IST-Africa 2016 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2016
ISBN: 978-1-905824-55-7

Game-Based Enabled e-Learning Model for e-Safety Education

Lusinda UNDERHAY, Agneita PRETORIUS, Sunday OJO
Tshwane University of Technology
Department of Computer Science, Faculty of ICT, Pretoria, South Africa
Tel: +27-12-829689, Email: underhayls@tut.ac.za, Ojoso@tut.ac.za

Abstract: Students at the Tshwane University of Technology (TUT) may be potential victims of cyber-crime. Students need to know how to avoid being victims of cybercrime and may not know how to gain the knowledge. Electronic Safety (e-Safety) education and awareness can be accomplished through game based media such as educational video games. However, these games mostly focus on narrow aspects, such as anti-phishing, secure logins, anti-virus etc., and are often not readily available. To gain full advantage of game based tools, e-Safety games need to be customised to satisfy the targeted organisation's security policies and needs. This study aims to propose a game-based e-learning model focusing on e-Safety education. As proof of concept a proposed prototype model will be developed, implemented and evaluated. The model is expected to unleash game-based learning benefits by enhancing engagement, improving motivation and influencing positive behaviour towards e-Safety education.

Keywords: cyber-crime, cyber threats, e-Safety awareness, e-Safety education, game-based learning, e-learning

1. Introduction

GBL promises to be a new successful approach in motivating today's students to learn about e-Safety, as many students may remain unaware of cyber-threats until they hear about it on the news, or it happens to someone they know; more importantly they need to know how to protect themselves from becoming victims. GBL can teach e-Safety skills in a fun and engaging environment by making use of video games. Engaging video games can assist with concentration retention, decision making and problem solving skills, logical thinking, creativity, team work and computer skills [1].

Although there are tools, games and simulators, that can be used to increase student's knowledge, they seem to focus on special areas of interests, and are often aimed at experts in these areas [2, 3, 4]. Access to these tools (especially the games) is often restricted [2].

It would be more beneficial for a TUT student to have an e-Safety game that is customised to their needs. If an e-Safety game is to be as effective as the face-to-face communication in a classroom environment, a customised design of a GBL environment needs to be developed [3]. Such a design should also consider the several cognitive learning styles that "individual gamers" have [5].

1.1 Cyber-Crime Vulnerability

Part of the cyber-crime vulnerability problem is that cyber-crime is highly technical and few people outside the "hacker" fraternity possess an understanding of how it is perpetrated. Most students are unaware of which sensitive information their computer systems store, and even less aware of where on the system it is stored. In addition, it is

often difficult to determine which information should be classified as sensitive because a single, apparently innocuous data item could be used to acquire more information [6, 7].

In a world of rapidly advancing technology, and especially with the increased use of the Internet for academic purposes [8, 9, 10], tertiary students extensively make use of the Internet for educational, social and entertainment purposes. Many students may become victims of cyber-crime and online fraud, as they may remain unaware of cyber-threats until they hear about it on the news, or it happens to someone they know; more importantly they need to know how to protect themselves from becoming victims.

Students often need to disclose their personal details to various organisations, such as the government, tertiary institutions, online employment agencies, etc. The security of their personal information cannot be a 100% guaranteed. Since most South African students rely on cell phones rather than landlines the pool of potential cyber-crime victims may number in the millions; an alarming observation as cyber-criminals become more effective in stealing sensitive data from various organisations [11, 12].

1.2 Game-based Learning

Game-based learning (GBL) is an educational, instructional method that makes use video games to teach a set of learning outcomes by engaging its intended players. GBL is used to achieve the learning outcomes by changing the behaviour of the players. University education is slowly moving away from the "traditional web-based Learning Management Systems (LMS) towards game-based learning environments, with the intention of integrating advantages of using games" [1]. GBL can teach e-Safety skills in a fun and engaging environment by making use of video games that can assist with concentration retention, decision making and problem solving skills, logical thinking, creativity, team work and computer skills [1].

