Issues in Informing Science + Information Technology

An Official Publication of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 20, 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.
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-

Accepting Editor: Eli Cohen | Received: January 4, 2023 | Revised: April 14, May 8, 2023 | Accepted: May 29, 2023

Cite as: 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

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

INTRODUCTION

The steadily increasing number of data breaches affecting the modern technological world has raised awareness among organizations of the need to improve individuals' security practices, both at work and at home (Alruwaili, 2019). Most companies recognize that poor employee security practices in the workplace can result in severe financial losses for organizations (Crossler & Belanger, 2014). However, organizations have only recently begun recognizing the dangers arising from employees' weak security practices outside the workplace. These include both the direct risks to the organization's infrastructure and productivity losses resulting from the psychological damage to employees who suffer from such attacks.

As employees' private security practices exist outside the control of corporate networks, traditional security solutions, such as firewalls and office-based security tools, cannot entirely prevent these damages (Dennis & Minas, 2018). For this reason, increasing numbers of organizations are turning toward cybersecurity awareness training programs to teach information technology users the importance of protecting their personal information and the actions they can take to defend themselves

from risks (Chong et al., 2019). Security awareness training programs can be defined as presentations intended to teach employees "to be aware of possible cyber risks and to behave accordingly" (Alruwaili, 2019, p. 1). Such programs are ubiquitous in the modern workplace, and many organizations dedicate a significant portion of their entire IT security budget solely to these programs (Kirova & Baumöl, 2018).

However, this increase in the number of training programs performed by organizations has done little to stem the tide of attacks. Studies show that awareness of threats and risks seems insufficient to motivate users to change their behavior (He et al., 2019). Xu and Guo (2019) note that adults of all ages in the workforce have developed a variety of coping mechanisms to justify not performing proper security behaviors, from procrastination to convincing themselves they can handle any negative results from their actions. Goyal Chin et al. (2016) identified the same issue among college students, whose knowledge of security risks and proper security actions fails to significantly improve poor security behaviors or practices in their daily lives. In fact, the study showed that, in some cases, individuals receiving security awareness training demonstrated less secure behavior after the training than individuals who did not receive the training (Goyal Chin et al., 2016).

The researchers concluded that the proliferation of technology and years of performing unsafe practices have desensitized users to security risks (Goyal Chin et al., 2016). To address the problem, van Niekerk et al. (2013) propose that national initiatives improve cybersecurity and turn their attention toward younger audiences, providing education to primary and secondary school children. They further posit that this training needs to be performed in a formal setting such as a school since children's parents also demonstrate poor cybersecurity practices and cannot be trusted to teach this information. The idea of providing education at a younger age to prevent desensitization has attracted much attention in recent literature.

While no mandatory cybersecurity curriculums are currently implemented in American schools, studies have been performed which involve providing cybersecurity awareness training programs to secondary school students (Alruwaili, 2019). So far, the studies have demonstrated positive results, especially in programs that involve gamification – the use of video games as part of the curriculum. Unfortunately, most of these studies involve single classes or week-long programs. Follow-up studies show that the benefits of these short-term classes often disappear over time (Amo et al., 2019). The findings suggest that long-term cybersecurity training programs are necessary to make significant and lasting changes in behavior.

In theory, implementing mandatory long-term courses focused on teaching students proper and healthy security behaviors would fill a need in existing public-school programs. Mandatory curriculums for developing healthy habits already exist in the form of health classes and sexual education courses (Young et al., 2016). However, mandatory classes do not exist for cybersecurity. Current classes addressing cybersecurity are optional, and most students choose not to take them (Stuparu, 2020). Future research is needed to determine what age groups are most receptive to cybersecurity training and the impact of making security awareness courses mandatory.

PROBLEM STATEMENT

The problem addressed in the proposed study was 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 (Tsimtsiou et al., 2019). Studies examining why security awareness training fails to improve behaviors suggest the problem results from a combination of unconscious behavioral patterns and pre-established habits created during youth (Dennis & Minas, 2018). Research shows that the power of established habits to create insecure behaviors applies equally to adults and college students (Goyal Chin et al., 2016). School-age children, however, have fewer life experiences and fewer established behaviors than

adults. van Niekerk et al. (2013) argue that teaching cybersecurity from an early age will improve security awareness among the public. Children's preoccupation with technology during their early teenage years suggests this age is an ideal time to shape their future technology behaviors (Little et al., 2013). Unfortunately, little effort has been made to provide cybersecurity education and guidance to American school children. Few school classes exist to teach children how to interact with modern technology in a safe and secure manner (Stuparu, 2020). Existing classes are voluntary, and most students choose not to take them. Recently proposed legislation, such as the Cybersecurity Grants for Schools Act of 2022 (2022), seeks to address the problem by funding security education in the state and local school systems. However, a significant lack of research exists regarding what school age is ideal for providing security awareness training to children and how to build a curriculum that will appeal to all types of students while maintaining learning goals (Van Mechelen et al., 2020). For this reason, research was needed to determine when and how a mandatory security awareness curriculum could be implemented in schools to produce positive behavioral changes.

PURPOSE

The purpose of the exploratory qualitative study was to explore 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. An exploratory method was the correct approach for studying a new subject never studied before or where refining explorations had only just begun (Bakker, 2019). Current Texas middle schools do not have mandatory courses that teach security awareness training using gamification (EdWeek Research Center, 2020). For this reason, quantitative studies and qualitative methods based on observation and narrative could not be used.

SIGNIFICANCE OF THE STUDY

The purpose of our exploratory qualitative study was to explore 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. The research is of great importance in our field and concentration, as demonstrated by the recently proposed Cybersecurity Grants for Schools Act of 2022. The bipartisan legislation proposes to allow monetary grants to governments and educational institutions for cybersecurity education and training programs (D. Johnson, 2022). Supporters of the bill emphasize that children need security awareness training to be taught alongside traditional classes like math and science so they can learn to protect themselves (Kelley, 2022).

Unfortunately, limited research has been performed in the United States on when and how to effectively implement a long-term curriculum into the school systems. Some experts argue that the training should be provided at a college level, while others argue for primary school, middle school, and high school (McQuaid & Cervantes, 2019; Stuparu, 2020; van Niekerk et al., 2013; Walker et al., 2018). There is also no agreement on how to provide training, as many schools and teachers do not have the right resources, knowledge, abilities, or aptitude to teach cybersecurity (Sezer et al., 2015). Researchers suggest gamified curriculums can address the issue, but existing gamification research focuses on short-term programs, and there is a need for more advanced studies on the effectiveness of long-term gamification courses (Gjertsen et al., 2017; Wu et al., 2021). By exploring the impacts of gamified cybersecurity education at the middle school level, the research study helps address the need illustrated by recent legislation to determine a way to provide security awareness training to America's children.

LITERATURE REVIEW

CYBER THREATS FACING SOCIETY

The fear of cyberattacks has become a significant concern for nations worldwide (von Solms & van Niekerk, 2013). These attacks are devastating to both humans and society at large for the harm they inflict upon their victims. Beyond simple financial damages, these crimes result in loss of intellectual property, greater unemployment rates, loss of trust in online activities, and reputational damages for organizations (Farahbod et al., 2020). Surveys show that American consumers and businesses suffer more economic damage in every category than in any other country.

Despite the dangers these attacks present to individuals, many organizations focus only on technical defenses and controls for protecting data (Chong et al., 2019). However, even the most advanced security controls and devices can be rendered useless due to insecure human behaviors. Williams et al. (2020) note that the biggest reason for the success of modern cyberattacks is their ability to take advantage of weaknesses in the human element. Estimates suggest that over half of all information security breaches are caused directly or indirectly by insecure behaviors performed by employees (Vance et al., 2012).

NEED FOR SECURITY AWARENESS TRAINING

Protecting organizations requires going beyond technical controls and requires companies to focus on protecting the users inside their organizations (von Solms & van Niekerk, 2013). This awareness must include workers' home-computer usage since a user who practices secure-computing habits at home is likely to carry these positive habits into their work lives (Xu & Guo, 2019). The best way to improve employees' habits is through security awareness training programs designed to keep individuals psychologically involved and invested in the training. Yoon et al. (2012) argue that information security education is critical for modern users to protect themselves from the growing variety of threats they face. Without proper training, users cannot be expected to know the many security risks they face or how to react to these dangers (Furnell et al., 2006).

Studies performed on the effectiveness of security education and training demonstrate promising improvements in participants' security knowledge due to these courses (Hagen et al., 2011). Unfortunately, the results from these studies suggest that knowledge of security ideas and higher levels of computer skills have little effect on whether users behave in a more secure manner (Kang et al., 2015). Literature on the subject shows that while people often know the correct security actions, they do not practice these activities in real life (Alruwaili, 2019). Hammond (2019) also found that although security training positively impacted users' intentions to behave securely, the training produced very little impact on users' actual behaviors.

