Article 4

Cybercrime Awareness: Development and Evaluation of an Adventure Game

Aznoora Osman, Nurul Syarafina Azizan
Faculty of Computer and MathematicalSciences
Universiti Teknologi MARA Perlis Branch, Malaysia

Abstract
This paper discusses the design and development of an adventure game about cybercrime. This game uses variety of multimedia elements including text, animation, image and 3D objects. The theme of this game focuses on identity theft and phishing. Therefore, the purpose of the game is to educate the learners about cybercrime and enhance their awareness towards online activities that could victimized them. This would ensure that they take precautions of their safety while using the Internet. In this research, agile method is used as the development methodology. It includes five phases which are brainstorm, design, development, quality assurance and deployment. The completed game was used as a treatment in a user testing involving 26 students from UiTMCawangan Perlis from different ages, gender, course and faculty. After treatment, subjects were administered with two instruments to measure their perception of awareness towards cybercrime and their perception of fun for the game. It was revealed that most subjects agreed that they had an increase in awareness after exposure to the game. The game was also positively perceived as fun, with regards to its graphical and instructional design, contents relevance with the theme and suitability of game duration. Some recommendations for future enhancements are also discussed.

Keywords: *Gamification, Cybercrime, Awareness, Phishing, Identity Theft.*

Introduction

Gamification describes the broad trend of employing game mechanics to non-game environment such as innovation, marketing, training, employee performance, health and social changes (Arnold, 2014). Gaming techniques in educations are very helpful in learning wider, longer and deeper ways, which in turn could help to motivate and improve learning performance (Morillas Barrio, Munoz-Organero, & Sanchez Soriano, 2016).

The internet and technology are going fast along the growth of living people and almost all the people relying on the machines (Dashora & Patel, 2011). As of 2015, Internet users in Malaysia, including those in urban and rural areas, have reached 20.1 million people(BERNAMA, 2016). With Internet connectivity, users gain benefits that enrich their lives, communication, entertainment, education and information seeking. Nevertheless, Internet also poses a threat to the community, for example exposure to cybercrime. Cybercrime is characterized as an expected demonstration including the utilization of PCs or different innovations and the criminal action must happen in a virtual setting (Singleton, 2013). Five cases of cybercrimes are duty discount extortion, corporate record takeover, fraud, robbery of touchy information and burglary of licensed innovation (Singleton, 2013). Cybercrime issue develops as fast as the progress of technology and the number of attacks increase sharply; however, many people are unaware how to protect themselves (Weber, 2009).

In Malaysia, 95% of parents are worried about their children safety online, with 60% of them admitted that their kids were cybercrime victims and 48% acted on their fears (Chin, 2016).

Manasrah, Akour, & Alsukhni, (2015) revealed that university students were not only the victims of cybercrime, but they were also the cyber attackers.

Therefore, there is urgent need to educate university students about cybercrime so that they could protect themselves from becoming the victims or the criminals. An adventure game is deemed the most suitable technique because gamification system increases student motivation (Domínguez, Saenz-de-navarrete, & Pagés, 2014) and games promote creativity and productivity during learning, through reward and badges in the games (Herro & Clark, 2016).

This project employs a game based learning to educate learners via computer games. The game was developed using software called Unity 3D. The development methodology used for this project is agile method. The game was then used as a treatment with target users to test its effect towards perception of awareness and perception of fun. The data was collected by using an awareness instrument and a fun evaluation instrument.

Methodology

Based on research carried out in early 2014, the methodology phase found by Rickinson& May (2009) are scoping, searching, selecting, analyzing, synthesizing and reporting were used in developing gamification (Caponetto, Earp, & Ott, 2014). For this project, agile method was chosen to develop an adventure game.

Agile method is focusing on fast production in working code and it is incremental development software ("Assumptions Under lying Agile Softwar e Development Pr ocesses," 2005). Steps involved in agile methodology are brainstorm, design, development, quality assurance and deployment.