Gaming is readily accepted by students as a form of gaining new skills and applying acquired knowledge [1]. Through GBI students can explore and experiment through a virtual "world through new roles and identities and the potential to encourage reflective practice by having them engage in a cycle of probing, hypothesizing, probing again, and rethinking their strategies" [13, 14], without the fear of failure or obtaining bad marks [13]. GBI can therefore assist in modelling students into more productive and engaging "future" employees.

One of the biggest benefits that e-Safety games can provide compared to the more traditional methods of training' is that the virtual environment can allow the trainees to practice their e-safety skills in a more realistic, stressful environment, which is key in being able to apply the theoretical knowledge.

2. Objectives

The aim of this study, therefore, is to develop a model and platform for game-based interactive multimedia e-learning pedagogical tool for e-Safety education, which is currently a work-in-progress.

The research objectives that are accomplished in this study include:

1. To develop an ontology of the e-Safety body of knowledge;
2. To determine what the current level of e-Safety awareness amongst TUT student;
3. To determine what combination of game genre, dynamics and mechanics will be appropriate for a game-based e-learning model for e-Safety education;
4. To develop a game-based e-learning model for e-Safety education;
5. To implement a prototype;
6. To conduct a usability evaluation of the model as a proof of concept.

3. Methodology

During conceptual modelling the common self-preventive measures that network providers encourage their clients, including students, to practice will be consulted to construct the ontology on how to present the e-Safety awareness content.

A questionnaire will be used to collect data about what a sample of TUT students know about e-Safety and the measures that they implement to protect themselves.

To construct the model, relevant literature is studied along with content analysis of existing e-Safety games to determine the best combination of game genre, dynamics and mechanics for a game-based model for e-Safety education.

The conceptual model is used to develop the game-based model and design the architecture based on the best combination of game genre, dynamics and mechanics to present the identified e-Safety objectives to be achieved.

The model will be prototyped and evaluated. To test the usability and to identify problems with the prototype the Heuristic Usability Evaluation (HUE) method will be used.

There are ten Usability Heuristics namely: visibility of system status; match between system and the real world; user control and freedom; consistency and standards; error prevention; recognition rather than recall; flexibility and efficiency of use; aesthetic and minimalist design; help users recognise, diagnose, and recover from errors; help and documentation.

3.1 Ontology of E-Safety Body of Knowledge

In order to construct the ontology on how to present the e-Safety awareness content, the common self-preventive measures that network providers encourage their clients, including students, to practice is consulted to develop the curriculum information.

This study's learning objectives are based on the common self-preventive measures that network providers encourage their clients, including students: read security concerns; use firewalls; verify content; practice safe surfing; practice safe shopping; use security software; use a secure wireless network; use strong passwords; use common sense; be suspicious; ensure physical security; perform network scanning; use intrusion alert programs; use encryption; perform data backups; use email filters; update software; log off/sign out of online accounts; be cautious when using free Bluetooth and Wi-Fi networks; keep social media accounts secure; be aware of mobile and wireless networks [15, 16, 17].

The ontology was developed using curriculum modelling and management to facilitate the accessing and retrieval of curriculum information, by linking learning units to learning objectives and their outcomes. The developed ontology is used to model the proposed game (Cyber Smart).

3.2 The Level of E-Safety Amongst TUT Students

Before the students are exposed to the study's proposed e-Safety game, an automated survey questionnaire, created in Microsoft Word 2010, will be used to collect data about what a sample of TUT students know about e-Safety and the measures that they implement to protect themselves.

The survey is titled "E-Safety Survey" and consists of three sections, namely:

1. Personal information - focuses on the participants' geographic and academic information, and their computer and Internet usage;
2. Internet access - focuses on the use to which the participants' Internet access is put;
3. Cyber-crime awareness – focuses on the participants' knowledge, attitude and behaviour [18] regarding the learning units that have been identified in Section 3.1.

The data will be analysed quantitatively [5] to summarise and determine student's level of e-Safety awareness [5].

The sampling of the TUT student population is conducted using convenience sampling, a form of non-probability sampling. With this type of sampling the findings can only be generalised to TUT students. Students (foundation to 3rd year) that are currently registered at the eMalahleni campus are called upon to take part in the study.

