ESTABLISHING CYBERSECURITY AWARENESS OF TECHNICAL SECURITY MEASURES THROUGH A SERIOUS GAME

Jaden Harding, Dirk Snyman and Günther Richard Drevin
School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom, South Africa

ABSTRACT

Cybersecurity is broadly considered an important concept for the protection of individuals and families, and also governments and organizations from online threats. This importance notwithstanding, there is a lack of understanding regarding cybersecurity globally, not only within the working class but within the general public. It can therefore be deduced, that there must also exist a lack of understanding regarding the technical principles of cybersecurity, such as how an individual's computer keeps them safe within an online environment using techniques such as firewalls and cryptography. This paper addresses this lack of understanding by means of a serious game.

KEYWORDS

Serious Games, Information Security Awareness, Cybersecurity

1. INTRODUCTION

Cybersecurity is broadly considered a very important concept for the protection of individuals and families, as well as government and organizations from online threats (Goutam, 2015). This importance notwithstanding, there is a lack of awareness regarding good cybersecurity practices, not only within the working class but also within the general public (Aldawood & Skinner, 2018). It further stands to reason that, given this lack of awareness, there should exist a lack of understanding regarding the technical principles of cybersecurity measures, e.g., how an individual's computer keeps them safe within an online environment using techniques such as firewalls and cryptography. This global phenomenon is further exacerbated in developing countries, such as South Africa. Technology is commonly used by many, but there is a lack of formal digital literacy which is a result of high levels of unemployment and lower levels of education (Sutherland, 2017). A possible modern solution to addressing the lack of digital literacy, is the use of serious games (Laamarti et al., 2014).

Serious games can be defined as an approach to active learning in which pedagogy is incorporated into a game with the purpose of providing organised education and training (Greitzer et al., 2007). These games involve activities that instruct and educate, yielding results such as skills and knowledge. The twofold goal behind a serious game is therefore: to be educational; and to be enjoyable and entertaining. Considering the immense growth and the expected future growth, as well as its current application in numerous areas (Laamarti et al., 2014), there is a consensus that serious games are a valid method for education and awareness.

Therefore, the aim of this paper is *to describe the initial development of a proof-of-concept serious game aimed at raising awareness and understanding of these cybersecurity techniques and practices*.

The remainder of the paper is structured as follows: **Section 2** provides a summary of the literature pertaining to cybersecurity awareness, and serious games. Literature on the combination of Serious games for teaching cybersecurity principles is discussed in **Section 3**, while **Section 4** is used to illustrate the proof-of-concept game that is proposed in this research. Finally, **Section 5** summarises the findings and possible future work.

2. RELATED LITERATURE

In this section, a brief overview of related literature is presented in a two-fold manner, i.e., literature about cybersecurity and related concepts is summarised, and a cursory overview of serious games is provided.

2.1 Cybersecurity Awareness

Cybersecurity and its awareness are the core themes of the given problem description; however, cybersecurity is a commonly used term, and its definition often varies depending on the context and interpretation. A definition which suits the purpose of this research is:

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU, 2009:2).

Cybersecurity produces defensive procedures, which conserve the integrity, availability and confidentiality of devices and data by protecting them against malware, vulnerabilities, and threats (Jang-Jaccard & Nepal, 2014). Malware refers to a large class of threats, which are loaded onto a system, compromising the integrity, availability, and confidentiality of data, without the knowledge of the user. Examples include viruses, spyware, trojan horses and bot executables (Jang-Jaccard & Nepal, 2014). A vulnerability is a weakness in a system's functionality or design, which allows an outside threat to execute code, gain access to private information and launch denial-of-service attacks. A threat refers to an activity that exploits a system's security flaws and consequently endangers it (Abomhara & Køien, 2015). Once present on a user's system, malware targets hardware, software flaws, and network infrastructure and protocol weaknesses (Jang-Jaccard & Nepal, 2014).

