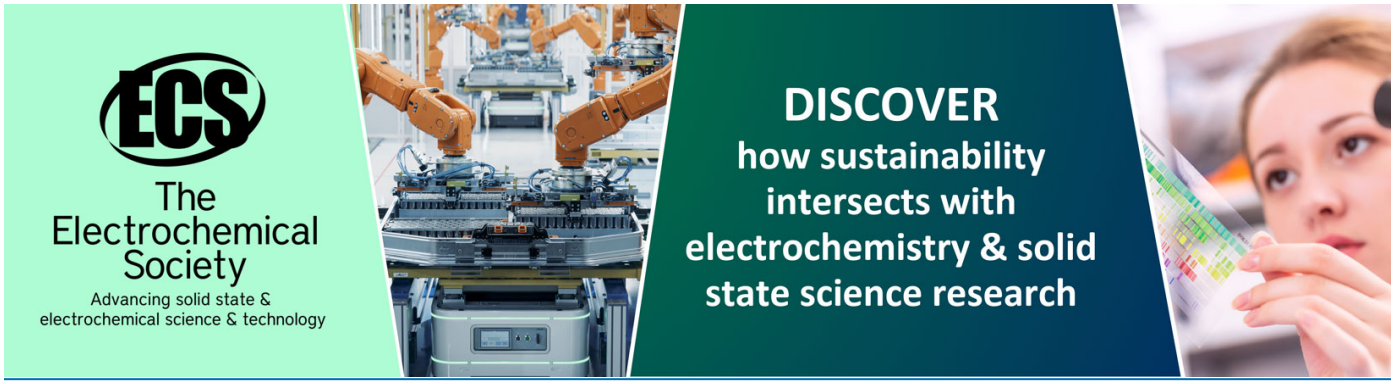
Malware Awareness Tool for Internet Safety using Gamification Techniques



Malware Awareness Tool for Internet Safety using Gamification Techniques

[1]Nurul Suraya Omar, [2]Cik Feresa Mohd Foozy, [3]Isredza Rahmi A Hamid, [4]Hanayanti Hafit, [5]Adila Firdaus Arbain, [6]Palaniappan Shamala

[1,2,3,4]Faculty Computer Science & Information Technology, University Tun Hussein Onn Malaysia, Johor, Malaysia.

[5]School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia.

[6]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Johor, Malaysia.

surayaomar1990@gmail.com, feresa@uthm.edu.my.

Abstract. Malwares are detrimental to those who are ignorant of their existence. However, the adverse effects of malwares can be easily avoided by being aware of Internet safety. In this paper, a malware awareness tool targeted for university students was developed. The Game Development Lifecycle (GDLC) model was applied in developing this tool. The tool development phase began with initiation, then pre-production, production, testing, beta testing, and ended with the release phase. Once the malware awareness tool was developed, functionality tests and awareness level tests were conducted on university students to ensure the tool is fully operative. Through the tests, it was shown that this tool was received with positive responses from its target users. As for the awareness level test, a majority of 15 students were aware of the purpose of the gamification in the malware awareness tool. In a nutshell, the malware awareness tool that was developed raised university student's consciousness on malwares and increased their awareness level pertaining to Internet threats.

1. Introduction

Nowadays, the Internet is a must-have and a necessity for every human being. The Internet being a medium that helps people with their daily affairs for purposes such as communication, business, entertainment, and so on. With the use of the Internet, everyday transactions become more accessible.

However, technology advancement exposes people to oblivious dangers and threats. With the increase in use of the Internet technology, cyber crime has also increased [1]. Cyber crime and cyber attacks exist in various forms and it is the responsibility of the Internet user to take their own precautionary steps in avoiding possible cyber attacks. Therefore, a proper guideline on Internet safety is needed to reduce the possibility of such attacks.

Creating awareness via modes such as campaigns, hands-on quizes or educational gamification are commonly used to raise awareness on Internet safety. Such awareness efforts are effective when created with a specific target group of Internet users in mind. Hence, this project focussed on the development of a malware awareness tool using the gamification techniques to increase malware awareness among university students. Such awareness would enable university students to defend themselves against online threats, especially in regards to malware issues.

In this project, the gamification technique is used to implement the awareness tool. By definition, gamification is the application of games that may be used in terms of competition, rewards, quantifying of player or user behaviour into a non-game context [2].

