Cybersecurity for Middle School Teachers

Cleve Hamasaki
Learning Design and Technology
University of Hawai‘i at Mānoa
cleve808@hawaii.edu

Abstract

The COVID-19 pandemic changed the landscape of middle school education. It influenced how educators teach in the classroom and increased the number of online tools and resources available for them to use. The educational technology (edtech) sector boomed with different applications designed to help educators instruct and assess their students in virtual learning environments. Though many edtech companies developed applications that were instrumental in helping students and teachers, some of these applications were designed to collect sensitive information (e.g., data habits, keystrokes, and contact lists). In addition, many edtech companies distributed or sold this sensitive information to third-party companies whose purpose may or may not have been for education. To address this complex issue, the author developed an instructional module designed to train middle school teachers about cybersecurity issues. The goal of the instruction was to help these educators protect themselves and their students from cyber threats. The instruction itself used a variety of instructional design principles, as well as digital safety models and teaching and learning strategies. Both a usability test and a learning assessment were conducted to show how effective the design of the instructional tool was for teaching cybersecurity. The results of the evaluation revealed that the instructional module was informative, engaging, and relevant, suggesting that the future development of this module could be used to train all educators in practicing safe cybersecurity habits.

Introduction

In the last five years, public middle and intermediate school teachers in the Hawai‘i Department of Education (HIDOE) have seen significant growth in the emergence of digital tools and services to enhance teaching and learning. These emerging technologies grew considerably during the COVID-19 pandemic as teachers rapidly transitioned from face-to-face instruction to distance learning (Singer, 2021). This transition forced many teachers to take it upon themselves to find applications to transfer paper assignments to digital ones quickly. In addition, teachers also found many educational technology (edtech) companies offering services to make it easier for them to instruct, assess, and motivate their students online (Veugen et al., 2022). Teachers knowingly (or unknowingly) allowed these applications and outside services to collect and track students through online assessment and monitoring tools that helped guide instruction and provide student feedback (Veugen et al., 2022). Using outside resources seemed like a good idea, especially when educators were forced to teach remotely with little prior training (Eadens et al.,

2022). Unfortunately, many educators did not know the consequences of using these digital tools and how their use could put their online data at risk.

Many educational technology companies (e.g., Schoology, ClassDojo, Remind, Padlet, Udacity, and others) provided useful tools and services for teachers designed to make learning fun and engaging. Unfortunately, these companies often collect large amounts of personal data and store them on their servers. Some of this data is stored temporarily and quickly deleted after a session. Other times, however, that data stays on companies' servers for longer periods of time. This reality begged the question: What happens to this data? And what do these companies do with the data?

These were important questions for teachers and parents to understand. According to Human Rights Watch (2022), some edtech companies tracked personal data for advertising by recording online browsing activity, creating targeted ads for users, and tracking IP addresses to identify a user's location. Teachers who used these edtech applications were also more prone to spam or junk email since their information was shared with other third-party vendors. In the worst cases, these emails included malicious software called "malware" that could potentially harm devices and compromise personal data, putting teachers and their schools at risk of potential data breaches.

The HIDOE has a list of approved edtech companies to ensure school data is protected. These companies have data sharing agreements (DSA) with the HIDOE to collect and compile student data. The DSA informs the HIDOE on how the data is used, stored, and shared. The DSA also provides details on the terms of the contract including how long the data is stored and what happens to the data once the contract expires. Allowing edtech companies to provide services to collect and aggregate data helps schools provide information that would guide learning objectives and support students. The data provides a wealth of information about their students (e.g., academic ability, intellectual disability, emotional disturbance, absenteeism, socio-economic status, and other personal student information). This information allows teachers to enhance their instructional practices by differentiating instruction for individual students, prescribing interventions for low-achieving students, providing social and emotional support, and developing short and long-term goals for all students. In addition, a school's aggregate student data and its comparison with other schools in the state are collected and reported using state assessments (e.g., the Smarter Balanced Assessment, Hawai‘i State Assessment in Science, Panorama Student Survey, Individual Achievement Test, Federal Impact Aid Survey) throughout the school year.

Even with DSAs in place, a 2019 report from the Network for Public Education and the Parent Coalition for Student Privacy gave HIDOE a grade of 'D+' in protecting student data. This grade was based on seven categories: parties covered and regulated, transparency, parental and student rights, limitations on commercial use of data, data security requirements, oversight and enforcement, penalties for violations, and other provisions (Strickland, 2019). Hawai‘i scored an 'F' in transparency, oversight and enforcement, and other provisions. Hawai‘i also scored low in data security requirements. These low grades were no surprise, as Edscoop (2019) reported that the personal information of about 70,000 Hawai‘i public school students might have been compromised because of unauthorized access to Graduation Alliance's database. Graduation

Alliance is a data and web hosting company contracted by HIDOE to create a website called "My Future Hawai'i." The company services Hawai'i schools by providing college and career planning resources for students (Johnston, 2019). Keeping online data safe was not just the state's responsibility but the responsibility of administrators, teachers, school staff, parents, students, edtech companies, and everyone who dealt with online data.

Problem Statement

One of the primary responsibilities of middle school teachers is to promote student learning and increase student achievement. In doing so, middle school teachers need to apply new and innovative ways of enhancing student engagement while creating a safe environment for their students (The Center for Comprehensive School Reform and Improvement, 2007). This was evident during the COVID-19 pandemic as teachers were immediately thrown into virtual teaching while trying to find digital tools and services to help them with online instructional delivery and assessments. Unfortunately, the pandemic caused many teachers to use tools and services that were not HIDOE approved. This left many teachers with a false sense of security that all educational digital tools and services could be integrated into their instruction even as they returned to their classrooms after the pandemic.

The problem is that many public middle school teachers do not know how to protect their devices and secure online data. This issue gets compounded when teachers share ideas about integrating emerging technologies that work well within their classrooms. Many teachers were excited to use new online tools to enhance teaching and learning, not knowing the consequences of signing up for tools or services that were not HIDOE compliant. Some of these consequences included being more susceptible to junk email and malware, and having their online data collected and shared. In short, teachers needed training in ways to protect online data, such as avoiding phishing emails, creating strong passwords, installing anti-virus software, regularly checking and updating hardware and software, and reading the privacy policy and terms of condition for any application (or extension) they install or use.

Audience Analysis

The target audience for this project was Hawai'i public middle school (sixth, seventh, and eighth grade) or intermediate school (seventh and eighth grade) teachers. These teachers are employed by the HIDOE and teach specialized areas (e.g., English, math, science, social studies, physical education, health, electives, and support services). Most teachers are between the ages of 23 to 70 years old with various years of experience. In general, these teachers understand the importance of professional development training by continuously looking for ways to make learning fun, engaging, and safe for students. However, in order for professional development to be successful and valuable for teachers, it has to directly connect to all content areas. In addition, professional development needs to be easy to understand in order for teachers to implement learned strategies into their lessons as quickly and effectively as possible.

In general, teachers have a basic understanding of pedagogical strategies in their content area. For example, they might utilize strategies to help plan lessons, manage classroom behavior, and allocate resources (e.g., time, money, and materials) to best support their students. Regarding their affective characteristics, teachers tend to be motivated to help improve their teaching practices to support student achievement. Teachers are motivated to support students

academically, emotionally, and socially. Occasionally, teachers are not motivated to learn if the training quality is poor, too time-consuming, too technical or confusing, not relatable to their teaching, or any combination of these reasons. Most teachers communicate with each other and share best practices. These best practices include strategies they learn from workshops, colleagues, or their own research. Best practices also included educational applications and tools to help with instruction, content material, and assessment. See Appendix A for a detailed description of the characteristics of middle school teachers.

Since cybersecurity issues increased over the past five years, getting teachers trained to understand cyber attacks to protect themselves and their students was important.

Project Goal

This project aimed to design and evaluate instruction to help middle school teachers explain the importance of cybersecurity and apply these skills to protect themselves and their students from cyber threats. The project contained instructional modules to help middle school teachers increase awareness of cybersecurity issues and develop skills to increase their confidence in handling cyber threats.

Literature Review

Overview

A literature review was conducted to learn about cybersecurity in public schools, professional development for middle school teachers, digital literacy professional development, and integrating a digital competence framework into cybersecurity training.

Cybersecurity in Public Schools

There was an increasing trend of cybersecurity incidents targeting public schools and school districts; therefore, training teachers on protecting online data was essential. A cybersecurity incident is "an event that actually or potentially jeopardizes a system or the information it holds." (U.S. Government Accountability Office, 2020, "What GAO Found" section). These incidents included, but were not limited to, data breaches, ransomware attacks, compromised emails, distributed denial of service attacks, and hacking. In 2021, 166 incidents were reported across 38 states though that number is most likely underrepresented (Levin, 2022). Although data risk management and security are at the forefront of many school districts, the lack of resources and unclear guidelines at the state and federal levels continue to pose risks for students, teachers, and school staff (Levin, 2022).

