

2021

## Development of a Pilot Training Program for Middle School Students to Reduce End-User Cyber Vulnerabilities

Connie D. Howard  
*Walden University*

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>



Part of the [Curriculum and Instruction Commons](#), and the [Public Administration Commons](#)

---

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact [ScholarWorks@waldenu.edu](mailto:ScholarWorks@waldenu.edu).

# Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral study by

Connie Dale Howard

has been found to be complete and satisfactory in all respects,  
and that any and all revisions required by  
the review committee have been made.

## Review Committee

Dr. Linda Sundstrom, Committee Chairperson, Public Policy and Administration Faculty  
Dr. Julian Muhammad, Committee Member, Public Policy and Administration Faculty  
Dr. Michael Brewer, University Reviewer, Public Policy and Administration Faculty

Chief Academic Officer and Provost  
Sue Subocz, Ph.D.

Walden University  
2021

Abstract

Development of a Pilot Training Program for Middle School Students to Reduce End-  
User Cyber Vulnerabilities

by

Connie Howard

MA, Walden University, 2006

BS, Cumberland University, 2000

Professional Administrative Study Submitted in Partial Fulfillment  
of the Requirements for the Degree of  
Doctor of Public Administration

Walden University

August 2021

## Abstract

This qualitative study contributes to the limited body of knowledge on cybersecurity in middle schools beyond awareness programs. The purpose was to develop a pilot training module for middle school students comprising an analysis of public documents to examine what topics should be included in a pilot training program to reduce problematic cyber practices. Attitude functional theory was used as the conceptual framework to provide insights into the process of persuading a positive behavioral change in a targeted group that is sustainable. A systematic analysis of national, state, and local public documents was conducted to compare practices, including a K–12 data breach national report, to understand what topics should be included in the pilot training module. The findings showed the need for training programs to further awareness; lead to positive outcomes, such as persuading students to take a more active role in their online safety; go beyond awareness training; and motivate students to sustain a positive behavioral change. A recommended implementation framework is described along with a pamphlet and corresponding Canvas module divided into quarterly lessons. These lessons are designed to ensure a positive social change by motivating and increasing student knowledge, targeting the middle school age range to reduce end-user cyber vulnerabilities.

Development of a Pilot Training Program for Middle School Students to Reduce End-  
User Cyber Vulnerabilities

by

Connie D. Howard

MA, Walden University, 2006

BS, Cumberland University, 2000

Professional Administrative Study Submitted in Partial Fulfillment  
of the Requirements for the Degree of  
Doctor of Public Administration

Walden University

August 2021

## Table of Contents

List of Figures .....	iv
Section 1: Introduction to the Problem .....	1
Problem Statement .....	1
Purpose of the Study .....	3
Evidence of the Problem .....	3
Evidence of the Problem in Professional Literature .....	4
Research Question .....	4
Nature of the Administrative Study .....	5
Significance.....	6
Summary and Transition.....	6
Section 2: Conceptual Approach and Background .....	8
Conceptual Framework.....	8
Concepts, Models, and Theories .....	8
Definitions.....	9
Relevance to Public Organizations .....	10
Role of the DPA Student.....	11
Summary and Transition.....	12
Section 3: Data Collection Process and Analysis .....	13
Practice-focused Questions .....	13
Data Collection Process .....	14
Rationale .....	14

Published Outcomes and Research .....	15
Archival and Operational Data .....	16
Analysis and Synthesis .....	17
Conclusion .....	18
Section 4: Evaluation and Recommendations.....	19
Findings and Implications.....	19
Recommendations.....	24
Strength and Limitations of the Project .....	32
Section 5: Dissemination Plan .....	34
Dissemination Plan .....	34
Summary .....	34
References.....	36
Appendix A: Beware of Phishing Handout .....	40
Appendix B: Dissemination Pamphlet.....	41
Appendix C: MS Pilot Cyber Security Quarterly Training Outline .....	42

## List of Tables

Table 1. Reference Tracker.....	16
Table 2. K-12 Cyber Incidents.....	21
Table 3. Student Internet Safety.....	23



## List of Figures

Figure 1. Enrollment Size .....	22
Figure 2. Community Type.....	24
Figure 3. Implementation Framework .....	25
Figure 4. Quarter 1 Implementation Framework .....	27
Figure 5. Quiz: Is Your Identity Safe?.....	28
Figure 6. Quarter 2 Implementation Framework .....	28
Figure 7. Example of Phishing Message.....	29
Figure 8. Beware of Phishing Handout Example.....	30
Figure 9. Click or Skip? .....	30
Figure 10. Quarters 3 and 4 Implementation Framework.....	31

## Section 1: Introduction to the Problem

Cybersecurity impacts public and nonpublic schools and districts from cyber incidents that could be either accidental or deliberate. When incidents occur, personal identifiable information (PII) is at risk of being exposed. Schools and districts are not required to report incidents; therefore, stakeholders could be unaware of systems that have been comprised (Readiness and Emergency Management for Schools Technical Assistance Center, 2017). These organizations will need to look at options to increase cybersecurity for students, faculty, and staff to defend against these furtive crimes that are anonymous threats and can be both accidental or intentional to the schools. In 2016, over 200 K–12 schools had cyber-related incidents consisting of ransomware, phishing, and data breaches (Herold, 2017). Schools not only need to plan for physical threats to the school but also various cyber threats.

Richardson et al. (2020) claimed the attacks on school systems exploit human vulnerabilities called the human factor. Over 95% of cyberattacks and breaches result from human error, such as clicking on a link or opening a file (Elgan, 2019; Richardson et al., 2020). Attackers can target humans easier and faster than attempting to target a system (Elgan, 2019). Education is a prime target because schools have a vast amount of information on both students, parents, teachers, and staff, such as social security numbers, financial data, and other forms of PII (Richardson et al., 2020).

### **Problem Statement**

The emergence of virtual classrooms has made schools realize they are not equipped to handle the growing issue of online bullying, hate speech, misinformation,

and cybersecurity (Castro, 2020). The problem addressed through this study was middle school students at the school district study site are issued Chromebooks to complete schoolwork without any training or best practices and are engaging in problematic cyber practices that create cybersecurity risks for the school district. In 2020, schools faced a new challenge with a 60% increase in online crimes in the education sector, according to Microsoft Security Intelligence (Castro, 2020). *Education Week* reported surveying over 500 K–12 technology leaders worldwide to understand their approaches regarding cybersecurity threats, and 77% of the leaders stated they would train information technology (IT) staff on techniques for dealing with cybersecurity (Lieberman, 2020). Lieberman (2020) reported that 63% of the surveyed leaders recognized the need for outside help and planned to purchase products and services specifically for cybersecurity. Even though K–12 leaders reported the need for purchasing cybersecurity programs, only 12% have budgeted funding for these initiatives (Lieberman, 2020).

Cybersecurity incidences do not represent the exact number of cases due to limited reporting requirements, and those disclosures that are required are often not publicly accessible (EdTech Strategies, 2021). This study contributes to the body of knowledge used to address cybersecurity, allowing educators to understand the necessity of information security awareness as an employee and an educator of others. Chou and Chou (2016) discusses the issues currently faced by teachers regarding the new educational trends and equipping students with relevant 21st-century skills. Technological advances will be reversed if human factors are not addressed (Nobles, 2018). These human factor vulnerabilities are addressed by raising awareness of

information security and educating teachers to reduce the human factor by requiring training and awareness programs that will not only improve and enhance the teacher's judgment when dealing with information security but also motivate students to change how they view cybersecurity (Chou & Chou, 2016).

### **Purpose of the Study**

The internet has provided individuals with anonymity that allows easy access for hackers. Parents, students, and teachers need to be aware that these threats exist, and school systems need to develop the best education cybersecurity practices. The purpose of this qualitative study was to develop a pilot training module for middle school students, based on best practices, to reduce problematic cyber practices. Implementing cybersecurity prevention and protection programs for districts could reduce the possibility of incidents by educating stakeholders on techniques for dealing with these security threats.

