Design of cyber security awareness game utilizing a social media framework

WA Labuschagne
UNISA
Pretoria, South Africa
wlabuschagne@csir.co.za

N Veerasamy
CSIR
Pretoria, South Africa
nveerasamy @csir.co.za

I Burke
CSIR
Pretoria, South Africa
Iburke@csir.co.za

MM Eloff
UNISA
Pretoria, South Africa
eloffmm@unisa.co.za

Abstract— **Social networking sites are a popular medium of interaction and communication. Social networking sites provide the ability to run applications and games to test users' knowledge. The popularity of social networks makes it an ideal tool through which awareness can be created on existing and emerging security threats. This paper proposes an interactive game hosted by social networking sites with the purpose of creating awareness on information security threats and vulnerabilities. The game applies principles of good game design which includes: the decisions over hypermedia, multimedia and hypertext to achieve perception, comprehension or projection, comprehensive database of questions, weighted system, use of practical data, automation, dynamcis, effort and user acceptance. The aim of the paper is show the effectiveness of using a virtual tool in cyber awareness creation. This paper will thus deal with the proposal of an interactive web-based game which informs and then tests users about potential security threats and vulnerabilities.**

Keywords- application, awareness, security, social networking, threat, vulnerability

I. INTRODUCTION

It is becoming increasingly important for all users, and not just technical staff, to be aware of safe cyber practices. Eminagaoglu et al. [1] state that not only technical security training of IT staff, but also information security awareness training and other awareness campaigns have become a "must" for everyone. Many users are ignorant of the range of threats spanning cyber space and the Internet. By using cyber security campaigns, awareness can be created on current threats, as well as educate users on best practices to identify and handle threats. Another prime target for awareness creation is universities. According to Rezgui & Marks [2], a number of universities now recommend providing security awareness training and education components for students and staff, and emphasize that everyone needs to be aware of up-to-date IT threats so they can apply the security lessons in the most effective way. Home users could also benefit from cyber security awareness campaigns that warn them of the latest threats or provide useful tips on safe internet surfing. Kritzinger & von Solms, [3] state the vulnerability of personal Internet users is due to the fact that they lack the information security knowledge to understand and protect their PC and therefore also their personal information.

One way of creating awareness is by utilizing popular mediums such as social networking sites. Social networking sites ideally serve the purpose of awareness creation as users are keen to try out new games and applications. Various marketing and educational schemes can benefit from the popularity and reach of social networking sites. Social networking sites have the ability to post results from quizzes and games allowing users to compare their scores. This approach could be utilized in order to create a game to measures and increase users' awareness on cyber security. This paper therefore proposes the design of virtual game with the goal of improving cyber awareness. The remainder of the paper is structured as follows: Section II provides a motivation for the game and Section III introduces the requirements for the game design. Section IV provides a brief overview of similar games aimed at increasing user security awareness Section V, explains the operation of the proposed game and the paper is concluded in Section VI.

II. MOTIVATION FOR GAME DESIGN

A. Directed Communication

Albrechtsen & Hovden [4] mention forms of one-directional communication such as pamphlets, emails, intranet pages, screen savers, posters, mouse pads, pens, games, formal presentations and training sessions which are largely aimed at transferring information from an authority to the target population. Furthermore, they wish to emphasise the importance of employee feedback and participation as it can greatly improve the employees' information security awareness and behaviour. This argument shows that success of employees

978-1-4577--1483-2/11/$26.00 ©2011 IEEE

retaining the security awareness knowledge is increased when users actively engage in the process and are not merely subject to one-sided instruction and distribution of facts. Rezgui & Marks [2] argue that it is paramount to enforce awareness and training as human errors are rated as among the top security threats. When considering the financial implications of a single case of abuse, the necessity of ensuring all users are aware of information security threats becomes obvious. Furthermore, Eminagaoglu et al. [1] show in a case study show that awareness training and related campaigns can have a positive effect on reducing security threats. In their study, the results showed that weak password usage was significantly decreased and users continually improved their awareness and complied with policies after under-going a security awareness training course. In addition, Dodge Jr. conducted a phishing email exercise by generating a phishing email with embedded links, as well requests for sensitive information [5]. After carrying out the experiment at a military academy the amount of students falling victim to the scam was measured. Thereafter training was given with the intent of reducing students' propensity of falling victim. By providing the awareness programme, the number of students at the university falling victim to the phishing exercise dropped each year which showed that they were now able to recognize potential scams. These results show that awareness levels can be increased through interactive content. This also indicates that the medium through which awareness material is provided also plays a significant role.

