



Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication
of the Informing Science Institute
InformingScience.org

InformingScience.org/Publications

Online July 5 – 6, 2023

MANDATORY GAMIFIED SECURITY AWARENESS TRAINING IMPACTS ON TEXAS PUBLIC MIDDLE SCHOOL STUDENTS: A QUALITATIVE STUDY

James J. Meadows Rice University, Katy, TX, United States jamesmeadowsiii@gmail.com
Samuel Sambasivam* Woodbury University, Burbank, CA, United States Samuel.sambasivam@woodbury.edu

* Corresponding author

ABSTRACT

Aim/Purpose	The problem statement in the proposed study focuses on that, despite the growing recognition that teenagers need to undergo security awareness training, little is known about the impacts security training experts believe implementing a mandatory gamified security awareness training curriculum in public middle schools will have on the long-term security behavior of students in Texas.
Background	This study was guided by the research question: What are the impacts security training experts believe implementing a mandatory gamified security awareness training curriculum in public middle schools will have on the long-term security behaviors of students in Texas? The study gathers opinions from experts on the impacts of security awareness training on students.
Methodology	Our research used semi-structured interviews with twelve experts chosen through the use of purposive sampling. The population for the study consisted of experts in the fields of security awareness training for and teaching middle school-aged children. Candidates were recruited through the CyberTexas Foundation and snowball sampling techniques.
Contribution	The research contributed to the body of knowledge by using interviews to explore the impacts of security awareness training on middle school students based on the opinions and views of the teachers and instructors who work with middle school students.

The full paper has been published as the following and is being presented at this conference:

Meadows, J. J., & Sambasivam, S. (2023). Mandatory gamified security awareness training impacts on Texas public middle school students: A qualitative study. *Issues in Informing Science and Information Technology*, 20, 67-94. <https://doi.org/10.28945/5129>

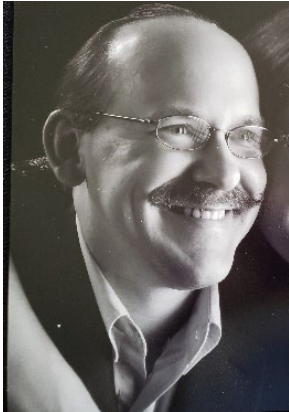
Abstract published in *Proceedings of InSITE 2023: Informing Science and Information Technology Education Conference*, July 5-6 [online], Article 24. Informing Science Institute. <https://doi.org/10.28945/5117>

(CC BY-NC 4.0) This article is licensed to you under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/). When you copy and redistribute this paper in full or in part, you need to provide proper attribution to it to ensure that others can later locate this work (and to ensure that others do not accuse you of plagiarism). You may (and we encourage you to) adapt, remix, transform, and build upon the material for any non-commercial purposes. This license does not permit you to use this material for commercial purposes.

Mandatory Gamified Security Awareness Training

Findings	The findings of this study demonstrate that middle school is an ideal time to provide cybersecurity training and will impact student behaviors by making them more conscious of cyber threats and preparing them to be more tech-savvy professionals. The research also showed that well-designed cybersecurity games with real-world application combined with traditional teaching techniques can help students develop positive habits. The research also suggests that teachers possess the skills to teach cybersecurity classes and the classes can be integrated into the current school day without the need for any significant changes to existing daily schedules.
Recommendations for Practitioners	A well-design gamification-based curriculum implemented in Texas Middle Schools, combined with traditional teaching techniques and repeated over an extended time period, will impact students' behaviors by making them more able to recognize and respond to cyber risks and will transform them into more secure and tech-savvy members of society.
Recommendations for Researchers	The research shows middle school instructors and technology experts believe the implementation of a security awareness training program in middle schools is both possible and practical, while also beneficial to the students. The recommendation is to encourage researchers to explore ways to build curricula and games capable of appealing to students and implementing the instruction into school programs.
Impact on Society	Demonstrating that training provided in middle school will make lasting impacts and improvements to student behaviors benefits children and their families in the short-term and workplaces in the long-term. The development of a more security-conscious workforce can reduce the significant number of data breaches and cyber attacks resulting from the poor security habits of companies' users.
Future Research	Future research that will add significant value to the body of knowledge includes testing the effectiveness of habit-shaping games to determine whether existing long-term games maintain student interest. Qualitative studies could interview parents of teenagers using habit-shaping games to determine the effectiveness of the applications. Another qualitative study could interview teachers to determine how teachers' ages affect their comfort level teaching technology classes. Both studies could provide valuable insights into how to implement security awareness training in schools.
Keywords	cybersecurity, security awareness training, gamification, security habits, middle school security training

AUTHORS



Dr. James Meadows has worked in and taught cyber security for over fourteen years and has represented Rice University as an information security expert on news stations around the world. Besides teaching, James has a passion for board games, running marathons, and software design, and has authored a number of fantasy novels. He currently lives in Houston, Texas, with his wife and children.



Dr. Samuel Sambasivam is Chair and Professor of Computer Science Data Analytics at Woodbury University, Burbank, CA. He is Chair Emeritus and Professor Emeritus of Computer Science at Azusa Pacific University. He served as a Distinguished Visiting Professor of Computer Science at the United States Air Force Academy in Colorado Springs, Colorado for two years. In addition, he has concurrently served 13 years of progressive doctoral teaching roles at Colorado Technical University (CTU) including chair of doctoral programs, lead computer science doctoral faculty instructing core/concentration computer science courses, and as dissertation chair/committee member. His research interests include Cybersecurity, Big Data Analytics, Optimization Methods, Expert Systems, Client/Server Applications, Database Systems, and Genetic Algorithms. He has conducted extensive research, written for publications, and delivered presentations in Computer Science, data structures, and Mathematics. Dr. Samuel Sambasivam earned his Ph.D. in Mathematics/Computer Science from Moscow State University, a Master of Science in Computer Science with Honors from Western Michigan University, Pre-PhD in Mathematics/Computer Science from Indian Institute of Technology (IIT) Delhi, a Master of Science Education in Mathematics with Honors from Mysore University (NCERT-Delhi), and a Bachelor of Science in Mathematics/Physics/Chemistry with Honors from the University Madras (Chennai). He is a voting senior member of the ACM.