### **Evidence of the Problem**

EdTech Strategies (2021) cataloged 348 publicly disclosed cybersecurity threats across 44 states in 2019. Of these threats, 95% of these incidents occurred in public school districts. These incidents include both students and staff data breaches, ransomware, or phishing. The number of incidents has tripled since 2018, likely due to technology increasingly playing a more extensive role in education (EdTech Strategies, 2021). In 2019, 60% of the reported incidents were unauthorized disclosure or breaches (EdTech Strategies, 2021). These data breaches could result in stolen identities and fraud not only for teachers but also for students. These cyberattacks have severe consequences;

for example, a school district in New York City paid \$100,000 to hackers to recover data that had been stolen (Klein, 2020). Herold (2017) discussed how Montana's school system had 2,100 students' identities compromised when their servers were hacked and ransomed for \$150,000 in cryptocurrency (i.e., Bitcoin).

### **Evidence of the Problem in Professional Literature**

The majority of cybersecurity research in K–12 schools focus on the human factor and how these events impact schools and districts. Cyber threats continue to evolve and transform requiring increased levels of security (Richardson et al., 2020). Cybersecurity risks in schools require removing the source, addressing the vulnerabilities, and lessening the impact (Richardson et al., 2020). The human factor (e.g., uneducated users) is one underlying reason these attacks are successful. Richardson et al. (2020) explained that 56% of employees that require the internet for their job do not receive any training regarding information security. Chou and Chou (2016) reported that stakeholders lack awareness or disregard information security, which is a problematic behavior that requires professional development to enhance the understanding of information security and its usefulness. To lessen this risk to schools, they will need to implement training programs paying particular attention to the human factor.

### **Research Question**

RQ: What topics should be included in a pilot training program to reduce problematic cyber practices?

### **Nature of the Administrative Study**

In this qualitative study, I conducted a document analysis of existing guidelines and best practices to address problematic behaviors that create cybersecurity risks for the school district study site. Previous research suggests a relationship between human factors and cybersecurity incidents (Chou & Chou, 2016; Nobles, 2018; Richardson et al., 2020). To develop a pilot training program, I analyzed publicly available cyber breach reports, sample policies, and sample cybersecurity training programs to reduce end-user problematic behaviors. First, I evaluated publicly disclosed cyber incidents involving K–12 schools to shed light on possible threats to and the vulnerabilities of the school district study site. This evaluation allowed for the determination if certain threats were more likely given specific district characteristics.

The findings in this study begin the inquiry process to gauge best practices from other school districts and evaluate procedures that could be improved or implemented within the county. This type of analysis provides educational policymakers with opportunities to create programs to educators, students, and communities by anticipating a range of outcomes for any future they encounter. I addressed a variety of limitations, challenges, and barriers while conducting this study, including the cyber breach reports analyzed may have been incomplete due to the voluntary nature of reporting agencies; most training is done for adults or high school students, so there was limited middle school student training information; and there was also limited information on middle school students' actual problematic cyber behaviors, so I needed to make basic assumptions concerning their problematic behaviors. Due to the rapid changes in

computer learning as a result of the COVID-19 pandemic, limited data were available on current practices.

### **Significance**

This study is significant because it creates a model for training middle school students on safe cybersecurity practices that could later be expanded to students of other ages and school district stakeholders. Teaching middle school students responsibility for their actions online creates a greater sense of digital citizenship. Organizations can prepare for risks by analyzing the nature of the threat being faced using the following aspects: preventable, strategic, and external risks (Kaplan & Mikes, 2012). The COVID-19 pandemic has forced schools into a new environment that they are ill prepared for because of outdated equipment, and users are forced to use online tools they do not fully understand. This inexperienced path was highlighted by the Zoombooming incidents occurring from low configured security settings placing classrooms at risk (Castro, 2020). The Federal Bureau of Investigation has reported that online crime complaints have quadrupled since the COVID-19 pandemic (Castro, 2020).

### **Summary and Transition**

Schools can implement strategies for preventing cyber incidents. These components build a solid foundation for positively affecting the community by teaching students digital citizenship. This study addressed a gap in the body of knowledge related to cybersecurity training materials for middle school students. The findings of this study can assist school districts in their efforts to implement cybersecurity training programs by answering the research question of: What topics should be included in a pilot training

program to reduce problematic cyber practices? In Section 2, I will discuss the theoretical concepts that supported this study included the attitude functional theory, focusing on the persuasive appeal of behaviors.



## Section 2: Conceptual Approach and Background

### **Conceptual Framework**

In this study, I collected data through document analysis of publicly available reports, policies, and sample training programs whose contents were aligned with the problem statement and purpose of this study as well as the gap in the literature. The problem addressed in this study was that without training or best practices to reduce the risks of problematic cybersecurity behaviors, middle school students are ill prepared for the responsibility of ensuring their information remains safe while online. The purpose of this study was to develop a pilot training module specifically designed for middle school students based on the research question addressed in this study.

In this section, I focus on the concepts, models, and theories that were used to address the study problem. A short description of the study's relevance is also provided with further details. Finally, my role as the DPA student is described along with an explanation of the motivations and perspectives regarding the choices of what topics should be included in a pilot training program.

### **Concepts, Models, and Theories**

The concept that provided the framework for this study was Katz's attitude functional theory in which the author stated that understanding motivation can provide insights that can be used to influence change. School systems need to reduce their vulnerabilities to cyber threats by developing a behavioral training program to assist stakeholders. Attitude functional theory was used to help understand motivating factors of students and provide insights into behavioral intentions to influence change in online

security (see Trim & Lee, 2019). In this study, useful programs and resources will highlight avenues for implementing a pilot training program beginning with the middle school level.

### **Definitions**

The following terms are used throughout this study and were defined by the International Association of Chiefs of Police (IACP) Law Enforcement Cyber Center and The National School Boards Association's guide for data security for schools.

*Cybersecurity*: An unauthorized intrusion into the normal operations of a computer or network (IACP Law Enforcement Cyber Center, 2015).

*Data breach*: Unauthorized disclosure of sensitive information to someone that is not authorized to view or receive the information (IACP Law Enforcement Cyber Center, 2015).

*Insecure practices*: Insufficient protection for collecting, sending, storing, and encrypting data (Czuprynski & Smith, 2017).

*Malware*: A virus that attacks a specific computer (IACP Law Enforcement Cyber Center, 2015).

*PII*: Unique pieces of information that could be used to identify individuals (IACP Law Enforcement Cyber Center, 2015).

*Phishing*: The attempt to simulate an email from a trusted source to bait individuals into revealing PII (IACP Law Enforcement Cyber Center, 2015).

*Theft*: Deliberate attacks on either systems or individuals to access sensitive data (Czuprynski & Smith, 2017).

### **Relevance to Public Organizations**

Developed in 1960, Katz reasoned in attitude functional theory that appealing to a targeted attitude with a persuasive appeal would reinforce the desired attitude (Carpenter, 2012). The purpose of a school safety framework is to assess the strengths and weaknesses to create a plan for promoting security and noting any gaps (Twigg, 2007). School management's perspectives on issues that arise due to cyber threats needs to be addressed to ensure that the environment remains safe and secure. In a conceptual framework for providing a safe school environment, Twigg (2007) listed six components: learning, management, resources, location and structures, families and inclusion, and events and activities. These areas affect the school environment, including individual hazards and associated risks such as cyber threats. The National Institute of Standards and Technology stated that a cybersecurity framework provides the use of a common language and methodology for managing risks to complement programs already in place (Keller, 2020).

Hackers are involved in computer system intrusions that are used to infiltrate networks (even protected networks). According to the National School Board Association, it is the responsibility of all school districts to safeguard their data by developing policies and procedures to safeguard information from insecure practices (Czuprynski & Smith, 2017). In 2019, according to the K-12 Cybersecurity Resource Center, EdTech Strategies noted their highest number of incidents reported (Klein, 2020). Hackers' breaches have led to serious consequences for school districts across the United States ranging from closing schools or postponing classes due to ransomware attacks to

phishing emails providing hackers with a window into the network. Many of these attacks are the result of a lack of awareness; schools have become a prime target to hackers, with more than 50% of the reported data breaches being caused by either staff or students (Richardson et al., 2020). Schools have rigid school safety policies to ensure the school's physical security; however, cybercriminals do not target a facility or computer but people. These cybercriminals, or hackers, look for user errors, such as unacceptable information security behaviors, that create such breaches.