B. Information Richness

Shaw, Chen, Harris and Huang [6] argue that the Web is an ideal tool to deliver security awareness as it is able to handle the needs of multimedia (audio, video and animation) to reflect real scenarios of information risks. This also raises the issue that information richness of different forms of multimedia can affect the effectiveness of online security awareness programs. Furthermore, they discuss three media that are pertinent to the influence of information richness on the effectiveness of online security awareness programmes. These are [6] :

- **Hypermedia**: interactive medium that consists of graphics, audio, video, plaintext and hyperlinks which makes it the richest medium of the three. Concepts can be arranged visually and not sequentially to help users understand critical concepts and their interrelation-ships.
- **Multimedia**: combines text, image, sound, music, animation, video and virtual reality but must be accessed in a linear sequence.
- **Hypertext**: does not incorporate feedback, language variety, multiple signals or personal focus.

Through their study on a selection of security inexperienced users, Shaw et al. [6] were able to deduce:

- That hypermedia and multimedia were more effective in enhancing users comprehension and projection ability of security awareness,
- Hypertext-based training was more effective than multimedia in enhancing users' perceptions of security risks.
- Perception refers to a basic awareness of the security topic.
- Comprehension entails understanding the technical operation of the exploit.
- Projection would involve predicting a future route to follow.

These results provide important insight when designing a game for security awareness creation. The richness of the media, together with the aimed level of awareness are important decisions in the design of a game to create security awareness. These decisions were considered in the design of the proposed security awareness game.

After having identified the necessity of creating security awareness and studying the mediums of content distribution, the discussion moves on to the compilation of essential requirements that will form the basis of the proposed game design.

III. REQUIREMENTS

In the previous section, the effect that media richness plays in affecting the awareness levels created were discussed. A decision on media richness is thus required when designing web-based game for awareness creation. In addition, other requirements for a web-based security awareness game should also be considered. The design of the game consists of different components, which should be taken into consideration to ensure that the objective of the platform is achieved, as well as to ensure that the users will be actively involved in the act of playing the security awareness game. Kruger and Kearner [7], Hsu and Lu [8], Shin and Shin [9], Johnston [10] and Priebatsch [11] proposed components that should be considered in the development of successful security awareness games using social networking sites. This section summarises some key requirements that fed into the design of the security awareness game for security awareness creation. These requirements include, but are not limited to, the following:

1) ***A comprehensive database of questions should exist*** – The nature of the proposed game would require a database of questions. This is used to determine the current knowledge level of the users and also be used as a critical game component.Quality time ought to be spent obtaining the right input for the game. A large set of questions also allows for a random set to be selected each time. An extensive database with questions should prevent the application from presenting the same questions to the user. The question database should ensure that the topic is sufficiently covered and that the topics cover the subject matter in depth while the range of topics are extensive.

2) ***Weighting of the questions*** – It is recommended to assign higher weights to questions that are more challenging. This would allow the game to progressively become more difficult as the users knowledge increases. In addition, the use

Acknowledgement must be made to the CSIR and the NRF for their financial support of this research.

of weights would create levels in the game which could be used to determine the current security awareness of the user.

3) ***The use of practical data*** – The data encapsulated in the questions should reflect real life scenarios that users could easily identify with. User participating in the game should be able to apply the knowledge acquired during the game play in their current environment. The relevance of the data should be applicable and disseminated into easy interpretable knowledge fragments. For example the user playing the game on the social networking site would not have the technical knowledge of a server administrator. Hence the questions should not cover server administration security threats. It will be more feasible to develop the question bank that covers security threats that are encountered by every day users. Commtouch [12] reported on the trends of Internet threats in the first quarter of 2011. These trends provide a list of threats that users need to be aware of and could be reflected in the content of the game play. These topics could be changed into the questions and placed into the different question topics that covers each security threat.

4) ***Tool should be automated*** – The mechanism used to conduct the security awareness program should be designed to function without the intervention and supervision of humans. All the required calculations should be computed by the system and guide the users through the entirety of the application. The removal of the human component from the system suggests that multiple users from numerous locations can play the game simultaneously. This is an important component since social networking sites are Internet based which allows multiple users to interact with the game.

