Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students

Hani Qusa
Computer and Information Science
Higher Colleges of Technology
Dubai, UAE
hqusa@hct.ac.ae

Jumana Tarazi
Computer and Information Science
Higher Colleges of Technology
Dubai, UAE
jtarazi@hct.ac.ae

2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) | 978-1-6654-1490-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCWC51732.2021.9375847

***Abstract*— People are considered the weakest point in the information systems which causes most of the cyber-attacks successful. The increasing numbers of cyber-attacks indicate that the traditional methodologies of training and awareness are still insufficient to build the necessary cybersecurity skills and capabilities. Gamification represents a promising methodology to change the behavior of people in the early stages. The objective of this research is not only to verify the effectiveness of gamification but also to provide a constructive application and to propose a framework that helps eventually and iteratively in improving the cyber-security skills and capabilities for high school students in early stages. In this research, we propose a novel framework for information security awareness and training programs, known as Cyber-Hero, that will help fight one of the most popular weaknesses in cybersecurity which is human error. The framework helps in transferring the learning of a narrative set of instructions to be acquired in a serious game, in which students in schools can engage with at an early stage. Such an engagement will educate students on how to create a strong password to protect themselves from cyber-attacks. The preliminary results show incremental progress in the skills and capabilities of cybersecurity for the students using the proposed framework.**

Keywords*— *Cybersecurity Simulations, Cybersecurity Exercises, Gamification, Awareness Campaign, Training Platform.

I. INTRODUCTION

This The fast development in business automation and services has caused an increase in cyber threats and attacks on these businesses. Thus, it has become a top priority for governments to develop and improve cyber security strategies that provide recommendations and guidelines for organizations to improve their resilience and deterrence to the new threats and attacks.

These strategies start at the business level and consider mainly reinforcing infrastructure security, developing security policies, and defining best practices. Beyond the business level, these strategies target the main risk that people face which is ignorance in cyber security issues. On the individual level, education, training, and awareness are the most popular tools used to improve the awareness of cyber security of the population to better fight cybercrimes.

However, to achieve business objectives it is incumbent upon employees to continuously educate and train themselves to enhance their work skills. This takes away from the employees' ability to concentrate on equipping themselves with cyber security knowledge, thus making them unable to protect themselves or prevent trivial cyber-attacks that they could encounter in their daily life.

Thus, it is imperative to develop educational, training, and awareness tools that employees can engage in to improve their cyber security knowledge, skills, and capabilities to mainly protect themselves in the workplace. Because of the fast development in adoption of technology, this engagement should happen early on in order to change employees' behavior and reaction in case they encounter cyber-attacks.

Gamification, serious games, and gamified training are new strategies that can help achieve the required awareness at the individual level. These strategies refer to a concept of using games with the purpose of including educational and pedagogical objectives in addition to fun and entertainment. The concept of gamification has gained a lot of popularity in the academia and industry in the past decade. Studies have shown that people learn only 20% of what they hear and read, but they can learn 90% of what they have practiced [8][9]. In an effective gamified environment, people can choose their actions, learn from the consequences of their actions, and make mistakes in risk-free settings through a process of experimentation which allows them to acquire more knowledge, experience, and skills in short time.

In this paper, we propose a novel framework for information security awareness training program that will help fight one of the most popular weaknesses in cyber security which is human error. In the developed framework, we gamified the training on generating new passwords, which is required from all students working with technology and represents the most challenging issue for most people. The framework helped in transferring the learning of a narrative set of instructions to be acquired in a serious game, in which students in schools can engage with at an early stage. Such an engagement will educate students on how to create a strong password to protect themselves from cyber-attacks.

The paper is structured as follows: In the second section, we present the background of information security awareness and training and we list most recent related works. In the third section we design the requirement for effective gamified cyber security awareness tool. In the fourth section, we describe our proposed framework for gamification of cyber security awareness. In the fifth section, we present the implementation and the results of preliminary testing of the developed framework. Finally, in the last section we conclude and present our future work

II. BACKGROUND AND RELATED WORKS

In the process of exploring state of the art, different terms were used interchangeably. For example, in the next subsections, employee, user, students, and player are used to describe the entity or the person who is targeted to have the necessary information, and security skills and capabilities.

978-0-7381-4394-1/21/$31.00 ©2021 IEEE

Similarly, information security and cyber security are used interchangeably.

