Grenze International Journal of Engineering and Technology, June Issue

Application of Gamification for Cyber Security Awareness

Prajakta Subhash Jagtap[1] and Dr. Manish Potey[2]
[1-2]K J Somaiya College of Engineering, Department of Computer Engineering, Mumbai-77, India
Email: Prajakta.jagtap@somaiya.edu, manishpotey@somaiya.edu

***Abstract*—With the expansion of technology and therefore the accessibility to the web within the recent decades, people are now connected across countries. Internet-enabled interconnectivity of ICT assets is increasingly adopted worldwide. Despite the benefits, threats to organizational assets are just around the corner. The vulnerability to such threats is increased when employees working with ICT systems are unaware of cyber security. Cybersecurity in itself includes the protection of frameworks, systems and projects from computerized assaults. There are several ways to raise cyber security awareness, but the increasing number of cyber security incidents suggests that these methods lack effectiveness. Gamification offers promising results due to its ability to counter several weaknesses of existing trainings, for example related to motivation and engagement. It is presumed that incorporating gamification in cyber security awareness trainings could increase their effectiveness.**

This paper evaluates the various game-based learning system in cybersecurity, identifying the varied tools exist, the advantages and shortcomings of every system and feasible ways to enhance on the prevailing systems. Thus, in this research, I would like to develop an alternative and joyful way to educate and encourage people to learn more about the security awareness. I develop a game, which is a security game for building security awareness by using Unity.

***Index Terms*— cyber security awareness, Attacks, Unity, gamification, framework design.**

I. INTRODUCTION

Security awareness is extremely important for Internet users. However, most of the people think that it's very technical and too difficult for them to know and understand. Moreover, they also consider that the knowledge of security cannot apply to their career or personal life. Consequently, they plan to ignore the importance of security awareness. In another perspective, people do not care about the harmful impacts that can come from the lack of security awareness. People do care only about their convenience when they are using the Internet. With this absolutely wrong perception, people unaware to share their personal information to malicious users or hackers.

Information, communication, and technology (ICT) is one of the most fast-paced fields in current societies all over the world [2]. Organizations are increasingly connecting their key ICT assets to the internet, which has several benefits. Business processes can be automated, communication is quicker, information can be stored more effectively. There is a constant increase in the estimated losses from cyber espionage and cyber-crime which results to billions every year. With the evolvement of the various disciplines over time, there is a constant shift in the view of threats and vulnerabilities in cybersecurity today. However, the interconnectivity poses

Grenze ID: 01.GIJET.8.2.7

increased or new risks, for example due to the introduced remote access. These risks are increased when employees who work with the ICT systems are unaware of proper behaviour or lack the required knowledge and skills in order to do this. Raising cyber security awareness seems easier said than done considering the vast amount of cyber related incidents, for instance severe data leaks of privacy sensitive information, ransomware that interrupts entire business processes and successful hacks targeting various corporations or critical infrastructures. All these incidents contained a human error that could have been prevented by sufficient cyber security awareness.

II. Literature Survey

A. Cyber Security

Cyber security refers to the body of technologies, processes, and practices designed to guard networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity is often described because the harmonization of capabilities in people, processes, and technologies; to secure and control both authorized and/or unlawful access, disruption, or destruction of electronic computing systems (hardware, software, and networks), the data and information they hold Thus, the triad of cyber security consists of people, processes and technologies.

TABLE I: TYPES OF ATTACKS

Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following • distributed denial of service attacks • impair or deny access to a service or application • resource depletion attacks
Malware	Any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.
Hacking	An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include − • data-leakage attacks • injection attacks and abuse of functionality • spoofing • resource manipulation • stolen credentials usage • backdoors • dictionary attacks on passwords • exploitation of authentication
Social Engineering	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes − • pre-texting (forged surveys) • inciting phishing • retrieving of information through conversation

B. Gamification Approach for Cyber Security Awareness

One of the key reasons behind lacking cyber security awareness in many organizations is the severe shortage of specialists regarding cyber security [2]. Next, it is often difficult for organizations to distinguish what knowledge and skills are relevant to raise cyber security awareness of its employees and how to do this effectively by training

Cyber security awareness can be defined as thoughtfulness on security, enabling individuals (workforce employees and managers) to recognize security concerns and respond accordingly [2].