The gamification technique is used as it is a more effective learning tool compared to campaigns or quizzes. In fact, gamification as a tool to expose students to an active learning process is not a new learning tool. Gamification techniques have been implemented widely in developed nations, especially to address the knowledge on cyber safety [3]. As a result, a fun and engaging learning environment for students is achieved.

As Internet safety issues are not new, actions must be taken to avoid falling victim to cyber attacks. It is found that youngsters or university students primarily became victims of such threats. Although many websites display information security protection on the Internet, those information are insufficient. The topic of Internet safety or online safety, cyber safety and cyber security is vast and also covers the issues of behavioural actions by Internet users when online. Hence, security organizations must also improve their cybersecurity efforts to be ahead with the current threats to reduce the possibility of cyber threats to Internet users.

According to the statistic on cyber attacks**,** cyber crimes increased in 2017 compared to 2016[1]. Current increasing cyber crimes are phishing, spam emails, cyberbullying, identity theft, malware and more. Cyber crime can happen when people share confidential information such as phone numbers, identity card numbers, passwords, and personal information for purposes such as Internet banking transactions, account updates and others.

Educating the Internet users at a young age regarding Internet safety issues need to be considered. It should be highlighted that children are stated as the most frequent ICT user in the family and that cyber attackers do not consider the victim's age to launch attacks [4]. Traditional methods such as campaigns and talks are difficult to roll-out considering students' current lifestyle where they are reliant and connected to the Internet technology at all times. Also, students lack the interest to listen to lectures and talks about cybersecurity awareness**.**

On the flip side, gamification is a preferable way to address the issues of creating awareness[5]. This is because gamification-based learning has more advantages than traditional based learning. It provides an interactive approach to train and educate users regarding the chosen topic. The content of the gamification itself can impart or enhance the target skills of the players via a fun and engaging manner [5]. Not only that, but it is also cost effective, scalable to cater to a large number of users, and customizable.

As malwares evolve together with the advancement of the Internet technology, the latest method of attack is unknown until a victim falters to the threat. In this case, students can never be too sure of their safety when online. Hence the development of this malware awareness tool could help students identify attacks, familiarize with the similarities among the popular methods of attack, and subsequently become more careful with their online activities.

In this paper, awareness on malwares was conducted through the gamification technique which was in the form of educational quizzes to educate students about the knowledge on malwares and to help students realize that malwares are not limited to just viruses. This is also to inform the students that there are other more dangerous malwares existing that are unknown. Hence, the malware awareness tool which is named MAL-NETS is developed for university students in order to increase their awareness towards malwares.

2. Related Works

Efforts to create awareness can be delivered through various modes such as traditional training, hands-on training, and gamification-based learning. However, nowadays people are more attracted to gamification-based learning. Besides the popularity of the mode itself, it also has many advantages compared to both traditional training and hands-on training. Its advantages are as shown in Table 1.

Based on the stated features in Table 1, the gamification technique has all the features outlined which are high engagement, user actively engaged to the method, fast response to user's mistakes, cost effectiveness, learning pace accommodate to individuals, low physical risk, standardized assessments allow users' comparison, and user could apply learning in real world.

Traditional training only has three features which are cost effective, low physical risk, and standardized assessments allow users' comparison. While for hands-on training, it has five features consisting of high engagement, user actively engaged to the method, fast response to user's mistakes, learning pace accommodate to individuals, and user could apply learning in real world.

Table 1: Comparison table of traditional training, hands-on training and Gamification Technique[7]

Features	**Traditional training**	**Hands-On Training**	**Gamification-Technique**
High engagement		X	X
User actively engaged		X	X
Fast response to user's mistakes		X	X
Cost effectiveness	X		X
Learning pace accommodate to individuals		X	X
Low physical risk	X		X
Standardized assessments allow users' comparison	X		X
User could apply learning in real world		X	X

2.1 Malware

Malware or malicious software is defined as a cyber attack that is distributed over an internetwork system. Such attacks increase in parallel with the advancement of computing technology [8]. Malwares exists in various forms according to the preference of the hacker who aims to gain profits from such an attack. Several types of malwares include viruses, worms, Spyware, Adware, Trojan, and Ransomware.