A. Effectiveness of Traditional Cyber Security Awareness

Nowadays, Information security awareness is an essential part of the success of any organization. According to [1], cyber security awareness is defined as the ability of the user to recognize or avoid behaviors that would compromise cyber security; it is the practice of good behavior that will lead to better cyber security, and the ability to act wisely and cautiously using sound judgment to increase cyber security.

Since employees play a major role in defending the organization's interest against socially engineered attacks, companies develop information security awareness programs in order to secure their data. These include traditional training such as online courses, security awareness camps and posters [4,5]. According to [2], these efforts show lack in effectiveness, which means that there is a lack in the practical exposure of the employees to real cyber-attacks. Through traditional raising awareness methods, employees learn theoretically about the attacks, however they may fail to identify the attack when they are actually faced with one. Consequently, this shows failure in changing the employee's behavior in response to cyber-attacks. Practically, the number of cyber-attacks resulting from human error is the best proof of this lack of effectiveness [6].

Basically, reducing the number of cyber-attacks can be achieved by motivating people to learn how to counteract these cyber-attacks. This means that there is still an imperative need to improve the effectiveness of gamification in the context of cyber security awareness.

In [2], the authors presented a set of challenges and factors that affect the implementation of any cyber security awareness programs. The two factors are mainly 1) personal, and 2) cultural and environmental factors. Another categorization of the effective implementation was presented in [3], in which authors categorize the factors that affect the behavior of users in facing cyber security situations as personal, economic, environmental, organizational, social, and constitutional factors. Studying these factors is necessary in to define the list of requirements that can enhance the performance and effectiveness of the any developed training framework.

B. Gamification of Information Security Awareness

Basically, gamification is the concept of applying game design principles in non-gaming contexts [7,8]. The main objective of gamification is to stimulate behavioral changes through increased motivation and engagement though interactive activities. Game-based learning provides a fertile ground for students to get involved in the learning process through exploring and experimenting in a risk-free environment. Nevertheless, the application of gamification of cybersecurity education has been limited to date [26].

It is worth noting that number of jobs in information security is expected to rise from 2012 to 2022 at a rate of 37%, the US bureau of Labor Statistics reported. In addition, there are 209,000 cybersecurity positions that remain vacant yearly. In order to match the growing demand for cybersecurity experts it is vital for tertiary education to generate the required cybersecurity expertise through recruiting, training, and graduating students proficient in this field [25].

In [9], the authors concluded by empirical studies that gamification has in fact shown positive effects in improving learning outcomes on multiple occasions. However, it was emphasized that the effect depends on the people and the context in which the technique has been applied. Therefore, motivation is the core of gamification, which leads to the fact that maximizing the effectiveness of any awareness and training program can be done by maximizing the motivation to learn.

Some educational games have been developed to train users in a specialized field. In [24] the authors conducted a study on the efficacy of using a game aimed at training officers in Scotland Police on how to respond to crimes cases. The study concluded that the game has good potential in achieving its objective.

There are also numerous cyber security games that have been developed. One example of an educational cyber security game targeting kids and young adults is the Webonauts Internet Academy which aims at educating users on proper online behavior [23]. Another example is Cybersecurity Lab. However, the duration of the game is about 75 minutes long which points to the fact that it does not engage the players in continuous improvement of cyber security skills [23].

A study conducted by Purdue University Northwest in 2016-2017 showed that exposing high school students to game-based learning of cybersecurity concepts and principles was very effective in developing students' cybersecurity awareness. The study showed that the innovativeness of the game-based approach facilitated the accessibility of cybersecurity concepts to the students involved in the study [25]. However, the study further investigated the gender factor in terms of using game-based learning to raise cyber-security awareness. The results showed that male students enjoyed the game-based approach more than females.

In terms of game-based mobile apps, an android app called NoPhish was developed in 2014 by the authors in [27] to educate learners on checking URLs to be able to differentiate between reliable and unreliable websites. The app utilized different gamification elements including having different levels and leaderboards so that learners are motivated to learn. The results of the study were promising however more work is needed to measure retention of knowledge in a few months.

C. Usefulness of existing frameworks

The In order to understand how to better design the requirement for an effective gamified framework for information security awareness, we list here different existing frameworks with different approaches to improve the motivation level using gamification.

The authors in [21] present the EMERGO framework which guides the development of scenario-based serious games which offers a tailored methodology and a generic toolkit for the efficient development and delivery of serious games for acquiring complex cognitive skills (also called competences) in higher education.

The authors in [10] discuss the Octalysis framework which is a very powerful framework that illustrates eight motivational drives that can be invoked in order to motivate people to perform their activities. As an example of the effectiveness of the framework, the authors used their framework to analyze the strengths and weaknesses of various products and experiences with respect to motivation.

