Cyber Security Education for Children through Gamification: Research Plan and Perspectives

Farzana Quayyum
Norwegian University of
Science and Technology
(NTNU)
Trondheim, Norway
farzana.quayyum@ntnu.no

Abstract

With the advancement of technology and the development of new tools, games, applications and social media sites, it is getting difficult every day to keep up with threats and vulnerabilities associated with these tools, apps or websites, especially for children. The goal of this research is to investigate and further develop new knowledge and tools that will be helpful and effective to teach the children about cyber security by performing various gamified actions in a playful, engaging and motivating manner. The methodology of this research would be both qualitative and quantitative, using interviews, questionnaires, focus group and observations. Initially, this project will define the theoretical and existing practices of cyber security awareness education for children. In the next phase, this research will design and implement interventions based on learning activities like workshops and collaborative tasks; followed by empirical test and evaluation of the proposed interventions.

Author Keywords

Cyber Security Education; Cyber Security Awareness; Internet Security; Children; Gamification.

CSS Concepts

• **Human-centered computing~Human computer interaction (HCI)**; *Haptic devices*; User studies; Please use the 2012 Classifiers and see this link to embed them in the text:
https://dl.acm.org/ccs/ccs_flat.cfm

Introduction

Children nowadays play a lot of online games and browse the internet for several hours every day. On the internet, they meet several opportunities as well as risks; but without relevant knowledge, it is difficult for them to assess the associated risks or threats of using the internet and digital systems. Sometimes they do not even realize the danger of the risks. Thus, they can

CHI 2020 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA.
© 2020 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6819-3/20/04.
DOI: https://doi.org/10.1145/3334480.XXXXXXX
*update the above block & DOI per your rights review confirmation (provided after acceptance)

easily fall victim to cyber security threats like social engineering, cyber stalking, hacking, viruses, and malware, etc. through search engines, online advertisements and social networking websites such as Facebook, Twitter and lots of other websites [1].

Game or application	Purpose or Goal
Anti-phishing Phil [15]	Training for links (URL) safety
CyberCIEGE [16]	Training on all kinds of social engineering threats
Serious games comprising of reward systems [17]	Training on mobile threats, phishing, and cyber-attacks
HATCH: Hack and Trick Capricious Humans [18]	Training on hacking, phishing, physical manipulations, spear phishing
Cyber security Lab [19]	Designed to teach young people basic cyber security skills

Table 1: Example of some cyber security-based games and gaming applications

While security practices rely on several factors, one of them is how well people are aware of the threats and how well they can assess the risk and apply their knowledge to mitigate threats [2]. Therefore, mitigating the human-related errors or vulnerabilities is a dominant factor for improving security either at a personal or organizational level; and we can do this by raising user awareness on cyber security and privacy issues [3, 4]. Considering the importance of human-related vulnerabilities, in this research we aim to focus on the education of children about cyber security awareness and online etiquette.

Background and Motivation

When education starts becoming fun and attractive, children also become more motivated and interested in learning. Using computer games for educational purposes is now very popular. According to [5], there are two categories of games that are used to educate and train users: gamification and serious games. Gamification's main goal is to foster more engagement in people by helping to create more robust experiences in everyday life events utilizing game mechanics; while serious games are designed to train and are used for stimulation and to educate in virtual environments with previously defined learning objectives [6, 7]. In recent years, gamification of applications is getting a lot of attention from various fields including education. Considering this popularity and momentum, in this research we will focus on gamification as the technique to educate children about cybersecurity awareness.

Various studies have been previously carried out and many cyber security-based gaming applications have been developed in the last few years to educate users; some examples are mentioned in Table 1. Most of the studies have indicated positive results and impact on the users, in using games and gaming applications as a tool for education on cyber security. But there are still many gaps and issues that need to be addressed by the community. For example, many of the games and applications are often part of research projects and get developed systematically or rapidly, after their evaluation they often disappear and are rarely available to the public [9]. Other issues that the researchers mentioned include showing positive feedback but not evaluating the impact and effects in terms of learning outcomes or not presenting a conclusive result from the research, using a small sample size for evaluation, etc. [9]. Thus, building upon previous research studies on motivating children about learning and practicing cyber security knowledge, the purpose of this research is to address the existing gaps and to investigate and further develop new knowledge and tools that will help teach the children about cyber security using gamification.