An additional definition of cyber security awareness is assessing the level of vulnerabilities in an entity, while providing participants with general knowledge in detecting and avoiding successful penetration attempts [2]. This definition differs from previous definition due to its adversarial perspective. A definition of cyber security awareness that widens this perspective is the ability of the user to recognize or avoid behaviours that would compromise cyber security; practice of good behaviours that will increase cyber security; and act wisely and cautiously, where judgment is needed, to increase cyber security.

In one of the research papers authors classified the games in 3 categories with their advantages and disadvantages. Based on this following table is generated.

TABLE II: CATEGORIES OF GAMES

Categories	Category 1 (Theoretical Approach)	Category 2 (One Player Game)	Category 3 (Multi Player Game)
Definition	This category involves only the theoretical description of themes and concepts of cybersecurity without a representation of the actual gameplay.	This category involves the games played by one person where the individual would be tested based on the understanding of cybersecurity concepts introduced in the application.	-This category involves more than one player where the individuals were tested based on the understanding of cybersecurity concepts introduced in the application. -It involves competition between different individuals or teams with reward-based outcomes.
E.g. of games	Control-Alt-Hack, Stop That Post and Shadow [15]	CyberProtect, CyberAware, Phish Guru, CyberCIEGE	CyberNEXS, InCTF, GenCyber and SecurityCom
Advantages	Increased awareness of risks involved in computer security and career opportunities associated with it.	-User friendly interface for interaction with learner -Clear cut objectives for the learner to get familiar with the concept of cybersecurity. -Guaranteed result of instant feedback for improved learning.	-It allows for increased situational awareness -It is flexible, scalable and highly interactive.
Disadvantages	-Longer assimilation time. -Inadequate pedagogical content.	Overtime it becomes a monotonous activity as it becomes less challenging to the learner involved.	It can be time consuming as it involves input from. different individuals or teams.

III. DESIGN DETAILS

A. Design of Cyber Security Framework

Step 1: **Analyze** needs and objectives to develop a cyber security awareness program.
Step 2: **Plan** your program stay on track and engage your workforce.
Step 3: **Deploy** an effective training/ program and observe behaviour changes that happen.
Step 4: **Measure** the performance of your program.
Step 5: **Optimize** campaigns accordingly and update program to incorporate new sight.
Fig I. represents the framework.

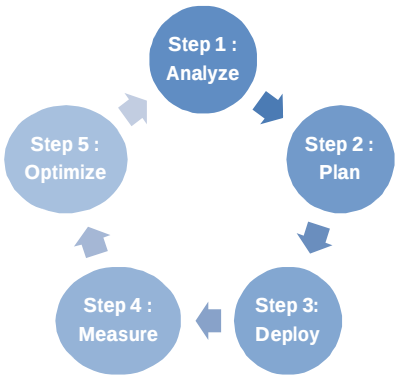

Fig 1: Cyber Security Awareness Framework

B Game Story

Our player has to learn more about security awareness through this game. In level 1 character has to collect good passwords if bad password collected points will be decreased. A character can save itself from many obstacles and can fire also. If it collects stars will get bonus points. In the left corner it shows bonus, points and timing also. In level 2 character named cyber girl has to collect 3 points for anti-phishing tips. As character collecting

more coins in the multiple of 3 it will get more tips. If cyber girl die because of any obstacle then this level can be replay by using restart option. In level 3 user has to spin the wheel named “Wheel of Security” then pointer will stop at one of the numbers from 1-12. Then it will display tip regarding malware protection.

C. System flow

First user has to complete the Pre-Quiz which contains basic question about cyber security then from the main screen we have to select one of the levels. From key help options user can see keyboards options to play level 1. From other options you can play level 2 and level 3. After finishing the level 3 user have to complete Post Quiz. Each quiz contains multiple choice questions and user need to answer it. Scores and time of each quiz’s is displayed in right corner. Each question carries ten marks. This chapter focused on different phases in the proposed system. Fig II. Shows System’s Flow.

IV. IMPLEMENTATION DETAILS

A. Hardware and Software Requirements

Table III shows the hardware and software specifications of game.