In [11], the authors summarize a set of platforms that depend on game Mechanics and Dynamics (MDA) framework which is used mainly for motivating and evaluating students' engagement in the class. MDA uses a set of common mechanics like points, levels, challenges, and others, and a set of dynamics such as rewards, status, accomplishment, and others. Both mechanics and dynamics are used in different ways (different platforms) to engage school students in the class.

Mechanics And Emotional (MDE) framework presented in [12] is a well-designed framework that includes the emotion principle in addition to dynamics and mechanics to improve the motivation and engagement of the end user. The authors applied the framework to 'The American Idol' TV show as a case study to prove the effectiveness of this combination.

Authors in [13] use a narrative approach in order to gamify educational content by creating several questions in the game. Each path motivates the player to reach to the end by knowledgeable background to get to the second phase. The authors assumed that narrative would help users to improve their motivation and engagement to create a deeper experience for a specific topic.

The Sustainable Gamification Design (SGD) framework presented in [14] is conscious of value creation benefits and value destruction risks. It is also human-centered and concerned about being ethically correct. The authors added drives of values and ethics in the gamification design that could be the center of the game and the motivation for employees in the organization to pursue.

In [15], the authors presented a framework which is dedicated to gamification of cyber security awareness. The framework is a set of practical steps that are considered as a guideline to develop and to evaluate serious games for cyber security awareness campaigns using a combination of different frameworks and platforms including the frameworks discussed in [16-19].

The 6D framework presented in [20] is the most practical framework providing a detailed guideline on how to create business-oriented motivational educational games. Through six main steps, the authors focus on the motivational factors and incentives to increase the level of engagement of employees and to adapt their behavior.

Through the discussion of the literature reviews, it's noticeable that the majority of gamified cyber security awareness training programs are actual games instead of applications of gamification. This is because most of the existing gamified cyber security awareness programs depend on general gamification frameworks which ignore the differences among target groups such as the age and the knowledge background.

III. Gamification Requirements for Effective Cyber Security Awareness

After reviewing the literature on gamification, two main dimensions of motivational factors emerge. The first dimension is the motivational factor which is used to enhance users' engagement level in order to achieve an educational objective. The second dimension relates to the methodology of implementing and deploying game-based learning. Most of the existing frameworks give more attention to the first dimension, while few frameworks involve the deployment methodology. In cyber security awareness, the deployment and implementation dimension are essential to the success of the gamified training.

In our proposed framework, we give attention to both dimensions while designing the steps of the serious game. In the next two subsections, we go in details of each dimension. After that, we combine them to form the comprehensive framework that can be used to develop gamified content for cyber security awareness

A. The Motivational Dimension

While developing serious games for cyber security awareness, one way to tell whether the developed game is effective or not is by checking if it triggers the player's emotions. For example, "Fun" is the representation of the best emotion that motivates a player to engage with the game. In addition to the positive emotions, such as competitiveness and achievement, negative emotions can be useful to engage players in the game. For example, frustration and disappointment after failing in the game would be a good incentive to play again in order to win. This consequently leads to enhanced learning of a specific topic.

For cyber security awareness, we believe that fear is the most suitable emotion to be used. The emotion of "Fear" will compel the player to do their best in learning and training in order to avoid the apparently bad consequences of their bad decisions. "Fear" will help in enhancing cyber security capabilities and skills in order to avoid bad consequences of their bad decision in case of facing cyber-attacks.

Therefore, the game must show the consequences of bad decisions in responding to cyber security situations. For example, the game should simulate the harmful effects and the number of losses resulting from the user's making bad decisions. In our implementation, we represent the fear by the countdown timer and by visualization of enemies

B. Deployment Methodology

In the deployment methodology, a comprehensive framework is designed in which a set of steps which have been extracted from existing frameworks and methodology and mixed with a newly designed time template resulting in generic and iterative steps which can be applied for most of gamified cyber security awareness content.

First, the framework should be able to evaluate and monitor the cyber security skill levels of the user. This will help in showing the knowledge acquisition progress in a quantitative way. Thus, in our framework, we adopt the idea of a pre-test and a post-test for better monitoring the progress. The objective of the pre-test and post-test is to enable the user to see their progress, which will positively motivation and encourage them to engaged in more advanced levels.