Research Goals and Method

This research targets 8-10th grade students (13-16 years old) of secondary schools. We are targeting this age group because many pieces of research, for example, [10, 11] show that children of this age are more prone to engage in risky internet behavior, as they have easy access to many kinds of digital devices and almost all possibilities that internet provides [10].

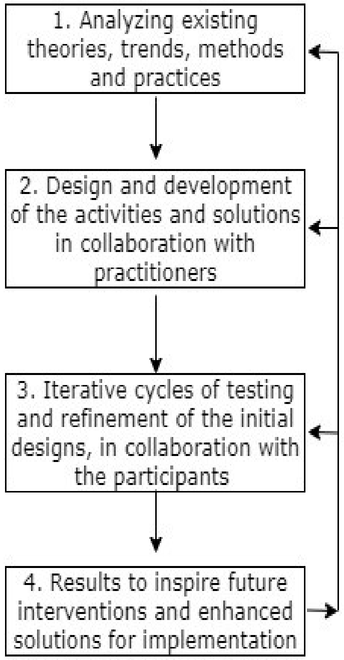
1. Analyzing existing theories, trends, methods and practices
2. Design and development of the activities and solutions in collaboration with practitioners
3. Iterative cycles of testing and refinement of the initial designs, in collaboration with the participants
4. Results to inspire future interventions and enhanced solutions for implementation

Figure 1: Design-based research approach, adapted from [14]

Research Questions

We can express the problem foundation of this research by the following research question.

RQ: How can we help children to learn about cyber security, using gamification?

To investigate this overall question and its parameters, we have defined the following sub-questions (SQ) that have been set as a part of this research.

SQ1: What are the trends in gamification of cyber security education?

SQ2: What type of cyber security knowledge and education do children need?

SQ3: How can we make a sustainable solution for cyber security education?

SQ4: How to measure the effectiveness of the proposed solution?

SQ5: How do gender, cultural differences, and social issues influence children's learning on cyber security?

Research Method

Considering the context of this research, we have chosen Design-Based research (DBR) as our research methodology. Design-Based research is "A systematic but flexible methodology aimed to improve educational practices through iterative analysis, design, development, and implementation, based on collaboration among researchers and practitioners in real-world settings, and leading to contextually-sensitive design principles and theories" [12].

Following the DBR process, as shown in Figure 1, we will perform iterative cycles, starting by surveying existing trends, methods and their limitations for achieving a high impact in cyber security education. We are currently conducting an in-depth systematic literature review based on the original guidelines as proposed by Kitchenham [13] to answer the first two sub-questions of this research (SQ1 and SQ2). The literature review initially resulted in 64 citations, but after applying some quality criteria, we finally ended up with 26 papers for in-depth review. In the next phase, we will design and implement interventions systematically with multiple iterations to refine and improve our initial designs, in collaboration with the participants (SQ3). But before proceeding with the interventions, we aim to interview and conduct focus group discussions with experts from the industry and academia to gather necessary information for designing or preparing the contents and activities for the interventions. These interviews and focus group discussions would also help us to signify our answer and finding from SQ2. In each intervention, specific learning outcomes will be addressed, and students will receive related information about cyber security and will be asked further to participate in various activities.

Data Collection and Analysis

After each intervention, empirical data will be collected for further analysis and evaluation regarding the students' perception and experience about the activities. Data from this stage will help us to answer the last two questions of this research (SQ4 and SQ5). The researcher will be present in all the interventions to observe the activities and products the participants will be developing during the interventions. At this stage, we also aim to collect the data by conducting pre/post questionnaires and interviews with the participants. The information obtained from the participants will be subjected to numerous analyses (both qualitative and quantitative) and a triangulation among different types of evaluation will be used to ensure the accuracy of the findings and reported results.

Conclusion

Multiple gaming applications and platforms are available and have been already used to support the teaching of cyber security education for children. Therefore, there are many opportunities for us to improve the existing teaching techniques and methods and also to find out new creative and innovative ways of teaching. We believe findings from our studies and measuring learning outcomes as well as the engagement of the children will help us to extend and refine our research framework by setting a new starting point. In our research, we will focus not only on designing, developing, and evaluating a new tool or solution but also on the sustainability of the proposed solution.