5) ***Game dynamics*** – All game design involves different gaming dynamics which incite users to come back and play again. Priebatsch [11] discussed four game dynamics that should be present in on-line games, namely Appointment, Influence and Status, Progression and Communal discovery dynamics. The Appointment dynamic ensures that users return to the game due to a tempral event which subconsciously commits the user to returning to play the game over time. The Influence and Status dynamic makes use of symbols for example badges representing status to compete with other peers. The Progression dynamic provides feedback to the user of progress made. The Communal discovery dynamic allows users to collaborate with other users to solve complex problems.

6) ***Easy accessible*** – The game developed should provide users easy access to the required resources. Resources that are located on a personal computer at home or located within a private internal network are not easily accessible. The Internet architecture is developed to provide mechanisms for users to access resources easily. For example, a user requires an Internet connection, computer with web browser and the address of the resource for access. Web sites are easily accessible and thus can cater ideally for the requirement of accessibility. The advances in personal computers, laptops, mobile devices allows users to access these web sites

7) ***Effortless*** – Computer/Graphical Interfaces provide users a mechanism to interact with technology, this would also imply that the interface determines how the user will experience this interaction. Human Computer Interfaces (HCI) is defined by Johnston, Eloff and Labuschagne [10] as: ”HCI deals with the interaction between one or more humans and one or more computers.” A list of ten critical factors, listed below, was developed by Nielsen [13]. These factors provides the users with an experience which build trust with the application, increase productivity and reduces erroneous use, which frustrates the user . The development of the interface that will be used by the users to interact with the game will incorporate these factors in the design. Social networking sites use these factors as part of its design in order to ensure ease of use. The factors from Nielsen are:

- **Visibility of system status**: The system should always keep users informed about what is going on, through appropriate feedback within reasonable time
- **Match between system and the real world**: The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
- **User control and freedom**: Users often choose system functions by accident and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support functions of undo and redo.
- **Consistency and standards**: Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
- **Error prevention**: Even more beneficial than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
- **Help users recognize, diagnose, and recover from errors**: Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
- **Recognition rather than recall**: Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
- **Flexibility and efficiency of use**: Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.

- **Aesthetic and minimalist design**: Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
- **Help and documentation**: Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

*8) **Acceptance by the user*** – The longevity of the game is determined by numerous factors. The game requires users to participate by playing with the designed tool. Also, it is critical for users to return to the game. The game would require factors that would entice users to return. The user interface as discussed earlier is one of the required factors. The Technology Acceptance Model (TAM) was originally proposed by Davis [14]. Furthermore, Moon [15] states that TAM provides determinants of individual adoption and can explain and predict the individual's acceptance of Information Technology (IT).Moreover, Moon states: "This model illustrates that the social behaviour is motivated by the attitude towards carrying out that behaviour, a function of one's beliefs about the outcome of the performing that behaviour and an evaluation of the value of each of those outcomes". Fig 1 illustrates the different determinants of TAM as orginally specifed by Davis [14].

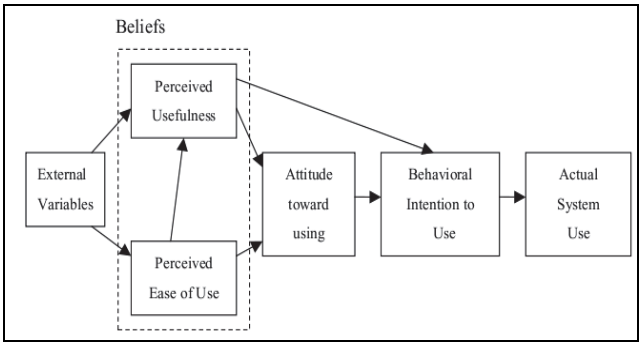

Figure 1. TAM Model

Users encountering new technology for the first time experience two determinants. The user questions the usefulness and the ease of use of the new technology. Perceived Usefulness (PU) and Perceived Ease of Use (PE) affect the belief of a user which influences the attitude towards using the technology, also affecting the behaviour to finally use the system [16]. The TAM has been extended by Hsu & Lu [8] to address on-line games (See Fig 2). Two additional determinants has been added: Social influences and Flow experience. Social influences has been identified to shape user behaviour through social norms demonstrated by other groups. People tend to look upon other's behaviour when faced with a situation whereby they do not know how to react [17]. Csikszentmihalyi [18] defined the concept of flow as "the holistic experience that people feel when they act with total involvement". This definition suggests that flow consists of four components—control, attention, curiosity, and intrinsic interest. The number of social networking sites have exploded in recent times providing platforms whereby users could create content, build relationships and also participate in entertainment such as playing games. Shin & Shin [9] identified the need to adapt the TAM to accommodate social networking sites with the addition of the following determinants: Perceived Playfulness (PP) and Perceived Security (PS). These two determinants addresses the level of curiosity during an interaction with technology and the security concerns that have been raised with use of social networking sites. They found that PP was related to PE and PU. Therefore the determinants: PE, PU, PS, PP and flow are important factors that need to be reflected in the design of a game utilising social networking sites.