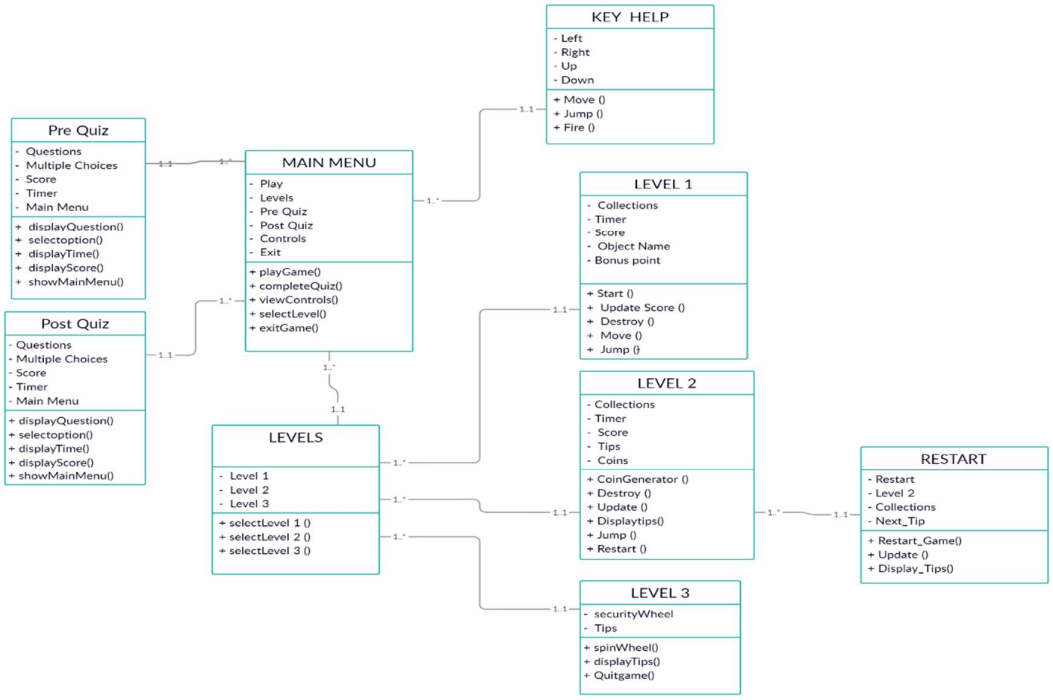

Fig 2: system’s flow

TABLE III: HARDWARE SOFTWARE REQUIREMENTS OF SYSTEM

Component	Specifications
Development Hardware	• CPU: Intel Core i7-6700 3.40GHz • GPU: Nvidia GeForce GT 730 • Memory: 8 GB
Operating System	Microsoft Windows 10 (64-bit)
Editor	Microsoft Visual Studio Community 2017
Graphics Developing Tools	Adobe Illustrator CC 2017 Adobe Photoshop CC 2017
Sound Developing Tools	GarageBand Audacity
Game Development Engine	Unity 2017

B. Software Details

1. Unity (Game Engine)

Unity is a cross-platform game engine developed by Unity Technologies, first announced and released in June 2005 at Apple Inc.'s Worldwide Developers Conference as a Mac OS X-exclusive game engine. As of 2018, the engine had been extended to support quite 25 platforms. The engine can be used to create two-dimensional, three-dimensional, virtual reality and augmented reality games, as well as simulations, movies and other experiences. The engine has been adopted by industries outside video gaming, like film, automotive, architecture, engineering and construction. Several major versions of Unity have been released since its launch. The latest stable version, 2019.3.1, was released in February 2020. Unity gives users the power to create games and experiences in both 2D and 3D, and hence the engine offers a primary scripting API in C#, for both the Unity editor in the form of plugins, and games themselves, also as drag and drop functionality. Prior to C# being the first programming language used for the engine, it previously supported Boo, which was removed with the discharge of Unity 5, and a version of JavaScript called UnityScript, which was deprecated in August 2017, after the release of Unity 2017.1, in favour of C#. Within 2D games, Unity allows importation of sprites and a complicated 2D world renderer. For 3D games, Unity allows specification of texture compression, mipmaps, and determination settings for each and every platform that the game engine supports and provides support for bump mapping, reflection mapping, parallax mapping, screen space ambient occlusion (SSAO), dynamic shadows using shadow maps, render-to-texture and full-screen post-processing effects. As of 2018, Unity has been used to create half of the new mobile games on the market and 60 percent of augmented reality and computer game content.