2.2 Comparison table of gamification articles

Seven papers that focussed on cyber security awareness through the gamification method had been reviewed. The reviewed article papers are as shown in Table 2. This study involved analysing different gamification articles that were published. These articles focussed on creating cybersecurity awareness and

also training using current development technologies such as 3D virtual situation or simulation, 2D design, mobile applications and web-based applications. With the increase in studies regarding cyber security, these articles discuss general issues.

Table 2: Comparison table of other cybersecurity gamification tool

No.	Paper	Gamification Name	Gamification Type	Results	Attacks mentioned	Age Range
1.	[9]	Anti-Phishing Phil	Mobile-based gaming application: Training for links (URL) safety	Improved user's learning on phishing threats.	Phishing	University students
2.	[10]	Internet Hero	Puzzle games	Improved user's awareness.	Spam emails Malware	Children 9-12 years old
3.	[11]	PicoCTF	Web-Based	Good review by students and teacher.	Brute force attacks SQL Injection	High school students
4.	[12]	CyberAware	Mini games	Majority players understand objectives in each mini game.	Malware Cyber-attacks Spam	Elementary students 9-11 years old
5.	[13]	What.Hack	Simulation games, puzzle games	Players have motive in identifying email's safety status.	Phishing	Students
6.	[14]	SecurityEmpire	Narrative gameplay	Students mostly agree with the games' level.	Scam Malware Password Cracking	High school students
7.	[15]	CyberCIEGE	Simulation games	Facing growing usage by educational institutions worldwide.	Spam emails Malwares Identity theft Password cracking	High school and graduate students

In Table 2, the seven existing cybersecurity gamification types are compared. The listed gamifications are Anti-Phishing Phil, Internet Hero, PicoCTF, CyberAware, What.Hack, SecurityEmpire, and CyberCIEGE. Anti-Phishing Phil is a mobile-based gaming application that conducts training for links (URL) safety to the users. The review of the paper says that the gamification techniques improved user's learning about phishing threats and that the article focused on phishing only. Internet Hero, consists of puzzle games which are proven to have improved user awareness in avoiding threats such as spam emails and malwares.

Third is PicoCTF which is a web-based gamification type. This game-like competition on computer security has obtained good responses from high school students and teachers. In this competition, avoidance from brute force attacks and SQL Injection are implemented. Fourth is CyberAware which comprises mini games that need to be accomplished by player thus results in the majority of players understanding the objectives in each mini game, which are to avoid cyber attacks, malwares, and spam. For What.Hack, it focused on simulation games and puzzle games. In this gamification, players have a motive to determine if the emails are safe and protected from phishing attacks.

Meanwhile, SecurityEmpire portrays a narrative gameplay and most of the students who tested the gamification agreed with the games' levels. Scam, malwares and password cracking are highlighted threats in this gamification. Lastly is CyberCIEGE which is popular in gamification when it comes to cybersecurity issues. It is a simulation game to educate people on the situations they might face when

confronted with threats. This gamification is widely used by educational institutions worldwide. It applies to spam emails, malware, identity theft, and password cracking issues.

In Table 3, the types of attack that are applied to every gamification as stated in the reviewed articles are tabulated and marked to be compared with one another.

Table 3: Attacks applied in the games

Paper \ Attack	Spam	Malwares	Cyber-attacks	Scam	Password cracking	Identity theft	Phishing	Brute force attacks	SQL Injection
[9]							X		
[10]	X	X							
[11]								X	X
[12]	X	X	X						
[13]							X		
[14]		X		X	X				
[15]	X	X			X	X			

In Table 3, the types of attacks that are mentioned in the gamification articles are listed and compared with one another. This is to tabulate the most popular types of attacks or threats that are applied so that the knowledge can be used to prevent Internet users from being attacked. In the table, malware is the most popular threat among the seven gamification articles reviewed. Malware threat scenarios have been implemented through gamification techniques and can be seen in four gamification articles above which are Internet Hero, CyberAware, SecurityEmpire, and CyberCIEGE. Such popularity shows that malware is the most common and popular cyber crime that is being conducted via the Internet.

As known, cybersecurity comprises a vast topic that needs to be covered and people need to be aware of the current cybersecurity issues happening around them. Hence, a streamlined gamification approach needs to be applied to generate awareness according to the types of cyber crime threats and attacks. Thus, this project will display the malware threats that are popular and implement the content of the four articles through gamification techniques and aim to educate people, especially university students regarding their exposure to malware threats when they are on the Internet.