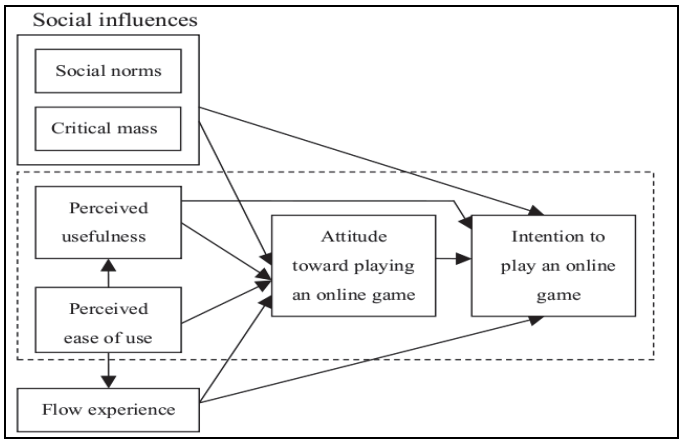

Figure 2. Extended TAM Model

IV. SECURITY AWARENESS GAMES

Cone [19] found that video games can be effective in basic information security training programs. His study focused on a game developed by the Center for Information Systems Security Studies and Research (CISR) for the Department of Defense of the United States of America called CyberCiege [20]. This game is a highly extensible game for teaching information assurance concepts and runs on a standalone computer system. The game is based on different scenarios whereby the user needs to take certain actions to learn about threats and acquire the knowledge to prevent and mitigate the threats. The scenarios include, but not limited to the following topics: Stopping Worms, Life with Macros, Identity Theft, Passwords, Physical Security, Patches, Filters, Encrypt Link and Identity management. The users learn about a topic through the use of the game and experience obtained through the approach of problem solving and critical thinking. Another game, from the USA Department of Defense called CyberProtect [21], provides users with an interactive security

experience. Screenshots from the CyberProtect game are shown in Fig 3 and Fig 4.

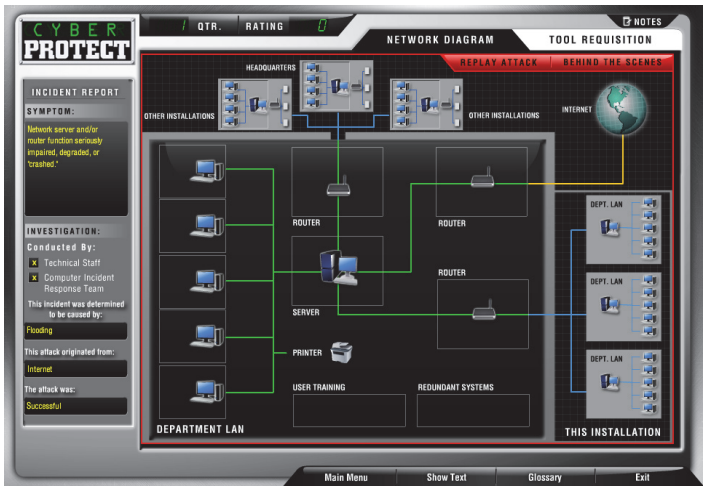

Figure 3. CyberProtect

Figure 4. Cyberprotect

This game is an on-line game but does not use a social networking site as the delivery platform. This game is also more focused on securing a network and all the threats that are in the network domain. This game is designed for a specific audience that has background knowledge in networking technology and implementing strategies to secure the network.

Social networking sites have numerous successful games for example Farmville, Mafia Wars, Farm Town and Petville. The success of these games could attribute to the design of future games.

Social networking sites provide an accessible portal through which to gain access to a networking site that already have an extensive user base. There is thus a gap for games using social networking sites and due to this requirement, the proposed design for such a game is given in the next section. There is thus a gap to use social networking sites to play games that promotes cyber security awareness. .

Using all these identified requirements, a proposed design for a security awareness game is given in the next section.