4. Technology Description

A game engine allows a designer/programmer to focus on the features that make their game unique by providing a platform that handles the game-related tasks such as rendering, physics and input and also provides reusable components.

To develop the proposed simulation/game, it was decided to use Unity 5D (the free version) due to its popularity, 3D game design and because it is easy enough for beginners to use as well as professionals. Unity 5D allows for components to be dragged and dropped with the occasional adapting of existing scripts, rather than coding to achieve certain preferences.

5. Developments

Before the game design for educational purposes can begin, what the player needs to learn from the game should be identified [14], see Section 3.1.

E-Safety awareness can be accomplished through educational video games [19] yet, these games mostly focus on special areas of interest, such as anti-phishing, secure logins, anti-virus ect., and are often not easily available [2]. If an e-Safety game is to be as effective as the face-to-face communication in a classroom environment, a customised design of a game-based learning environment needs to be designed [3]. Such a design should also consider the several cognitive learning styles that "individual gamers" have [5].

5.1 Game Genre, Dynamics and Mechanics

To construct the model, relevant literature is studied along with content analysis of existing e-Safety games (CyberNexs [14], a proposed social media game [19], Paradise Model [5], and Simposter [2]) to determine the best combination of game genre, dynamics and mechanics for a game-based model for e-Safety education.

Between the mentioned four games the most popular genre used is Role Playing Games, where players take on the role of the system administrator responsible for securing and protecting networks and systems which involves survival dynamics. The game mechanics are influenced by the game's learning units, game genre and dynamics; therefore there is no relationship between the four games' mechanics.

The game genre for the study's proposed game Cyber Smart is a Role Playing Games, where players take on the role of the system administrator of one of the labs in at the TUT eMahlaleni campus, and will be responsible for securing and protecting networks and systems which involves survival dynamics.

Game mechanics describe the rules and how the state of the game changes [14]. The game mechanics that [14] explains, will be applied to Cyber Smart as follows:

1. Setting and narrative - the role of the main character is reduced "to a cursor for the player's actions" (Lode, 2012:38). The game takes place in the system administrator's office. As the system administrator, players use the computer which will stimulate experimentation and exploration regarding the application of e-Safety in the lab;
2. Victory condition - to be victories in Cyber Smart the player needs to pass all learning units, thereby successfully securing and protecting the lab's networks, systems and

devices;
3. Progression of play - Cyber Smart is not a multi-player game therefor the game does not need progression of play to describes whether players need to take turns;
4. Player actions - in the Cyber Smart game the player's actions will include clicking on the mouse and typing on the keyboard that will affect the status of the game;
5. Game views - Cyber Smart will provide the player with enough information about the game's state and the learning units. The player's actions will change the state of the game for better or worse and they will continually receive new information to analyse and act on.

5.2 Modelling and Design

[20] states that the conceptualization step defines the ontology's scope based on its concepts, relations and constraints, and attributes by modelling the knowledge:

1. Gameplay components - the Cyber Smart game interacts with the player through the output channels, the screen and speakers and the player in turn interacts with the game through input channels, the mouse and keyboard;
2. Pedagogical (goal) rules - in the Cyber Smart game the player's actions will include clicking on the mouse and typing on the keyboard. Pedagogical (goal) rules describe the actions that the player can take in order to either win or lose the game. Therefore in Cyber Smart the player's goal is to take the necessary actions to successfully achieve each of the learning unit's outcomes, if the player fails to do so the game is lost [20];
3. Actions – governed by rules and in the Cyber Smart game the player's actions will include clicking on the mouse and typing on the keyboard that will affect the status of the game;
4. Game objects - the Cyber Smart game has a player object (the student) and several non–player objects such as a desktop computer, mouse, keyboard, etc;
5. Game bricks - the play bricks for the Cyber Smart game would include select, write (type) and manage, the goal bricks would include avoid, secure (e.g. securing of a network/device) and implement (e.g. implementing best practices).