HABITS BEHAVIOR THEORY

Habit Theory explains the problem by noting that too many behavior-change programs focus on conscious, rational motivations and not on the unconscious factors influencing behavior (Pinder et al., 2018). While behavior change may be initially motivated by conscious motivations and interventions, user behaviors tend to eventually fall back to habit and context-based routines. In other words, people are so used to behaving in an insecure manner that they continue to execute poor behaviors automatically despite knowing better (Vance et al., 2012). Solving this discrepancy between user knowledge and actions requires users to develop new thought patterns and habits to replace existing tendencies (Bada & Nurse, 2019).

Creating secure habits is vital because habitual actions allow a behavior to continue even after conscious motivation and intentions dissipate (Gardner et al., 2012). Unconscious activities performed by habit make up a large percentage of the actions performed by most individuals (Martin, 2018).

Even when the user intends to behave securely, weak intentions are often overridden by habits (Gardner et al., 2020). As these habits can lead to negative and positive behaviors, developing and creating positive habits becomes an integral part of ensuring individuals perform healthy behaviors (Fiorella, 2020). Otherwise, the unconscious awareness will likely continue to execute negative behaviors automatically, without any conscious intent or guidance (Bargh & Morsella, 2008).

Changing behaviors because of external demands or breaking existing habits is significantly more challenging than creating habits (Gardner et al., 2012). The challenge associated with breaking habits is relevant in information security, where poor habits for at-home computer usage lead individuals to practice unsafe security behaviors at work and hinder attempts to enforce proper security responses (Poleon, 2020). These negative habits are reinforced by the prevalence of in-home computing, which allows users to make numerous insecure computing decisions every day (Wash & Rader, 2015). Such habits are made harder to break by the length of time during which the insecure actions are performed and strengthened through constant repetition (Poleon, 2020). Such habits affect how individuals perform at home and play an important role in determining whether they follow proper security procedures and policies at work (Vance et al., 2012).

Security Awareness Training for Youth

K. Johnson (2017) proposes the creation of a more secure workspace by implementing cybersecurity training programs at high schools and middle schools so users already have robust cybersecurity knowledge and practices in place before joining the workforce. Likewise, psychologists are increasingly noting that training targeted toward younger age groups is critical for shaping the healthy behaviors and actions that young people will carry with them for the rest of their lives (Bay et al., 2012). Pye (2016) suggests K-12 education is the ideal time to teach a cybersecurity curriculum because children are just learning about computers. Students at this age are more interested and willing to promote security behaviors in their personal lives. Without training, children lack the skills to understand or assess the numerous risks and dangers to their safety and privacy present in the modern internet environment (Quayyum et al., 2021).

Security training from parents

Studies show that parents also feel worried about their children's cyber safety (Boyd et al., 2011). However, because many parents did not grow up with modern electronics and smart devices, they do not understand the threats and dangers their children face (Plowman et al., 2010). Even parents who know what security actions are necessary and appropriate to protect their children fail to enact these actions in their family practices. Worse, a study by Boyd et al. (2011) showed that while parents are concerned about their children's safety online, more than half were knowingly complicit in allowing their children to break laws and access materials deemed unsafe for their age group. For this reason, Stuparu (2020) suggests that, while parents need to be included in the cyber education program and provided resources to support their children's learning, the development of more secure behaviors must start at school.

Security Awareness Training in Schools

Smith (2018) states that schools need to actively develop a mandatory cybersecurity curriculum for school children that is tailored to their knowledge and skill levels. Studies show that even a single class about proper online behaviors taught during regular class time by a trained teacher can change the behaviors of secondary school children (Walther et al., 2014). While many experts agree that this training must occur in either middle or high school, other researchers go further, emphasizing that training should be completed before eighth grade, when problematic behaviors become the worst (Petruzzelli & Sharma, 2019; Roberts, 2014).

Studies further suggest that this training needs to be part of an extended program, not just a single class or session (Amo et al., 2019). A study by Amo et al. (2019) found that a multiple-day course

with simulated cyber defense activities was more effective than a single intervention for middle school students. A mandatory curriculum for middle schools is also crucial because statistics demonstrate that most students are not choosing to take technology electives or classes that would provide them with the necessary cybersecurity awareness (Stuparu, 2020). Despite this need, current educational curricula are found to be lacking in digital security (Basarmak et al., 2019). Van Mechelen et al. (2020) note that few attempts have been made to study or design any form of curriculum to teach children how to interact with modern technology properly.

GAMIFICATION

A possible solution is using a curriculum taught through game-based education (Smith, 2018). Video games have been recognized for many years as a significant source from which young people learn new skills and habits outside of educational contexts (González & Aguilar, 2019). Using video games as a tool for teaching non-gaming concepts is called gamification and has been used for many years to affect behaviors among groups, such as pilots and military trainees, and to develop situational memory patterns (Dennis & Minas, 2018; Treiblmaier et al., 2018). Gamification takes advantage of the motivational and addictive nature of games and transforms them into tools that shape students' attitudes, abilities, and performance (Chapman & Rich, 2018).

GAMIFICATION AND CYBERSECURITY

Despite the success of gamification in other industries, the use of gamification for teaching information security awareness is still a relatively new concept (Treiblmaier et al., 2018). So far, however, the field of cybersecurity is one area where gamification techniques are shown to be particularly effective (Rowe et al., 2011). Wu et al. (2021) found that students using a gamified system showed significant improvements in cybersecurity knowledge compared to students who attended lecture-based training. Subjects put through training programs involving gamification also demonstrated a greater willingness and higher motivation to follow information security ideas taught by the games (Gjertsen et al., 2017). The results led Khando et al. (2021) to suggest gamification as one of the most effective tools for creating interest and motivating users to follow information security awareness practices.

Apart from video games, Denning et al. (2013) successfully improved security knowledge among secondary school students using non-electronic gamification. Their research using a card game suggests that even gamification tools such as tabletops games can be effective at increasing cybersecurity knowledge. Many students become so engrossed with the games that they were observed playing the game independently between classes (Jin et al., 2018). Ultimately, research suggests that employing unique approaches such as gamification to address the challenges of teaching cybersecurity can play a key step in improving cybersecurity interest and training (Snyder, 2018).

GAMIFICATION AND BEHAVIOR CHANGE

Of course, to be effective in teaching security, gamification must move beyond simply teaching knowledge to produce real-world behavior changes (Giannakas et al., 2019). Gamification is the perfect medium for creating these changes since gameplay forces the participants to continually repeat healthy security habits (Pinder et al., 2018). The user is trained to develop a plan of identifying a particular scenario and taking specific actions every time the scenario plays out (Clarke et al., 2017). Clarke et al. (2017) suggest that gamification allows the action to be performed enough that it becomes habitual. The positive habits developed in this way can be equally resilient and resistant to change as negative ones (Pinder et al., 2018).

Research has shown a positive correlation between gamification and the creation of healthy habits (Sarbadhikari & Sood, 2018). Gamification achieves this goal by motivating users to perform positive actions and rewarding them when they perform those actions (Santos et al., 2021). On an intrinsic level, the sense of achievement, whether through earning a prize, gaining a level, or completing a

challenge, makes the player feel like they are achieving some greater accomplishment or mastering a new skill (Gjertsen et al., 2017). On a physiological level, Silic and Lowry (2020) note that playing video games causes the body to release chemicals that make the participant more receptive to developing habits and shifting behaviors. While some of these rewards may be temporary, once the action is established as a habit, studies demonstrate that the habit will continue to be repeated even after the reward is no longer present (Pinder et al., 2018).

A study by Yildiz Durak (2019) highlights the effectiveness of games in impacting the behaviors of high school students. His research demonstrates that video games can play an essential role in shaping high school students' behaviors, values, and personality traits in their everyday lives. The impact playing video games has on children's behaviors is shown to be greater than the impacts teenagers experience from watching videos or participating in non-interactive activities (Hourcade, 2015). Hourcade (2015) reports that adolescents and teenagers are more likely to model their behaviors and activities after the behaviors and activities they perform in video games and other interactive electronic media. Teenagers' tendency to model their behaviors based on video games makes gamification a promising solution for addressing the challenges and resource limitations facing the teaching of Information Security curriculums in secondary schools (Wu et al., 2021).

RESEARCH METHOD AND DESIGN

The research method selected for this study was qualitative exploratory research. Qualitative research methods involve collecting and analyzing experiences, behaviors, and opinions to gain insights into a phenomenon (Håkansson, 2013). Qualitative exploratory research is considered an ideal approach for understanding the complex phenomenon of school education and educational programs, including the social phenomena and interactions between teachers, students, and parents (Gunnulfsen, 2021). Qualitative research methods provide a more comprehensive approach to understanding and studying instruction in educational contexts (Meyer & Schutz, 2020).