On March 25, 2022, the New York City Public Schools, the largest school district in the United States, reported a cyberattack exposing the personal records of 3 million former and current students. The attack stemmed from using Illuminate Education products, a company known for its student tracking services (Singer, 2022). In May, the Los Angeles Unified School District, the second largest school district in the United States, reported that the Illuminate Education incident exposed over 600,000 records of their students and faculty members (Woolfolk, 2022). In a separate incident, the Chicago Public Schools, the third largest school district in the United States, exposed 560,000 records of former students and faculty members. In this case, the Chicago Public Schools blamed the breach on the company, Battelle for Kids, which did not

immediately report that a ransomware attack had also hit them in December 2021 (Merrod, 2022).

These breaches, which exposed millions of student and faculty records, should have been a wake-up call for teachers, schools, and districts (Singer, 2022). In 1998, the Federal government enacted The Child Online Policy Protection Act of 1988 (COPPA), giving parents primary control of their child's online private information (Federal Trade Commission, 2022). Websites and online services must also disclose that they knowingly collect and use personal data from children under 13. They must report if they disclose children's personal information to other third parties. When schools contract online servicing companies (e.g., student tracking, monitoring, direct instruction), the school becomes the intermediary between the servicing company and parents (iKeepSafe, 2022). However, when teachers use online services not contracted by the school or by the HIDOE, the teachers become the intermediary between the servicing company and parents. Therefore, the teacher is responsible for protecting their students' data.

Training Middle School Teachers in Protecting Online Data

According to a report from the Center for Democracy and Technology (CDT), many parents expressed concern that students and teachers did not receive enough substantive training on data privacy and monitoring practices (Laird et al., 2022). However, teachers were unmotivated to attend professional development training that was not relevant, meaningful, and achievable. Time was precious for teachers, and the time spent away from the classroom to attend professional development training was valuable time spent away from doing more meaningful work (e.g., grading papers, creating lesson plans, assessing data) (Farrah, 2021). Professional development should recognize that teachers are of different ages and come from diverse backgrounds with different skill sets, interests, challenges, strengths, cognitive abilities, and social and emotional needs. Therefore, it was crucial to consider learners' variability in professional development training for middle school teachers (Barbara Bush Foundation for Family Literacy, 2022). Making professional development engaging for middle school teachers should be a social experience, not just a formal one (Matherson & Windle, 2017). Middle school teachers enjoyed bouncing ideas off of one another and sharing their own experiences of what works and what does not work within their classrooms. This communication between teachers built learning capacity, fostered teacher development, and created a learning community. Another critical aspect of building engaging professional development was providing opportunities for active participation and hands-on practice of learned skills (Matherson & Windle, 2017). Teachers were motivated to learn when they saw the relevance of the topic and its potential to improve student learning. Building off of this information, it was clear that this project's instructional delivery needed to be designed with real-world scenarios, allowing teachers to think critically about the content. The project design also included lessons that allowed teachers to participate in discussions, self-reflection, and hands-on activities to make the professional development sessions more meaningful.

School safety had always been a concern for school administrators. Principals and school leaders constantly revisited safety protocols and procedures to deal with emergencies such as fires, evacuations, school shootings, bomb threats, and pandemic outbreaks (Chung, 2021). However, schools rarely teach digital safety. Even when schools dedicated computer courses to teaching

cyber safety, it had little impact on students' online behaviors. The International Society for Technology Education (ISTE) standards provided a blueprint to help in the development of integrating technology into curriculum and instruction. Unfortunately, there was a lack of resources and instructional strategies focusing on the professional development of data protection for middle school teachers (Vejmelka et al., 2020).

Digital Competency vs. Digital Literacy

In his book, Gilster (1998) described the term *digital literacy* as "the ability to use and evaluate digital resources, tools and services properly, and apply it to lifelong learning processes" (p. 220) . This mainly means building one's technical skills to apply them to a given task. This definition can also be applied to similar terms (e.g., information, computer, media, and multi-modal literacy) (Falloon, 2020). With the emergence of cloud computing, video conferencing, smart devices, artificial intelligence, blockchain, and other digital trends, the term digital literacy, according to Gilster, should be reconsidered. In addition to evaluating and applying digital resources, teachers should understand the safety and security of using emerging technologies and analyze how these resources impact cultures, individuals, and society. The Digital Competency Framework for Citizens (Vuorikari, 2022) did this by introducing learners to digital skills and knowledge needed to be digitally competent.

The European Commission's Digital Competency Framework for Citizens (Vuorikari, R., 2022), provided a common understanding of what digital skills and knowledge is needed to be digitally competent. These skills included information and digital literacy, communication and collaboration, digital content creation, safety, and problem solving. The focus of this project was on the safety component which addressed protecting devices and online data.

In the United States education system, most schools used the ISTE standards to help integrate technology into teaching and learning with the goal of inspiring learners and increasing student achievement. (ISTE, 2022). The problem with the ISTE standards for educators was that while these standards are designed to help educators transform their students into becoming empowered learners of technology, it lacks substance in online safety. The ISTE standards group data security, digital literacy, media fluency, and other online social issues under the 'citizen' standards. While this may have been well-intentioned, the European Commission had a standalone safety standard under which data security practices and protecting devices fall under, thereby addressing the importance of these issues.

Summary

The readings provided insight into why middle school teachers need professional development training to protect devices and online data. Cybersecurity incidents were on the rise, with more cybercriminals attacking educational institutions, which is a cause of concern for school officials, especially teachers. Although data procedure practices are needed, planning for professional development training needs to be well-designed and meaningful for teachers. Given this information, this project's instruction encouraged middle school teachers to use safe digital practices by increasing their knowledge about digital safety terms (e.g., malware, social engineering, phishing, and other terms) and developing their skills on applying their knowledge to their professional practices. The content needed to be brief, the instructional delivery needed

to be engaging, and assessment activities needed to allow teachers to practice and apply what they learned with a chance to collaborate and communicate with their peers.

Instructional Analysis

Overview

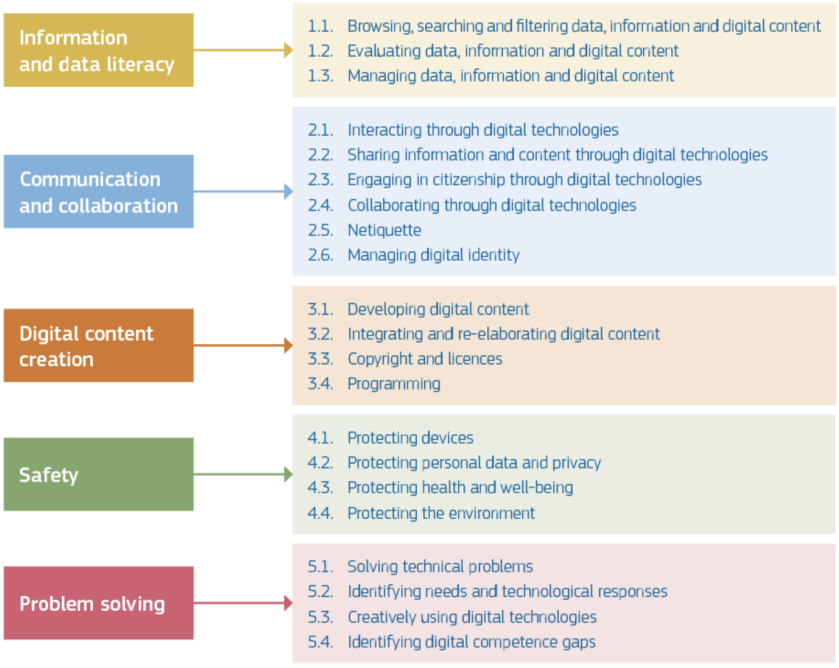
The project's instructional goal was to help middle school teachers evaluate and process cybersecurity information to perform skills that will protect them and their students from cyber threats. The instructional analysis included determining the instructional scope, instructional breakdown of the module (i.e., how the instruction of concepts and skills are chunked), instructional strategy or learning theories essential in creating the instructional content, and performance objectives for each learning activity. The details section of this document describes the technology used for the building design and instructions.

Instructional Scope

The scope of the instruction's content incorporated the European Commission's Digital Competence Framework for Citizens (Vuorikari. et al., 2022). This framework has five major components, but due to the time restrictions of designing this project, the instruction focused on the "safety" component. This framework component emphasized cybersecurity and how to protect devices and data from cyber threats. Figure 1 shows the European Commission's Digital Competence Framework for Citizens reference model (DigComp).