The instructional strategy for Cyber Smart will take on a combination of application methods that involve practical activities such as role play where players apply behaviour-related principles, simulations and serious gaming where players interact with the system to be able to understand the underlying principles.

The delivery strategy for Cyber Smart will be to setup it up in one of the labs to allow the students to play the game based on their availability.

5.3 Heuristic Usability Evaluation (HUE)

The purpose of the evaluation will be to verify and improve the quality of Cyber Smart based on its learning units. The Heuristic Usability Evaluation (HUE) method will be used for the evaluation.

6. Results

An ontology of the e-Safety body of knowledge was developed using curriculum modelling and management by linking learning units to learning objectives and their outcomes.

The level of e-Safety awareness amongst TUT students are still unclear as the survey is still a work-in-progress.

Relevant literature is studied along with content analysis of four existing e-Safety games (CyberNexs [14], a proposed social media game [19], Paradise Model [5], and Simposter [2]) to determine which of the games satisfies this study's required learning

objectives (see Section 3.1). The games are also reviewed to determine the best combination of game genre, dynamics and mechanics for a game-based model for e-Safety education.

The e-Safety learning objectives, which were identified for this study's e-learning model, are covered in only one of the four games (not necessarily from the same game), namely: the use of a firewall; practicing safe surfing; the use of security software; using a secure Wi-Fi network; using a strong password; being suspicious; performing data backups; and securing social media accounts.

None of the four games included reading security concerns; verifying content; practicing safe shopping; using common sense; using email filters; updating software; logging off; taking caution when using Bluetooth and Wi-Fi networks; and mobile and wireless awareness; thereby creating an opportunity to develop a game that does create awareness regarding these matters.

Between the four games the most popular genre used is Role Playing Games, where players take on the role of the system administrator responsible for securing and protecting networks and systems which involves survival dynamics.

The game mechanics are influenced by the game's learning objectives (identified in Section 3.1), game genre and dynamics; therefore there is no relationship between the four games' mechanics.

The development, implementation and evaluation of the game-based e-learning model for e-Safety education, Cyber Smart, are still a works-in-progress.

7. Business Benefits

Greater e-Safety awareness amongst TUT students will be beneficial not only to TUT, but also to the South African and international communities. By raising awareness of e-Safety on campus in general, the study's proposed simulation/game, Cyber Smart, may enable students to recognize new cyber-threats and report such incidents to authorities.

As a result of the globalization of ICT, it is reported that 75% of student's prefer to use computers for their studies, even if they are not required to do so [9]. Although there is adequate access to the campus computers, students remain creative in finding computers to access off-campus, and how they connect to such computers [9]. Accessing an Internet cafe's computer may increase students' exposure to cyber-crime because they will be relying on the possibly inadequate safeguards provided by others. Their own awareness and knowledge may help them avoid situations that may be harmful, and it will be beneficial for them to transfer the acquired knowledge into the workforce.

A greater awareness and knowledge of e-Safety amongst TUT students may spread into the wider community (parents, siblings, friends, etc.) by osmosis, thereby fostering a general understanding of the risks associated with global network access (from the Internet to cellular phones). This in turn may lead to fewer victims amongst not only students but in the population at large.

8. Conclusions

All of the games, simulators and quizzes discussed are aimed at teaching e-Safety and relevant to this study. The differences between the works are that some are intended for children, more advanced computer users, an intended industry, general computer users, or short games concentrating on a specific task.

It was discovered that the most popular genre used is Role Playing Games, where players take on the role of the system administrator responsible for securing and protecting networks and systems which involves survival dynamics. The game mechanics are influenced by the game's learning objectives, game genre and dynamics.

The best practice that network providers encourage their clients to engage in aligns with the learning objectives for this study's e-Safety game prototype.

References

[1] MINOVIĆ, M., MILOVANOVIĆ, M., & STARČEVIĆ, D. 2011. Modelling knowledge and game based learning: model driven approach. *Journal of Universal Computer Science*, 17(9), 1241.

[2] GILBERG, F.P. 2006. Can Network Security be Fun? An agent-based Simulation Model and Game proposal. Master of Science in Information Security, Master's Thesis, Gjøvik University College.