The research method selected for the study involved performing semi-structured interviews. Interviews were an ideal choice for the study. Interviews allow for high-quality descriptions of situations and can reveal unknown and unanticipated rationales for accepting or rejecting an idea that may not be identified by a literature review alone (Merriam & Tisdell, 2016). The interviews followed a semi-structured format. Semi-structured interviews consisted of predetermined questions, but they allow the interviewer to insert additional questions to obtain further details (Mills et al., 2014). The approach was considered a better choice than structured interviews for exploratory research because semi-structured interviews allow greater interaction between the interviewer and the interviewee. The interviewer can use answers and responses provided by the interviewee to obtain more details and depth on the research topic.

PARTICIPANTS

The population for the study consists of cybersecurity awareness training experts from Texas. The professionals were initially recruited through the CyberTexas Foundation. These professionals work with schools across the state to provide summer boot camps and training programs to children and teenagers of all ages, including middle and high school (CyberTexas Foundation, 2018). Due to a lack of existing cybersecurity programs in middle schools, additional teachers were recruited from other computer science disciplines. The population of experts provides the insights necessary for developing a holistic understanding of the research topic.

A purposeful sampling method was used to select and identify the 15 research participants. The qualified study participants possessed a variety of job titles depending upon whether education was their fulltime job or their work in education was a secondary profession. The years of experience and time spent teaching and interacting with middle school students varied from one year to twenty-two years. Eight of the study participants were male, while seven were female.

Research Question

The research question for this qualitative exploratory study is:

> 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?

Data Collection

Because of restrictions implemented during the Covid-19 pandemic, the semi-structured interviews were conducted through Zoom, an online communication platform. Modern research suggests that video interviews are less daunting or intimidating than in-person interviews and support the establishment of rapport and open communication between participants (Weller, 2017). Video-based interviews are also less expensive, safer, more environmentally friendly, and more time-efficient than in-person interviews while also allowing the researchers to access hard-to-access participants (Krouwel et al., 2019).

After each interview, the researchers had a third party, Transcription Puppy, transcribe the interview. Before providing services, Transcription Puppy provided a non-disclosure agreement to ensure the confidentiality of all data. Having a third party transcribe the interview ensured the integrity of the information since researchers often allow biases or memories of lived experiences to color their transcription, resulting in an unfaithful representation of the information conveyed (Shelton & Flint, 2019). Each interviewee received transcriptions of their interviews to confirm that the transcribed information was accurate (Hagens et al., 2009).

Data Analysis

The transcribed data was entered into the ATLAS.ti tool after each interview. ATLAS.ti also allowed the researchers to enter pseudonyms and false information to secure the confidentiality of all participants and ensure all identifying information would be kept secret (Kaiser, 2009). Once interview data was loaded into ATLAS.ti, the program developed a set of codes and themes based on an initial review of interview transcripts and notes. The ATLAS.ti program also assisted the researchers in identifying irrelevant and unnecessary data allowing us to focus on the major themes and topics identified in the interviews.

The coding process involved three phases. The first phase arose after ATLAS.ti completed the coding process. The first phase was initial coding, where the researchers broke down the data into smaller segments and compared the data segments with other resources (Mills et al., 2014). Initial coding helped determine what data was relevant to the study and what the data was saying. The phase established the foundation for the subsequent exploration of patterns identified in the data (Linneberg & Korsgaard, 2019). At the end of Initial Coding, several core ideas and categories were identified.

The second phase of the coding process was Axial Coding. During this phase, the researchers reviewed all of the interviews again, focusing on the core ideas and categories identified during Initial Coding (Creswell et al., 2007). The process helped the researchers understand how the interviews shaped and were shaped by the core ideas and topics. Next, a diagram was constructed to connect all core ideas and categories (Mills et al., 2014).

After Axial Coding was completed, the final phase involved the construction of a "storyline." The storyline provided a narrative and helped the researchers identify any weaknesses or holes in their research (Mills et al., 2014). The storyline connected the data's key concepts, categories, and relationships (Birks et al., 2009).

FINDINGS

All participants were interviewed for approximately 30 minutes to 1 hour through Zoom. Questions 1 and 2 sought to establish the demographics of the participants. The job titles revealed that many of the participants possessed primary jobs working in the cybersecurity industry and worked in education as a secondary job. No two individuals possessed the same job title. The wide variety of job titles is unsurprising as organizations maintain very little consistency in the naming conventions and responsibilities assigned to cybersecurity roles (Catarino et al., 2016). The diverse roles of the participants allowed the researchers access to a variety of backgrounds and viewpoints.

Question 8 was an introductory question, designed to determine whether participants knew what gamification was before asking questions related to the subject. All participants were familiar with the use of gamification in education. Subjects also demonstrated a wide gap in years of experience working with middle school students. The participant with the most experience had worked in academia for more than twenty-two years while several participants possessed only one year of experience. The average participant possessed between three to ten years of experience working with students in the educational system.

INTERVIEW QUESTION 3

In what ways do you feel middle school is or is not an appropriate time for providing behavior-based training, like security awareness training?

The collected data for Interview Question 3 showed two themes, whether: (a) middle school training is appropriate because of the prevalence of technology and internet usage by middle school students, and (b) security awareness training needs to start earlier than middle school. Eight participants felt middle school was an appropriate time for security awareness training due to the prevalence of technology in the lives of middle school students. Participants expressed the opinion that middle school students were gaining greater access to technology and more independence in how they use the technology. One participant explained, "6th through 8th grades is a perfect age to start this training as this is when I see students start to have more autonomy with their personal devices and online accounts."

Seven participants expressed an opinion on whether security awareness training should be provided at a younger age than middle school. Some participants felt that many students are coming into contact with technology earlier than middle school and believed the training needed to start at these younger ages. As one participant stated, "We want to get them as young as possible, first, second-grade. Kids are resilient. They're not the same first and second graders we were when we were younger." Other participants discussed how elementary school students are carrying around iPhones and tables. They felt the presence of technology in elementary schools meant the training needed to be started at a younger age.

INTERVIEW QUESTION 4

Based on your experience, to what extent, if any, do you feel that good security habits taught in middle school impact the students' long-term security behaviors?

Aggregated data for Interview Question 4 reflected two themes: (a) good security habits will impact students' long-term behaviors because students are impressionable, and (b) good security habits taught in middle school impact students' long-term behaviors by teaching them about future risks. Other teachers felt that in order for good security habits to impact long-term security behaviors, the training needs to be repetitive.

Seven participants identified middle school as an ideal age for the development of habits because middle school students were more "impressionable". One participant explained by stating, "What they learned [in middle school] really molds a lot of who they are." A participant with experience

teaching both high school and middle school students specifically emphasized that the training needed to be completed before eighth grade because middle school students were more "malleable". Another participant noted, "When you build in those habits at that age, like the junior high, seventh, and eighth grades, by high school they don't even think about it anymore." They felt middle school was the ideal age to target for shaping long-term behaviors.

Eight teachers expressed the opinion that good security habits impact students' long-term behaviors because it teaches them about future risks. They believed that making students aware of the risks at a younger age would lead them to remember those risks when making future decisions. One participant explained, "I see from those who haven't been exposed to security, or the value of security, how dangerous it can be for them." Participants felt that by developing awareness of the risks at a younger age, the students will make better decisions as they get older. As one participant said, "it may be one of those things that doesn't immediately impact them in a large, grandiose, way … but it's those habits that they're going to pick up."

Two teachers expressed the opinion that in order for good security habits to impact students' long-term behaviors the training needed to be regularly repeated. They felt that a single class in middle school was not sufficient to have a lasting impact. Further reinforcement was necessary to change students' long-term actions. As one participant said, "the way to be successful is where security awareness training is repetition." The other noted, "if you think about parenting a child, you tell them something one time, then they hear it. But the next week, they forget." The participants felt that a single class, without continuing training, lacked the power to affect long-term behaviors.

Interview Question 5

How prepared do you believe middle schools and teachers are to implement cybersecurity awareness training curriculums?

The data for Interview Question 5 demonstrated three themes. All of the themes focused on the teachers. Participants expressed mixed opinions on whether middle school teachers were prepared to teach security awareness training classes. Some participants felt teachers were prepared to teach security awareness. Other participants indicated that teachers could teach security awareness but they first needed to receive direct training in the subject. A final group of participants felt teachers lacked the technical experience necessary to teach security awareness.

Five participants felt that middle school teachers are prepared to teach security awareness training to students. They felt teachers' previous experience taking security awareness training classes made them well-equipped to teach the subject. They noted that teachers go through multiple cybersecurity awareness training classes every year and should be able to transfer that instruction to their classes. As one participant noted, "cybersecurity awareness training is the basic. It's not that difficult. It's not really that technical." Another participant that most teachers tend to be in their 20s, 30s, and 40s and computer technology is second nature to them. The participants felt that teachers possessed sufficient knowledge to teach the subject.

Six participants felt that middle school teachers can be prepared to teach security awareness training to students if they first receive proper training. The training described varied from receiving classroom instruction to a fully prepared out-of-the-box curriculum. One participant explained, "there needs to be training provided to all the teachers in the middle school on how to implement it correctly." As long as teachers receive this training, the participants felt the teachers would be able to provide the training to students.