Figure 1

DigComp Reference Model.



Note. A snapshot of the Digital Competence Framework for Citizens used by the European Commission (Vuorikari et al., 2022).

The scope was small due to the lack of time and resources to create an instructional course incorporating other digital competencies (e.g., cyberbullying, netiquette, copyright and licensing, and other digital competency areas).

Once the scope was narrowed, it was critical to revisit the cognitive characteristics of middle school teachers before designing the instruction and breaking down and chunking the sequence of events. Appendix B shows the first draft of the instructional scope in planning and determining the teachers' prior knowledge and the concepts and skills they will learn through the instructional module.

Before building the behaviors for each concept and skill, several entry-level skills were identified for all middle school teachers. One entry-level skill was that teachers were assumed to be experts in the content area they taught. In other words, teachers could be trained in the subject matter and were considered experts in their field. A second identifiable entry-level skill was that teachers would have basic computer skills prior to the instruction. Finally, teachers had skills in managing behavior, delivering instruction, creating lesson plans, and other teaching responsibilities. Identifying these entry-level skills saved time and resources to focus on only cybersecurity.

Once the entry-level skills were identified, it was essential to review the affective characteristics of teachers that would need to be considered before determining the instructional scope. One factor was that most middle school teachers needed more knowledge of cybersecurity. They had heard the term used but needed to learn what it meant. Teachers with little knowledge about cybersecurity generally had two different trains of thought. One train of thought was that the school's technology personnel and the state's information technology (IT) department were responsible. The second train of thought was that it was important but not as crucial as other teacher responsibilities, such as grading assignments, attending parent-teacher conferences, differentiating instruction, and helping students to succeed. The scope of this project's instruction was planned with those thoughts in mind. After this module, teachers could recognize cybersecurity threats and build healthy habits to protect their devices and online data.

Instructional Breakdown & Sequence

The project's instruction was chunked based on the new instructional scope (see Appendix C), which combined device and data protection into one cohesive instructional unit rather than two separate units. The reason for the change was that participants needed to know about data and device protection first, before learning about cybersecurity threats. The instructional content and objectives were still chunked into concepts and skills; however, some of the concepts would be introduced *after* prior skills were learned.

Throughout this research project, cognitive and affective domains were taken into consideration. In order to facilitate the cognitive domain, the instructional delivery had been sequenced according to Bloom's taxonomy (Anderson et al., 2001). The middle school teachers were presented with basic concepts about cybersecurity and specific vocabulary terms (such as data, social engineering, malware, and phishing). Consequently, teachers could analyze and apply these concepts in their classrooms. By integrating solid foundational knowledge and challenging learning tasks, each learning activity would build upon the previous lesson, increasing the teachers' depth of knowledge in the subject area being taught.

For the affective domain, the instructional delivery integrated motivational strategies from Keller's (1983) ARCS model. These strategies ensured that the delivery of instruction was geared toward teachers and kept them motivated throughout the unit. Therefore, instructional delivery would capture the teachers' attention, make it relevant, build their confidence in applying new knowledge, and increase the satisfaction of learning about cybersecurity.

Instructional Strategy

The overall module combined direct and indirect instruction with engaging activities using the "watch it, do it" strategy. This strategy took concepts used by the Cognitive Apprenticeship model (Collins et al., 1988) to help others learn. These concepts included observation, imitation, modeling, and reflection to reinforce lesson concepts. Direct instruction would be delivered through multimedia presentations consisting of video, audio, images, text, and animation. Direct instruction combined the ARCS model (Keller, 1983) and the Cognitive Theory of Multimedia Learning (Mayer, 2005) to ensure that the multimedia content engaged the teachers. The words and visuals of the instruction needed to be purposeful, allowing teachers to process the information into working memory (Mayer, 2005). Slides and images accompanied video lectures to emphasize content and helped teachers comprehend the material.

While video lectures offered an example of direct instruction, learning activities provided the teachers with indirect instruction, encouraging them to learn by doing and thinking critically. These learning activities integrated one or more of the following: quizzes, surveys, reflections, and scenarios. These activities provided teachers with relevant tasks to develop their critical thinking skills regarding protecting devices and online data. The five principles of the Discovery Learning Model (Bruner, 1961) were used to design the teacher learning activities. These principles included problem solving, learner management, integrating and connecting, information analysis and interpretation, and failure and feedback. Learning activities needed attention-grabbing techniques such as interactives and visual aids to stimulate teacher interest and curiosity.

Performance Objectives

Performance objectives were separated into eight mini-lessons (see Appendix D). Lessons 1-4 focused on data, which included terms such as data sharing, personal identifiable information, privacy policies, and other data material. In these lessons, teachers saw how companies collect and use data to help and inadvertently harm their users. These lessons trained teachers on the dangers of using online applications and third-party plugins. Lessons 5-8 centered on cybersecurity threats. In these lessons, teachers went through lessons and activities regarding malware, social engineering, phishing, and ways to protect themselves from such threats.

Instructional Details

As mentioned earlier, this course consisted of one module with eight mini-lessons. A breakdown of the lesson and activities can be seen in Appendix E. The estimated time to complete the entire module was about an hour. The module interface was an online modified version of a "hyperdoc" created in Google Slides, allowing the teacher to go through each lesson and activity linearly. A hyperdoc is a digital document that houses different parts of a unit/lesson plan in one central location (Gonzalez, 2017).

There were several reasons for using a hyperdoc rather than other instructional solutions (e.g., websites, learning management systems, instructional applications, and other delivery tools). The first was its simplicity. Since a hyperdoc uses Google applications such as Google Docs, Sheets, Slides, Draw, and other applications, teachers would only need a little training in using these applications. The second reason was its flexibility in embedding different multimedia tools and technologies. According to Moreno's (2005) cognitive affective theory of learning from media, learners are more motivated to learn when the instruction aims to develop understanding using exciting visuals and problem-based scenarios. In addition, video instructions and assessment activities allowed teachers to engage with the content at their own pace. The third reason was its functional interface, making it easier to navigate without having other distractions that may cause the teacher to lose focus or disengage with the content.

Each lesson began with a video explaining a specific topic (e.g., personally identifiable information, privacy policy, phishing, and other topics) along with images, animation, audio and video clips to support the instruction. By delivering the instruction in this way, teachers would be motivated to see the topic's relevancy and be attentive to the instruction and activities that followed. The instructional videos were edited using Final Cut Pro and WeVideo. Aside from the instructional videos, learning activities throughout the module allowed teachers to demonstrate lesson objectives through multiple-choice questions, matching activities, or scenario-based problems. Many learning activities in the module were broad enough to reach all teachers despite their grade level or subject matter. Yet, these activities were valuable enough to continue practicing these concepts in their classrooms once they had completed the module.

Project Evaluation

Evaluation Goal

This project's evaluation aimed to check and validate the instructional unit's usability and learning effectiveness. The usability testing would check the design, navigation, and content components. The learning effectiveness validated participants' performance after going through the 'cybersecurity for middle school teachers' unit. In addition to evaluating learning effectiveness, participants completed a retrospective survey to measure how much they enjoyed (or didn't) the overall instructional module.

Participants

A recruitment letter was sent to various educators to participate in a usability testing and to evaluate the learning effectiveness of the *Cybersecurity for Middle School Teachers* module. This letter included information about the purpose of both the usability and learning effectiveness testing, including a consent form with information on how their data results would be used, shared, stored, and deleted. Once received, participants from both the usability testing and learning effectiveness evaluation were contacted separately with further instructions. Four participants (n=4) agreed to perform the usability test. The participants were: a seventh-grade English teacher, a student services coordinator (SSC), a seventh-grade math teacher, and a seventh-grade science teacher. The participants' data helped to improve the module before the learning effectiveness evaluation was conducted.

Once the improvements to the module were made, nineteen participants (n=19) were recruited to evaluate its learning effectiveness. Participants were sent a letter (see Appendix F) with the instructions on how to do the evaluation, along with a unique user code to conceal and protect their identities. The instructions included links to a demographic and pre-test survey form, the *Cybersecurity for Middle School Teachers* module, and the post-test and retrospective survey. The letter also reminded the participants how their data would be used, shared, stored, and deleted. These participants included general education and special education (SPED) teachers, counselors, and other support staff.

Evaluation Instruments

A Google Form pre-survey was used to gather demographic information from participants prior to evaluating the learning effectiveness of the module. Participants answered general questions including how long they had been teachers and what subject(s) they taught. See Appendix G for a detailed list of pre-survey questions. The decision to use Google Forms was an obvious choice since most public school teachers are familiar with Google applications and also for its simplicity in creating fillable forms. Google Forms also has the feature of exporting demographic data into various formats, which makes it manageable to organize the information.

