Proceedings of the 2020 AIS SIGED International Conference on Information Systems Education and Research

SIGED: IAIM Conference

12-21-2020

THE USE OF GAMIFICATION TO TEACH CYBERSECURITY AWARENESS IN INFORMATION SYSTEMS

Joshua C. Nwokeji
Department of Computer and Information Science Gannon University, Erie PA, USA,
nwokeji001@gannon.edu

Richard Matovu
Department of Computer and Information Science, Gannon University, Erie PA, USA,
matovu001@gannon.edu

Bharat Rawal
Department of Computer and Information Science Gannon University, Erie PA, USA,
rawalksh001@gannon.edu

The Use of Gamification to Teach Cybersecurity Awareness in Information Systems

Extended Abstract

Joshua C. Nwokeji
Department of Computer and Information Science
Gannon University, Erie PA, USA
nwokeji001@gannon.edu

Richard Matovu
Department of Computer and Information Science
Gannon University, Erie PA, USA
matovu001@gannon.edu

Bharat Rawal
Department of Computer and Information Science
Gannon University, Erie PA, USA
rawalksh001@gannon.edu

Abstract:

This paper investigates the impact of gamification in teaching and learning cybersecurity awareness. The increasing rate of cyber-attacks and data breaches in recent times, have made cybersecurity awareness a critical learning objective in Information Systems (IS) curriculum globally. However, teaching and learning cybersecurity awareness can be challenging, especially to smaller colleges and universities who have meagre resources. Moreover, learning cybersecurity principles requires understanding of concepts that are usually unfamiliar to students in the IS major. In order to effectively deliver the desired learning objectives in cybersecurity awareness, IS educators can adopt pedagogical approaches, e.g., gamification, that are interactive, fun and appealing to students. Gamification which has been defined as the use of game components to deliver learning objectives in a given area, offer an alternative that is affordable, easy to learn and requires very little to no overhead cost. Currently, the authors are designing 3 gamified activities that can be used to teach and learn cyber security awareness. We intend to validate the effectiveness of these activities using experimental approaches. Students will be randomly selected from universities in Northern Pennsylvania, USA, and divided into experimental and control group. Experimental group will be asked to complete the gamified activities. Data will be collected using questionnaire. Data analysis will be by means of statistical approaches such as ANOVA, paired t-test of factor analysis. We hope that the results of our study will support the use of gamification in teaching and learning cybersecurity awareness.

Keywords: Gamification, Cybersecurity, Cyber awareness, Cyber-attacks, Cyber-threats

I. Introduction

The increasing rate of cyberattacks and data breaches due to human errors, has made cybersecurity awareness a necessary learning outcome in the information systems curriculum (Abawajy 2014; Pawlowski and Jung 2019). Insufficient awareness of basic cybersecurity concepts has been identified as a major factor currently threatening the security of information technology (IT) infrastructure in contemporary organizations (Olano et al. 2014). In recent times, a considerable amount of damaging cyberattacks and data breaches, for example see (Green et al. 2020), result from ignorance and lack of awareness by users of IT systems. Indeed, the consequences of such cyberattacks and data breaches can be very severe to

individuals, academic institutions, private organizations and government. According to the "Cost of Data Breach" Report published by IBM (IBM Security 2019), USA organizations lost an average of USD 8.19 Million to data breaches in 2019. This report also noted that data breaches increased at an alarming rate of 130% between 2006 and 2019. Organizations are now faced with the daunting challenge of protecting their data, software, hardware and other information systems infrastructure from the nefarious activities of cybercriminals (Pawlowski and Jung 2019).

Cybercriminals can attack IT infrastructure by exploiting vulnerabilities in four major aspects of information systems, these include hardware, networks, software and users. Hardware and networks vulnerabilities results from weaknesses in networks devices, servers, routers, CPUs, PCs and other hardware devices used in an organization; while software vulnerabilities result from weaknesses in software such as operating systems, firmware, database systems, and enterprise applications (Green et al. 2020; IBM Security 2019). In the fourth aspect, cybercriminals exploit lack of training or insufficient awareness of basic cybersecurity concepts of the users (Green et al. 2020; IBM Security 2019; Olano et al. 2014). Due to recent advances in cybersecurity and information systems assurance, computing experts have developed and deployed sophisticated strategies to mitigate hardware, network and software vulnerabilities. For instance, firewalls, security groups, cryptographic systems, as well as advanced encryption and hashing mechanisms have been deployed in recent times to secure information systems infrastructure from cybercriminals (Abawajy 2014)(Akbari Roumani et al. 2016). However, insufficient awareness of cybersecurity concepts, threats and attacks by users have not been properly addressed (Olano et al. 2014). Moreover, many scholars (Olano et al. 2014)(Abawajy 2014)(Raman et al. 2014) have emphasized the need for users of information systems to receive adequate training and awareness of basic cybersecurity concepts.