A third group felt middle schools lacked the technical expertise necessary to provide security awareness classes. Four participants noted that middle schools suffered from a lack of technology-savvy teachers. Participants that schools struggle to find teachers capable of teaching Computer Science

and related technical topics. As a result, they felt teachers lacked the knowledge and skills to teach cybersecurity concepts. "We have to bring cyber people in to do that," one participant stated. Another explained, "when it gets too technical, a lot of [teachers] just - they don't want anything to do with it." They felt the teacher's lack of technical knowledge left schools unprepared to implement a cybersecurity curriculum.

Interview Question 6

Would you support or oppose the idea of making cybersecurity awareness training courses mandatory? Why or why not?

The collected data for Interview Question 6 showed three main themes: (a) security awareness training should be mandatory for children's safety; (b) security awareness training should be mandatory for students' futures; and (c) mandatory security awareness training for all students was impractical. Participants also raised the theme of when mandatory security awareness training could be performed.

Eight participants felt that cybersecurity awareness training should be mandatory for the safety of students. They felt the students faced a number of dangers and threats if they did not receive the training. Participants compared security awareness to CPR training, noting that all students are required to take CPR training so they know what actions to take in a critical situation. Another participant compared a cybersecurity curriculum to the "stranger danger" training provided to elementary school students. They noted that these trainings are required for students because they save lives. Participants felt students needed the same awareness of security risks in order to "keep themselves safe, and their families."

Five participants felt that cybersecurity awareness training should be mandatory for the future of students. Some discussed the future in terms of college, noting "we can start [security training in middle school] so that one day when workforce students get to college, there is far less of having to drink from the hose." Others discussed the future in terms of professional careers, stating that the training could "introduce them to new career ideas that are going to be essential in the future." Others spoke of security training being important for growing productive citizens and for the future welfare of the country. As one participant stated, "We teach them good habits now. They're more likely to be those productive citizens in their colleges and in the workforce."

Three participants felt that making security awareness training mandatory for all students was impractical. The participants felt that mandatory security awareness training was a good idea, but also felt implementing training for all students would face insurmountable obstacles. One of the participants focused on the challenges of finding a time when all of the students could take the class. Other participants focused on students in life skills and special education classes that lacked the mental capabilities to understand the materials. One of the participants also expressed concerns that some parents would provide pushback on having their children take the course. For these reasons, they felt implementing a mandatory curriculum was not feasible.

Six participants discussed the topic of when mandatory security awareness should be performed. The participants supported the idea of training because they felt that times existed within the school day that could be used to implement the training. Many of them proposed different times as the ideal place for the training. Two participants suggested that training could take place during advisory and grading periods. Participants noted, "most junior highs, at least in the area that I'm at, have an advisor time which occurs daily, and [training] could be implemented into part of that curriculum." Two other participants proposed the idea of the training occurring during homeroom or a similar "enrichment time." The times available for the training helped support their feeling that the training should be mandatory.

Interview Question 7

What are some of the biggest challenges, if any, that you see to the implementation of a mandatory cybersecurity curriculum in middle schools?

The collected data for Interview Question 7 showed four main themes: (a) lack of technical talent among teachers; (b) schools lacking the time to teach the subject; (c) problems with student maturity; and (d) challenges managing the curriculum. Seven participants felt that one of the biggest challenges to the implementation of a mandatory cybersecurity curriculum in middle schools was the lack of technical talent among teachers. As one participant said, "for teachers, [technology] wasn't the main function of the educational training or the programs they went into didn't have an emphasis or cybersecurity." They pointed out how skilled technology professionals often went to work for private companies rather than schools and noted how schools face a challenge in hiring teachers for computer science-related courses. They felt the lack of knowledge was one of the biggest challenges to the implementation of a mandatory cybersecurity curriculum.

Eight participants felt that one of the biggest challenges to the implementation of a mandatory cybersecurity curriculum in middle schools was finding time to teach the subject. Participants noted that teachers faced so many obligations that finding time to implement the training would be difficult. As one participant said, "it is everything else that absolutely should be mandatory … How much time do you have in school?" Participants felt that teachers would feel security awareness training was just "something extra that they have to do in their already busy out-of-time days and schedules". Participants also noted that mandatory training could not be performed in electives such as physical education, because not all of the students were taking them. On the other hand, participants felt that classes on tested subjects would have a difficult time finding opportunities to teach cybersecurity. Altogether, the participants believed finding time to squeeze these materials into the class would be a challenge.

Seven participants felt that one of the biggest challenges to the implementation of a mandatory cybersecurity curriculum in middle schools was the maturity of students. These participants expressed the opinion that teaching to a vast range of maturity levels among students would be a challenge. The participants felt that some students would not understand the value of the classes. As one interviewee noted, "there is a vast range of maturity on whether or not [students] take it seriously." Other participants noted how there is a wide gap in the comfort level different students felt with technology. As one participant said, "I've had students who were smarter than their teachers on tech-related topics, and students that had no clue how to click a link or hover over a link at all." They felt the diverse maturity levels of the students would make implementing a mandatory security awareness curriculum difficult.

Five participants felt that one of the biggest challenges to the implementation of a mandatory cybersecurity curriculum in middle schools was managing the curriculum. The challenges they identified included both building the curriculum and keeping the curriculum up-to-date. As one participant explained, "educational material can have a very slow process to approval, which in the InfoSec Industry, can make the material outdated fairly quickly." Other participants expressed concerns about the cost of finding the right people to build a curriculum and the tendency for standardized curriculums to have significant holes. They felt designing and maintaining a curriculum capable of keeping up with the rapidly evolving threats and dangers in cybersecurity would be a challenge to the implementation of a mandatory curriculum.

Interview Question 9

How effective do you feel security awareness training programs involving gamification could be in shaping the habits and behaviors of middle school children?

The collected data for Interview Question 9 showed five main themes: (a) participants noted that middle school students respond positively to gamified activity; (b) participants were also familiar with training where gamification was effective; and (c) participants felt gamification helped shape student behaviors by providing hands-on experience. Participants also raised concerns about: (d) how the games need to be applicable to the students; and (e) how different students respond differently to gamification.

Ten teachers felt that gamification could be effective in shaping the habits and behaviors of middle school students because middle schoolers respond positively to games. They described students as being drawn to games and enjoying them. Participants noted how both students and teachers enjoy incorporating gamification into their classes. As one interviewee put it, "anytime the kids think it's a game, or they think they're playing, they're much more likely to participate." Another participant noted that "if you apply [gamification] to any subject, the kids respond way better, retention goes way up, and interest holds longer over time." The participants felt students' interest in games made them an effective tool for shaping behaviors.

Seven participants felt that gamification could be effective in shaping the habits and behaviors of middle school students because they had seen gamification be effective in other training. One participant discussed seeing successful gamification programs taught at all ages, from elementary school students learning their ABCs to medical students learning to perform trauma diagnosis. Several also talked about witnessing the effectiveness of gamification for teaching cybersecurity, noting such games as "Cyber Threat Defender," and "CyberSiege." The success of gamification in other areas of education led the participants to feel the training would also be effective in a middle school cybersecurity curriculum.

Four participants felt that gamification could be effective in shaping the habits and behaviors of middle school students because it provides hands-on experience. The participants felt the interactive nature of the games allowed students to internalize cybersecurity lessons. As one participant explained, "[students] put their own spin on it. That makes it their own, and that just gives them more power. That empowers them to remember and feel good about it." They also noted how teachers are seeking to find ways to "get kids off textbook theory and more of a hands-on approach." Participants felt the interactive, hands-on nature of the games made them ideal for shaping student behaviors.

Eight participants felt that, for gamification to be effective in shaping the habits and behaviors of middle school students, the games needed to be applicable to the students. They felt the games needed to be designed in a way that translated security concepts into direct behaviors that students could apply to their lives. Otherwise, they felt the games would lose their effectiveness. Participants noted, "There's a danger of [the game] being trivial and not supporting any kind of education or learning." The game needs to be designed in a way that students could say, "This is a game, but this is also what we do." On the one hand, participants noted there was a risk of a game being "too cheesy or just too obvious that it's super education, and [students] are just doing this to check on the box." Participants felt building a game that allowed students to learn applicable skills without losing student interest was the key to shaping the habits of middle school students.

Five participants felt that a challenge for gamification to be effective in shaping the habits and behaviors of middle school students is that different students respond differently to gamification. They felt the difference between how students react to different games could affect whether students benefit from the training. One noted that not all students are tech-savvy and felt the less technically-inclined students "might find [gamification] a little intimidating." Another discussed how different students like different types of games and no single type of game or entertainment is going to appeal to all of them. Participants felt that while some students would "run with the game", there would be other students who would not excel in the environment. They felt students' diverse reactions to games would limit the effectiveness of a gamified training program in shaping student behaviors.