[3] YAP, J. 2011. Virtual Fun And Challenge: Case Study Of Learning Cybercrime In Second Life. In: *Proceedings of the 2011 IEEE Defense Science Research Conference and Expo (DSR), August 3-5, 2011.* Singapore.

[4] NÄCKROS, K. 2001. Game-Based Instruction within IT Security Education. Degree of Licentiate Philosophy, Stockholm University and Royal Institute of Technology.

[5] NÄCKROS, K. 2002. Empowering Users to become Effective Information Security and Privacy Managers in the Digital world through Computer Games: Positioning computer games as means to increase information and communication security awareness. Stockholm: Stockholm University and Royal Institute of Technology.

[6] INFORMATION SERVICES & TECHNOLOGY. S.a. *Removing Sensitive Data* [Online]. S.l.: IST.mit.edu. Available from: http://ist.mit.edu/security/remove_sensitivedata [Accessed: 07/03/2012].

[7] VILJOEN, JJS. June 27 2011. *E-Safety research proposal.* [E-mail]. Mailing to lsunderhay discussion list at lsunderhay@gmail.com. (June 27 2011).

[8] JONES, S. 2002. The Internet Goes to College. Pew Internet & American Life.*USDLA Journal*, 16(10), n10.

[9] CZERNIEWICZ, L. & BROWN, C. 2009. A Virtual Wheel of Fortune? Enablers and Constraints of ICTs in higher education in South Africa. *Bridging the knowledge divide: Educational technology for development*, 57-76.

[10] DAMOENSE, M.Y. 2003. *Online learning: Implications for effective learning for higher education in South Africa.* Australian Journal of Educational Technology, 19(1):25-45 [Online]. S.I.: Ascilite.org.au. Available from: http://ascilite.org.au/ajet/ajet19/damoense.html [Accessed: 19/03/2013].

[11] ITWEB. 2010. *Rica leaves subscribers vulnerable* [Online]. S.l.: Defenceweb.co.za. Available from: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=10660:rica-leaves-subscribers-vulnerable&catid=7:Industry&Itemid=116 [Accessed: 07/08/2011].

[12] PROTECTING Data, Intellectual Property and Brand from Cyber Attacks. 2013. *Cybershield Magazine*, 2, Mar-Apr.:25.

[13] PHO, A. & DINSCORE, A. 2015. *Game-Based.* Chicago: Association of College and Research Libraries.

[14] NAGARAJAN, A., ALLBECK, J.M., SOOD, A. & JANSSEN, T.L. 2012. Exploring Game Design for Cybersecurity Training. In: *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, May 27-31, 2012.* Bangkok, Thailand.

[15] IRVINE, C. E., THOMPSON, M. F., & ALLEN, K. 2005. CyberCIEGE: gaming for information assurance. In: *Proceedings of the 2005 IEEE Symposium on Security & Privacy, May 8-11, 2005.* California, USA.

[16] RAMESH, P. & MAHESWARI, D. 2012. Survey of cyber crime activities and preventive measures. In: *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, October 26-28, 2012.* Coimbatore, India.

[17] UNDERHAY, L.S. 2012. Evaluation of e-Safety awareness and its relation to cyber-crime in South Africa. Software development, BTech, Tshwane University of Technology.

[18] KRUGER, H.A., & KEARNEY, W.D. 2006. A prototype for assessing information security awareness. *Journal of computers & security,* 25(4), June:289-296.

[19] LABUSCHAGNE, W.A., VEERASAMY, N., BURKE, I., & ELOFF, M.M. 2011. Design of cyber security awareness game utilizing a social media framework. In: *Proceedings of the 2011 IEEE Conference* ON Information Security South Africa (ISSA), *15-17 August, 2007.* Johannesburg, South Africa.

[20] RAIES, K. & KHEMAJA, M., 2014. Towards gameplay ontology for game based learning system design process monitoring. In: *Proceedings of the Second International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM), October 1-3, 2014.* Salamanca, Spain.