With the increasing use of network devices among the public, cyberattacks are becoming more common, and the security precautions against them are a vital part of Information Technology governance (Ben-Asher & Gonzalez, 2015). Reports of cyberespionage, cybercrimes, and the exploitation of data breaches emerge daily, as organisations and government agencies are compromised, and sensitive information is stolen. Essential infrastructure such as financial markets, communication systems, and electric power grids are vulnerable to cyberattacks (Spidalieri & Kern, 2014). Furthermore, a need for education and awareness of cybersecurity is essential. Society cannot expect modern security technologies, which are crucial components of cybersecurity, to secure an organisation's information and operations alone, nor should cybersecurity experts be the only ones with the responsibility of preventing and suppressing cyber threats, but all members of organisations share responsibility (Spidalieri & Kern, 2014) which can only be facilitated through a keen awareness of cyber threats.

Cyber risk in an organisation can be attributed to two types of employees: malicious or negligent: Malicious insiders are employees who intentionally endanger or harm an organisation, in order to benefit themselves or an outside entity. They might do so by stealing or distributing sensitive information, damaging networks and network devices, or committing fraud for financial gain. Negligent or error-prone insiders unintentionally harm or endanger an organisation through carelessness or a lack of knowledge. This can occur by an employee sharing too much personal information online, falling victim to phishing attempts, losing hardware with sensitive information, or accidentally creating a vulnerability when configuring software (Bailey et al., 2018).

2.2 Serious Games

Serious games are the method by which this research paper plans to attempt to increase awareness of cybersecurity. Suitable definitions for serious games are:

"Serious games are designed to have an impact on the target audience, which is beyond the pure entertainment aspect. One of the most important application domains is in the field of education given the acknowledged potential of serious games to meet the current need for educational enhancement" (Bellotti et al., 2013:1).

Considering the significant growth in the field of serious games within the 21st century, it is a consensus that serious games are a valid form of education and learning (Laamarti et al., 2014). Blunt (2009), conducted three studies in an attempt to confirm the validity of serious games. The first study was conducted at a

university to analyse the impact of the implementation of a simulation game into an Introduction to Business and Technology course. One-fifth (227) of the total students (1028) played the game, and the results indicated that students who did not play the game averaged just under 80%, and those who did, averaged just over 90% for the course test. The second study evaluated the addition of another simulation game, on university economic course students, to better understand the application of various concepts. 322 of the total 556 students played the game, and the results indicated, similarly to the first study, that the average of students who did not play the game was just below 80%, and those who did average above 90%. The aim of the final study was to compare the effectiveness of the implementation of a serious game, by means of various variables such as test score, gender, ethnicity, and age, on third-year management students. Half of the class was given the game to play. The final results indicated that the average test scores of students who had not played the game were below 70%, and those who did play the game averaged just below 90%. From these three studies on a variety of students, it is seen that serious games are effective and viable forms of learning and education.

Serious games are applicable in a number of areas such as education and training, wherein games are used in classrooms for education, as the study by Blunt (2009) confirms; well-being, wherein serious games are used to increase the physical activity of its players, through motivation and reward systems; advertisement, where specific brands and products are promoted to players while playing the game; cultural heritage, which allows players to interact with reconstructed scenes from virtual representations of history and ancient sites, and interpersonal communication, with games that allow players to speak in the game and improve their communication skills and in some games, learn culturally appropriate expressions and gestures (Laamarti et al., 2014).

Examples of successful serious games are Supercharged!, a game created with the goal of improving physics education, focusing on electromagnetism (Jenkins et al., 2003); Biohazard, a component of the training program for firefighters to perform effectively in terrorist situations (Carnegie Mellon Entertainment Technology Center & Scientists, 2004); Re-Mission, which was used to improve the knowledge and understanding of cancer patients, on how various treatments such as chemotherapy work, which in turn improved their well-being (Tate et al., 2009); and SnowWorld, used to lessen pain and distract patients who suffered burns during daily wound cleaning and physical therapy (Hoffman, 2004).