Furthermore, the game should not exceed a specified time. The time duration of the game should be configured according to the target groups. For example, gamified cyber security awareness for school students will have a 5 to 10 minutes duration. While for employees in organization, the game will have a 2-3 minutes duration. Moreover, the game should be deployed in a periodic manner; each time, the user will be updated with the result of the previous endeavor and the new progress level. The player should repeat the game in a periodic manner.

IV. Proposed Gamification Framework

After By reviewing the literature on using gamification to develop information security awareness training programs, we noticed that there is a lack in of a comprehensive framework that serves this purpose.

The proposed framework in this paper can be described as an incrementally monitored and evaluated progress of information security skills and capabilities acquired through the game.

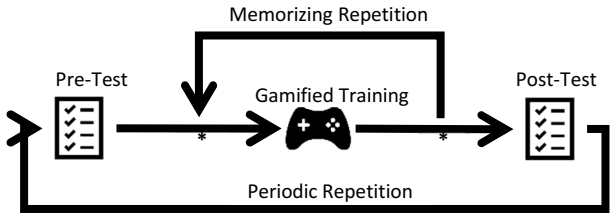

Fig 1: Proposed Gamification Framework.

The platform will allow the students (the players) to create their own accounts in their schools. The account will offer a set of serious games for different topics in cyber security such as password creation, phishing recognition, and other topics. Each game spans a short time (for example five minutes) that will be repeated periodically to enforce the acquired knowledge. The platform will evaluate the students' cyber security awareness level and classify it according to predesigned criteria. The platform will keep monitoring these levels through long periods in order to measure the progress of the students.

A. Pre-Test Phase

The objective of this phase is to measure the level of information security skills and capabilities by passing a test consisting of set of questions. These questions are multiple choice questions which are selected randomly from a database. Each user will have a different set of questions. The questions are grouped by level of difficulty. Each group of questions has almost the same set of questions with a different set of answers. The answers to the questions are close to each other. The objective is to enhance the concentration of the user to find the correct answer. The results along with the questions will be stored for each user in order to be used for timely analysis of the user's progress. In this phase, results will not be shown to the user. This is important to keep the user focused on the next level of the game and not be distracted by the result.

B. Gamified Training Phase

The user will be introduced to a set of instructions to learn about the components of the game and what to do in order to pass the game successfully. The user then starts to play the game. In our scenario, the game is developed as a maze that the main character (the cyber hero) will go through to reach to the closing door. During the walk, the user will collect a set of tips. Each tip gives an important hint on how to provide better security and will display for a while and then disappear. Once the cyber-hero collects all the tips and reaches the door, a pop-up window will appear. In this window the user will be tested on the knowledge provided in the tips in a very short time. In case of applying all the knowledge acquired from all the tips, the security level of the door will be upgraded by showing that the cyber-hero has won the game and the attacker in the surrounding area has lost the game. The case will be reversed if the player doesn't apply any of the tips. The game is designed to finish in a specific time interval (for example, in our testing configuration we set up the duration of the game to 90 seconds and it can be repeated a maximum three times to improve the retention of security information skills in memory). We believe that such a scenario will help in retaining the content of the tips in memory for a longer time.

C. Post-Test Phase

The last phase is another test with a list of questions that are very similar to the pre-test questions. The user will take the test and the result in this phase will be displayed to the user. This will help the user have a better feeling about winning and will show the difference between the pre-test and post-test levels. The framework will store the pre-test and post-test results for each user.

In our design, the framework will allow and encourage the users to repeat the game in a periodic manner which can be setup for different target groups.

V. Implementation and Testing

Currently, we developed a prototype (Demo) using Construct3 game development toolkit [22]. Construct3 is a fun and engaging tool for students to create games using HTML5 technology. In addition to the easy drag-and-drop tool, Construct3 improves game development by enabling writing several plugins and behaviors using JavaScript. Thus, the end users with machines having any type of operating system and any web browser can easily test and use our developed game.

The objective of our experimentation is to check the progress and enhancement of new password generation for different target groups. This will consequently help to measure and design the best criteria for improving information security skills and capabilities in general. For this purpose, a set of 30 students of different ages (between 9-22 years old) and different education levels (Primary schools, Secondary schools, Colleges/Universities) and different programs (from IT and non-IT programs) were selected to run our designed experiment. The experiment was run bimonthly for two months.