3. Methodology

The methodology used to develop the malware awareness tool was discussed thoroughly so that the aim of this project, which is to increase the awareness in regards to malware among university students can be delivered smoothly. The methodology applied helps in getting better results in terms of the awareness level created in the students who use the MAL-NETS gamification system. The Game Development Life Cycle (GDLC) model is applied in developing this system. This model is suitable for gamification tools that require simple actions from user. There are six phases involved in GDLC starting with the initiation phase and proceeding with pre-production, production, testing, beta phase and release phase [16]. Figure 1 shows the GDLC model phases followed with the details of each phase involved in the model.

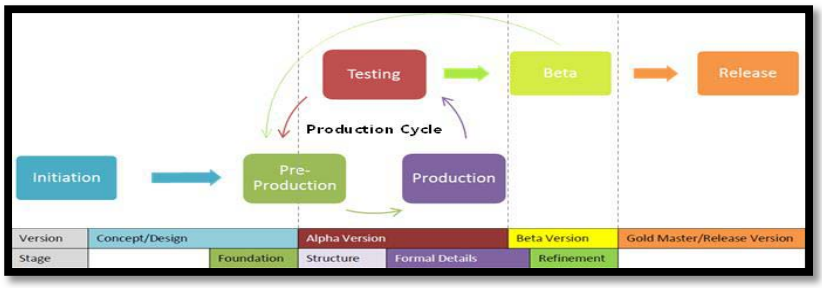


Figure 1: Game Development Lifecycle Model [16]

4. Result and Discussion

The interface used for the gamification system is important in deciding the gamification design. Good interfaces create positive moods to the players when answering questions provide commercial value to the gamification system itself. The section below shows the interfaces of the developed gamification system, MAL-NETS. The interface of the system includes the main menu, register, login, gamification level, score and others. The sample of questions are as shown in Table 4 below.

Table 4: Attacks applied in the games [17]

Sample of Question
1. Which method is NOT an efficient way to prevent malware attacks? A. Using and updating legitimate security software and performing daily scans. B. Having firewall on. C. Never use an electronic device. D. None of the above. Answer: B Explanation: Firewalls can only protect from worms and they can be disabled by complex malware once they infect victim's computer.
2. What is the software that is designed to exploit a computer user and covering computer viruses, worms, adware etc? A. Ransomware B. Keylogger C. Worms D. Malware Answer: D Explanation: Malware is short for malicious software that encompasses computer viruses, worms, Trojan horses, spyware, adware etc to interfere with normal computer operation.

4.1 Alpha Testing

The testing phase consists of alpha testing and beta testing. The alpha test was carried out to determine the functionality and the effectiveness of the malware awareness tool. The results of the alpha test are as shown in Table 5.

Table 5: The results of Alpha testing

Alpha Testing Checklist			
Application Name	**MAL-NETS**		
Element	Expected Result	Pass/Fail (P/F)	Actual Results/Comments
Play Game	Proceeds with the awareness quiz session	P	As expected, results without any errors/bugs
Pause Game	Pauses the quiz session and provides options to user to quit or continue the game	P	As expected, results without any errors/bugs
Exit Game	Exits the game to home page	P	As expected, results without any errors/bugs
Awareness Quizzes	The questions of the quizzes are presented to the user randomly	P	As expected, results without any errors/bugs
Score Game	The user's gained score whenever questions are answered correctly	P	As expected, results without any errors/bugs
User-Friendly User Interface	The interfaces of the malware awareness tool are easy to understand.	P	As expected, results without any errors/bugs

4.2 Beta Testing

Beta testing aims to identify the satisfaction level of the students on the tool developed. For testing purposes, 15 respondents have been selected randomly from various educational backgrounds. The figure below shows the results of the beta test that have been conducted.