The main goal of serious games, and therefore the greatest challenge, is twofold. Firstly, and most importantly, serious games must be educational. Secondly, the game must be entertaining and captivating (Bellotti et al., 2013). Some challenges such as those from the social, educational, and technological dimensions should also be considered. The social dimension involves the negative view games have from society, as they have been associated with addiction, violence, and sexism in extreme cases (Griffiths, 2010). Games also seem a more playful and less serious activity for the education system. The educational dimension is connected to concerns about the educational value of games, their effectiveness when compared to traditional methods, and the issues that arise when assessments are considered. The technological dimension consists of issues such as the cost of creating and implementing the game, and the tools necessary to facilitate the game (Fernández-Manjón et al., 2015).

2.3 Cybersecurity Awareness Through Serious Games

From the literature regarding cybersecurity awareness and serious games respectively, we can now deduce that there is a lack of, and need for, awareness of cybersecurity and that serious games are capable of being more effective than traditional methods for educating and increasing awareness, due to their interactive nature.

There is a need to properly inform and teach users how to protect themselves from cyber risks, considering how often cyberattacks are successful. It has been suggested that serious games can be used for cybersecurity training and awareness and that the use of such training and awareness programs has the potential to attract more individuals to the field, which in turn can help close the cybersecurity workforce gap (VanSteenburg, 2017).

Le Compte et al. (2015) state that it will be advantageous to gamify cyber security education and training. While serious games have shown pedagogic value in this field, they have only been applied in a small number of contexts, and some limitations have been identified. Le Compte et al. (2015) propose that serious games could be utilised in more informal settings, and still produce comparable pedagogical outcomes. Using

serious games in this manner has the potential to reach a wider audience than more formal serious games, and still adhere to national cyber strategies.

There has been an increase in the use of serious games for cybersecurity training and education over recent years, however, VanSteenburg (2017:56) remarks that *"Research is still limited, and additional studies must be conducted to better understand the specific elements of serious games that are effective"*

Therefore, serious games are an appropriate and effective way of increasing awareness and educating learners and the general public of cybersecurity and its principles. The next section shows the proof-of-concept cybersecurity game that is developed to raise awareness of technical cybersecurity measures.

3. CYBERSCENE GAME

CyberScene is a proof-of-concept single-player mobile serious game, which aims to educate the public about technical cybersecurity principles by means of various mini-games. These mini-games will cover a number of topics and increase awareness and educate the player, while they play. An example of one of these mini-games is a *cryptography cipher-solving game*. The game will consist of various phases wherein the user will learn more about and then solve a specific cipher:

Cipher information – After selecting a difficulty, the user will be given information regarding a specific cipher. As can be seen in Figure 1, the user receives a theoretical explanation of the Caesar cipher, as well as an image to further help them understand.

Cipher testing – To further improve understanding, the user is given a screen wherein they are allowed to test the cipher previously discussed. In Figure 2, the user is able to enter any sentence or arrangement of letters, as well as the numeric value that the sentence should shift left, to personally test the cipher and learn by these means.

Cipher solving – Finally, the user will be prompted with a series of questions, which ask them to apply the previously learnt cipher to a given input. In Figure 3, the user is asked to apply the Caesar cipher to a simple sentence. When the user enters their solution, a simple message will alert them whether they are correct, or whether they need to try again. When they solve the cipher, they can return to the difficulty selection screen, or continue questions of the previously chosen difficulty.

The paper is concluded in the following section where future work is also discussed.