### **Role of the DPA Student**

As a high school and middle school teacher for 19 years and a Navy intelligence analyst for almost 5 years, I understand the importance of protecting your information from potential threats. I remember when students would only use a computer when a teacher was monitoring every step in a computer lab during school hours. Even before the COVID-19 pandemic, schools were beginning to implement 1-1 technology to students. This technology implementation was to enhance students' learning and allow students to further their learning with advanced concepts even after school hours. However, due to the COVID pandemic, the introduction of 1-1 technology was fast tracked, resulting in limited training for both students and teachers.

As a middle school teacher, I have seen students displaying inappropriate online behaviors varying from cyberbullying to unsafe practices, such as clicking on emails from unknown sources. As a parent of both a high school and middle school student, I am motivated to ensure that all students have the tools to be responsible digital citizens. Producing a pilot training course or module that allows school systems to train students in

best practices will reduce these problematic cyber practices. I developed this professional administrative study to address the public administrative issue related to the lack of cybersecurity training materials for middle school students. The purpose of this study was to develop a program or outline based on best practices for middle school students that will reduce the human factor causing these insecure online practices. There was a potential researcher bias concern related to the analysis of documents in this study because the documents used were not produced explicitly for research purposes; consequently, I made certain assumptions regarding middle school end-user behaviors.

### **Summary and Transition**

The concepts supporting this study included the attitude functional theory, which focuses on motivating factors to provide insights into behaviors. I used these insights when developing a pilot training course to target the attitudes of middle school students and reinforce positive, end-user behavior.

In the following section, I will discuss the sources used for this study and provide a rationale of the data collection process used as well as a justification of the validity, limitations, and challenges involved in the study. A review of published research and archival data related to the practice problem is also presented. Finally, I provide an outline of the analysis and synthesis of the procedures used to manage outliers and missing information.

### Section 3: Data Collection Process and Analysis

The purpose of this study was to develop a pilot training program to reduce problematic cyber practices among middle school students. The problem was that with the implementation of 1–1 technology and online classes due to the COVID-19 pandemic, middle school students at the study site were issued Chromebooks to complete work without any training on how to safely use the technology. In this section, I discuss the organizational problem and how this study addresses the research question. Additionally, I provide a short description of the rationale behind conducting a qualitative document analysis of sources that include published research and operational data.

#### **Practice-focused Questions**

I conducted this study to answer the following research question: What topics should be included in a pilot training program to reduce problematic cyber practices? A document analysis to compare the policies and programs from three school systems within Tennessee with similar demographics using data from public documents was used to determine possible procedures and guidelines to prevent and reduce cyber threats. Schwartz (2018) discussed how necessary training in best practices with students is essential in protecting their personal or school-issued computers and preparing them for threats they could also face in the workforce. Educational staff and students lack an understanding of cybersecurity issues that are typically the concern of school leaders and technology managers instead of teachers and students (Richardson et al., 2020). Therefore, there is a need to incorporate comprehensive and persuasive training that will

ensure behaviors to encourage accountability related to the roles and responsibilities of protecting school systems' cybersecurity.

### **Data Collection Process**

I conducted a qualitative document analysis to review and evaluate documents to determine policies as guidance for action. In carrying out this systematic analysis, I interpreted the meanings of data to advance and develop the knowledge required for this study (see Bowen, 2009). Educational leaders must be knowledgeable regarding policies; therefore, I conducted a document analysis to interpret policies to their simplest form to use them as guidelines by evaluating their histories and purposes (see Cardno, 2018). The types of documents used during this systematic process included, but were not limited to agendas, minutes of meetings, brochures, program proposals, maps, and charts (see Bowen, 2009).

### **Rationale**

Qualitative research requires robust data collection with advantages and limitations. Bowen (2009) discussed several advantages, including efficiency, availability, and lack of obtrusiveness and reactivity. During this study of cybersecurity within school systems, my use of this type of approach reduced the need for ethical approval to access underaged students' data (IRB number 05-24-21-0033944). The data selection of documentation was an effective method instead of data collection. The unobtrusive manner of document analysis reduced ethical concerns and protected the confidentiality of staff and students, allowing me to obtain the organization's permission without highlighting their struggles (specifically a school or school district). The

disadvantages of the qualitative method include insufficient detail, low retrievability, and biased selectivity (Bowen, 2009). Documents analyzed in the current study were not produced explicitly for research purposes; therefore, details may be insufficient and contain biases unknown to the researcher (see Cardno, 2018).

### **Published Outcomes and Research**

The public documents that were reviewed include those on state information security awareness, district online technology policies and security procedures, and Tennessee Department of Education security awareness. Additionally, national data, including a K–12 data breach report titled, “National School Board Association (NSBA) Data Security for Schools: A Legal and Policy Guide for School Boards” and the U.S. Department of Education’s report on “Protecting Student Privacy,” were used.

An analysis and comparison of policies and procedures within similar school systems and other K–12 school data highlighted gaps for which improvements could be recommended. This study consisted of a document analysis to understand cyber threats and compare best practices for addressing them. The document analysis was inquiry based to gather best practices and evaluate procedures that could be improved or implemented. The results of this analysis will provide educational policymakers with opportunities to design or implement programs that broaden the knowledge of their staff members and students.

In this qualitative document analysis, I explored and compared the strategies implemented by school systems to minimize information security threats. A literature review in the field of educational information systems security at national, state, and local



levels was used to identify themes and patterns with which to answer the research question. I review various documents and literature, including peer-reviewed journals and articles, websites, and reports. The databases and search engines used to locate relevant sources for this study included those accessible through the Walden University Library, such as ProQuest, SAGE Premier, and EBSCOhost. The key word search terms or combination of terms included *information security*, *education*, *cybersecurity*, and *data breach*. The goal was to have more than 80% of the outcomes, research, and literature reviewed to have been published within 5 years of my anticipated graduation date of 2021. Table 1 displays the distribution of references, showing in 87% of the sources published within the last 5 years.

**Table 1**

*Reference Tracker*

	Recent references between 2016-2021	Older references before 2016	Total	% of recent references
Peer-reviewed articles	7	2	9	78%
Web pages	7	1	8	89%
Periodicals	1	0	1	100%
Reports	3	0	3	100%
Other	4	2	6	67%

**Archival and Operational Data**

The analysis of operational data delivered by K–12 Cybersecurity Resource Center provided a quantitative empirical database of information that catalogs and analyzes data from publicly disclosed incidents regarding public, K–12 sources across the United States (EdTech Strategies, 2021). The statistics on cybersecurity incidents from

EdTech Strategies (2021) is a definitive source of vendor-neutral and reliably actionable data for stakeholders, such as U.S. policymakers, school leaders, IT managers, and advocates of civil liberties. The publicly disclosed sources included public schools and districts, charter schools, and other public education agencies or vendors. A limitation to many data breach incident sources was that incident reporting varies between states; therefore, the data set is incomplete and represents a small fraction of incidents. This database operates in a structured and repeatable manner with a common language called Vocabulary for Event Recording and Incident Sharing that consistently categorizes information (EdTech Strategies, 2021). This site offers maps, charts, and categories to personalize information between states and districts to analyze multiple years for comparison.

### **Analysis and Synthesis**

By exploring the cyber threats within a given specific state or school system, I designed a plan, including best practices, to reduce the number of possible threats to schools highlighting possible human factors. Self-reporting is often limited due to state-reporting regulations, resulting in school districts resisting reporting incidents, so it does not reflect poorly on the IT management practices within their system. Understanding the most common threats to schools allows educators the opportunity to create policies and procedures to confront these digital threats. In this study, I highlighted a few actionable steps to ensure cyber safety habits for not only faculty and staff but also students. The analysis and synthesis of this information provides clarity regarding possible threats,

increases the available information regarding the role of the human factor from literature reviews, and provides opportunities for implementations of training and curriculum.