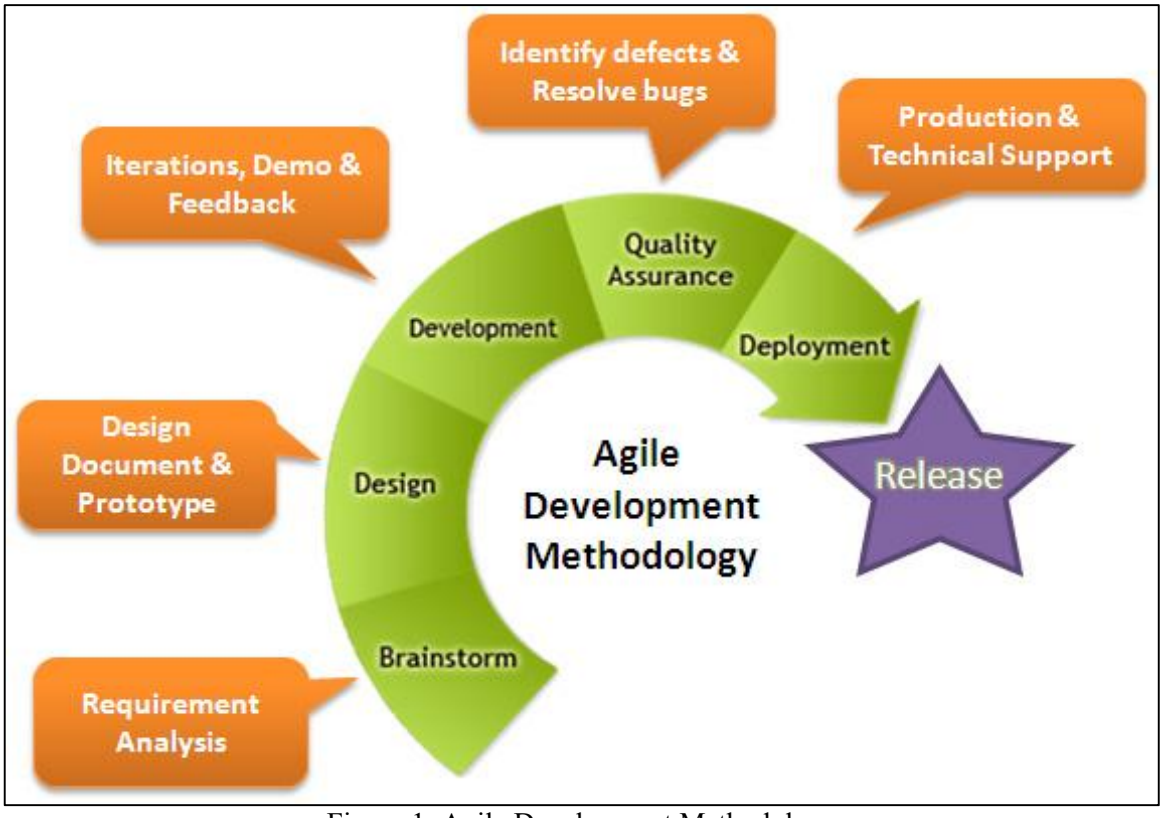

Figure 1: Agile Development Methodology

a) Brainstorm

In this phase, it focuses on defining the topic, identifying the problem statement, objective, and scope of the project. The method that was used is to find related journals and articles about cybercrime, gamification, educational learning and online safety. The deliverables are problem statement and current issues of the project topic and aims and objective. Also, relevance tree and the related table were formed.

b) Design

This phase includes design document. For the design, the document needs to developing the initial content idea, storyboard was created for the project flow, plan the task for challenges in the games and prepare a script. For developing the initial content idea, a framework from Nah et.al was adapted for this project development. In this project, C# will be used for the script language in Unity 3D. The deliverables for this phase are the interface design, storyboard, and contents related to cybercrime.

c) Development

In development phase, the project has been developed by using a software named Unity 3D and Adobe Photoshop. Both of the software use for graphic and multimedia purpose. The hardware requirement is a computer processor Core i5, RAM size is 4.00 GB and windows edition is Windows 10 Pro which can support this project. The user also has to give a feedback after using an application. The method for measure a feedback is use fun evaluation which measures how much fun one's having or had while playing games. The deliverable is cybercrime awareness the educational games for university students.