The evaluation instruments used for the usability testing was done using Zoom and Google Sheets. Like Google Forms, most public school teachers were familiar with using different HIDOE applications such as Zoom and Google Sheets. Zoom provides the proctor of the usability test to go through the various tasks with their participants while observing and recording their experiences. An observation checklist created in Google Sheets allowed the proctor to document the participants' experiences with the hyperdoc.

Several instruments were used to evaluate the unit's learning effectiveness, such as Nearpod activities to assess the participants' knowledge after viewing an embedded lesson video and a pre and post-survey created in Google Forms. These were designed to demonstrate the participants' comprehension of the importance of protecting online data. The Nearpod assessments included multiple-choice questions, matching activities, reflections, and problem-based scenarios.

Implementation Procedure

Appendix H shows the procedure workflow in the order in which evaluations were conducted.

The initial step was to recruit participants for the usability testing through email. The email included an invitation letter explaining the purpose of the usability test and learning effectiveness evaluation. Also included with the invitation letter was a consent form asking for the participants' permission to use the information they provided during the usability test.

Three teachers participated in the usability test. They were each asked the same questions and performed the same tasks. The script for proctoring the usability test was influenced by Krug (2010). One of the usability tasks that the participants demonstrated was finding information on phishing emails. The participants had to describe the process of finding this information. The proctor would listen to the participants and document the information they shared while going through the task. For a complete description of the script used for the usability test, see Appendix I.

Nineteen teachers participated in the asynchronous learning effectiveness evaluation. Each teacher completed a Google Form pre-survey before going through the cybersecurity unit. At the end of the unit, the participants completed a post-survey. Aside from the demographic questions teachers filled out in the pre-survey, the assessment questions found in the pre and post-surveys were identical. These questions ranged from multiple-choice questions, matching questions, and problem-based scenarios. Table 1 shows an example of a multiple-choice question.

Table 1

Example of a Multiple-Choice Question on the Pre- and Post-Surveys

"Which of the following definitions best describes 'terms and conditions?'

A. An agreement that sets the rules and guidelines that users must agree to and follow to use and access another party's website or mobile app.
B. An agreement that businesses use to protect themselves from lawsuits
C. A handshake agreement
D. An agreement between the user and other users.

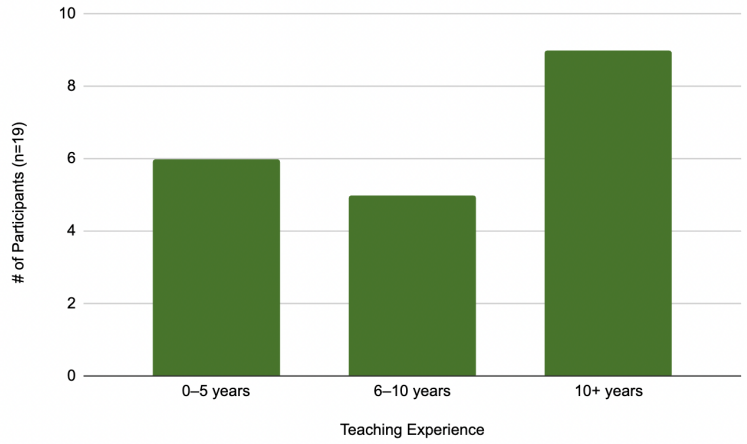
See Appendix J for a list of learning objectives and instructional assessments for pre and post-test questions.
.

Data Analysis Plan

Once the participants' demographic information was collected through Google Forms it was automatically organized in Google Sheets for viewing. Bar graphs conveyed aggregate data about the participants. Figure 5 shows an example of participants' years of teaching experience..

Figure 5

Participants' Years of Teaching Experience

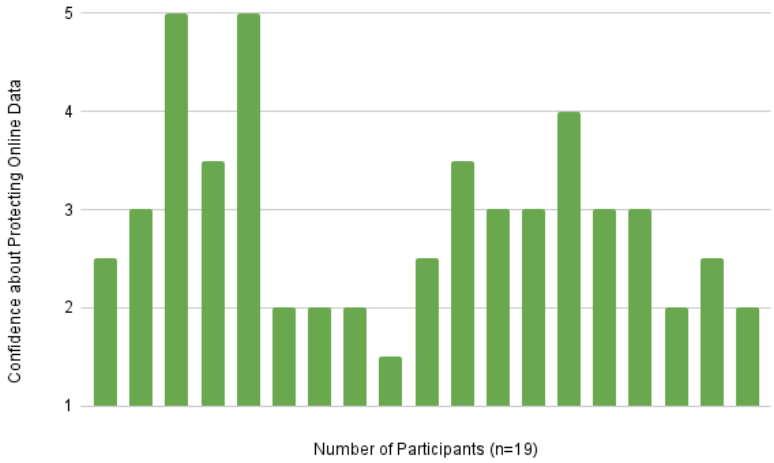


Results from the usability test were presented using several charts and illustrations. A Likert-scale allowed the participants to reflect on their own beliefs about online data and student safety. An example of a Likert-type scale question was "On a scale of one to five (where one means strongly disagree and five means strongly agree), I am confident about protecting online data." See Appendix K for an extensive list of Likert-scale questions completed by participants.

Figure 6 shows a bar graph presenting the Likert-scale results about how confident participants felt about protecting their online data. The data ranged from five (very confident in protecting their online data) to one (not very confident).

Figure 6

Likert-Scale Result of Participants' Confidence Level in Protecting Online Data



A word cloud like the one shown in Figure 7 provided another way to present the usability data, such as positive and negative comments about the delivery tool.

Figure 7

Word Cloud Positive and Negative Comment Comparisons from Usability Test

A post-survey was taken at the end of the module to measure how well the teachers liked (or disliked) the training, their confidence level about protecting online data and devices, and whether they would recommend this training to others. Also, participants were encouraged to make suggestions for improving the module if a second version were to be created. See Appendix K for a detailed list of post-survey questions.

Results

Usability Testing

A usability test was conducted to evaluate the functionality and practicality of using a hyperdoc as the instruciton's delivery tool. The purpose of this test was to gain insight into ways to improve the existing module before evaluating its learning effectiveness. Four participants were recruited to assess the user experience of a hyperdoc and identify strengths (i.e., positive feedback) and weaknesses (i.e., negative feedback) within the design, navigation, and content of the hyperdoc. All four participants were educators with over 10 years of experience at a public school. Three of the four participants were classroom teachers (e.g., English, math, and science). The other participant worked as a student services coordinator and counselor. The test took about 45 minutes and was conducted using Zoom, a web conferencing platform that allowed both the participant and the tester to meet remotely. Zoom allowed the participant to share their computer screen, allowing the tester to see how well a participant performed on specific tasks.

Table 2 shows the overall percentages of positive and negative comments on design, navigation, and content from all four participants in each area. The table also separates each category percentage into three sub-categories: main interface, video lessons, and activity tools.

Table 2

Count and Percentage of Positive and Negative Comments by Category (n = 4)

Category	Total Comments	Positive Comments	Negative Comments
Design	27	20 (74%)	7 (26%)
Main Interface	13	10 (77%)	3 (23%)
Video Lessons	9	7 (78%)	2 (22%)
Activity Tools	5	3 (67%)	2 (23%)
Navigation	12	11 (92%)	1 (8%)
Main Interface	9	9 (100%)	0 (0%)
Video Lessons	1	1 (100%)	0 (0%)
Activity Tools	2	1 (50%)	1 (50%)
Content	24	17 (71%)	7 (29%)
Main Interface	7	4 (57%)	3 (43%)
Video Lessons	11	8 (72%)	3 (28%)
Activity Tools	6	5 (83%)	1 (17%)
Total	63	48 (76%)	15 (24%)

The design, navigation, and content of the delivery tool had positive feedback scores above 70% or higher. The navigation score had the highest, with an overall positivity score of 92%. The navigation of the activity tool had the highest negative feedback at 50%, although only two participants commented on that sub-category.

Table 3 shows the overall comment count and a breakdown of the percentage of positive and negative feedback for each sub-category.

Table 3

Count and Percentage of Positive and Negative Comments by Sub-Category (n = 4)

Sub-Category	Count	Positive Comment	Negative Comment
Main Interface	29	23 (79%)	6 (21%)
Video Lessons	21	16 (76%)	5 (24%)
Activity Tools	13	9 (70%)	4 (30%)
Total	63	48 (76%)	15 (24%)

Overall, participants gave the most feedback about the main interface, followed by the video lessons and activity tools. The main interface received the highest positive feedback, with 79% of the comments being positive. In contrast, the activity tools received the highest level of negative comments at 30%.