V. DESIGN OF GAME

The basic outline of the game is presented in this section. The design of the game takes into consideration the various requirements discussed in the previous sections. The design of the game is given in the conceptual prototype explained in this section. Principles that the requirements capture are incorporated in the conceptual prototype that has been partially tested but not deployed in the social networking site environment as yet. Fig 5 shows the high-level design of the game. To commence the game, the user logins on the login screen. Thereafter the user is presented with the topic tree which shows topics graphically and in a listed format. The Topic Tree page also displays the most recent achievement by the user. Once the user has selected a topic (for example password security), he/she is provided with the option to choose a video, slide show or quiz. The slides and videos are used for education purposes while the quiz feature is used to determine the knowledge that the user currently has or has acquired. The other options for the user include viewing achievements on the My Profile Page or viewing the current leader board. In general, the user has the ability to log-out which returns the game to the login screen once again. The dashed lines indicated the interlinking between the web pages. The arrowheads on the dashed lines show the navigational direction of the pages. The arrows show the functional flow of the game from login, to topic selection, proceeding to either learning or testing and thereafter viewing of individual achievements or the leader board.

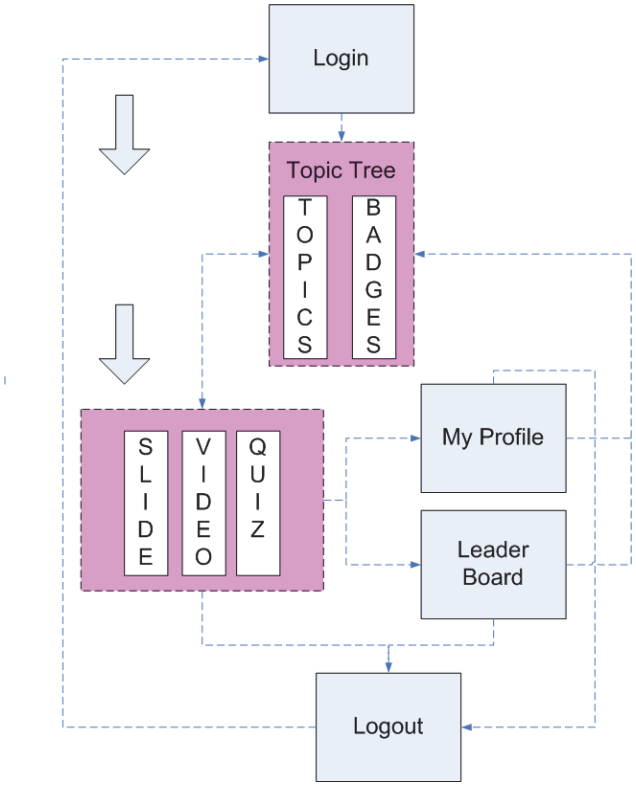

Figure 5. High-level design of game

Screenshots from the conceptual prototype are now provided to show the functional flow explained in the high-level design diagram (in Fig 5).

The overall objective of the project is to primarily promote perception and thereafter comprehension. To achieve this, the findings given in Section II B stipulate that hypertext and multimedia would be ideal. Therefore, the game aims to incorporate components of multi-media and hypertext in order to present an inviting and engaging forum for users to interact with (see Fig 6 and Fig 7). In Fig 6, users may use the hyperlinks on the left or the interactive hotspots to select a security awareness topic. In each topic view, Fig 6, users can choose to view tutorial material related to the topic or attempt answering a quiz related to the topic.

Fig 6 also shows the weighting requirement. The layering of subject matter as described by Khan [22] addresses the requirement of using a weighted method to incorporate the difficulty of content. Each level represents a more complex level of topics. In order for the user to advance to more advanced topics, a user is required to 'unlock' the next level. Users need to answer ten consecutive questions correctly on the preceding level. Questions are chosen at random from the pool of compiled questions for each level. This shows the compliance to the requirement of having a comprehensive database of questions. The questions have been constructed using practical knowledge (see Fig 8). For example Fig. 8 illustrates the testing of a user's knowledge of sensible passwords, which take into consideration complexity and the possibility of remembrance. The example questions also reflect practical mathematical probabilities of guessing or determining passwords. With these statistics users can understand at a basic level the ease of password cracking that uses dictionary words or plain obfuscation.