Cybersecurity awareness is thus an important subject that must be taught, not only to Information Systems (IS) majors, but also to other computing and non-computing majors. However, teaching and learning cybersecurity awareness is by no means an easy task. Cybersecurity awareness requires understanding, differentiation and application of concepts that are usually unfamiliar to students. In order to effectively deliver the desired learning objectives in cybersecurity awareness, educators should adopt pedagogical approaches that are interactive, fun and appealing to students. Gamification is an excellent example of this type of approach and has been defined as the use of digital and non-digital games or game components, especially in non-entertainment context, to achieved desired objectives (Schöbel et al. 2020).

Gamification has been successfully applied to deliver important outcomes in other disciplines and can also be used to deliver learning outcomes in cyber awareness. For example, two studies (Alqahtani et al. 2020; Scholefield and Shepherd 2019) have used gamified mobile application to motivate students learn cybersecurity concepts. Moreover, there has been a growing interests in the use of gamification in pedagogy in recent times (Ofosu-Ampong 2020; Schöbel et al. 2020). Unlike existing pedagogical methods such as project-based learning (Aqlan and Nwokeji 2018; Nwokeji et al. 2018; Nwokeji and Frezza 2017) and flipped classroom (Lage et al. 2000; Nwokeji et al. 2019; Nwokeji and Holmes 2017), gamification has more potentials to facilitate the understanding of complex and unfamiliar concepts associated with cybersecurity (Olano et al. 2014). The benefits of using gamification as pedagogical methods have been well researched and reported in literature. For instance, Gamification can help students to acquire desired competences such as problem solving skill, critical thinking and teamwork (Ofosu-Ampong 2020; Schöbel et al. 2020).

In spite of these potential benefits, only a handful of published work e.g., (Alqahtani et al. 2020; Lika et al. 2018; Quayyum 2020; Scholefield and Shepherd 2019) have contributed to the application of gamification in teaching cybersecurity awareness in the IS literature. Moreover, other available publications such as (Alotaibi et al. 2016; Quayyum 2020) are either literature reviews or analysis of challenges in using gamification to IS courses. Unfortunately, these usually lack the actual design, implementation and use of digital or non-digital games elements in teaching IS courses. While we commend the contributions of the existing publications, we believe that more studies in this area will be beneficial to IS educators, especially those considering or planning to integrate gamification in their cybersecurity or other courses. In order to bridge this gap in literature and support research endeavor in the area of gamification in IS education, the authors are currently designing game components that can be used to teach cybersecurity awareness to students. The research questions (RQ) under consideration are as follows: RQ1: *Does gamification improve students' knowledge and awareness of cyber-attacks and cyber-threats?* RQ2: *How do students perceive the use of gamification as an instructional method in a cybersecurity course?* We plan to answer

these research questions and thus validate our game components by conducting experiment with students from 2 universities in Northwestern Pennsylvania, USA. Students will be divided into experiment group and control group. The experiment group will be asked to complete the gamified activities, which we are currently designing using the principles of gamification. While the control group will not participate in the activities. Before the experiment, we will ask all participants (both experiment and control group) to complete a questionnaire without telling them about the experiment or the reason they are completing the questionnaire. This questionnaire will ask these students to rate their knowledge and awareness of randomly selected popular cyberattacks and cyberthreats (n=18). Afterwards, we will divide the experimental group into teams to perform 3 gamified activities. To ensure that our study is salient, appropriate and relevant to our study audience (i.e., young students that aren't technically sophisticated), we selected these cyberattacks, threats from two popular cybersecurity youth competitions run throughout the US i.e., CyberPatriots[1] created by Air Force Association, and GenCyber[2] funded by NSA and NSF. At the end of these activities, we will administer another questionnaire identical to the first questionnaire to the experimental groups, so that they can rate their knowledge and awareness of those same (n=18) cyberattacks and threats, after they completed the gamified activities. Data analysis will be by means of various statistical methods (such as ANOVA, t-test, among others) to ensure accuracy of our results. The results will be submitted for consideration in IS journal or conference proceedings afterwards.

II. Reference

Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods," *Behaviour & Information Technology* (33:3), Taylor & Francis, pp. 237–248.

Akbari Roumani, M., Fung, C. C., Rai, S., and Xie, H. 2016. "Value Analysis of Cyber Security Based on Attack Types," *ITMSOC: Transactions on Innovation and Business Engineering* (1), ITMSOC Working Group, pp. 34–39.

Alotaibi, F., Furnell, S., Stengel, I., and Papadaki, M. 2016. "A Review of Using Gaming Technology for Cyber-Security Awareness," *Int. J. Inf. Secur. Res.(IJISR)* (6:2), pp. 660–666.