For the usability test, participants were also asked to complete three tasks. The first task directed the user to find a topic of interest and what they might learn from that lesson. Table 4 shows how many participants completed this task and how long it took them to complete it. Participants selected different topic areas to choose. Two of the four participants were interested in learning about private identifiable information, one participant was interested in learning about social engineering, and the last participant wanted to learn more about phishing techniques.

Table 4

Task One Completion Rate and Time (n=4)

Name	Task Completed	Time to Completion (seconds)
Participant 1	1	2.00
Participant 2	1	4.00
Participant 3	1	4.00
Participant 4	1	3.00
Average	1	3.25
Std Dev	0	0.96

The result of Table 4 shows that the participants all completed the task in an average of 3.25 (*SD*=0.96) seconds. Some participants took longer than expected due to not being able to decide if the block was a lesson or an activity.

The second task asked participants how many lessons were in the module. The results of Table 5 shows all participants completed the task with an average time of 5.00 seconds (*SD*=1.41).

Table 5

Task Two Completion Rate and Time (n=4)

Name	Task Completed	Time to Completion (seconds)
Participant 1	1	4.00
Participant 2	1	7.00
Participant 3	1	5.00
Participant 4	1	4.00
Average	1	5.00
Std Dev	0	1.41

The last task asked the participants where they could find information on phishing emails and what were two red flags to look out for if an email looks suspicious. This task directed the participants to click on a link and watch a video to answer the question about phishing emails. Table 6 shows that while all participants completed the task, they all varied in how long they took to complete the task. The average time was 703 seconds (*SD*=127.26).

Table 6

Task Completion and Time of Completion for Task Three (n=4)

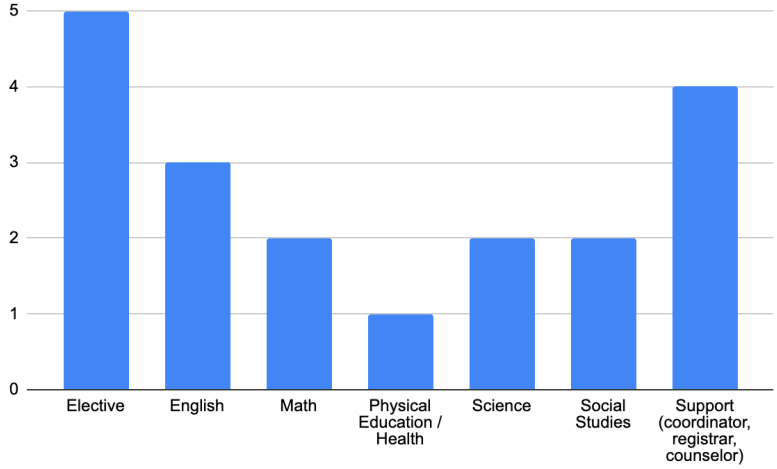
Name	Task Completed	Time to Completion (sec)
Participant 1	1	645
Participant 2	1	686
Participant 3	1	886
Participant 4	1	596
Average	1	703
Std Dev	0	127.26

Learning Effectiveness

Once changes were made to improve the delivery tool, 25 middle/intermediate school educators were contacted to participate in evaluating the learning effectiveness of the module. The participants were given three weeks to complete the asynchronous module. Before starting the lessons and activities, participants completed a demographic survey and a pre-test. In the end, 19 participants completed the module, surveys, and tests. Five (26%) of the participants had between zero to five years of teaching experience, five (26%) of the participants had between six to ten years of teaching experience, and nine (47%) of the participants had over ten years of experience. Figure 8 shows a breakdown of the participants' subject area.

Figure 8

Number of Participants Per Subject Area (n = 19)



Prior to taking the training module, participants were asked how confident they were in protecting their data and devices from cyber threats. Using a Likert scale, a five represented that the participant was very confident while one represented the participant was not very confident. The participants' average score (*M*) was a 2.89 (*SD*=0.98), which meant that participants were not confident in protecting data and devices from cyber threats. This data was important to determine whether or not completing the training module had increased the participants' confidence. Once the module was completed, participants were asked how confident they were in protecting their data and devices from cyber threats. Results from before and after the module are shown in Table 7.

Table 7

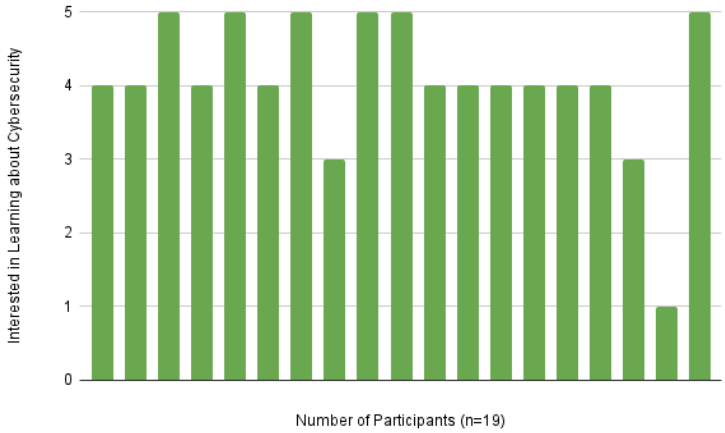
Participants' Confidence about Protecting Online Data and Devices from Cyber Threats (n=19)

	n	M	SD	Min.	Max
Before the Module	19	2.89	0.98	1.5	5
After the Module	19	4.63	0.50	4	5

Figure 9 shows a bar graph representing a 5-point Likert scale to determine if participants were interested in learning about how to protect their data and devices from cyber threats. A five represented that the participant was very interested while one represented that the participant was not very interested in this topic. The participants' average score was a 4.05 (SD=0.97).

Figure 9

Participants' Interest in Learning About Cybersecurity



After completing the module, participants were given a Likert-scale survey to rate their satisfaction of the delivery tool and if they would recommend this module to a colleague, family member, or friend. A score of five meant the participants strongly recommended the delivery tool to others, while one indicated the participants would strongly not recommend the module to others. On average, the participants scored the module 4.74 (*SD*=0.45).

When comparing the participants' pre and post-test scores, 18 of the 19 (95%) exceeded their pre-test scores by an average of five points (SD=2.48). Out of a possible score of 29 points, the most improved participant went from a score of 17 to 27. One participant did not improve and scored 25 points on both tests.

Discussions

The Cybersecurity for Middle School Teachers module was created to train educators to protect their data and devices from cybersecurity threats. Looking at the usability testing data, most participants commented on the design of the module; therefore, revisions were made to the main interface. Several participants noted that finding the link to start the module was difficult. They also mentioned that the interface lacked color and that they didn't enjoy the grayscale look. One participant said, "The starting point could be a different color so that it is distinguishable from the other sections. Also, there needs to be more color to zhuzh it up." Another participant commented that the words 'Do' and 'Watch' should be bold, making it easier for participants to navigate and find information. Figure 10 shows the original design of the main interface, while Figure 11 shows the new design after adding color.

Figure 10

Initial Interface Design of the 'Cybersecurity for Middle School Teachers' Module