d) Quality Assurance

Quality assurance means to identify defect and resolve bugs. This phase follows the development phase so that improvement can be done for this game application. The method uses for identifying defect and bugs through usability test. After finding the defect and bugs, a developer has to improve and update the application. The deliverable is updated and improve the project.

e) Deployment

The last phase in agile development methodology is deployment which means updated and fix the defects or error before. After fixing all the errors and defects, the application is ready to use. The adventure game about prevention of cybercrime is ready to be released. This phase also includes documentation project. All the documents from the first phase has been documented in detail by using Microsoft Word and Mendeley for reference manager.

Game Environment and Contents

The game environment was designed to resemble an actual office that is equipped with common office furnitures and computers. The main screen has a cartoon-like background image of a police officer holding a magnifier to scheme through a person who is portrayed as a cybercriminal. There is a button labeled “Play Now” that brings the player to a 3-D game scene. In this scene, players could view how to play the game by choosing the “How to Play” button. It gives instructions about specific keyboard keys to be used, and the role of mouse to control the movement of the actor.

Rules and mission of the game are presented in dialog callouts to mimic a conversation between a spy and the boss. The mission of the game is to catch a cybercriminal. The prime suspect is described by the boss to be one of the employees at the office. The suspect is not known by the players; however, it is their mission to correctly identify the employee, by embarking on the exploratory journey.

The game uses exploratory approach to complete the mission. The players embark on an adventure to capture a cybercriminal. The game requires players to maneuver around an office space, hit certain animated objects and answer the corresponding questions pertaining to identity theft and phishing, which are two of the most common cybercrimes. The answers were in multiple choice. Players would earn some points to their score when they answer each question correctly. The instructional contents were subtly embedded into the game via these questions. With every answer (correct and incorrect), it comes with a hint of who the criminal is. A correct answer entitles the players to a worthier hint, while an incorrect answer leads to vague hint. To proceed with the journey, players with incorrect answer were enforced to keep on choosing the answer until they get it right. The purpose is to make sure that they gain some understandings about cybercrime while playing. There is also a time countdown that indicates the remaining time to complete the mission. The game was developed to be accomplished within 10 to 15 minutes. This is to ensure players motivation and interest to complete the game is maintained.

Towards the end of the game, players are required to identify the criminal by choosing a picture of an employee from all pictures in the screen. With correct answer, players are congratulated and given a trophy image on the screen, as well as a display of score points. Additionally, an image of the criminal is portrayed to be miserably locked up in prison. The game can be played again by hitting the “Play Again” button, or hitting the “X” button to exit from the game.

User Testing and Findings

An experiment with a sample of target users was conducted with 26 students from UniversitiTeknologi MARA (UiTM) Perlis Branch, who were enrolled in different courses, aged between 19 and 21 years old. The researchers, who acted as the facilitators, started the session with a brief introduction about the experiment, the game contents and the instruments that subjects were supposed to answer. The session took about 50 minutes, where 5 minutes was allocated for briefing, 5 minutes for subjects to explore the game before actual treatment started, 30 minutes for treatment (playing with the game) and 10 minutes for subjects to answer the instruments. As a token of appreciation, all participants were presented with small gifts after completing the session.

The purpose of awareness evaluation was to discover end user’s opinion and awareness of issues in cybercrime, mainly identity theft and phishing. The purpose of fun evaluation was to evaluate the game with regards to its design, contents and play duration. It was employed to discover subjects’ perception of fun after playing with the game. Table 1 describes the analysis of results for both instruments.

Overall, it was revealed that the game received positive response for its ability to enhance level of awareness about cybercrime. Before exposure to the game, about 65% of subjects were not aware about cybercrime issues. After treatment, about 80% of subjects agreed that their awareness has increased. This could be an indicator that game based learning has an impact in enhancing general knowledge among its users/players. Meanwhile, for fun evaluation, every item received convincing response, with more than 50% of subjects agreed and strongly agreed

to the statements, such as the clarity of instructions, contents that complement the theme, suitability of graphics/illustrations and duration of the game.