### **Conclusion**

In conclusion, in this qualitative study I focused on the development of a pilot training module for middle school students to address the lack of cybersecurity training materials. The conceptual framework supporting this study, attitude functional theory, was focused on motivating factors that provided insights to influence change. A document analysis was an effective method of exploring and comparing different strategies implemented by school systems to minimize information security threats. I conducted a literature review in the field of educational information systems security at a variety of levels, such as national, state, and local, to identify themes and patterns to answer the research question. The findings and implications were used to report and analyze the data collected. In the following section, I will discuss the recommendations and findings, which will be provided to the study site client organization along with a pilot training module.

#### Section 4: Evaluation and Recommendations

In this qualitative study, I conducted a document analysis to explore the policies and guidance provided at the national, state, and local levels. In this, I discuss the data analyzed K-12 Cybersecurity Resource Center from EdTech Strategies to answer the study's research question: What topics should be included in a pilot training program to reduce problematic cyber practices? I used document analysis to compare the policies and programs from three school systems in Tennessee and develop a recommendation of an implementation framework for a pilot training program.

#### **Findings and Implications**

The U.S. Department of Education (2020) has provided best practice guides, scenarios, and handouts related to various data security issues designed for educational stakeholders, including parents but not necessarily designed for students. The NSBA recommended six policies and procedures each district should have: a written information security program, a chief privacy officer, an incident response plan, an acceptable use policy, employee training, and cybersecurity insurance (Czuprynski & Smith, 2017). At the national level, employee training is recommended; however, they do not mention training students. According to EdTech Strategies (2021), data breaches involving the unauthorized disclosure of student data and compromising their PII are among the most common types of incidents. One implication is that students should take an active role in the prevention of protecting their PII.

On the state level, the Tennessee State Government (n.d.) gives security awareness tips to adults, educators, and kids to protect students and their identities online.

The State of Tennessee Treasury Department (2009) has created a risk management video focusing on adults in the workforce called *Justice Protect* concentrating on protecting PII and providing guidelines for shopping online, creating passwords, phishing scams, and accessing public wireless networks.

Another finding is that cyber security should not be a one-time lesson taught at the beginning of the school year and forgotten. Online safety should become a part of the school's culture and embedded into lessons when possible. With their *Digital Citizen Curriculum*, Common Sense (2021) has created a curriculum designed to assist students in taking an active role in their online footprints. According to the attitude functional theory, using influential messages to target middle schoolers will persuade the end user and advocate for a positive digital footprint.

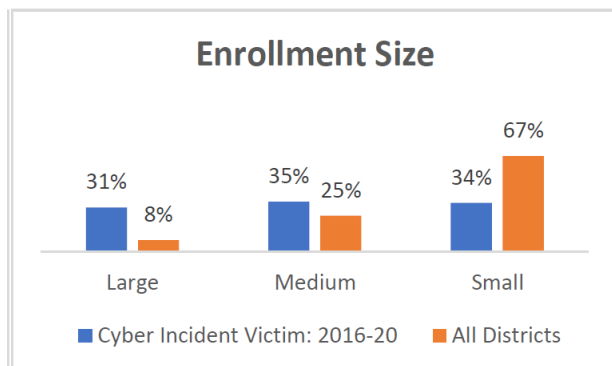
Not all cyber threats require hackers to be highly sophisticated. According to NSBA, phishing emails are a typical example of a simple way hackers can gain access to PII (Czuprynski & Smith, 2017). EdTech Strategies (2021) explained that incident types can co-occur, such as a phishing email could cause a data breach or delivery of malware onto a system. According to EdTech Strategies, phishing incidents have continued to decrease over the past 3 years (see Table 2). Email phishing is still a common occurrence; however, they are less likely to be reported because these incidents are commonly handled by IT staff at the district level.

**Table 2***K-12 Cyber Incidents*

	2018	2019	2020
Denial of service	9.84%	1.15%	5%
Phishing	15.57%	8.05%	2%
Ransomware	9.02%	17.82%	12%
Unauthorized disclosure/breach	46.72%	60.06%	36%
Other incidents	18.85%	12.93%	45%

*Note.* Adapted from “The K-12 Cybersecurity Self-Assessment,” by EdTech Strategies, 2021, The K-12 Cybersecurity Resource Center (<https://k12cybersecure.com>).

I selected three similar K–12 school districts in the state of Tennessee of medium size, consisting of between 50–95 schools within their districts to explore and compare their different strategies in preventing cyber incidents. For the purpose of this research, the three districts will be labeled as A, B, and C. Figure 1 displays the district enrollment size ranges for reported cyber incidents in 2016–2020, which fell between 30%–35% no matter the enrollment size. Therefore, the small number of large schools in districts causes them to have a higher chance of cyber incidents followed by medium-sized districts. Each district is similar in size, but not necessarily demographics.

**Figure 1***Enrollment Size*

*Note.* From “The K-12 Cybersecurity Self-Assessment,” by EdTech Strategies, 2021, The K-12 Cybersecurity Resource Center (<https://k12cybersecure.com>).

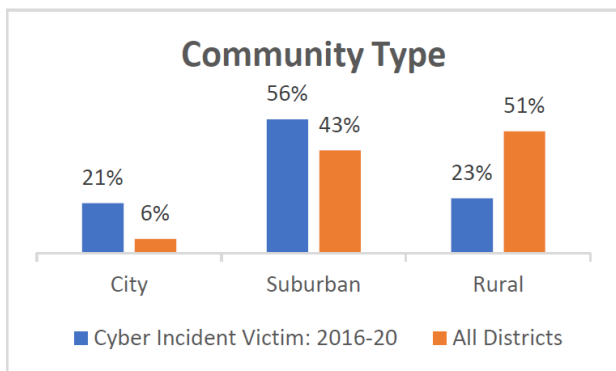
Each district offers websites to include professional development training opportunities for staff and acceptable use forms for parents and students. Table 3 shows which districts provides links to either videos or recommendations within their county homepages to improve online safety. Each district also provides a technology acceptable use policy as suggested by the NSBA on their corresponding websites, and all three districts are providing opportunities for training at various levels, from watching a video to avoid malware to providing links to curriculum lessons for digital citizenship. Districts A and C have links on their county website for optional tools for awareness information available by links or videos; however, District B is the only district that requires teacher lead instruction to be given to students regarding internet safety (see Table 3).

**Table 3***Student Internet Safety*

	District A	District B	District C
Do not share PII	X	X	
Protect Passwords	X	X	
Phishing, scams, malware	X	X	X
Student Resource links	X	X	
Cybersecurity Newsletters	X		

School sizes and community types within those districts will vary. Figure 2 indicates that city and suburban districts have recorded 76% of all reported cyber incidents between 2016–2020. Even though only 23% of rural communities have reported cyber incidents (EdTech Strategies, 2021), it does not mean a training program would not be beneficial in each community type. EdTech Strategies (2021) noted that small and rural areas correlate and may be limited in their ability to identify cyber incidents versus the larger school districts. Larger more urban districts have more students, resulting in a higher chance of being affected by the end-user actions in comparison to the smaller, more rural districts with fewer students, resulting in fewer chances of end-user actions. These results highlight why size and community type do play a role; however, they are not definitive indicators given that public disclosure is not mandatory for cyber incidents at schools.



**Figure 2***Community Type*

*Note.* From “The K-12 Cybersecurity Self-Assessment,” by EdTech Strategies, 2021, The K-12 Cybersecurity Resource Center (<https://k12cybersecure.com>).

Student training is not always required at the district level but is an option if the parent or guardian wants to follow the provided district links. This option leaves the students or parents responsible for trying to train themselves in cyber security. One recommendation at the district level is to make this training mandatory instead of optional. National, state, and local levels maintain that awareness is vital to ensuring online security for students. The overall implication combining these levels is that not only is awareness essential but also that required training to motivate and extend knowledge will influence behavioral changes.