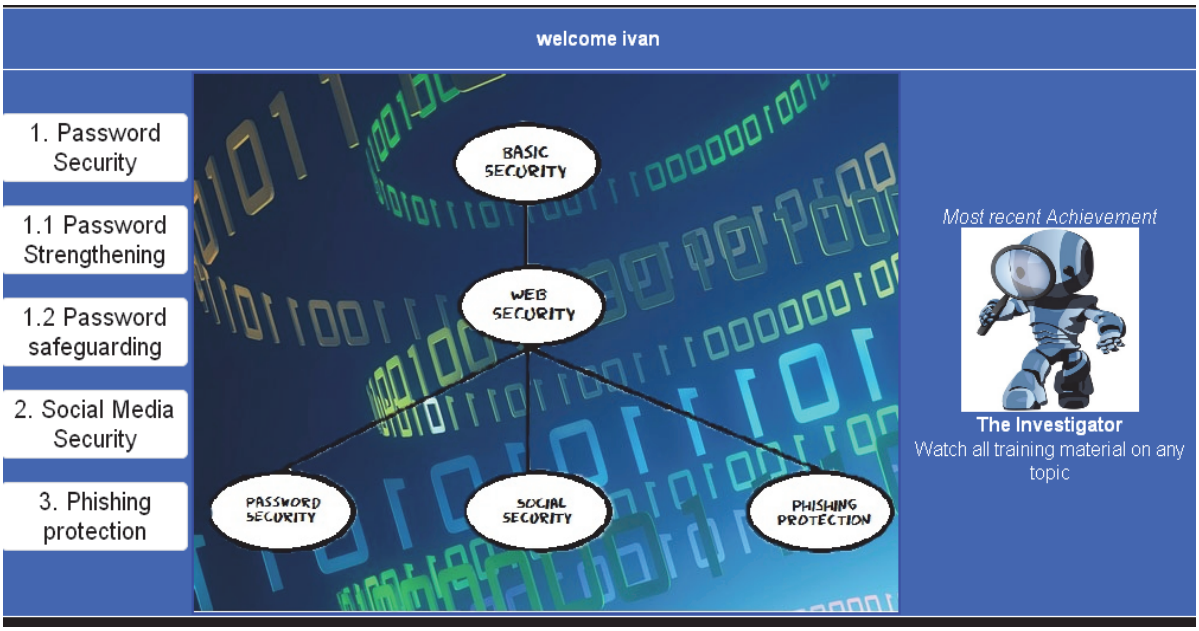

Figure 6. High-level view of game

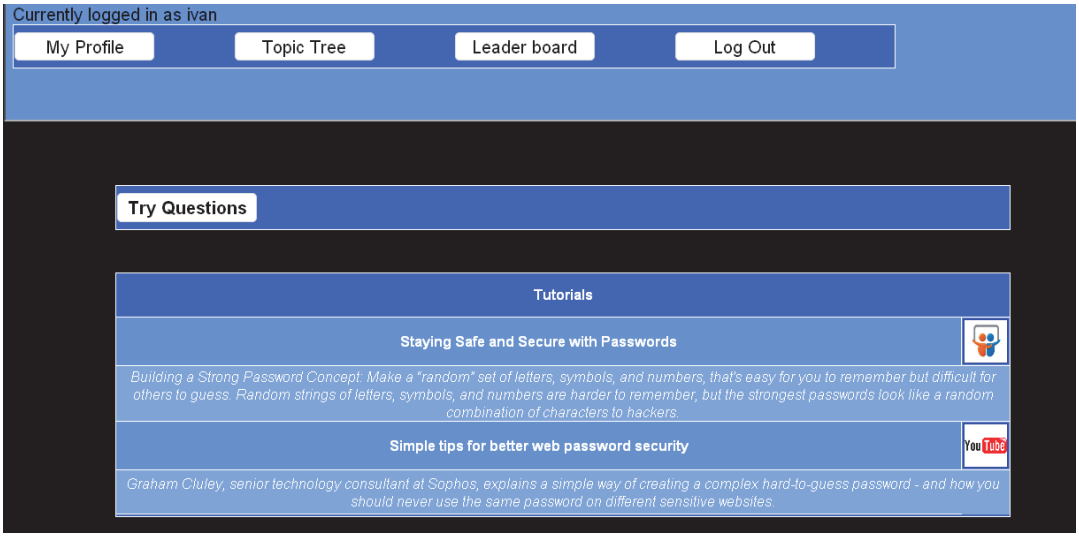

Figure 7. Mix of hypertext and multimedia

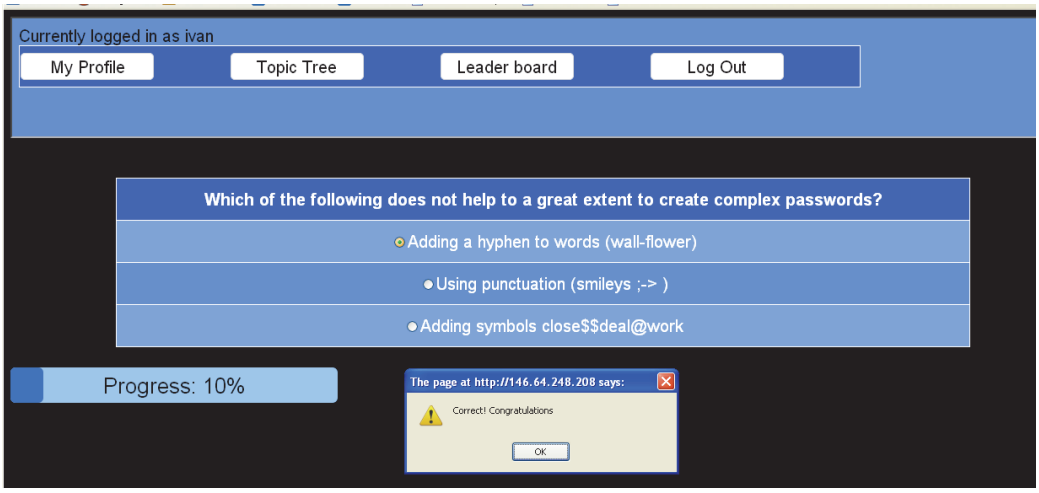

Figure 8. Sample question and status

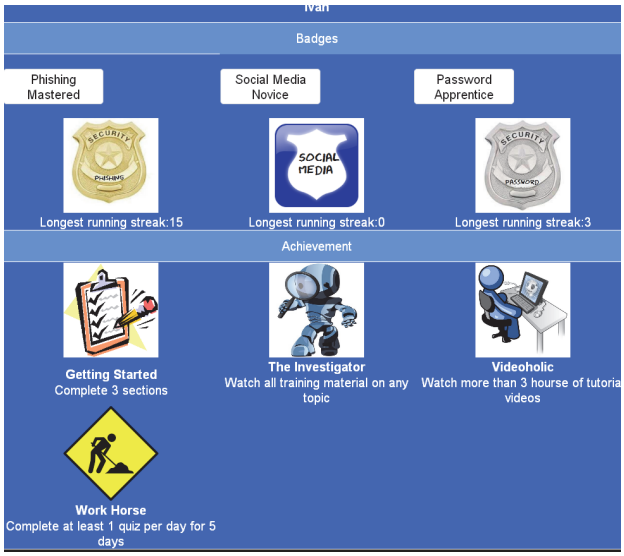

Figure 9. Badge and achievements

The online-game application is automated and does not required human intervention to operate. The game has notifications listing recent achievements. Badges can be awarded to indicate a run of correctly answered questions (see Fig 9). This achievement system promotes return visits as users attempt to attain better scores. For ease of access, the game has been designed to be easily linked to social networking site APIs. Thus, the application can appear as a link on Facebook and users can play the game. Users have the ability to view their friends' scores and thus their friend's progression with the subject matter.

With regards to an effortless interface, the tool directly applies some of the necessary criteria explained by Nielsen [13]. In particular, the system has hyperlinks and status bars to indicate to the users their current location and status. Furthermore, the system has been designed to minimize errors by using hyperlinks for easy navigation and capturing user input through selection controls. Users do not have to recall their current position in the system but can use the controls to identify the desired location. In addition, the interface has been designed with a pleasing aesthetic design, using the theme of cyberspace and security. Relevant information is displayed to ensure that the user understands the instructions and maintains navigational control.

A user's profile displays the badges and achievements attained by the user. The badge and achievement system encourage users to try and attain better scores and complete more sections. By using a social networking application to run the game, users can view their friends' activity and this would also encourage repeat use. In this way, by placing the game in a popular medium such as social networks, the appeal of the game is strengthened and this also promotes user acceptance.

The game has been designed with ease of use and usefulness in mind. Minimalist and intuitive controls, as well as questions providing practical advice form part of the game. Furthermore, since the tool can be linked to social network sites, this provides the requirement of enabling social influences. Since users can view their friends' activities, as well as learn from the game, better online behaviour will be encouraged. With regards to flow, users are able to choose whether they would like to learn more about the security topics from tutorials or take the quizzes. Users are free to curiously navigate the site. By using the mix of hypertext and multi-media the user's attention is attempted to be sustained and thus interest generated from using the game. The basic intuitive design supports effortless playfulness with the game. As the system will rely on social networks for user control, an intrinsic amount of security has been inherited. In addition, the game is simplistic in nature and thus there are no significant potential security flaws. Overall, the game has been designed taking into consideration the various requirements prescribed by the literature.