Interview Question 10

In what ways do you believe the long-term use of gamification as part of a mandatory school cyber security curriculum would be successful and/or unsuccessful in changing middle school students' security behaviors?

The collected data for Interview Question 10 showed four main themes. Participants noted that in order to successfully change middle school student's behaviors gamification needs to be applied over a long-term period. Additional themes discussed the need for games to incorporate constantly evolving goals and challenges, and for games to be a supplement to other education approaches. Participants also expressed concern that the long-term use of gamification would result in students losing interest.

Eight teachers felt that in order for gamification to be effective in changing students' behaviors it needs to be applied over an extended period of time. The period of time ranged from across an entire school year to spanning multiple years. Participants felt that applying gamification over an extended period of time was necessary to get support from the teachers and to positively impact the students. As one participant explained, "if you don't keep doing it, you're going to forget it. So, if we teach somebody something in middle school and then they don't touch it again until potentially college, they forget." Another participant noted, "the average IQ person (90-110) has to be told three times for it to get to long-term memory. And, for every ten points lower, it [increases exponentially] … So, if you don't get them interested in doing something over and over and over, it's really not going to make it." The general feeling was that gamification needed to be a long-term part of any effective curriculum.

Six teachers felt that in order for gamification to remain effective in changing students' behaviors over a long-term application, the game needs to have evolving goals and challenges. Participants discussed that games keep students' interest longer when they are trying to win or accomplish some objective. As one participant explained, "that is the whole point of gamification. They earn their points or their tokens or whatever they're doing to get new skins or items." Participants said the drive to get new prizes or accomplishments is what keeps students interested in the game. "They want that extra badge," one participant noted, "They want another higher score." Participants felt similar rewards and constantly evolving challenges were necessary for long-term gamification to be effective.

Five teachers felt that in order for gamification to remain effective in changing students' behaviors over a long-term application, the games needed to be used as a supplement to other educational approaches. Other education approaches included lectures and readings. One participant explained, "kids like a buffet of learning. They want to have a choice on what they learn and you can give [gamification] to them as an option." The participants felt gamification worked best when integrated into current teaching styles and curriculums. As a participant noted, "I think doing it, just a game, just the whole time, that might lose some of the value of it." The participants felt gamification worked better as something teachers employed a couple of days a week or offered students at the end of a class.

Two teachers expressed the view that applying gamification over a long-term period would lose its effectiveness at changing student behaviors because students would get bored. One participant described their concerns that doing games over an extended period of time could result in "students who are click-your-way-through" and "not paying attention.". Another participant brought up their experience dealing with students during the aftermath of Covid. They noted how after years of using an online curriculum, students came back saying, "Don't make us sign in. We don't want to have to be on a computer." Students wanted personal interaction. For this reason, participants felt long-term use of gamification would reduce the effectiveness of a cyber curriculum.

DISCUSSION

Twenty-six themes were identified in the data from the 10 interview questions asked by the researchers. Once the data was analyzed, the investigators identified three major themes. The three major themes interviewees focused on: (a) how the student's relationship with technology affects the impact of the training, (b) how the gamification's design affects the impact of the training, and (c) how repetition affects the impact of the training. The prevalence of the three themes suggests that respondents felt that students' interactions with technology, the design of the gamified curriculum, and the frequency of training repetition were the most importance elements in shaping the impacts of a mandatory gamified cybersecurity awareness program on middle school students.

INTERPRETATION OF STUDY FINDINGS

CENTRAL THEME 1: STUDENT'S RELATIONSHIP WITH TECHNOLOGY AFFECTS THE IMPACT.

The research participants focused on how students' relationships with technology will affect the impacts of security awareness training. The participants focused on the fact that middle school was a time when students were increasing their technology usage and being more responsive to technology training. Participants' opinions support the argument that middle school years are the most promising opportunity to shape future security behaviors (Pye, 2016). Participants also noted that middle school is when many students are getting their first personal email addresses, starting to spend significant time on their cell phones, and beginning to use the internet regularly as part of their classes. They further noted that middle school is a time many other behavior-shaping classes are taught, suggesting that early teenage years were the most promising times for shaping and developing behaviors (Little et al., 2013).

Participants felt targeting students during a time when they were increasing their technology usage would produce long-term positive impacts. The two main impacts participants believed security awareness would have on middle school students were developing an awareness of risks and forging a more productive and secure workforce. Participants felt that even if students were not immediately facing threats and cyberattacks, the seeds of knowledge planted by the training would provide students with a greater chance of recognizing dangerous situations in the future. They also felt security awareness training in middle school increased students' interest in pursuing careers in cybersecurity and prepared them to be more secure members of the workforce. These views align with existing expert opinions that cybersecurity is necessary to protect students from the dangers of modern society and that countries with existing security awareness school curriculums possessed more tech-savvy and safe workforces (Pye, 2016; Stuparu, 2020).

CENTRAL THEME 2: GAMIFICATION DESIGN AFFECTS THE IMPACT.

Another common theme throughout the research was how the design of the gamified training curriculum affects the impact of the training. All the participants recalled experiences where they had seen gamification be effective in shaping student behaviors and confirmed that students respond positively to gamified learning. The views aligned with existing research indicating that students enjoy gamification and are more engaged and interested when lessons involve games (Chapman & Rich, 2018). However, participants also discussed experiences where poorly designed games failed to either maintain the interest of students or produce any positive impacts on student behaviors. In order to produce lasting positive impacts on student behaviors, they felt the games need to be designed to mimic real-world interactions and possess constantly evolving goals, prizes, and challenges.

Participants discussed experiences with educational games that failed to use hands-on, interactive experiences to teach the materials. They noted that games that failed to place the students in practical

scenarios and real-world situations might provide students with knowledge but will not produce actual changes in behaviors. As existing literature notes, simply providing knowledge without producing behavior change defeats the purpose of the class (Giannakas et al., 2019). For this reason, a well-designed game needs to use practical and interactive activities that will train students to behave in specific ways when confronted with security threats.

At the same time, participants emphasized that the game needs to be designed in a way that is enjoyable and keeps students' interest. Otherwise, students will view the game as merely something they have to do and just click through the activities. Participants felt games needed to have constantly evolving goals, prizes, and challenges to keep students coming back to the activities and lessons. These opinions support research by Micallef and Gamagedara (2018) suggesting rewards play an important role in the effectiveness of gamification. Only if the game were designed with prizes to keep students' interest and applicable, real-world exercises, would the gamified curriculum be effective in positively impacting student behaviors.

Central Theme 3: Repetition of Training Affects the Impact.

Another common theme participants discussed was how the repetition of the training affects the impact on middle school students. Participants felt that a single class was not sufficient to produce lasting effects on the students. Instead, they felt that security awareness training needed to be part of a long-term program taught over an extended time frame. The effectiveness of training implemented as part of an ongoing and continuing curriculum has been demonstrated in other countries (Stuparu, 2020). Participants expressed the opinion that training needs to take place over multiple sessions and classes, either throughout the school year or over multiple school years. They felt constant reinforcement was necessary to ensure the lessons and impacts from the training extended beyond simply the short-term.

Practical Implications of Findings

The study presented data showing that teachers and security education experts believe the heavy usage of technology and the growing number of cybersecurity threats make security awareness training in middle schools important for the safety and welfare of Texas students (Quayyum et al., 2021). The researchers suggest that the findings uncovered in the research support the belief that middle school is an ideal time to implement security awareness training and that training using gamification can produce lasting changes in the behaviors of middle school students.

The first finding was that middle school is an ideal age for impacting and shaping student behaviors. The results of the research show that cybersecurity experts and teachers agree that middle school is the ideal time to shape students' future behaviors. Middle school is the time when behavior-based training like health classes, sexual education, and good citizenship are taught because students are old enough to understand the concepts. Likewise, during middle school, students are beginning to increase their technology usage and develop their relationship with technology, making them more responsive to training designed to change and shape their behaviors than high school students.

The development of positive habits is middle school will impact students by helping them develop an awareness of the threats and dangers around them. Middle school students will be prepared to face the threats and dangers currently confronting them and will also be prepared for threats they are not currently encountering. Health classes and CPR classes taught in middle schools are designed to prepare students with the proper way to act even though they may not encounter a situation requiring those skills for many years. In the same way, security awareness training in middle schools can shape students' habits before they encounter many dangers and attacks. As a result, when they encounter these threats and dangers in the future, they will be able to recognize them and know how to act in both their personal lives and work lives.

The second finding was that gamification can be a key tool in impacting children's behaviors. Every participant was able to recount experiences where they had seen gamification be successful in teaching behaviors in a scholastic environment and many used game-based education in their own classes. The collected evidence supported existing research that suggests gamification is a more effective teaching method than other non-interactive activities (Hourcade, 2015). Several participants related their experiences with cybersecurity games aimed at teenagers that simulated real-world threats and situations and they discussed how student's security behaviors showed improvement afterward. Overall, experts felt gamification employing hands-on, practical activities was a critical part of ensuring security awareness positively impacted middle school students.