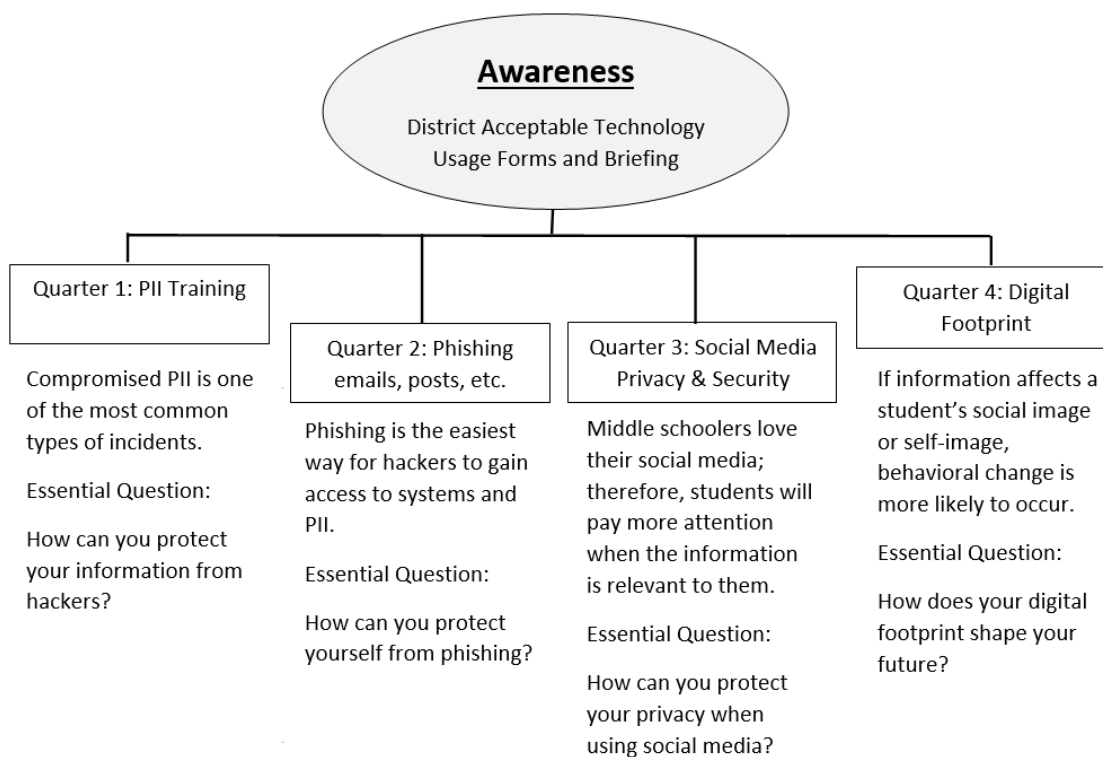
### **Recommendations**

The findings in this study highlight the need for more specified training beyond awareness. Awareness programs are designed to inform individuals instead of affecting behavioral change (Bada et al., 2019). Figure 3 provides a visual outline of the possible flow of quarterly training. The order of the training corresponds to the importance

according to the findings of this study. During training each quarter, teachers will need to address issues that middle school students face and target that specific age group. The challenge is that the curriculum for this age group is limited.

### Figure 3

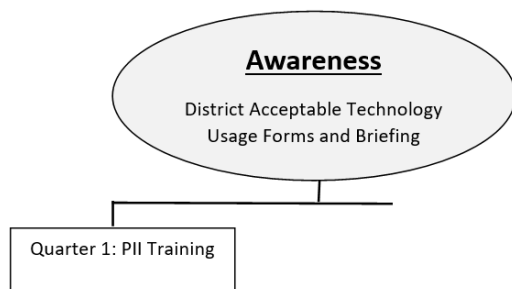
#### *Recommended Implementation Framework of Quarterly Lessons*



Most existing training programs focus on jobs or banking information that middle school students can not relate to. According to the attitude functional theory, motivating factors assist in influencing behavioral changes and intentions by targeting attitude in a compelling way (Carpenter, 2012). This study has resulted in three potential implications for positive social change: (a) students should take an active role in protecting their PII to reduce end-user vulnerabilities; (b) cyber security should not be a one-time lesson taught

at the beginning of the year and forgotten; and (c) awareness is beneficial, but training students to be digital citizens is essential to motivate and extend knowledge that will influence sustainable behavioral changes for the end user. Trim and Lee (2019) explained that behavioral changes are likely to occur when individuals understand how this new information could affect them positively or negatively.

The first potential implication is that students should take an active role in protecting their PII to reduce end-user vulnerabilities. My recommendations regarding this implication include taking the awareness briefing already established within many districts and revising them into actionable steps towards developing a pilot training program for middle students to create a cyber security culture. Figure 4 shows that Quarter 1 focuses on the first implication for positive social change by allowing students to take an active role in prevention. This lesson will highlight PII training, which, as previously stated, is the most common type of incident. Students will gain a basic understanding of what classifies as PII and how they can take steps to prevent this information from becoming compromised.

**Figure 4***Recommended Quarter 1 Implementation Framework*

Compromised PII is one of the most common types of incidents.

Essential Question:

How can you protect your information from hackers?

The module for Quarter 1 will consist of a discussion topic, two videos, and a quiz. The discussion topic asks: “Is there anything that you own that you think someone else might want to steal? Why would they steal it?” The instructor can list what some answers are and then have the students explain why they feel it would be stolen. Generally, the answers will be physical objects. The instructor can then ask, “Do you think only physical items are valuable to you?,” which is a good way to introduce PII. This question can be used to present the video, *Personal Identifiable Information (PII)*, that defines PII and gives examples for students that will be used to answer the following quiz questions titled, *Is your identity safe?* (see Figure 5). The final video of this module is titled, *Online Privacy for Kids – Internet Safety and Security for Kids* (Smile and Learn, 2020). This video addresses how kids use social media to communicate information to both friends and family and stresses the importance of being mindful of what is posted and shared online to ensure your PII is protected.

## Figure 5

### Quiz: Is Your Identity Safe?

**Question 1** 1 pts

Unique pieces of information that could be used to identify individuals is called private individual information.

True

False

---

**Question 2** 1 pts

Physical items are not the only valuable thing that can be stolen. Your identity could be valuable to thieves.

How could thieves use someone else's personal information?

Edit View Insert Format Tools Table

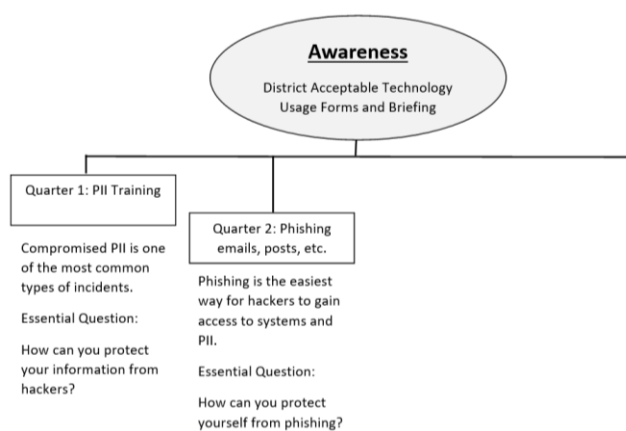
12pt Paragraph **B** *I* U T<sup>2</sup>

*Note.* From the Quarter 1 Module Quiz.

Training for students focuses on the second implication for positive social change by not just having a one-time lesson but multiple training sessions throughout the year (see Figure 6).

## Figure 6

### Quarter 2 Implementation Framework



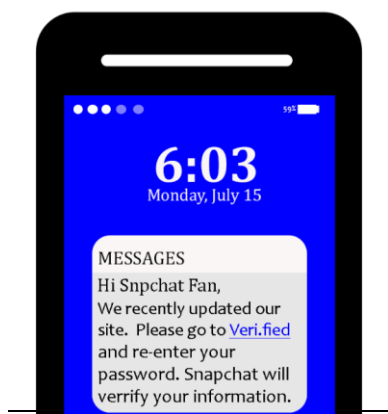
*Note.* This framework builds on the previous training from Quarter 1.

The second quarter leads to gaining an understanding of the definition of phishing and how students can identify and protect themselves from phishing attempts, not only

from emails, but also social media platforms. Middle school students can easily prevent phishing attempts by understanding how to identify these attacks. Phishing can be found on many platforms and emails as shown in Figure 7. These attacks can be identified by looking for items such as grammar mistakes, urgency or pressure to act now, and the possibility of losing access to something meaningful (Common Sense, 2021; Czuprynski & Smith, 2017).