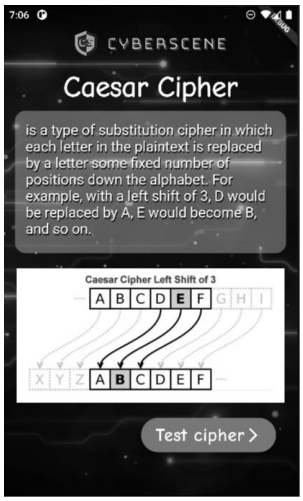

Figure 1. Layout of cipher information screen

Figure 2. Layout of cipher testing screen

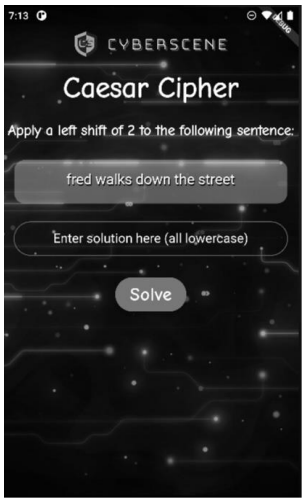

Figure 3. Layout of cipher solving screen

4. CONCLUSION AND FUTURE WORK

Given that the current version of Cyberscene is a proof-of-concept, there are various limitations which cannot be addressed at the given time. Incentives are an important concept within serious games, to improve enjoyability, and will be implemented in future research. CyberScene has a variety of advantages which will allow it to be a successful game. The game is mobile-accessible and user-friendly, allowing a large portion of the general population to access it. The difficulty is scalable and therefore allows for a larger player base. Given the mini-games style of the game, it is easy to provide future updates with new games providing previously unknown information in the field of cybersecurity, which provides endless applications to inform and educate users. Future work includes expanding the mini-game to provide the user with incentives, and competitively driven rewards. With the implementation of a user login, gamification elements such as achievements and badges can be incorporated. These include timed achievements, to measure how quickly they are able to solve ciphers. Users could also receive a CyberScene currency, which would allow them to redeem in-game items or purchase locked mini-games that address further security awareness concepts.

REFERENCES

Abomhara, M. and Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility:65–88.*

Aldawood, H. and Skinner, G., (2018). December. Educating and raising awareness on cyber security social engineering: A literature review. In 2018 *IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. IEEE, pp. 62-68.

Bellotti, F., Kapralos, B., Lee, K., Moreno-Ger, P. and Berta, R. (2013). Assessment in and of Serious Games: An Overview. *Advances in Human-Computer Interaction, 2013:136864.*

Ben-Asher, N. and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48:51-61.*

Blunt, R. (2009). Do Serious Games Work? Results from Three Studies. *eLearn, 2009(12):Article 1.*

Carnegie Mellon Entertainment Technology Center and Scientists, M. C. F. o. A. 2004. Team Hazmat.

Fernández-Manjón, B., Moreno-Ger, P., Martinez-Ortiz, I. and Freire, M. (2015). Challenges of serious games. *EAI Endorsed Transactions on Serious Games, 2(6).*

Goutam, R.K., (2015). Importance of cyber security. *International Journal of Computer Applications*, *111*(7).

Greitzer, F.L., Kuchar, O.A. and Huston, K., (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. *Journal on Educational Resources in Computing (JERIC)*, *7*(3): 2:1-2:16.

Griffiths, M. (2010). Adolescent video game addiction: Issues for the classroom. *Education Today, 60(4):32-34.*

Hoffman, H. G. (2004). Virtual-reality therapy. *Scientific American, 291(2):58-65.*

ITU (2009) 'Overview of Cybersecurity', *Recommendation ITU-T X.1205*. Available at: http://www.itu.int/rec/T-REC-X.1205-200804-I/en.

Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80(5):973-993.*

Jenkins, H., Klopfer, E., Squire, K. and Tan, P. (2003). Entering the education arcade. *Computers in Entertainment (CiE), 1(1):1-11.*

Laamarti, F., Eid, M. and El Saddik, A. (2014). An Overview of Serious Games. *International Journal of Computer Games Technology, 2014:358152.*

Le Compte, A., Elizondo, D. and Watson, T. (2015). A renewed approach to serious games for cyber security. *Proceedings of the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace: IEEE, pp. 203-216.*

Spidalieri, F. and Kern, S. (2014). Professionalizing cybersecurity: A path to universal standards and status. *Newport, RI: Pell Center for International Relations and Public Policy, Salve Regina University.*

Sutherland, E., 2017. Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication, 20:83-112.*

Tate, R., Haritatos, J. and Cole, S. (2009). HopeLab's approach to Re-Mission. *International journal of Learning and Media, 1(1):29-35.*

VanSteenburg, M. (2017). Applications of serious gaming to cybersecurity training and awareness. Master's Thesis, *Utica College.*