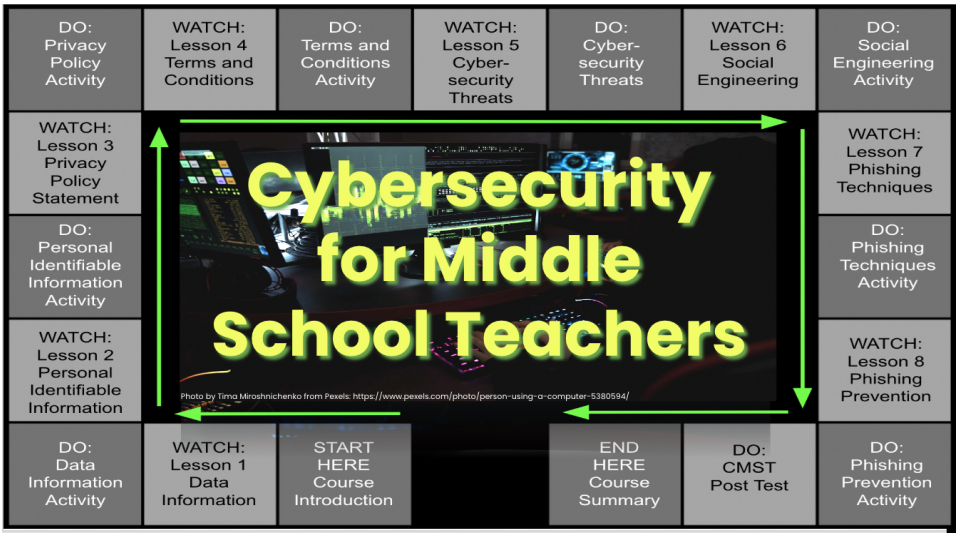
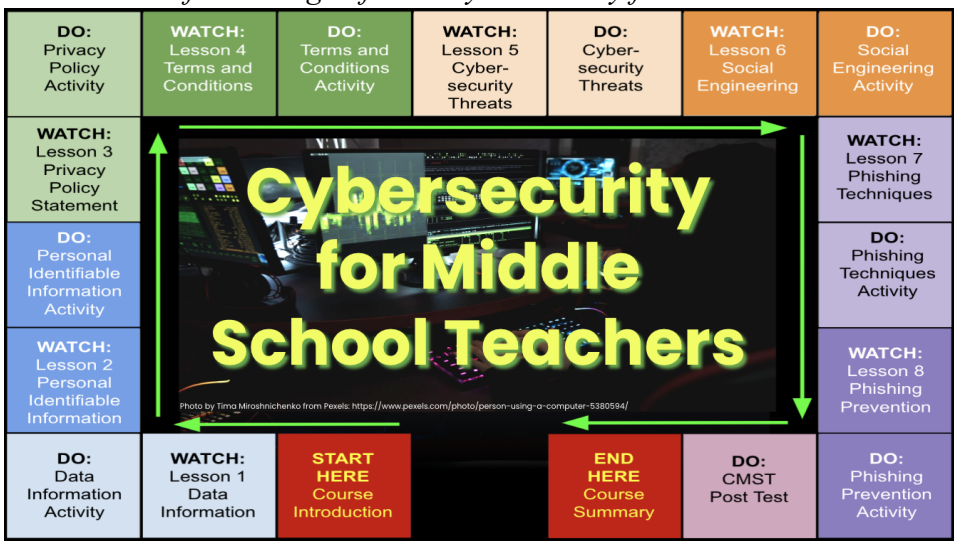


Figure 11

Revisited Interface Design of the 'Cybersecurity for Middle School Teachers' Module



In addition to the overall interface, negative comments were also made about the videos. During the usability test, there were discrepancies in how long participants would take to complete the task due to video issues. Participants complained about videos buffering or the choppiness when viewing the videos. It was determined that the video issues were due to them being uploaded and played directly from Google Drive. The videos were transferred from Google Drive to a YouTube channel to address these problems. Figure 12 shows a video experiencing buffering issues, while Figure 13 shows the same video hosted on a YouTube channel.

Figure 12

Some Participants Experienced Buffering Issue

Note. Example of a video lesson that experienced choppiness when played off of Google Drive.

Figure 13

Lesson Seven Video on YouTube

Note. Example of a video lesson played off of YouTube with no buffering issues.

The retrospective survey results suggested the changes made to the main interface and videos were positive. Based on a five-point Likert-scale, with one representing "strongly disagree" and five representing "strongly agree," the nineteen participants (n=19) scored the engagement of the training module at 4.37 on average (*SD*=0.68). In addition, one participant said, "I enjoyed the presentation slides and how it was well organized. It was easy to follow, and color coding was very helpful too." A second participant added, "The module was easy to navigate and had a consistent process."

During the learning effectiveness evaluation, 18 out of 19 (95%) participants improved upon their pre-test scores by an average of 5 points, with only three participants scoring 20 points or lower (out of 29), and no participants scoring lower than 19 points. These results suggested the hyperdoc was an effective tool in helping participants learn about cybersecurity, and the learning activities worked well in reinforcing concepts. Additionally, the participants' Likert-scale results indicated that teachers felt more confident about their cybersecurity knowledge and skills after the training module. One participant said, "The combination of instructional videos and activities were very good. The videos were clear and precise with good examples and explanations." Another participant said, "I (also) felt really good when I got 100% correct on the quiz!"

Data from individual pre and post-test questions suggested that participants improved their skills in identifying and analyzing terms and condition statements. One of the questions asked the participants to read a terms and condition policy and describe why it was problematic. Four (21%) participants answered this question correctly during the pre-test, but all 19 (21%) participants could answer the question correctly on the post-test. A second question asked the participants to read a different terms and condition policy and explain why it was problematic. Ten (53%) participants answered this question correctly on the pre-test, but all 19 (100%) participants answered the question correctly on the post-test. These two data points suggested that the instructional tool effectively improved participants' knowledge and skills in identifying and analyzing problematic terms and conditions statements.

For the majority of the individual question results, most participants improved their post-test scores compared to their pre-test scores. However, some results suggested that the instructional tool still needs improving. For example, one participant scored 25 points on the pre and post-tests. When investigating further, the participant missed several post-test questions they correctly answered on the pre-test. While their scores were above average, it also indicated that some of the questions may have been problematic. Looking at each question and score from the post-test, this participant missed questions many other participants had also answered incorrectly. These results suggested that the delivery tool needed to prepare the participants for these questions. There was also an outlier in one of the scores in which participants answered correctly on the pre-test but incorrectly on the post-test. One of these questions dealt with recognizing phishing and legitimate emails. Seventeen (89%) participants answered the question correctly in the pre-test, but 15 (79%) answered incorrectly in the post-test. Looking at the results, the participants thought that the legitimate email was a phishing email, suggesting that they may have been overly cautious when differentiating emails.

Conclusion

The *Cybersecurity for Middle School Teachers* module was designed and developed to teach educators about the importance of cybersecurity and enhance their skills to keep data and devices safe from cyber threats. Literature reviews and target audience analysis were essential to the instructional tool's initial design. The content design focused on the DigComp Framework, specifically data and device safety. In delivering the information to teachers, the content needed to be easy to understand, relevant, and scaffolded. Using the ARCS Model of Motivation (Keller, 1987), it was important to create an instructional tool that grabbed the learner's attention, increased their confidence, was relevant and practical, and satisfied them once they completed

the module. The ‘watch-do’ strategy allowed the teachers to learn from watching videos, followed by learning activities designed to reinforce the concepts.

The usability testing allowed participants to evaluate the overall design of the module, including its navigation and content. The design of the instructional tool was modified using the results and comments from the participants. After improving the hyperdoc, participants evaluated the learning effectiveness of the module, including its instruction and learning activities. After comparing and analyzing the pre and post-test scores, the results suggested the learning tool effectively taught educators the importance of cybersecurity. In addition, the retrospective survey results indicated that most participants agreed the module increased their confidence in practicing safe cybersecurity habits and acknowledged that the module should be offered to all educators.

While the overall module design and development were successful, some areas could be improved. The first improvement would be to include learning objectives, terms, and concepts at the beginning of each lesson. These components make it clear to the participants what will be taught in each lesson. Participants said that it would have been nice to let the user know what lessons and activities were completed so they could visually see their progress. Another area that needs improvement is the learning activities. Most of the activities were done using multiple-choice questions or matching. It may have been better to include other assessment activities, such as linking to additional resources for further understanding of the topic. The final improvement to this module would be updating it to the current technology trends.

With more fine-tuning and substance, the overall vision is to see The *Cybersecurity for Middle School Teachers* module added as a professional development course for all HIDOE staff. The goal is to help them protect themselves and their students from cybersecurity issues. The module will also be constantly updated to follow the latest technology trends. For example, artificial intelligence and bots like ChatGPT are becoming more relevant in composing letters, emails, and conversations. Consequently, phishing or unsolicited emails may look exactly like legitimate emails, and what was used to distinguish fake from real emails may no longer be accurate. It will also be essential to get feedback regularly from the users to improve this course in the future.

References

Barbara Bush Foundation for Family Literacy and Digital Promise (2022). Promoting digital literacy for adult learners: a resource guide. Barbara Bush Foundation for Family Literacy and Digital Promise. Washington, DC. https://www.barbarabush.org/wp-content/uploads/2022/04/Digital-Literacy-Resource-Guide-for-Adult-Learners-.pdf

Bruner, J. (1961). The Art of Discovery. *Harvard Educational Review.* http://psycnet.apa.org/record/1962-00777-001

Center for Comprehensive School Reform and Improvement (2007, April). Using positive student engagement to increase student achievement. *The Center for Comprehensive School Reform and Improvement Newsletter*. https://files.eric.ed.gov/fulltext/ED497205.pdf

Chung, L. E. (2021). Educators' Stress Levels and the Perception of Emergency Preparedness (Order No. 28544249). Available from ProQuest Dissertations & Theses Global. (2545969589). https://www.proquest.com/dissertations-theses/educators-stress-levels-perception-emergency/docview/2545969589/se-2

Collins, A., Brown, J. S., & Newman, S. E. (1988). Cognitive apprenticeship.*Thinking: The Journal of Philosophy for Children*, *8*(1), 2-10.