### Figure 7

*Example of Phishing Message*



*Note.* Image of a possible phishing message from a student's smart phone.

The module for Quarter 2 will consist of a video, handout, and quiz. Google For Education (2017) video titled *Stay Safe from Phishing and Scams*. This video will be used as an introduction to how students can identify phishing emails and scams online. The handout titled *Beware of Phishing* uses screen shots from various online platforms to help identify what could be a phishing scam as shown in Figure 8. Students can discuss what phishing clues they notice in the images from the handout in Appendix A.

## Figure 8

### *Beware of Phishing Handout Example*

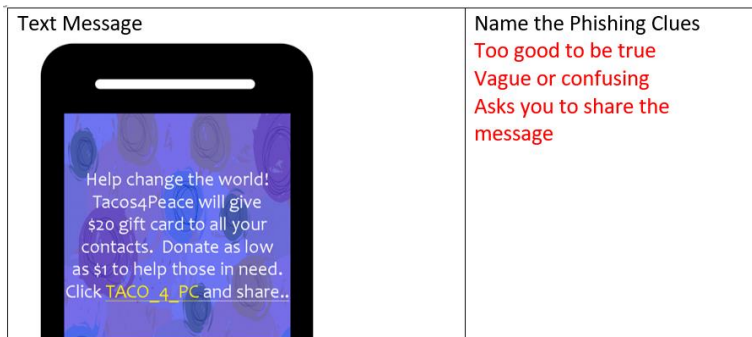
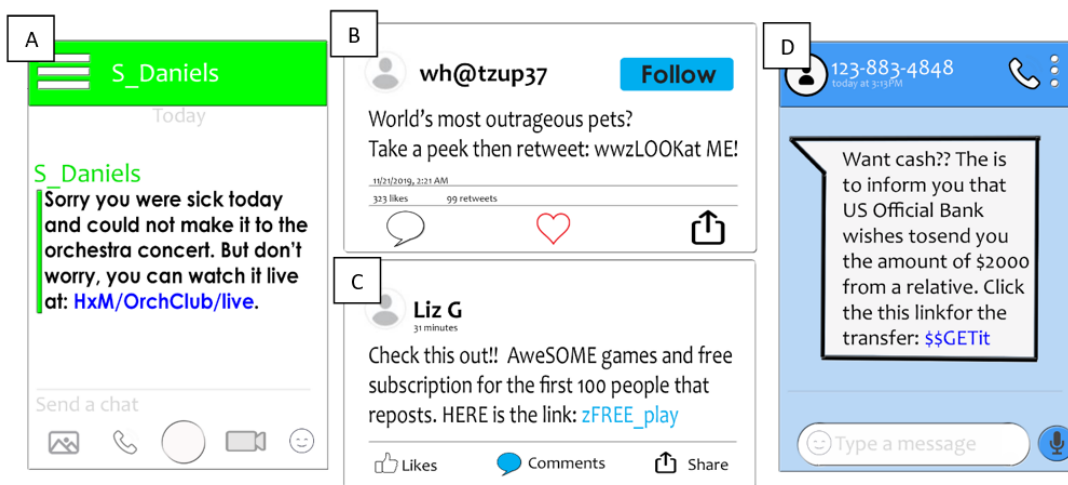


Figure 9 shows the images from the True/False Quiz regarding whether they should click on the message or skip it due to being a scam. The only safe message is image A from a teacher regarding an absence.

## Figure 9

### *Click or Skip?*



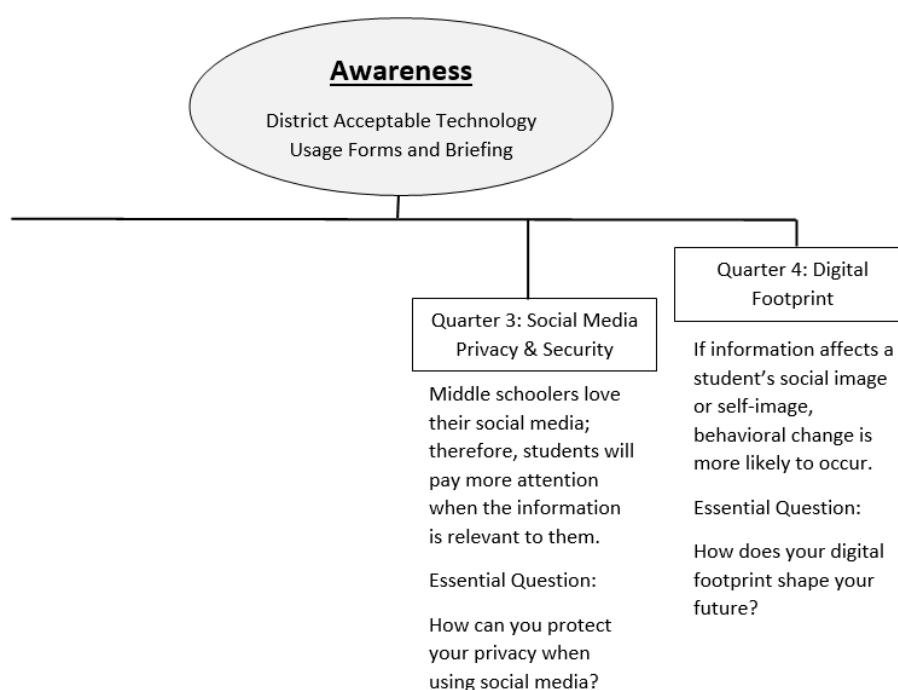
*Note.* These images can be used for discussions in pairs or as a group.

Figure 10 shows the final two quarters focus on the last implication for positive social change by implementing training that motivates and extend the student's

knowledge to influence sustainable behavioral change reducing end-user vulnerabilities. These lessons focus on the student privacy and digital footprint surrounding social media. This Implementation Framework moves beyond awareness to create specified training target middle school students and advocating future positive digital citizens.

### Figure 10

#### *Quarter 3 and 4 Implementation Framework*



*Note.* These final two quarters focus on behavioral changes towards becoming a digital citizen.

The module for quarter three consists of two discussions and a video. The first discussion is titled *Have you seen a screen like this before?* It uses a popular social media screen that many middle schoolers would be familiar with. The question is asked “When someone signs up for and uses Snapchat, what information do you think they are sharing? Who are they sharing it with?”. This question is posted as a discussion and



students will reply to the question posted. Within the Canvas module, the instructor can either allow students to respond to others or just have them look at the replies from other students. At this age, kids are registering for different platforms that require signups in which they are sharing a variety of information with other users. The video from Royal Bank of Canada Cyber Security (2017) titled *Keep it Private* discusses the importance of not sharing too much information online and how to keep your information confidential. This video leads into a discussion regarding privacy settings.

The final module used in quarter four training consist of a video and discussion. The video titled *Which Me 2021, Common Sense (2021)* used students from middle and high school discussing the pressure of presenting themselves online. This video leads to the discussion topic of *Who are you online?* The students are asked to list one benefit and one drawback of presenting yourself in different ways online. After the student posts their reply, they are asked to respond to one person adding to their comment. This discussion could be completed as a discussion in class or completely through the discussion post.

### **Strength and Limitations of the Project**

The development of a pilot training program for middle school students has both strengths and limitations. The main limitations focus on reporting of cyber incidents, limitations on middle school cyber security material, and literature. Since incidents do not need to be reported, reports such as phishing emails are often not reported if there is no monetary loss. The district generally handles these incidents with IT departments or students are overlooked due to not being reported. Next, a curriculum material designed

specifically for middle school students in cyber security is limited; therefore, would need to be designed before teaching the topics. Teachers presenting these lessons may not feel appropriately prepared to present and lead these discussions around cyber security unless detailed lessons and scripts are provided. Lastly, the literature surrounding cyber security training generally focuses on adults 18 years or older and not children younger than 18. These limitations on the project does not minimize the need for this type of project.

