.codingame.com/start>> [Accessed 19 March 2021].
- [5] CodeCombat, “CodeCombat - Coding games to learn Python and JavaScript” Available from: <<https://codecombat.com>> [Accessed 24 March 2021].
- [6] Thinkful, “Learn Ruby on Rails as You Modify a Craigslist Clone”, Available from: <<https://www.thinkful.com/learn/ruby-on-rails-tutorial/>> [Accessed 22 March 2021].
- [7] Prnewswire.com, “Siemens Industry I. Siemens Launches Plantville - An Innovative Gaming Platform to Showcase Products and Solutions for Industry and Infrastructure”, Available from: <<https://www.prnewswire.com/news-releases/siemens-launches-plantville--an-innovative-gaming-platform-to-showcase-products-and-solutions-for-industry-and-infrastructure-118571809.html>> [Accessed 25 March 2021].
- [8] Medium, “Gamification in Product Design”, Available from: <<https://medium.com/manabie/gamification-in-product-design-c6ab78b5dc8c>> [Accessed 4 December 2020].
- [9] Rpgmakerweb.com, “Make Your Own Game with RPG Maker”, Available from: <<https://www.rpgmakerweb.com>> [Accessed 17 March 2021].
- [10] SurveyMonkey, “SurveyMonkey: The World’s Most Popular Free Online Survey Tool”, Available at: <<https://www.surveymonkey.com>> [Accessed 16 January 2021].
- [11] Us.norton.com, “What is phishing? How to recognize and avoid phishing scams”, Available from: <<https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html>> [Accessed 10 March 2021].
- [12] Inspired eLearning, “3. USB Baiting: Don't Take the Bait | Inspired eLearning Resources”, Available from: <<https://inspiredelearning.com/resource/usb-baiting-dont-take-bait/>> [Accessed 10 March 2021].
- [13] Safecomputing.umich.edu, “4. Phone Scams and Voice Phishing (Vishing) / safecomputing.umich.edu”, Available from: <<https://safe-computing.umich.edu/be-aware/phone-scams>> [Accessed 12 March 2021].
- [14] Hooghiemstra, D., 2017. “Gamification in Japan: a critical analysis”, Masters. Leiden University.
- [15] Gjære, E. and Bartnes, M., 2017. “Gamification of Information Security Awareness and Training”, Proc. of 3rd International Conference on Information Systems Security and Privacy, Available at: <https://www.researchgate.net/publication/314523152_Gamification_of_Information_Security_Awareness_and_Training> [Accessed 10 November 2020].
- [16] Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M., 2016. “A Review of Using Gaming Technology for Cyber-Security Awareness”, International Journal for Information Security Research, 6(2).
- [17] AlexWen, Z., Lin, Z., Chen, R. and Andersen, E., 2019, “What. Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game In: Human Factors in Computing Systems”, Glasgow, Scotland, UK. Available at: <<https://dl.acm.org/doi/abs/10.1145/3290605.3300338>> [Accessed 16 December 2020].

- [18] Alzahrani, A., Alharthi, A., O. Alassafi, M. and Albugmi, A., 2018, "A Framework For Gamified E-Learning Systems Acceptance In Saudi Arabian Universities : Gamified Elearning Systems", International Journal of Advance Research in Computer Science and Management, 5(4). Available at: <https://www.researchgate.net/publication/327680647_A_Framework_For_Gamified_E-Learning_Systems_Acceptance_In_Saudi_Arabian_Universities_Gamified_Elearning_Systems> [Accessed 8 September 2020].
- [19] Scholefield, S. and A. Shepherd, L., 2019, "Gamification Techniques for Raising Cyber Security Awareness", Proc of 1st International Conference on HCI for Cybersecurity, Privacy and Trust, Available from: <https://www.researchgate.net/publication/331916014_Gamification_Techniques_for_Raising_Cyber_Security_Awareness> [Accessed 10 August 2020].