Eadens, D. W., Maddock, D., Thornburg, A. W., & Abernathy, D. F. (2022). K-12 teacher perspectives on the pandemic pivot to online teaching and learning. *Journal of Pedagogical Research*, 6(1), 131-151. https://dx.doi.org/10.33902/jpr.2022175776

European Commission, Joint Research Centre, Vuorikari, R., Kluzer, S., Punie, Y. (2022). *DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes*, Publications Office of the European Union. https://data.europa.eu/doi/10.2760/115376

Falloon, G. (2020). From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Education Tech Research Dev* 68, 2449–2472. https://doi.org/10.1007/s11423-020-09767-4

Federal Trade Commission (2022). Children's online privacy protection rule (COPPA). *Federal Trade Commission*. Washington, DC: FTC. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Gonzalez J. (2017, June 11). How HyperDocs can transform your teaching. *Cult of Pedagogy.* https://www.cultofpedagogy.com/hyperdocs/

Human Rights Watch (2022). How dare they peep into my private life. Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic. Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments#4182

iKeepSafe (2022). COPPA 101 for educators. iKeepSafe Coalition. Washington DC. http://archive.ikeepsafe.org/wp-content/uploads/2015/08/COPPA-101-educators.pdf

International Society for Technology in Education. (2022). *ISTE standards: Educators*. https://www.iste.org/standards/iste-standards-for-teachers

Janssen, J., Stoyanov, S., Ferrari, A., Punie, Y., Pannekeet, K., & Sloep, P. (2013). Experts' views on digital competence: Commonalities and differences. *Computers & Education*, 68, 473–481. https://doi.org/10.1016/j.compedu.2013.06.008

Johnston, R. (2019, July 13). Student data systems compromised in Hawaii, Tennessee. Edscoop. https://edscoop.com/graduation-alliance-data-exposure-hawaii-tennessee/

Keller, J. M. (1987). Development and use of the ARCS model of instructional design. *Journal of Instructional Development*, 10(3), 2–10. https://doi.org/10.1007/BF02905780

Krug, S. (2010). *Rocket surgery made easy: The do-it-yourself guide to finding and fixing usability problems.* New Riders.

Laird, E., Grant-Chapman, H., Venzke, C., Quay-de la Vallee, H. (2022). *Hidden harms: The Misleading promise of monitoring students online.* Center for Democracy & Technology. https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Report-Final-Accessible.pdf

Levin, Douglas A. (2022). The state of K-12 cybersecurity: Year in review – 2022 annual report. *K12 Security Information Exchange (K12 SIX)*. https://www.k12six.org/the-report

Matherson, L. & Windle, T. (2017). What do teachers want from their professional development? Four emerging themes. *The Delta Kappa Gamma Bulletin: International Journal for Professional Educators, 83*(3), 28-32. https://www.dkg.org/DKGDocs/2017_Jour_83-3_Systems-to-Address-Quality-Teaching.pdf#page=28

Moreno, R. (2005). Multimedia Learning with Animated Pedagogical Agents. In R. E. Mayer (Ed.), *The Cambridge handbook of multimedia learning*. Cambridge University Press. https://doi.org/10.1017/CBO9780511816819.032

Strickland, R. (2019). The state student privacy report card: grading the states on protecting student data privacy. Network for Public Education and Parent Coalition for Student Privacy. https://files.eric.ed.gov/fulltext/ED612839.pdf

U.S. Government Accountability Office (2020, September). Data security recent K12 data breaches show that students are vulnerable to harm (Accessible version). *Report to the Republican Leader, Committee on Education and Labor, House of Representatives*. Washington, DC: GAO https://www.gao.gov/assets/710/709463.pdf

Vejmelka, L., Katulic, T., Jurić, M. & Lakatoš, i. M. (2020) Application of the general data protection regulation in schools: a qualitative study with teachers, professional associates and principals, 2020 *43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1463-1469, doi:10.23919/MIPRO48935.2020.9245209.

Veugen, M., Gulikers, J. & den Brok, P. (2022). Secondary school teachers' use of online formative assessment during COVID-19 lockdown: Experiences and lessons learned. *Journal of Computer Assisted Learning*. https://dx.doi.org/10.1111/jcal.12699

Woolfolk, J. (2022, September 12). Ransomware attacks target schools; threaten to expose students, teachers personal data. Bay Area News Group and Tribune Media Services. https://www.al.com/news/2022/09/ransomware-attacks-target-schools-threaten-to-expose-students-teachers-personal-data.html?outputType=amp

Appendices

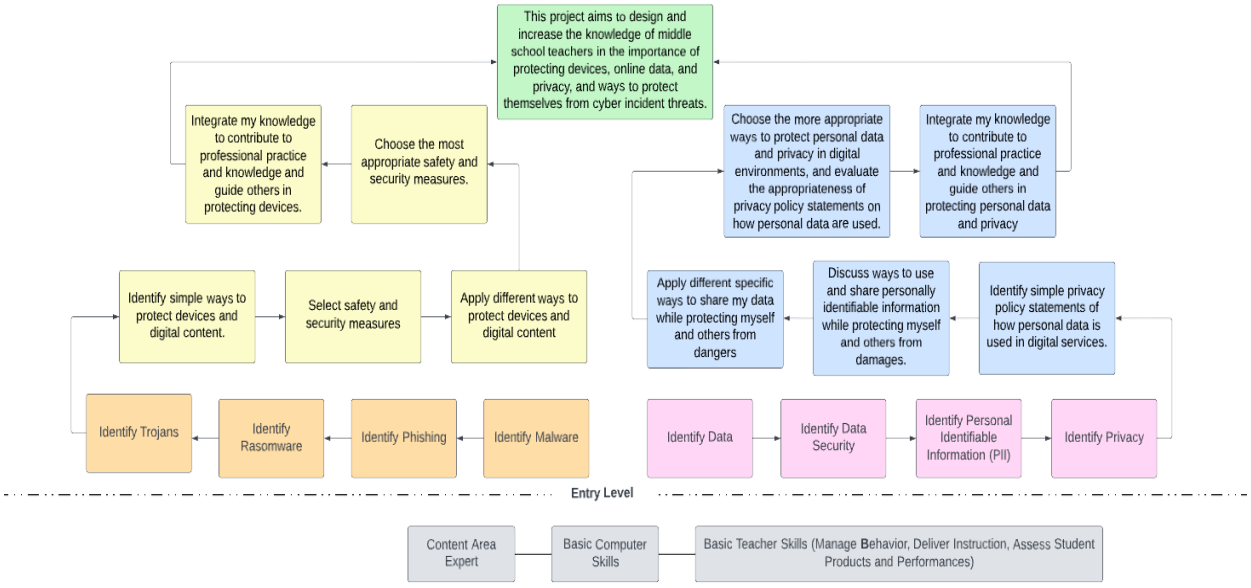
Appendix A

Learner Characteristics of Middle School Teachers

Affective Characteristics	Cognitive Characteristics
● Motivated to support and encourage students. ● Motivated to support students academically, emotionally, and socially. ● Motivated to keep their students safe. ● Motivated to improve their teaching. ● May not be motivated to learn if the topic is not relatable. ● May not be motivated to learn if the topic is too time-consuming.	● Understand technical information from reading materials and video resources. ● Has limited knowledge and experience with digital literacy and data security. ● Has a broad understanding of different learning applications and tools. ● Research applications that could help improve curriculum and pedagogy. ● Uses and develops learning strategies to help student achievement.
Social Characteristics	**Physiological Characteristics**
● Teaching in a middle or intermediate school. ● Diverse backgrounds (e.g., culture, race, religion). ● Ages range varies from 22 years old and above ● At least a bachelor's degree and a teaching certificate. ● Shares materials and resources with other teachers. ● Provides constructive feedback to other teachers to improve best practices.	● Engages with different teaching applications and learning tools. ● Listens to audio and video resources (with accessible tools if necessary). ● Communicates and engages in 'one-to-one' or group discussions.