The development of this program lessens the cyber security risks to students. This program is designed to encourage feedback from not only teachers but students as well. The training should take between 10-30 minutes of instructional time each quarter. This time could be achieved during homeroom or enrichment time, minimizing the amount of academic time being used. In addition to students gaining insights from these trainings to reduce end-user behavior, teachers could also better understand cyber security, ultimately improving their chances of human error. The implementation framework for this pilot training program is just the beginning of creating social change. Future applications could be implementing these recommendations to determine if the individual districts can see a reduced number of cyber security incidents. Additionally, future applications could incorporate more training designed to happen more than quarterly, including possible concepts such as cyber bullying. These pieces of training and cyber security practices will be able to eventually expand to elementary grades ensuring a new atmosphere of digital citizenry.

## Section 5: Dissemination Plan

### **Dissemination Plan**

A briefing will be held with the local school district's security team and possibility the IT department to present the findings orally and begin a plan of action to communicate the case study's findings. I will provide a pamphlet (see Appendix A) with a quick explanation of the findings from the project to one Tennessee school district. Within this pamphlet, a description of the implementation framework will be outlined. The pilot training Canvas course outline will also be included as will additional links and digital lessons designed specifically for middle school students. Additionally, an outline (see Appendix B) of the implementation for the Canvas course explaining the instructional time, discussion questions, and videos will be included for dissemination to the district's school safety and IT directors.

This product was designed specifically for middle school student use with minimal work for the teachers when implementing this program. This program can be piloted at any middle school within the county and can be focused on a specific grade level or school. The effectiveness of the program and design could then be analyzed and adjusted for future dissemination to a broader audience within the district.

### **Summary**

In summary, the purpose of this qualitative study was to develop a pilot training module or course for middle school students using concepts from the attitude functional theory to motivate sustainable behavioral changes for the end user. The COVID-19 pandemic highlighted how ill prepared school systems were with the rapid changes

revolving around 1–1 technology in the classroom. School systems need to move away from awareness programs and incorporate more student training. The framework developed in the current study creates actionable steps that can be used to not only increase awareness, but also stimulate and broaden knowledge of cyber security topics to reduce end-user cyber vulnerabilities.

## References

- Ayres, S. (2020). *As classrooms go back online, will hackers find opportunities?* Spectrum News. <https://spectrumlocalnews.com/tx/san-antonio/news/2020/07/23/cybersecurity-schools-online-learning>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019, January 9). Cyber security awareness campaigns: Why do they fail to change behaviour? [https://arxiv.org/abs/1901.02672?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%253A%2Barxiv%252FQSXk%2B%2528ExcitingAds%2521%2Bcs%2Bupdates%2Bon%2BarXiv.org%2529](https://arxiv.org/abs/1901.02672?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A%2Barxiv%252FQSXk%2B%2528ExcitingAds%2521%2Bcs%2Bupdates%2Bon%2BarXiv.org%2529).
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Cardno, C. (2018). Policy document analysis: A practical educational leadership tool and a qualitative research method. *Educational Administration: Theory & Practice*, 24(4), 623–640.
- Carpenter, C. (2012). Functional attitude theory. In J. P. Dillard, & L. Shen (Eds.), *The SAGE handbook of persuasion: Developments in theory and practice* (pp. 104–119). SAGE Publications, Inc. <https://doi.org/10.4135/9781452218410.n7>
- Castro, D. (2020). School's in session: States need to invest in cybersecurity to help students safely shift to online learning. *Government Technology*, 33(6), 7.
- Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, 334. <https://doi.org/10.1016/j.chb.2016.08.034>

- Czuprynski, C. N., & Smith, R. (2017). *Data security for schools: A legal and policy guide for school boards*. National School Boards Association. [https://cdn-files.nsba.org/s3fspublic/reports/Data\\_Security\\_Guide\\_5\\_Jan2017.pdf](https://cdn-files.nsba.org/s3fspublic/reports/Data_Security_Guide_5_Jan2017.pdf)
- Common Sense. (2021, February 23). *Digital citizenship curriculum*. <https://www.common sense.org/education/digital-citizenship/curriculum?topic=privacy--security&grades=6%2C7%2C8>
- EdTech Strategies. (2021) *The K-12 Cybersecurity Self-Assessment*. The K-12 cybersecurity resource center. <https://k12cybersecure.com>.
- Elgan, M. (2019, October 2). *Why humans are a growing target for cyberattacks - and what to do about it*. <https://securityintelligence.com/articles/why-humans-are-a-growing-target-for-cyberattacks-and-what-to-do-about-it/>
- Google For Education. (2017). *Stay safe from phishing and scams*. YouTube. [https://www.youtube.com/watch?v=R12\\_y2BhKbE](https://www.youtube.com/watch?v=R12_y2BhKbE)
- Herold, B. (2017). Schools struggle with hacking, other cyber threats: New survey data show IT leaders underestimate cybersecurity challenges. *Education Week*, 37(14), 1.
- International Association of Chiefs of Police. (2015, October 26). *IACP glossary*. <https://www.iacpsybercenter.org/resources-2/glossary/>
- Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework: Smart companies match their approach to the nature of the threats they face. *Harvard Business Review*, 6, 48.
- Keller, N. (2020). *Uses and benefits of the framework*.

<https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework>

Klein, A. (2020, March 23). *Cyberattacks force schools to bolster online security.*

EducationWeek. <https://www.edweek.org/ew/articles/2020/03/18/cyberattacks-force-schools-to-bolster-online-security.html>

Lieberman, M. (2020, March 23). *4 big cybersecurity priorities for schools: Training, purchasing, monitoring, and budgeting.* Education Week.

<https://www.edweek.org/ew/articles/2020/03/18/4-big-cybersecurity-priorities-for-schools-training.html?print=1>

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, 9(3), 71-88.

<https://doi.org/10.2478/hjbpa-2018-0024>

Readiness and Emergency Management for Schools Technical Assistance Center. (2017).

Cybersecurity considerations for K-12 schools and school districts. Cybersecurity for schools fact sheet.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, 27(2), 23–39.

Royal Bank of Canada Cyber Security. (2017). *Keep it Private.* YouTube.

<https://www.youtube.com/watch?v=EuPmIEH8zLg>.

Schwartz, S. (2018). Schools teach “cyber hygiene” to combat phishing, identity theft. *Education Digest*, 1, 4.

Smile and Learn. (2020). *Online privacy for kids - Internet safety and security for kids*.

YouTube. <https://www.youtube.com/watch?v=yiKeLOKc1tw>

State of Tennessee Treasury Department. (2009). *Just Protect*.

<https://nowuseit.state.tn.us/Mediasite/Play/51d03a5b541647eca9149fea4c12053>

9.

Tennessee State Government. (n.d.). *Data downloads & requests*.

<https://www.tn.gov/education/data/data-downloads.html>.

Tennessee State Government. (n.d.). *Security awareness*.

<https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies/security-awareness.html>

Trim, P. R. J., & Lee, Y.I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing*

*Management*, 83, 224–238. <https://doi.org/10.1016/j.indmarman.2019.04.003>

Twigg, J. (2007). “*Staying safe*”: *A conceptual framework for school safety*.