2. Visual Studio Community (Editor)

A fully-featured, extensible, free IDE for creating modern applications for Android, iOS, Windows, as well as web applications and cloud services.

Features:

- Lightweight and modular installation
- Cloud-connected
- Powerful coding tools
- Advanced debugging
- Web tools
- Access to free tools and resources

V. RESULTS

Figure III represents scores of Pre-quiz and Post-quiz of group-I i.e. group of students.
Figure IV represents scores of Pre-quiz and Post-quiz of group-II i.e. group of faculties.
Figure V represents scores of Pre-quiz and Post-quiz of group-III i.e. group of employees.

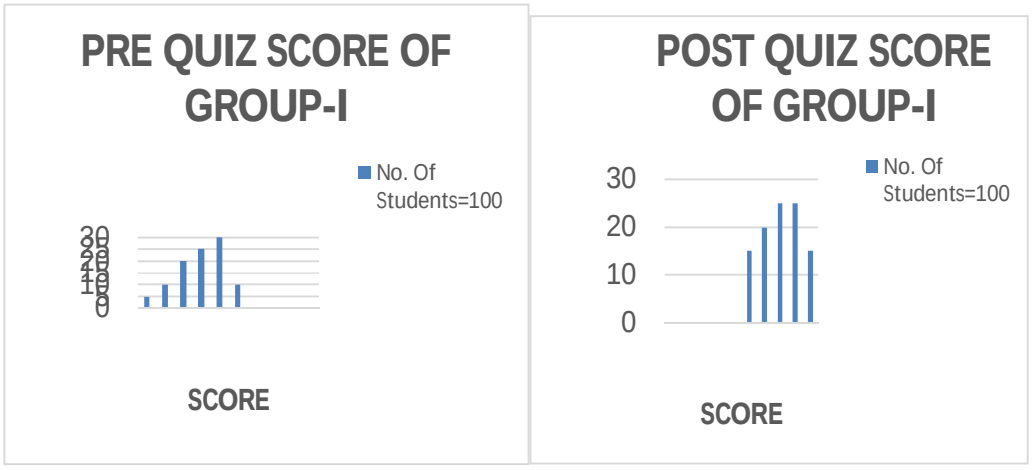

Fig 3: Pre-Quiz and Post-Quiz scores of Group-I

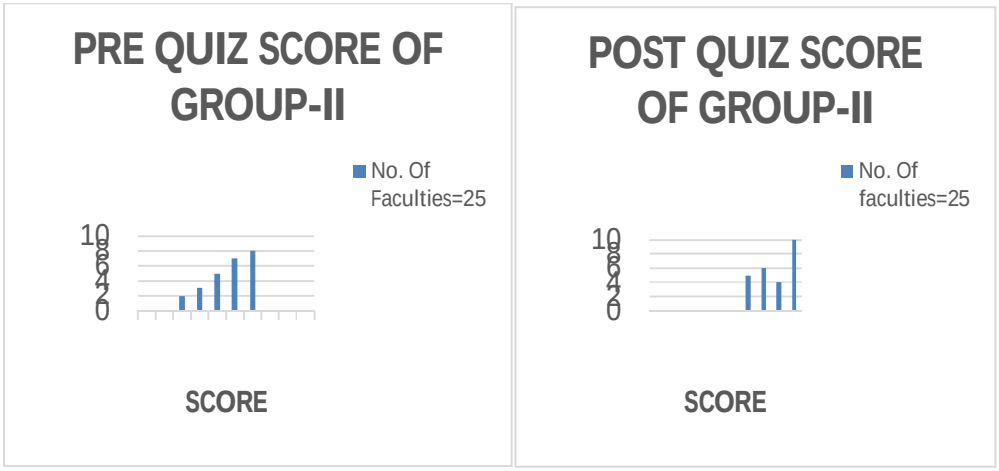

Fig 4: Pre-Quiz and Post-Quiz scores of Group II

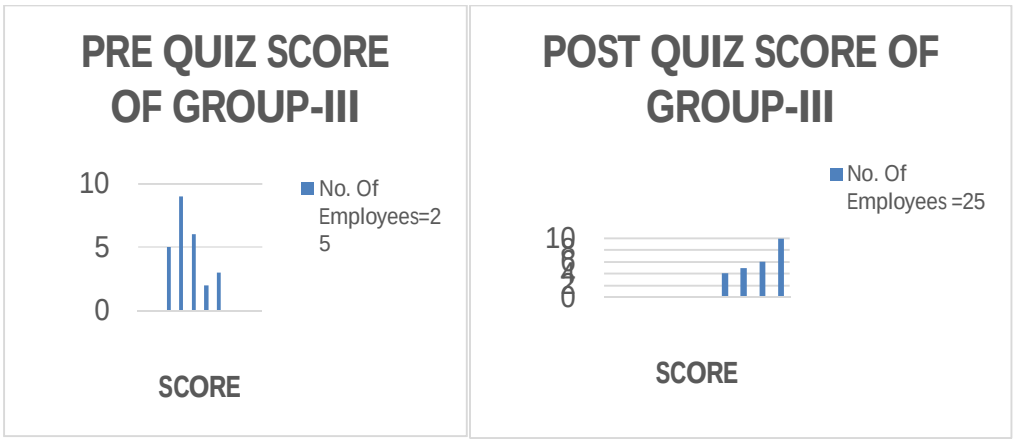

Fig 5: Pre-Quiz and Post-Quiz scores of Group III

VI. Conclusion

Cybersecurity plays a prominent role in the society today. According to literature studies, gamification concepts for the purpose of raising cyber security awareness are more effective. Incorporating games into learning has proven to improve the learning outcome overtime. Valid tools have been developed to consolidate and enhance learning. The multiplayer game approach can be identified as one of the best interactive mediums for GBL with more advantages and less disadvantages. We evaluated effectiveness of this gamification approach over existing materials with three groups of users and noted that they enjoyed this approach and gained knowledge about cyber security. Gamifying education provides a more enjoyable experience for every learner and it gives them a reason to take a personal interest in their education. Gamifying cybersecurity training motivates employees to play an active role in preventing cyber threats at your organization.

Acknowledgement

I wish to express my deep sense of gratitude to my guide Prof. Dr. Manish Petey sir for his valuable and firm suggestions, guidance, encouragement and constant support throughout this work without which it would not be possible to do this work. He took deep interest in checking minute details of the Report and guided me throughout the year. He has been constant source of inspiration.