Alqahtani, H., Kavakli-Thorne, M., and Alrowaily, M. 2020. "The Impact of Gamification Factor in the Acceptance of Cybersecurity Awareness Augmented Reality Game (CybAR)," in *International Conference on Human-Computer Interaction*, pp. 16–31.

Aqlan, F., and Nwokeji, J. C. 2018. "Applying Product Manufacturing Techniques to Teach Data Analytics in Industrial Engineering: A Project Based Learning Experience," in *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1–7.

Green, A. W., Woszczynski, A. B., Dodson, K., and Easton, P. 2020. "Responding to Cybersecurity Challenges: Securing Vulnerable US Emergency Alert Systems," *Communications of the Association for Information Systems* (46:1), p. 8.

IBM Security. 2019. "Cost of a Data Breach Report." (https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.127586571.703341566.1581607433-1758793570.1580324565&_gac=1.255946361.1581607433.CjwKCAiAhJTyBRAvEiwAln2qB--ADUK_ndICq-iJGXRL8eZ9d03FP3NTf5-FsQwiNbRqADh7E_haQRoCDjQQAvD_BwE).

Lage, M. J., Platt, G. J., and Treglia, M. 2000. "Inverting the Classroom: A Gateway to Creating an Inclusive Learning Environment," *The Journal of Economic Education* (31:1), Taylor & Francis, pp. 30–43.

[1] https://www.uscyberpatriot.org/

[2] https://www.gen-cyber.com/

Lika, R. A., Murugiah, D., Brohi, S. N., and Ramasamy, D. 2018. "NotPetya: Cyber Attack Prevention through Awareness via Gamification," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 1–6.

Nwokeji, J. C., Aqlan, F., Olagunju, A., Holmes, T., and Okolie, N. C. 2018. "WIP: Implementing Project Based Learning: Some Challenges from a Requirements Engineering Perspective," in *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1–5.

Nwokeji, J. C., and Frezza, S. T. 2017. "Cross-Course Project-Based Learning in Requirements Engineering: An Eight-Year Retrospective," in *Proceedings - Frontiers in Education Conference, FIE* (Vol. 2017-Octob). (https://doi.org/10.1109/FIE.2017.8190731).

Nwokeji, J. C., and Holmes, T. S. 2017. "The Impact of Learning Styles on Student Performance in Flipped Pedagogy," in *Proceedings - Frontiers in Education Conference, FIE* (Vol. 2017-Octob), pp. 1–7. (https://doi.org/10.1109/FIE.2017.8190522).

Nwokeji, J. C., Stachel, R., and Holmes, T. 2019. "Effect of Instructional Methods on Student Performance in Flipped Classroom," in *2019 IEEE Frontiers in Education Conference (FIE)*, pp. 1–9.

Ofosu-Ampong, K. 2020. "The Shift to Gamification in Education: A Review on Dominant Issues," *Journal of Educational Technology Systems*, SAGE Publications Sage CA: Los Angeles, CA, p. 0047239520917629.

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Sohn, I., and Thomas, D. 2014. "SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Pawlowski, S. D., and Jung, Y. 2019. "Social Representations of Cybersecurity by University Students and Implications for Instructional Design," *Journal of Information Systems Education* (26:4), p. 3.

Quayyum, F. 2020. "Cyber Security Education for Children Through Gamification: Challenges and Research Perspectives," in *International Conference in Methodologies and Intelligent Systems for Techhnology Enhanced Learning*, pp. 258–263.

Raman, R., Lal, A., and Achuthan, K. 2014. "Serious Games Based Approach to Cyber Security Concept Learning: Indian Context," in *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*, pp. 1–5.

Schöbel, S., Janson, A., Jahn, K., Kordyaka, B., Turetken, O., Djafarova, N., Saqr, M., Wu, D., Söllner, M., Adam, M., and others. 2020. "A Research Agenda for the Why, What, and How of Gamification Designs: Outcomes of an ECIS 2019 Panel," *Communications of the Association for Information Systems* (46:1), p. 30.

Scholefield, S., and Shepherd, L. A. 2019. "Gamification Techniques for Raising Cyber Security Awareness," in *International Conference on Human-Computer Interaction*, pp. 191–203.

III. Appendix

Dr. Joshua C. Nwokeji is an associate professor (information systems) and graduate program director at the department of computer and information science (CIS), Gannon University, Erie PA. He receives his Ph.D., from Middlesex University London, United Kingdom.

Dr. Richard Matovu is an assistant professor (cybersecurity) at the department of computer and information science (CIS), Gannon University, Erie PA. He receives his Ph.D., from Texas Tech University, USA.

Dr. Bharat Rawal is an associate professor (cybersecurity) and director of cybersecurity program at the department of computer and information science (CIS), Gannon University, Erie PA.