The third finding was that long-term gamification can be effective but the games must be combined with traditional educational approaches. Gamification alone is not enough to teach cybersecurity awareness to middle school students. Teacher and administrator experiences following Covid showed that students do not want to spend all of their time on computers. Students thrive when classes employ a variety of teaching techniques. Cybersecurity education programs in middle schools need to include traditional teaching techniques such as lectures, videos, and readings, in addition to educational games. A gamified cybersecurity curriculum alone would not be sufficient to make lasting impacts on students' cybersecurity behaviors and produce long-term behavioral changes. In order to make lasting positive improvements in students' security habits, schools need to rely upon teachers to teach the materials to the students.

Fortunately, the fourth finding shows that teachers possess the skills to teach the subject. Seventy-four percent of Texas teachers are 49 or younger (National Center for Educational Statistics, n.d.). They have grown up with the internet and modern computer technology and receive cybersecurity awareness training every year as part of their responsibilities. Plus, recent requirements to adopt technology into their classes during Covid, and the constantly changing curriculums mandated by schools, demonstrate that teachers possess the skills and resiliency to adapt to new educational mandates. If teachers are provided with a well-developed curriculum and provided training in the curriculum, they are capable of teaching security awareness to their students.

The fifth finding shows that schools possess the time and opportunity to provide security awareness training to students. Although schools have busy schedules and crowded curriculums, homeroom periods, advisory periods, and the use of computers and internet resources in core classes provide teachers with an opportunity to teach cybersecurity awareness. Many teachers also allow students to play games at the end of class if the students finish quizzes or activities. Teachers could use the free periods as an opportunity to teach security principles by allowing students to play games designed to teach cybersecurity ideas and behaviors. Schools need to have the time to teach the classes because security awareness training classes need to take place over an extended period of time in order to have a lasting impact on students.

Ultimately, the findings suggest that a security awareness curriculum taught over an extended period of time by trained teachers using a combination of traditional teaching techniques and cybersecurity games implementing hands-on practical security behaviors will positively impact student security behaviors. The curriculum will target middle school students at an age when they are increasing their use of technology and susceptible to training. The training will help students in both learning to recognize threats and developing into more tech-savvy professionals.

LIMITATIONS OF STUDY FINDINGS

Limitations are constraints and weaknesses in a study that are outside of the researchers' control but may affect the research study's design, results, and conclusions (Theofanidis & Fountouki, 2018). Four major limitations affected the study. Many of these limitations stemmed from the fact that current Texas middle schools do not have mandatory courses that teach security awareness training using gamification (EdWeek Research Center, 2020).

The first limitation was the inability to collect data from middle school students. Since no mandatory security awareness training courses exist in middle schools, no resources existed for the researcher to perform quantitative analysis, case studies, or observation (EdWeek Research Center, 2020). Further, experimentation was not possible since middle school students are a protected group (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 2014). Instead, the researchers were required to rely upon interviewees honestly sharing their experiences and opinions about middle school student education and behavior change programs.

The second limitation related to the difficulty of recruiting participants for the study. The CyberTexas foundation, a state-wide organization that provides cybersecurity boot camps and training programs to middle school and high school students, had agreed to assist with the recruitment of teachers to participate in the study (CyberTexas Foundation, 2018). Unfortunately, the organization's outreached efforts failed to produce many volunteers. As a result, the researchers were forced to resort to a variety of purposeful sampling techniques, including snowball sampling, which involves obtaining new participants through assistance from existing participants, and opportunistic sampling, which involves expanding the sampling criteria in response to new ideas and themes that emerge during the course of information gathering (Suri, 2011).

The use of additional purposeful sampling techniques and the extension of sampling criteria proved necessary to get the number of participants required to achieve saturation. The combining of multiple purposeful sampling techniques does not reduce the integrity of the research. Suri (2011) notes that researchers often employ a combination of two or more sampling strategies to ensure data collection is adequate to meet the needs and purpose of the study. Mixing purposeful sampling techniques provides flexibility and can be strategically utilized to develop high-level conclusions (Patton, 2002).

The final limitation, the broad range of work roles, was the result of the difficulty in recruiting participants. Many of the CyberTexas coaches turned out to either teach subjects other than cybersecurity, be school administrators, or be security professionals who teach or work with middle school students in their spare time. The limitation does not reduce the integrity of the research as schools often possess diverse faculty populations and network with colleagues from other backgrounds (Patterson & Mikovits, 2021). Obtaining views on the education of middle school students from multiple perspectives and backgrounds results in richer information saturation. Although the teachers, administrators, and security professionals answered the questions from different perspectives, ATLAS.ti coding indicated that the majority of the responses focused on the same themes and the sample size was sufficient to attain saturation.

RECOMMENDATIONS FOR FURTHER RESEARCH

Data collected from the participants suggests that teachers possess the skills and schools have the available time, to implement a security awareness training curriculum, supported by gamification, that would produce long-term improvements in student security habits. However, the games need to be designed with prizes and awards that appeal to students and the training needs to be provided over an extended period of time so students can integrate the knowledge. The research study prompted areas for further research.

Recommendation 1: Test Habit Shaping Games. The research proposes that a game with goals, objectives, and rewards can keep students interested and produce lasting behavioral changes. Habitica is an example of a game targeted at young adults that is designed to help them develop proper habits through completing goals, achieving objectives, and earning rewards (Ionescu, 2022). However, no studies or research have been performed to determine whether Habitica, or similar games, keep the long-term interest of young adults or whether the games make a lasting impact on their behaviors. Future research can test the effectiveness of existing long-term behavior-shaping games to determine their effectiveness over an extended period of time. Since middle school students are a protected

group, the research study would need to be a qualitative study involving interviewing parents of teenagers who use Habitica or similar behavior-changing applications (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 2014).

Recommendation 2: Teacher Technology Comfort By Age. Although statistics show that 74% of Texas teachers are 49 or younger and have grown up using computers and technology, the statistics also show that 26% of teachers are 50 or older (National Center for Educational Statistics, n.d.). The wide age discrepancy may indicate that some teachers will feel more comfortable teaching cybersecurity classes after receiving training than other teachers. Research is needed to determine how teachers from various age groups respond to teaching cybersecurity lessons after receiving training. A discrepancy between the skill levels of older teachers versus younger teachers may have important implications for how schools need to implement cybersecurity awareness classes. A qualitative study could allow teachers of various ages to teach a security awareness class to a group of students and later report on their level of comfort or discomfort while teaching the lessons.

CONCLUSION

The purpose of the proposed exploratory qualitative study was to explore 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. Current Texas middle schools do not have mandatory courses that teach security awareness training using gamification (EdWeek Research Center, 2020). For this reason, the study used a qualitative exploratory method, relying upon the viewpoint and experiences of the participants (Cotton, 2021). Purposive sampling resulted in fifteen participants sharing their ideas and experiences related to the impacts of providing mandatory gamified cybersecurity awareness training in Texas middle schools.

The research question asked what 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. Participant answers identified three major themes. The primary themes focused on: (a) the students, (b) the teachers, and (c) the curriculum. After interviews were completed using semi-structured questions, the transcripts were created by Transcription Puppy, reviewed by the researchers, and imported into ATLAS.ti for coding and evaluating patterns within the content of the interviews (Paulus & Lester, 2016). To protect the credibility and confirmability of the research, each participant received a copy of their transcript to review and confirmed that the scripts accurately reflected their opinions and viewpoints (Connelly, 2016).

The first theme identified by the study was that middle school students' relationship with technology affects the impact of security awareness training. Middle school students are beginning to interact heavily with technology and, unlike high school students, are young enough to still be malleable and responsive to behavior-shaping curriculums. The second primary theme focused on gamification needs to be designed with hands-on, real-world activities to shape students' habits and rewards to keep students' interest. A poorly designed game will not keep students' interest or produce positive changes in their long-term behaviors. The third theme focused on the need for a security awareness curriculum to be repetitive, extending over multiple lessons and years to reinforce the positive impacts over an extended period of time.

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 applications combined with traditional teaching techniques can help students develop positive habits. The researchers suggest 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. Integrating the training into current school schedules will allow the classes to be taught over an extended period of time, producing a repetition that will reinforce the positive impacts of the training program.

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.

REFERENCES

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science*, *10*(5), 1-3. https://doi.org/10.26483/ijarcs.v10i5.6476

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity interventions for teens: Two time-based approaches. *IEEE Transactions on Education, 62*(2), 134-140.