I would also like to thank the experts namely Prof. Dr. Dipak Sharma and Prof. Dr. Siddappa Bhusnoor who were involved in the validation survey for this research project. Without their passionate participation and input, the validation survey could not have been successfully conducted.

I would like to express my sincere gratitude towards my parents, my family and friends, for always being there with me. With all respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly. Without their silent support and encouragement for this work could not have been possible.

REFERENCES

[1] Awojana, Tolulope, and Te-Shun Chou. "Overview of Learning Cybersecurity Through Game Based Systems." 2019 CIEC (2019).
[2] Rieff, Iris. "Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach." (2018).
[3] Visoottiviseth, Vasaka, et al. "POMEGA: Security Game for Building Security Awareness." 2018 Seventh ICT International Student Project Conference (ICT-ISPC). IEEE, 2018.
[4] Lika, Reyner Aranta, et al. "NotPetya: cyber attack prevention through awareness via gamification." 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE). IEEE, 2018.
[5] Yonemura, Keiichi, et al. "Practical security education on operational technology using gamification method." 2017 7th IEEE International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, 2017.
[6] Alotaibi, Faisal, et al. "A review of using gaming technology for cyber-security awareness." Int. J. Inf. Secur. Res.(IJISR) 6.2 (2016): 660-666.
[7] Boopathi, K., S. Sreejith, and A. Bithin. "Learning cyber security through gamification." Indian Journal of Science and Technology 8.7 (2015): 642-649.
[8] Le Compte, Alexis, David Elizondo, and Tim Watson. "A renewed approach to serious games for cyber security." 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. IEEE, 2015.
[9] Sheng, Steve, et al. "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish." Proceedings of the 3rd symposium on Usable privacy and security. 2007.
[10] CONE, BENJAMIN D., ET AL. "A VIDEO GAME FOR CYBER SECURITY TRAINING AND AWARENESS." COMPUTERS & SECURITY 26.1 (2007): 63-72.