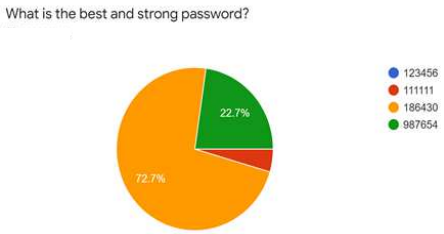

Fig 2: Post-Test sample question-Experiment 1

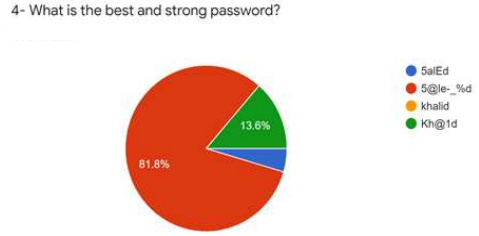

Fig 3: Post-Test sample question-Experiment 4

Each student was examined in the pre-test by a set of five questions from the same level of difficulty. Then, the student engaged in the serious game called Cyber-Hero, where the instructions in how to play the game are given through a conversation between the user (the cyber hero) and the attacker/hacker. As described earlier, the student collects a set of tips which are easily understandable and available in each password generation instructions. For example, tip 1 as is: "To generate strong password, add a combination of digits and characters."; and tip 2 is: "To generate a strong password, add a combination of alphabetic and non-alphabetic characters.". The students should avoid the spiders that affect the game negatively by removing the tip power from the hero. After collecting all the tips, the student must reach the door, in order to enforce the security by inserting a new password. The student must follow the instructions provided in the collected tips to win the game, otherwise the hacker will win the game and be able to enter the castle. Lastly, the student finalizes the experiment by passing the post-test and answering the questions which are like the pre-test questions

Fig 4: Demo Implementation

The Pre-test and post -Test answers samples are shown in the figure 2 and figure 3. The results reflect the improvement in the way of selecting the passwords. For example, in figure 2, we notice that the correct answer to the proposed questions got 72.2% of the total answers. After the same group of students repeated the game four times, the correct answers to a group of questions with a higher level of difficulty got 81.8% of the total answers. This was done by asking the same students to log into their account and play same game with a different set of questions.

The overall enhancement shows that an average of 5% improvement in selecting a stronger password was achieved. The main goal of the developed serious game is to use narrative instructions for setting a new password in a gamified manner. This achievement was accomplished in a period of two months. It is thus considered as a proof of concept that can be exploited in the future to generalize such gamified information security awareness training for long periods leading to better results.

VI. Conclusion and Future Work

The automation of many services in an organization will result in cyber security threats that will endanger the existing systems given the current human behavior in regard to information security. We believe that such a change needs, in addition to the great efforts in human resource, a time to be more effective.

In this paper we proposed a framework that would be able to change human behavior in information security at an early stage by targeting students in schools as we believe that the information risks become more and more challenging. The proposed solution will target one critical issue which is the password selection in case of creating new password or changing the old ones.

In our framework, gamification has proven to be successful in making the necessary changes in human behavior by combining fun and education for improving the selection of passwords as a case study to have more secure personal account in the digital world. We believe that the 5% improvement in a period of two months, can be generalized and raised by extending the period to a one year of framework implementation.

In our future work, we are going to have more designed experimentation to discover the exact criteria that affects the creation of passwords for different target groups. Furthermore, we are going to gamify some other critical issues which are usually included in information security awareness campaigns such as phishing and plagiarism. Our target groups will be mainly the schools' students, whom currently have less information security skills and capabilities, however they need it in the near future where there will be real risks.

Acknowledgment

The success and the final outcome of this research required a lot of assistance from many people and we are extremely thankful to the students: Shamma Hussain, Hessa Jassem, Hajar Yaqoub, and Hanan Yousuf from (Security and Forensics students in CIS department in HCT) for their support and assistance in the testing and collecting of the results for the research as part of the graduation work.

References

[1] Toth, P., & Klein, P. (2013). A role-based model for federal information technology/cyber security training. NIST special publication, 800(16), 1–152.

[2] [2] Bada, Maria, Angela M. Sasse, and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?." arXiv preprint arXiv:1901.02672 (2019).

[3] [3] Aldawood, Hussain, and Geoffrey Skinner. "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues." Future Internet 11, no. 3 (2019): 73.

[4] [4] Zulkurnain, A.U.; Hamidy, A.K.B.; Husain, A.B.; Chizari, H. Social engineering attack mitigation. Int. J. Math. Comput. Sci. 2015, 1, 188–198.

[5] Olusegun, O.J.; Ithnin, N.B. People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization. arXiv, 2013; arXiv:1309.0188.