Bada, M., & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Bakker, J. I. (Hans). (2019). Grounded theory methodology and grounded theory method: Introduction to the special issue. *Sociological Focus*, *52*(2), 91–106. https://doi.org/10.1080/00380237.2019.1550592

Bargh, J. A., & Morsella, E. (2008). The unconscious mind. *Perspectives on Psychological Science*, *3*(1), 73–79. https://doi.org/10.1111/j.1745-6916.2008.00064.x

Basarmak, U., Yakar, H., Güneş, E., & Kuş, Z. (2019). Analysis of digital citizenship subject contents of secondary education curricula. *Turkish Online Journal of Qualitative Inquiry*, *10*(1), 26–51. https://doi.org/10.17569/tojqi.438333

Bay, J. L., Mora, H. A., Sloboda, D. M., Morton, S. M., Vickers, M. H., & Gluckman, P. D. (2012). Adolescent understanding of DOHaD concepts: A school-based intervention to support knowledge translation and behaviour change. *Journal of Developmental Origins of Health and Disease, 3*(6), 469-482. https://doi.org/10.1017/S2040174412000505

Birks, M., Mills, J., Francis, K., & Chapman, Y. (2009). A thousand words paint a picture: The use of storyline in grounded theory research. *Journal of Research in Nursing*, *14*, 405-417. https://doi.org/10.1177/1744987109104675

Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. (2011). When parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act.' *First Monday*, *16*(11). https://doi.org/10.5210/fm.v16i11.3850

Catarino, T., Fragoso, B., Mira da Silva, M., & Vasconcelos, A. (2016, June). Inconsistencies in information security roles. *Proceedings of the 13th European Mediterranean & Middle Eastern Conference on Information Systems*, Krakow, Poland.

Chapman, J. R., & Rich, P. J. (2018). Does educational gamification improve students' motivation? If so, which game elements work best? *Journal of Education for Business*, *93*(7), 315–322. https://doi.org/10.1080/08832323.2018.1490687

Chong, I., Xiong, A., & Proctor, R. (2019). Human factors in the privacy and security of the internet of things. *Ergonomics in Design*, *27*(3), 5-10. https://doi.org/10.1177/1064804617750321

Clarke, G., Kehoe, J., & O'Broin, D. (2017, October). The effects of gamification on the formation of a habit of studying in tertiary level students. *Proceedings of the European Conference on Games Based Learning*, 871-880.

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing, 25*(6), 435-436.

Cotton, A. (2021). *Identification of manual cybersecurity tasks for artificial intelligence automation conversion: A qualitative study* [Doctoral dissertation, Colorado Technical University].

Creswell, J. W., Hanson, W. E., Plano Clark, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. *The Counseling Psychologist*, *35*(2), 236–264. https://doi.org/10.1177/0011000006287390

Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMAS Database: The DATABASE for Advances in Information Systems*, *45*(4), 54-71. https://doi.org/10.1145/2691517.2691521

Cybersecurity Grants for Schools Act of 2022. (2022). House Resolution 6868. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/6868

CyberTexas Foundation. (2018). *Homepage*. https://cybertexas.org/main

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013, November). Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. *Proceedings of the 2013 ACM Conference on Computer & Communications Security, Berlin, Germany,* 915-928. https://doi.org/10.1145/2508859.2516753

Dennis, A., & Minas, R. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *SIGMIS Database*, *49*, 15-37. https://doi.org/10.1145/3210530.3210533

EdWeek Research Center. (2020). *The state of cybersecurity education in K-12 schools*. Cyber.org. https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63-71.

Fiorella, L. (2020). The science of habit and its implications for student learning and well-being. *Educational Psychology Review*, *32*(3), 603-625. https://doi.org/10.1007/s10648-020-09525-1

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35. https://doi.org/10.1016/j.cose.2005.12.004

Gardner, B., Lally, P., & Rebar, A. (2020). Does habit weaken the relationship between intention and behaviour? Revisiting the habit-intention interaction hypothesis. *Social & Personality Psychology Compass*, *14*(8), 1-24. https://doi.org/10.1111/spc3.12553

Gardner, B., Lally, P., & Wardle, J. (2012). Making health habitual: The psychology of 'habit-formation' and general practice. *British Journal of General Practice*, *62*(605), 664–666. https://doi.org/10.3399/bjgp12X659466

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, *28*(3), 81–106. https://doi.org/10.1080/19393555.2019.1657527

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of information security awareness and training. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 59–70. https://doi.org/10.5220/0006128500590070

González, J. M. M., & Aguilar, B. S. (2019). How do teenagers interact with video games? Preferences and performative skills. *Revista Latina de Comunicación Social*, *74*, 360-382.

Goyal Chin, A., Etudo, U., & Harris, M. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235-252. https://doi.org/10.15388/infedu.2016.12

Gunnulfsen, A. E. (2021). Applying the integration dimensions of quantitative and qualitative methods in education policy research: Lessons learned from investigating micro policymaking in Norwegian schools. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211028349

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140-154. https://doi.org/10.1108/09685221111153537

Hagens, V., Dobrow, M. J., & Chafe, R. (2009). Interviewee transcript review: Assessing the impact on qualitative research. *BMC Medical Research Methodology*, 9(47). https://doi.org/10.1186/1471-2288-9-47

Håkansson, A. (2013, July). Portal of research methods and methodologies for research projects and degree projects. *Proceedings of the World Congress in Computer Science, Computer Engineering and Applied Computing, Las Vegas, USA*, 67-73

Hammond, S. T. (2019). *Threat and coping appraisals on information security awareness training effectiveness: A quasi-experimental study* [Doctoral dissertation, Capella University].

He, W., Ash, I., Answer, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital.* Advance online publication. https://doi.org/10.1108/JIC-05-2019-0112

Hourcade, J. P. (2015). *Child-computer interaction.* http://homepage.divms.uiowa.edu/~hourcade/book/child-computer-interaction-first-edition.pdf

Ionescu, S. (2022, July 8). *Habitica review.* https://www.techradar.com/reviews/habitica

Jin, G., Tu, M., Kim, T., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning, 12*(1), 150-158. https://doi.org/10.11591/edulearn.v12i1.7736

Johnson, D. (2022). House set to debate bills on cyber education, President's Cup and TikTok. *SCMedia.* https://www.scmagazine.com/analysis/application-security/house-set-to-debate-bills-on-cyber-education-presidents-cup-and-tiktok

Johnson, K. (2017). *The training deficiency in corporate America: Training security professionals to protect sensitive information* [Doctoral dissertation, Walden University].

Kaiser, K. (2009). Protecting respondent confidentiality in qualitative research. *Qualitative Health Research*, *19*(11), 1632–1641. https://doi.org/10.1177/1049732309350879

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. *Proceedings of the Eleventh Symposium on Usable Privacy and Security,* 39-52. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf

Kelley, A. (2022). *Security would receive funding for cyber education programs under bipartisan bill.* https://www.nextgov.com/cybersecurity/2022/03/schools-would-receive-funding-cyber-education-programs-under-bipartisan-bill/362728/

Khando, K., Gao, S., Islam, S., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kirova, D., & Baumöl, U. (2018). Factors that affect the success of security education, training, and awareness programs: A literature review. *Journal of Information Technology Theory and Application*, *19*(4), 56-82.

Krouwel, M., Jolly, K., & Greenfield, S. (2019). Comparing Skype (video calling) and in-person qualitative interview modes in a study of people with irritable bowel syndrome - An exploratory comparative analysis. *BMC Medical Research Methodology*, *19*(1), 219. https://doi.org/10.1186/s12874-019-0867-9

Linneberg, M. S., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal*, *19*(3), 259-270. https://doi.org/10.1108/QRJ-12-2018-0012

Little, L., Bell, B., Defeyter, G., Read, J. C., Fitton, D., & Horton, M. (2013, June). Behaviour change interventions: Teenagers, technology, and design. *Proceedings of the 12th International Conference on Interaction Design and Children*, *New York, USA,* 610-612. https://doi.org/10.1145/2485760.2485894

Martin, P. (2018). *Habit analysis: Using decisions analysis to take control of habits* [Doctoral dissertation, Stanford University].

McQuaid, P. A., & Cervantes, S. (2019). How to achieve a seasoned cybersecurity workforce. *Software Quality Professional*, *21*(4), 4-10.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Meyer, D., & Schutz, P. (2020). Why talk about qualitative and mixed methods in educational psychology? Introduction to special issue. *Educational Psychologist*, *55*(4), 193-196. https://doi.org/10.1080/00461520.2020.1796671

Micallef, N., & Gamagedara, A. (2018). Security questions education: Exploring gamified features and functionalities. *Information and Computer Security*, *26*(3), 365-378. https://doi.org/10.1108/ICS-03-2018-0033

Mills, J., Birks, M., & Hoare, K. (2014). Grounded theory. In J. Mills, & M. Birks (Eds.), *Qualitative methodology* (pp. 107-122). Sage. https://doi.org/10.4135/9781473920163

National Center for Educational Statistics. (n.d.). *Average and median age of public school teachers and percentage distribution of teachers by age category, sex, and state: 2017-2018*. https://nces.ed.gov/surveys/ntps/tables/ntps1718_fltable02_t1s.asp

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (2014). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. *Journal of the American College of Dentists*, *81*(3), 4-13.