Acknowledgements

I would like to thank my supervisors, Letizia Jaccheri (letizia.jaccheri@ntnu.no), Deepti Mishra (deepti.mishra@ntnu.no) from The Department of Computer & Information Science, Norwegian University of Science and Technology (NTNU) and Aida Omerovic (Aida.Omerovic@sintef.no) from SINTEF Digital (Norway) for their support and guidance.

References

[1] Hamdan, Z., Obaid, I., Ali, A., Hussain, H., Rajan, A. V. and Ahamed, J. (2013). Protecting teenagers from potential internet security threats", International Conference on Cur-rent Trends in Information Technology (CTIT), pp. 143-152.

[2] Gjertsen, E., Gjære, E., Bartnes, M. and Flores, W. (2017). Gamification of Information Security Awareness and Training. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), pp 59-70.

[3] Giannakas, F., Kambourakis, G., Papasalouros, A., and Gritzalis, S. (2016). Security education and awareness for k-6 going mobile. International Journal of Interactive Mobile Technologies (ijim), 10(2), 41- 48.

[4] Giannakas, F., Papasalouros, A., Kambourakis, G and Gritzalis, F. (2019). A comprehensive cybersecurity learning platform for elementary education, Information Security Journal: A Global Perspective, 28:3, 81-106.

[5] Kim, B. (2015). The popularity of gamification in the mobile and social era, Library Technology Reports, 51(2), 5–9.

[6] Karagiorgas, D. N. and Niemann, S. (2017). Gamification and Game-Based Learning, Journal of Educational Technology Systems, 45(4), 499–519.

[7] Kim, J. T. and Lee, W. H. (2015). Dynamical model for gamification of learning, Multimedia Tools and Applications, 74(19), 8483–8493.

[8] de Byl, P. (2013). Factors at play in tertiary curriculum gamification. International Journal of Game-Based Learning, 3(2), 1-21.

[9] Roepke, R. and Schroeder, U. (2019). The Problem with Teaching Defense against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In Proceedings of the 11th International Conference on Computer Supported Education - Volume 2, pages 58-66.

[10] Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K. and Sirivianos, M. (2016). Cyber security risks for minors: A taxonomy and a software architecture, 11th Inter-national Workshop on Semantic and Social Media Adaptation and Personalization, pp. 93-99.

[11] Guan, J. and Huck, J. (2012). Children in the digital age: exploring issues of cybersecurity, In: Proceedings of the 2012 iConference, pp 506-507.

[12] Wang, F. and Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. Educational Technology Research and Development, volume 53, 5–23.

[13] Kitchenham, B. A. (2004). Procedures for Undertaking Systematic Reviews, Joint Technical Report, Computer Science Department, Keele University (TR/SE-0401) and National ICT Australia Ltd. (0400011T.1).

[14] Reeves, T.C. (2006). Design research from a technology perspective. In J. van den Akker, K. Gravemeijer, S. McKenney & N. Nieveen (Eds.), Educational design research, p. 52-66. London: Routledge.

[15] Arachchilage, N. A. G. and Love, S. (2013). A game design framework for avoiding phishing attacks, Computers in Human Behavior, vol. 29, no. 3, pp. 706–714.

[16] Raman, R., Lal, A. and Achuthan, K. (2014). Serious games based approach to cyber security concept learning: Indian context, 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*,* Coimbatore, pp. 1-5.

[17] Micallef, N. and Arachchilage, N. A. G. (2017). Involving Users in the Design of a Serious Game for Security Questions Education. arXiv preprint arXiv:1710.03888.

[18] Beckers, K., Pape, S. and Fries, V. (2016). HATCH: hack and trick capricious humans-a serious game on social engineering, in Proceedings of the 30th International BCS Human Computer Interaction Conference: Companion Volume, p. 34: BCS Learning & Development Ltd.

[19] “Cybersecurity Lab | NOVA Labs | PBS.” [Online]. Retrieved March 28, 2020 from http://www.pbs.org/wgbh/nova/labs/lab/cyber.