[https://www.preventionweb.net/files/3925\\_Stayingsafe.pdf](https://www.preventionweb.net/files/3925_Stayingsafe.pdf)

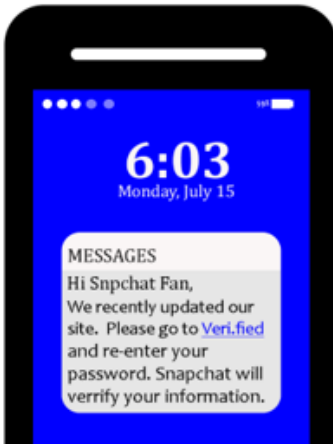

U.S. Department of Education. (2020, February 1). *Security best practices | Protecting student privacy*. <https://studentprivacy.ed.gov/topic/security-best-practices>



Appendix A: Beware of Phishing Handout

BEWARE OF PHISHING

NAME \_\_\_\_\_

<p>Text Message</p>  <p>Help change the world! Tacos4Peace will give \$20 gift card to all your contacts. Donate as low as \$1 to help those in need. Click <a href="#">TACO_4_PC</a> and share..</p>	<p>Name the Phishing Clues</p> <ul style="list-style-type: none"> <li>Too good to be true</li> <li>Vague or confusing</li> <li>Asks you to share the message</li> </ul>
<p>Log-in Screen</p>  <p>6:03 Monday, July 15</p> <p>MESSAGES Hi Snpchat Fan, We recently updated our site. Please go to <a href="#">Veri.fied</a> and re-enter your password. Snapchat will verify your information.</p>	<p>Name the Phishing Clues</p> <ul style="list-style-type: none"> <li>Spelling errors</li> <li>Generic greetings</li> <li>Shortened URL</li> <li>Claims to be from a legitimate company</li> </ul>
<p>Website Pop-up</p>  <p><b>CONGRATLATIONS!</b></p> <p><b>You maybe a winner!</b></p> <p><b>Win up to \$500,000,000 U.S. Cash!</b></p> <p>See if you arre an instnt winner by clicking <a href="#">Is.BM,e</a> now!</p>	<p>Name the Phishing Clues</p> <ul style="list-style-type: none"> <li>Too good to be true</li> <li>Spelling errors</li> <li>Shortened URL</li> </ul>

## Appendix B: Dissemination Pamphlet

### What topics should be included in a Pilot training program to reduce problematic cyber practices?

**LITERATURE REVIEW**  
Research indicates over 95% of cyber-attacks and breaches result from human error, such as clicking on a link or opening a file (Richardson, Lemoine, Stephens, & Waller, 2020; Elgan, 2019). Attackers can target humans easier and faster than attempting to target a system (Elgan, 2019). Education is a prime target because schools have a vast amount of information on both students, parents, teachers, and staff, such as social security numbers, financial data, and other forms of PII (Richardson et al., 2020).

**STATISTICS**  
In 2020, schools faced a new challenge with an increase in online crimes by 60% in the education sector, according to Microsoft Security Intelligence (Castro, 2020). Education Week reported surveying over 500 K-12 technology leaders worldwide to understand their approaches regarding cybersecurity threats (Lieberman, 2020).

### REFERENCES

EdTech Strategies. (n.d.) The K-12 Cybersecurity Self-Assessment. The K-12 Cybersecurity Resource Center - <https://k12cybersecure.com>.

Elgan, M. (2019, October 2). *Why Humans Are a Growing Target for Cyberattacks - And What to Do About It*. <https://securityintelligence.com/articles/why-humans-are-a-growing-target-for-cyberattacks-and-what-to-do-about-it/>

Castro, D. (2020). Schools in Session: States need to invest in cybersecurity to help students safely shift to online learning. *Government Technology*, 33(6), 7.

Lieberman, M. (2020, March 23). 4 Big Cybersecurity Priorities for Schools: Training, Purchasing, Monitoring, and Budgeting. *Education Week*. <https://www.edweek.org/ew/articles/2020/03/18/4-big-cybersecurity-priorities-for-schools-training.html?print=1>.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, 27(2), 23-39.

WALDEN UNIVERSITY

# PILOT MIDDLE SCHOOL CYBER SECURITY TRAINING

*Schools are in a unique position to implement strategies that are essential in preventing cyber incidents. These components will build a strong foundation that could affect the entire community by teaching digital citizenship.*

**EDTECH STRATEGIES DATA**

	2018	2019	2020
Denial of Service	9.84%	1.15%	5%
Phishing	15.57%	8.05%	2%
Ransomware	9.03%	17.82%	13%
Unauthorized Disclosure/Breach	46.72%	66.06%	36%
Other incidents	18.85%	12.93%	45%

Note: Adapted from "The K-12 Cybersecurity Self-Assessment," by EdTech Strategies, n.d., The K-12 Cybersecurity Resource Center (<https://k12cybersecure.com>).

**IMPLICATIONS**  
EdTech Strategies (n.d.) explain that incident types can co-occur such as a phishing email could cause a data breach or delivery of malware onto a system. Phishing incidents have continued to decrease over the past three years (EdTech Strategies, n.d.). Email phishing is still a common occurrence; however, they are less likely to be reported because these incidents are commonly handled by IT staff at the district level.

**IMPLICATIONS FOR POSITIVE SOCIAL CHANGE**

- 1) Students should take an active role in the prevention of protecting their PII to reduce end-user vulnerabilities.
- 2) Cyber security should not be a one-time lesson that is taught at the beginning of the year and forgotten.
- 3) Awareness is beneficial, but training students to be digital citizens is essential to motivate and extend knowledge that will influence sustainable behavioral changes for the end-user.

**IMPLEMENTATION FRAMEWORK**

**Awareness**  
Digital Acceptable Technology Usage Forms and Briefing

**Quarter 1 - Phishing**

Compromised PII is one of the most common types of incidents. Phishing is the easiest way for hackers to gain access to systems and PII.

Essential Questions:  
How can you protect your information from hackers?  
How can you protect yourself from phishing?

**Quarter 2 - Phishing, emails, posts, etc.**

Making it the easiest way for hackers to gain access to systems and PII.

Essential Questions:  
How can you protect your information from hackers?  
How can you protect yourself from phishing?

**Quarter 3 - Social Media Privacy & Security**

Making it the easiest way for hackers to gain access to systems and PII.

Essential Questions:  
How can you protect your information from hackers?  
How can you protect yourself from phishing?

**Quarter 4 - Digital Footprint**

Making it the easiest way for hackers to gain access to systems and PII.

Essential Questions:  
How can you protect your information from hackers?  
How can you protect yourself from phishing?

**CANVAS COURSE OUTLINE**

**Quarter 1 - Personal Identifiable Information (PII)**  
Safe or Unsafe? *Discussion Topic*  
Personal Identifiable Information (PII) *Video*  
Is your identity safe? *Quiz*  
Online Privacy for Kids - Internet Safety and Security for Kids *Video*

**Quarter 2 - Phishing**  
Stay Safe from Phishing and Scams *Video*  
Beware of Phishing discussion *Document*  
Click or Skip? *Quiz*

**Quarter 3 - Social Media: Privacy & Security**  
Have you seen a screen like this before? *Discussion Topic*  
RBC Cyber Security - Keep it Private *Video*  
Privacy Settings *Discussion Topic*

**Quarter 4 - Digital Footprint**  
Which Me\_2021\_UPDATE\_SITE *Video*  
Who are you online? *Discussion Topic*

## Appendix C: MS Pilot Cyber Security Quarterly Training Outline

### Quarter 1 - Personal Identifiable Information (PII)

- [Safe or Unsafe?](#) Discussion Topic (5-10 minutes depending on discussion)
- [Personal Identifiable Information \(PII\).mp4](#) Video (1:18) – possible discussions of video content
- [Is your identity safe?](#) Quiz (5-10 minutes)
- [Online Privacy for Kids - Internet Safety and Security for Kids.mp4](#) Video (2:56) – possible discussions of video content

### Quarter 2 - Phishing

- [Stay Safe from Phishing and Scams.mp4](#) Video (3:13) - possible discussions of video content
- [Beware of Phishing discussion PDF.docx](#) – Can be completed individually or in groups. Students can chart results NOTE: Key found under files on Canvas Module. (10-15 minutes if you want groups to share out their findings)
- [Click or Skip?](#) Quiz (5-10 minutes)

### Quarter 3 - Social Media: Privacy & Security

- [Have you seen a screen like this before?](#) Discussion Topic: Sample student responses: information required during sign-up (*name, phone number, and birthday*), "snaps" or content that the user creates, which might be shared with Snapchat or with friends of the user, things you browse when you're using the app, your location (5-10 minutes depending on discussion)
- [RBC Cyber Security - Keep it Private.mp4](#) Video (2:19) - possible discussions of video content
- [Privacy Settings](#) -Discussion Topic: Sample student response: Turn off cookies in your browser settings, review app's privacy settings and opt out of any sharing. (5-10 minutes depending on discussion)

### Quarter 4 - Digital Footprint

- [Which Me 2021 UPDATE SITE.mp4](#) Video (1:55)- possible discussions of video content
- [Who are you online?](#) Discussion Topic: Sample student responses: Benefit-having fun posting and sharing messages, drawback- post or comment on things that should not be associated with your actual life. (5-10 minutes depending on discussion)