Table 1: Description of User Testing and Results – Awareness and Fun

Items	Analysis
Before playing the game, were you aware about the cybercrime issues?	65.4% of the respondents vote for yes and 34.6% vote for no about their awareness on cybercrime issues before playing the game.
After playing the game, have your awareness increased?	38.5% of the respondents strongly agreed, 42.3% agreed, 7.7% neither agreed nor disagreed and 11.5% disagreed about the increased of awareness level.
The instructions given are clear	38.5% of the respondents strongly agreed, 26.9% agreed, 30.8% neither disagreed nor agreed and 3.8% disagreed the instruction given is clear.
The game test my general knowledge about cybercrime	65.4% of the respondents strongly agreed, 30.8% agreed and 3.8% disagreed the game test their general knowledge about cybercrime.
I like the graphics/illustration	7.7% of the respondents strongly agreed, 46.2% agreed, 30.8% neither agreed nor disagreed and 15.4% disagreed that they liked the illustration or graphics.
How many minutes did it take you to finish the game?	76.9% of the respondents answered below then 10, 19.2% between 10 to 20 minutes and 3.9% is between 21 to 30 minutes.
Was the game too short, too long or just right?	57.7% of the respondents thinks the game was just right, 38.5% it is too short and 3.8% too long.
How much did you like the game?	7.7% of the respondents strongly agreed, 46.2% agreed, 30.8% neither agreed nor disagreed and 15.4% disagree about their feeling towards the game.
Were the questions in game related with the theme?	96.2% of the respondents chose yes and 3.8% chose no.

Some recommendations were given by subjects, as enhancements in future work. These includes adding relevant background sound to trigger excitement to complete the game, enlarging the game window and reducing the walking speed of the actor in the game so that players could keep pace.

Conclusions

As a conclusion, the study has achieved it objectives which are to identify the issues in cybercrime, to investigate the gamification framework to support the development of the project, to develop adventure game about cybercrime, to evaluate the game effectiveness in enhancing awareness of cybercrime and to measure in terms of fun evaluation. 3D animated objects, graphics (such as buttons, background image, characters image), texts and spoken sound were successfully integrated into the game. All the multimedia elements have purpose to gain attention from the players and to sustain their motivation. In addition, it enriched the learning experience while playing the game. It can be concluded that, despite some of its shortfall, the exploratory game has demonstrated its capability to create awareness about serious issue like cybercrime.

References

Assumptions Under lying Agile Softwar e Development Pr ocesses. (2005), *16*(4), 62–87.

Caponetto, I., Earp, J., & Ott, M. (2014). Gamification and Education: A Literature Review. *Proceedings of the European Conference on Games Based Learning*, *1*(2009), 50–57. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84923559781&partnerID=tZOtx3y1%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=eue&AN=99224935&site=ehost-live

Dashora, K., & Patel, P. P. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240–259.

Domínguez, A., Saenz-de-navarrete, J., & Pagés, C. (2014). Computers & Education An empirical study comparing gami fi cation and social networking on e-learning. *Computers & Education*, *75*, 82–91. https://doi.org/10.1016/j.compedu.2014.01.012

Herro, D., & Clark, R. (2016). An academic home for play: games as unifying influences in higher education. *On the Horizon*, *24*(1), 17–28. https://doi.org/10.1108/OTH-08-2015-0060

Manasrah, A., Akour, M., & Alsukhni, E. (2015). Toward improving university students awareness of spam email and cybercrime: Case study of Jordan. *2015 1st International Conference on Anti-Cybercrime, ICACC 2015*. https://doi.org/10.1109/Anti-Cybercrime.2015.7351955

Morillas Barrio, C., Munoz-Organero, M., & Sanchez Soriano, J. (2016). Can Gamification Improve the Benefits of Student Response Systems in Learning? An Experimental Study. *IEEE Transactions on Emerging Topics in Computing*, *4*(3), 429–438. https://doi.org/10.1109/TETC.2015.2497459

Singleton, T. (2013). The top 5 Cybercrimes, (October), 17.