VI. FUTURE WORK

This work involved the development of a conceptual prototype that encapsulated the identified requirements to enhance security awareness. Future work entails the expansion into a functional prototype that can be effectively used as part of a security awareness programme. In addition, once adequate testing has been completed, the game can be deployed in a social networking site environment.

VII. CONCLUSION

This paper presents the design of an online game, which utilizes social networking sites, to promote cyber security awareness. Initially, decisions need to be made over hypermedia, multimedia and hypertext to achieve perception, comprehension or projection. The game also incorporates various requirements that promote good game design. These include: comprehensive database of questions, weighted system, use of practical data, automation, dynamics, effort and user acceptance. These principles have been applied in the completion of a prototype. Overall, the designed application aims to create awareness on cyber security topics by using a virtual tool to educate and test users using a social networking environment.

REFERENCES

[1] M. Eminagaoglu, E. Uçar and S. Eren, "The positive outcomes of information security awareness training in companies-A case study," Information Security Technical Report, vol. 14, pp. 223-229, 2009.

[2] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," Computers & Security, vol. 27, pp. 241-253, 2008.

[3] E. Kritzinger and S.H. von Solms, "Cyber Security for home users: A New Way of Protection through Awareness Enforcement," Computers & Security, vol. 29, pp. 840-847, November. 2010.

[4] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," Computers & Security, vol. 29, pp. 432-445, 6. 2010.

[5] R.C. Dodge, "Phishing for user security awareness," Computers & Security, vol. 26, pp. 73-80, 2007.

[6] R.S. Shaw, C.C. Chen, A.L. Harris and H. Huang, "The impact of information richness on information security awareness training effectiveness," Computers & Education, vol. 52, pp. 92-100, 1. 2009.

[7] H.A. Kruger and W.D. Kearney, "A prototype for assessing information security awareness," Computers & Security, vol. 25, pp. 289-296, 2006.

[8] C.L. Hsu and H.P. Lu, "Why do people play on-line games? An extended TAM with social influences and flow experience," Information & Management, vol. 41, pp. 853-868, 2004.

[9] D.H. Shin and Y.J. Shin, "Why do people play social network games?" Computers in Human Behavior, 2010.

[10] J. Johnston, J.H.P. Eloff and L. Labuschagne, "Security and human computer interfaces," Computers & Security, vol. 22, pp. 675-684, 12. 2003.

[11] S. Priebatsch, "The game layer on top of the world," vol. Podcast, 2010.

[12] I. Commtouch, "Internet Threats Trend Report," Commtouch., 2011.

[13] J. Nielsen, "10 Heuristics for User Interface Design," Available at http://www.useit.com/papers/heuristic/heuristic_list.html, Accessed 20110121.

[14] F.D. Davis, "A technology acceptance model for empirically testing new end-user information systems: theory and results," Doctoral Dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1986.

[15] J.W. Moon and Y.G. Kim, "Extending the TAM for a World-Wide-Web context," Information & Management, vol. 38, pp. 217-230, 2001.

[16] M. Chuttur, "Overview of the technology acceptance model: Origins, developments and future directions," 2009.

[17] R.B. Cialdini, Influence: The Psychology of Persuasion, Collins, 1998, pp. 336.

[18] M. Csikszentmihalyi, Flow: The Psychology of Optimal Experience, Harper Perennial, 1991, pp. 320.

[19] B.D. Cone, C.E. Irvine, M.F. Thompson and T.D. Nguyen, "A video game for cyber security training and awareness," Computers &.Security., vol. 26, pp. 63-72, 2. 2007.

[20] The Center for Information Systems Security Studies and Research, INC., "CyberCIEGE Educational Video Game," "CyberCIEGE Educational Video Game," Available at: http://www.cisr.us/cyberciege/,Accessed 20110110.

[21] Department of Defence (United States of America), DOD., "CyberProtect," Available at http://iase.disa.mil/eta/cyber-protect/launchpage.htm., Accessed 20110110.

[22] S. Khan, "Let's use video to reinvent education," Availabe at http://www.ted.com/talks/salman_khan_let_s_use_video_to_reinvent_education.html, Accessed 20110121.,