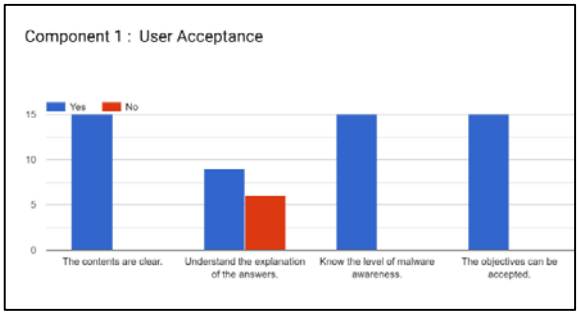


Figure 2: User acceptance

Based on Figure 2, all respondents agreed that the content of the tool is clear, respondents know their levels of malware awareness, and the objectives can be accepted. Whereas in terms of understanding the explanation of the answers, there were 9 respondents who agreed with the statement while the other 6 respondents did not agree.

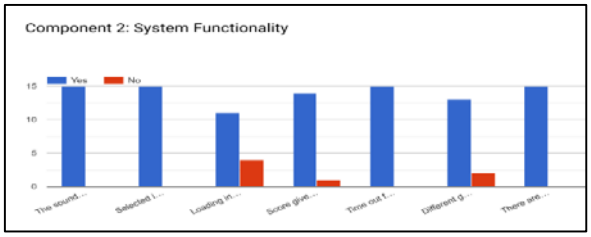


Figure 3: Tool functionality

5. Conclusion

The students who have tested the tool gained Internet safety awareness. From their experience with MAL-NETS, students who have become aware of malwares become cautious of cyber threats. Consequently, students will be more careful in accessing the Internet and would be more careful. As an outcome from this project, students could identify their awareness level based on the collected scores after answering all the questions. On top of that, the students could learn something new and have fun with the gamification method and inadvertently become drawn to it.

This tool was developed with the purpose of educating university students regarding malware awareness on Internet safety practices by implementing gamification techniques. This gamification system, MAL-NETS was developed using Unity which is a famous game development software. This tool uses a 2D display to convey malware awareness. It had been proven that this system could educate students who were previously unaware regarding malwares. This statement is supported by the test result retrieved from the tests that were conducted among university students.

Acknowledgement

This research is supported by Universiti Tun Hussein Onn Malaysia under Tier 1 Grant Scheme Vot H101.

References

[1] P. Passeri, "2017 Cyber Attacks Statistics," *Hackmageddon.com*, 2018. [Online]. Available: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics.
[2] J. Woodcock and M. R. Johnson, "Gamification: What it is, and how to fight it," *Sociol. Rev.*, 2018.
[3] E. Kritzinger, "Enhancing cyber safety awareness among school children in South Africa through gaming," in *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 2015.
[4] J. Zufic, T. Zajgar, and S. Prkic, "Children online safety," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 2017.
[5] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "Enhancing cyber security awareness with mobile games," in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018.
[6] L. Underhay, A. Pretorius, and S. Ojo, "Game-based enabled e-learning model for e-Safety education," in *2016 IST-Africa Conference, IST-Africa 2016*, 2016.
[7] J. N. Tioh, D. M. Mina, and D. D. W. Jacobson, "Cyber Security Social Engineers An Extensible Teaching Tool for Social Engineering Education and Awareness," in *Proceedings - Frontiers in Education Conference, FIE*, 2019.
[8] K. Mathur, M. T. Scholar, and S. Hiranwal, "A Survey on Techniques in Detection and Analyzing Malware Executables," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2013.
[9] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput. Human Behav.*, 2014.
[10] F. Kayali *et al.*, "A case study of a learning game about the Internet," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[11] P. Chapman, J. Burket, and D. Brumley, "PicoCTF: A Game-Based Computer Security Competition for High School Students," *Usenix*, 2014.
[12] F. Giannakas, G. Kambourakis, and S. Gritzalis, "CyberAware: A mobile game-based app for cybersecurity education and awareness," in *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2015*, 2015.
[13] Z. A. Wen, Y. Li, R. Wade, J. Huang, and A. Wang, "What.Hack: Learn phishing email defence the fun way," in *Conference on Human Factors in Computing Systems - Proceedings*, 2017.
[14] "SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education," *Secur. Dev. Eval. a Digit. Game to Promot. Cybersecurity Educ.*, 2014.
[15] M. F. Thompson and C. E. Irvine, "CyberCIEGE Scenario Design and Implementation," *Usenix*, 2014.
[16] R. Ramadan and Y. Widyani, "Game development life cycle guidelines," in *2013 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2013*, 2013.
[17] "Computer Awareness for Upcoming Exams Set 86 (Malicious Programs)," 2017.