[6] Abawajy, Jemal. "User preference of cyber security awareness delivery methods." Behaviour & Information Technology 33, no. 3 (2014): 237-248.

[7] Robson, Karen, Kirk Plangger, Jan H. Kietzmann, Ian McCarthy, and Leyland Pitt. "Is it all a game? Understanding the principles of gamification." Business Horizons 58, no. 4 (2015): 411-420.

[8] Werbach, Kevin, and Dan Hunter. For the win: How game thinking can revolutionize your business. Wharton Digital Press, 2012.

[9] Hamari, Juho, Jonna Koivisto, and Harri Sarsa. "Does Gamification Work?-A Literature Review of Empirical Studies on Gamification." In HICSS, vol. 14, no. 2014, pp. 3025-3034. 2014.

[10] Chou, Yu-kai. "Actionable gamification." Beyond points, badges, and leaderboards (2015).

[11] da Rocha Seixas, Luma, Alex Sandro Gomes, and Ivanildo José de Melo Filho. "Effectiveness of gamification in the engagement of students." Computers in Human Behavior 58 (2016): 48-63.

[12] Robson, Karen, Kirk Plangger, Jan H. Kietzmann, Ian McCarthy, and Leyland Pitt. "Is it all a game? Understanding the principles of gamification." Business Horizons 58, no. 4 (2015): 411-420.

[13] Marczewski, Andrzej. "Even Ninja Monkeys like to play." London: Blurb Inc (2015).

[14] Raftopoulos, Marigo. "Towards gamification transparency: A conceptual framework for the development of responsible gamified enterprise systems." Journal of Gaming & Virtual Worlds 6, no. 2 (2014): 159-178.

[15] Le Compte, Alexis, David Elizondo, and Tim Watson. "A renewed approach to serious games for cyber security." In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 203-216. IEEE, 2015.

[16] Winn, Brian M. "The design, play, and experience framework." In Handbook of research on effective electronic gaming in education, pp. 1010-1024. IGI Global, 2009.

[17] Mitgutsch, Konstantin, and Narda Alvarado. "Purposeful by design?: a serious game design assessment framework." In Proceedings of the International Conference on the foundations of digital games, pp. 121-128. ACM, 2012.

[18] Arnab, Sylvester, Theodore Lim, Maira B. Carvalho, Francesco Bellotti, Sara De Freitas, Sandy Louchart, Neil Suttie, Riccardo Berta, and Alessandro De Gloria. "Mapping learning and game mechanics for serious games analysis." British Journal of Educational Technology 46, no. 2 (2015): 391-411.

[19] Nadolski, Rob J., Hans GK Hummel, Henk J. Van Den Brink, Ruud E. Hoefakker, Aad Slootmaker, Hub J. Kurvers, and Jeroen Storm. "EMERGO: A methodology and toolkit for developing serious games in higher education." Simulation & Gaming 39, no. 3 (2008): 338-352.

[20] Werbach, Kevin, and Dan Hunter. The gamification toolkit: dynamics, mechanics, and components for the win. Wharton Digital Press, 2015.

[21] Nadolski, Rob J., Hans GK Hummel, Henk J. Van Den Brink, Ruud E. Hoefakker, Aad Slootmaker, Hub J. Kurvers, and Jeroen Storm. "EMERGO: A methodology and toolkit for developing serious games in higher education." Simulation & Gaming 39, no. 3 (2008): 338-352.

[22] https://www.construct.net/en

[23] Scholefield, Sam, and Lynsay A. Shepherd. “Gamification Techniques for Raising Cyber Security Awareness.” Lecture Notes in Computer Science (2019): 191–203. Crossref. Web.

[24] Coull, N., Donald, I., Ferguson, I., Keane, E., Mitchell, T., Smith, O. V., ... Tomkins, P. (2017). On the use of serious games technology to facilitate large-scale training in cybercrime response. European Police Science and Research Bulletin, Special Conference Edition(3), 123-130.

[25] Jin, Ge & Tu, Manghui & Kim, Tae-Hoon & Heffron, Justin & White, Jonathan. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. Journal of Education and Learning (EduLearn). 12. 150. 10.11591/edulearn.v12i1.7736.

[26] S. Tang and M. Hanneghan, “A Model-Driven Framework to Support Development of Serious Games for Game based Learn.

[27] Canova, Gamze & Volkamer, Melanie & Bergmann, Clemens & Borza, Roland. (2014). NoPhish: An Anti-Phishing Education App. 188-192. 10.1007/978-3-319-11851-2_14.