Patterson, B., & Mikovits, J. (2021). How diverse is your research sample? Prioritizing inclusivity in nursing education research. *Nursing Education Perspectives*, *42*(1), 3-4. https://doi.org/10.1097/01.NEP.0000000000000768

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage.

Paulus, T. M., & Lester, J. N. (2016). ATLAS.ti for conversation and discourse analysis studies. *International Journal of Social Research Methodology, 19*(4), 405–428. https://doi.org/10.1080/13645579.2015.1021949

Petruzzelli, E., & Sharma, N. (2019). Closing the gaps in cybersecurity. *Chemical Engineering Progress*, *115*, 35-39.

Pinder, C., Vermeulen, J., Cowan, B., & Beale, R. (2018). Digital behaviour change interventions to break and form habits. *ACM Transactions on Computer-Human Interaction*, *25*(3). https://doi.org/10.1145/3196830

Plowman, L., McPake, J., & Stephen, C. (2010). The technologisation of childhood? Young children and technology in the home. Children & Society, 24(1), 63–74. https://doi.org/10.1111/j.1099-0860.2008.00180.x

Poleon, V. (2020). *Millennials' information security habits and protection motivation intention: A quantitative study.* (Publication No. 28028857) [Doctoral dissertation, Capella University]. ProQuest Dissertations and These Global.

Pye, K. (2016). *Teaching cybersecurity in K-12 schools*. (Publication No. 10155676) [Master's thesis, Utica College]. ProQuest Dissertations and Thesis Global.

Quayyum, F., Cruzes, D., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*. https://doi.org/10.1016/j.ijcci.2021.100343

Roberts, J. M. (2014). Critical realism, dialectics, and qualitative research methods. *Journal for the Theory of Social Behaviour, 44*(1), 1–23. https://doi.org/10.1111/jtsb.12056

Rowe, D., Ekstrom, J., & Lunt, B. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 Conference on Information Technology Education*, 113-122. https://doi.org/10.1145/2047594.2047628

Santos, S. A., Trevisan, L. N., Veloso, E. F. R., & Treff, M. A. (2021). Gamification in training and development processes: Perception on effectiveness and results. *Revista de Gestão*, *28*(2), 133-146. https://doi.org/10.1108/REGE-12-2019-0132

Sarbadhikari, S. N., & Sood, J. M. (2018). Gamification for nurturing healthy habits. *The National Medical Journal of India*, *31*(4), 253-254. https://doi.org/10.4103/0970-258X.258236

Sezer, B., Yilmaz, R., & Fatma Gizem, K. Y. (2015). Cyber bullying and teachers' awareness. *Internet Research*, *25*(4), 674-687. https://doi.org/10.1108/IntR-01-2014-0023

Shelton, S. A., & Flint, M. A. (2019). The spacetimemattering and Frankenstein-esque nature of interview transcriptions. *Qualitative Research Journal*, *19*(3), 202-212. https://doi.org/10.1108/QRJ-03-2019-104

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Smith, C. (2018). *Cyber security, safety, & ethics education* [Master of Science in Cybersecurity dissertation, Utica College].

Snyder, J. C. (2018). A framework and exploration of a cybersecurity education escape room [Master of Science dissertation, Brigham Young University].

Stuparu, A. (2020). *Education pathways to national cyber resilience: The Australian story* [Doctoral dissertation, Australian National University].

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal*, *11*(2), 63-75. https://doi.org/10.3316/QRJ1102063

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative Nursing*, *7*(3), 155-163. http://doi.org/10.5281/zenodo.2552022

Treiblmaier, H., Putz, L., & Lowry, P. B. (2018). Research commentary: Setting a definition, context, and theory-based research agenda for the gamification of non-gaming applications. *AIS Transactions on Human-Computer Interactions*, *10*(3), 129-163. https://doi.org/10.17705/1thci.00107

Tsimtsiou, Z., Drosos, E., Drontsos, A., Haidich, A., Dantsi, F., Sekeri, Z., Dardavesis, T., Nanos, P., & Arvanitidou, M. (2019). Raising awareness on cyber safety: Adolescents' experience of a primary healthcare professional-led, school-based, multi-center intervention. *International Journal of Adolescent Medicine and Health*, *31*(6). https://doi.org/10.1515/ijamh-2017-0072

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and Protection Motivation Theory. *Information & Management*, *49*(9), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Van Mechelen, M., Gilutz, S., Hourcade, J. P., Baykal, G. E., Gielen, M., Eriksson, E., Walsh, G., Read, J., & Iversen, O. S. (2020, June). Teaching the next generation of child-computer interaction researchers and designers. *Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts*, *London, UK,* 69–76. https://doi.org/10.1145/3397617.3398068

van Niekerk, J., Thomson, K., & Reid, R. (2013). Cyber safety for school children: A case study in the Nelson Mandela Metropolis. In R. C. Dodge, & L. Futcher (Eds.). *Information assurance and security education and training*. Springer. https://doi.org/10.1007/978-3-642-39377-8_11

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Walker, V., Bowkett, G., & Duchaine, I. (2018). All companies are technology companies: preparing Canadians with the skills for a digital future. *Canadian Public Policy*, *44*(S1), S153-S158. https://doi.org/10.3138/cpp.2018-011

Walther, B., Hanewinkel, R., & Morgenstern, M. (2014). Effects of a brief school-based media literacy intervention on digital media use in adolescents: Cluster randomized controlled trial. *Cyberpsychology, Behavior, and Social Networking*, *17*(9), 616-623. https://doi.org/10.1089/cyber.2014.0173

Wash, R., & Rader, E. (2015). Too much knowledge? Security beliefs and protective behaviors among united states internet users. *Proceedings of the Eleventh Symposium on Usable Privacy and Security,* 309-325.

Weller, S. (2017). Using internet video calls in qualitative (longitudinal) interviews: Some implications for rapport. *International Journal of Social Research Methodology*, *20*(6), 613–625. https://doi.org/10.1080/13645579.2016.1269505

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), e23692. https://doi.org/10.2196/23692

Wu, T., Tien, K., Hsu, W., & Fu-Hsiang, W. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences*, *11*(19), 9266. https://doi.org/10.3390/app11199266

Xu, Z., & Guo, K. (2019). It ain't my business: A coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management*, *32*(5), 824-842. https://doi.org/10.1108/JEIM-10-2018-0229

Yildiz Durak, H. (2019). Human factors and cybersecurity in online game addiction: An analysis of the relationship between high school students' online game addiction and the state of providing personal cybersecurity and representing cyber human values in online games. *Social Science Quarterly*, *100*(6), 1984–1998. https://doi.org/10.1111/ssqu.12693

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-415.

Young, H., Kolto, A., Reis, M., Saewyc, E. M., Moreau, N., Burke, L., Cosma, A., Windlin, B., Saoirse, N. G., & Godeau, E. (2016). Sexual health questions included in the health behaviour in school-aged children (HBSC) study: An international methodological pilot investigation. *BMC Medical Research Methodology, 16*.

APPENDIX A: INTERVIEW PROTOCOL

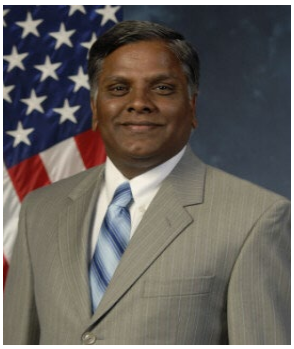
1. Initiate the conference call via Zoom and test to ensure the connection is established.
2. Greet the participant and thank them for participating in the study.
3. Ensure the participant is in a comfortable and distraction free environment where they can talk freely.
4. Explain the purpose of the study.
5. Review the informed consent form (which they signed before the interview was scheduled) and ensure they are comfortable with the interview process. Ensure the participant knows they have the right to terminate the interview at any time without reason.
6. Ensure the Zoom name of the participant is changed to a pseudonym so no identifying information is recorded.
7. Start the recording and assign an identification number to each participants interview.
8. Ask interview questions per interview script and follow-on questions for clarification.

APPENDIX B: INTERVIEW QUESTIONS

1. What is your current job title?
2. How many years have you spent interacting and working with middle school students?
3. In what ways do you feel middle school is or is not an appropriate time for providing behavior-based trainings, like security awareness training?
4. Based upon your experience, to what extent, if any, do you feel that good security habits taught in middle school impact the student's long-term security behaviors?
5. How prepared do you believe middle schools and teachers are to implement cybersecurity awareness training curriculums?
6. Would you support or oppose the idea of making cybersecurity awareness training courses mandatory? Why or why not?
7. What are some of the biggest challenges, if any, that you see to the implementation of a mandatory cybersecurity curriculum in middle schools?
8. How familiar are you with the use of gamification in education?
9. How effective do you feel security awareness training programs involving gamification could be in shaping the habits and behaviors of middle school children?
10. In what ways do you believe the long-term use of gamification as part of a mandatory school cyber security curriculum would be successful and/or unsuccessful in changing middle school students' security behaviors?

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.