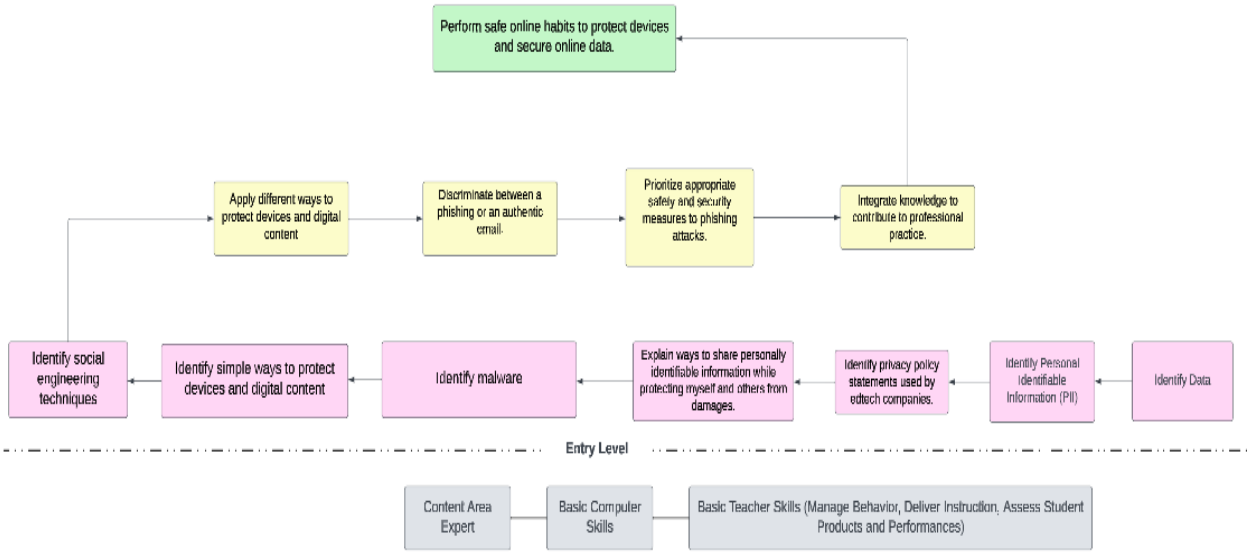
Appendix B

First Draft of Instructional Scope



Appendix C

New Instructional Scope



Appendix D
Performance Objectives

Objective No.	Behavior	Performance Objectives
1	Define data	Given the term, the teacher will choose the definition that describes data with 100% accuracy.
2	Identify data	Given a list of words, teachers will be able to identify all choices that could represent the term “data” with 100% accuracy.
3	Define Personally Identifiable Information (PII)	Given the term, the teacher will choose the definition that describes personally identifiable information with 100% accuracy.
4	Identify Personally Identifiable Information (PII)	Given a list of words, teachers will be able to identify all choices that represent the term “personally identifiable information” with 100% accuracy.
5	Define a Privacy Policy	Given the term, teachers will be able to select the correct definition that applies to a “privacy policy statement” with 100% accuracy.
6	Define Terms of Condition Statement	Given the term, teachers will be able to select the correct definition that applies to a “terms of condition statement” with 100% accuracy.
7	Identify phrases that edtech companies may use in their privacy policy statements.	Given an edtech company’s privacy policy, teachers will be able to examine problematic wording that could put online data at risk with 100% accuracy.
8	Explain which privacy policy and terms of condition statements are problematic	Given several privacy policies and terms of condition statements from different edtech companies, the teacher will be able to explain which ones may be problematic with 100% accuracy.
9	Identify cybersecurity threats	Given a list of different cybersecurity threats, the teacher will be able to match the

		threat with its definition with 100% accuracy.
10	Identify ways to protect devices	Given a list of choices, the teacher will be able to identify ways to protect devices by selecting all options that apply with 100% accuracy.
11	Identify social engineering techniques	Given a list of different social engineering terms, the teacher will be able to identify social engineering terms by the techniques with its correct definition with 100% accuracy.
12	Identify different types of phishing attacks	Given several emails, the teacher will be able to correctly identify the different types of phishing attacks with 100% accuracy.
13	Discriminate between a phishing and an authentic email	Given several emails, the teacher will be able to discriminate between a phishing and an authentic email.
14	Evaluate cybersecurity threats	Given a scenario that describes a cybersecurity threat, the teacher will be able to evaluate the type of threat.
15	Perform the device protection strategies to avoid data being compromised	Given a cybersecurity threat scenario, the teacher will be able to perform device protection strategies to help avoid data being compromised.

Appendix E

Instructional Breakdown of Lessons and Activities

Steps	Activity	Duration	Run Time
1	Email participants	2 weeks out	00:00
2	Watch: Course Overview Video	2 minutes	2:00
3	Watch: Data Information Video	3 minutes	5:00
4	Do: Data Information Activities	1 minute	6:00
5	Watch: Personally Identifiable Information Video	3 minutes	9:00
6	Do: Personally Identifiable Information Activities	1 minute	10:00
7	Watch: Privacy Policy and Terms of Condition Video	3 minutes	13:00
8	Do: Privacy Policy and Terms of Condition Activities	1 minute	14:00
9	Watch: Cybersecurity Threats Video	3 minutes	17:00
10	Do: Cybersecurity Threats Activities	1 minute	18:00
11	Watch: Ways to Protect Devices Video	3 minutes	21:00
12	Do: Ways to Protect Devices Activities	1 minute	22:00
13	Watch: Social Engineering Video	3 minutes	25:00
14	Do: Social Engineering Activities	1 minute	26:00
15	Watch: Phishing Attack Video	3 minutes	29:00
16	Do: Phishing Attack Activities	1 minute	30:00
17	Watch: Phishing Email Prevention	3 minutes	33:00
18	Do: Phishing Email Activities	1 minute	34:00
19	Watch: Evaluating Cybersecurity Threats	3 minutes	37:00
20	Do: Evaluating Cybersecurity Threats Activities	3 minutes	40:00
21	Do: Device Protection Strategies Activities	3 minutes	43:00
22	Watch: Course Summary	2 minutes	45:00
23	Do: Course Reflection	2 minutes	47:00

Appendix F

Sample Email Letter to Pariticpants

Aloha (name)

I am Cleve Hamasaki, a graduate student at the University of Hawaii's Department of Learning Design and Technology (LTEC). I am following up with you on our last conversation about your willingness to participate in evaluating my instructional tool. I have developed a module on cybersecurity for middle school teachers to provide them with important information when dealing with online data. The learning tool I have created is a 'hyperdoc,' which allows the user to engage in both the instructional content and activities in one area. This evaluation aims to assess the module's learning tool rather than your knowledge of the material. As you go through the different lessons, consider the module's content and design (e.g., material difficulty level, instruction flow, font size, color scheme, and other content and design components).

By participating in this evaluation, you will first be asked to fill out a demographic survey and take a pretest. After completing the pretest, you will take the training module. This eight-lesson module is asynchronous and can be done at your own pace. The entire module should take anywhere from 40 to 60 minutes to complete. During this time, you will be given instructional videos to watch and learning activities to engage in. At the end of the module, you will take a post test and fill out a 'retrospective survey' to measure the learning effectiveness of my delivery tool.

Remember that all your responses to the survey and assessments are anonymous and confidential. The user code I will provide you is used to track and compare your answers to other participants; be assured that no personal information (e.g., email and full name) will be collected or shared with anyone.

I included your 'user code' below, which you will enter before taking the surveys and pre and post tests. Also, please use this code throughout the module activities (Nearpod). All answers will be anonymous and shared only with my university advisors and me. I will destroy all user data once I have gathered all the necessary information.

Please follow the directions below:
Your 'user code' is: (user code)

Please use this unique user code anytime it asks for your 'user code' (e.g., surveys and tests) or 'name' (e.g., Nearpod activities**)**

Step 1: Complete the Demographic Survey and Pretest.
Link: (link address)

Step 2: Go to Cybersecurity Training Module and complete all the lessons and activities. You can start by watching the video in the red, 'START HERE' block.
Link: (link address)

Step 3: Complete the Post Test and Retrospective Survey.
Link: (link address)

I would greatly appreciate it if you completed the lessons as soon as possible and no later than (date)

Thank you again for taking the time to complete this module. Your help is greatly appreciated! Please let me know if you have any questions or concerns.

Sincerely,

Cleve Hamasaki

Appendix G

Participant Demographic Survey

1. How long have you been a teacher?
    a. 0 - 5 years
    b. 6 - 10 years
    c. 10+ years

2. What is your highest academic degree?
    a. Bachelor's degree
    b. Masters degree
    c. Doctorate

3. What subject(s) do you teach?
    - Elective
    - English
    - Math
    - Science
    - Social Studies
    - Other

4. In the past FIVE years, how many personal development workshops have you taken?
    a. None
    b. 1 - 4
    c. 5+

5. I am confident in using technology in the classroom
    a. Strongly Disagree
    b. Disagree
    c. Agree
    d. Strongly Agree

6. I believe student safety is important.
    a. Strongly Disagree
    b. Disagree
    c. Agree
    d. Strongly Agree

7. I am confident about protecting online data.
    a. Strongly Disagree
    b. Disagree
    c. Agree
    d. Strongly Agree

8. I am confident about protecting my devices from cyber threats.
    a. Strongly Disagree

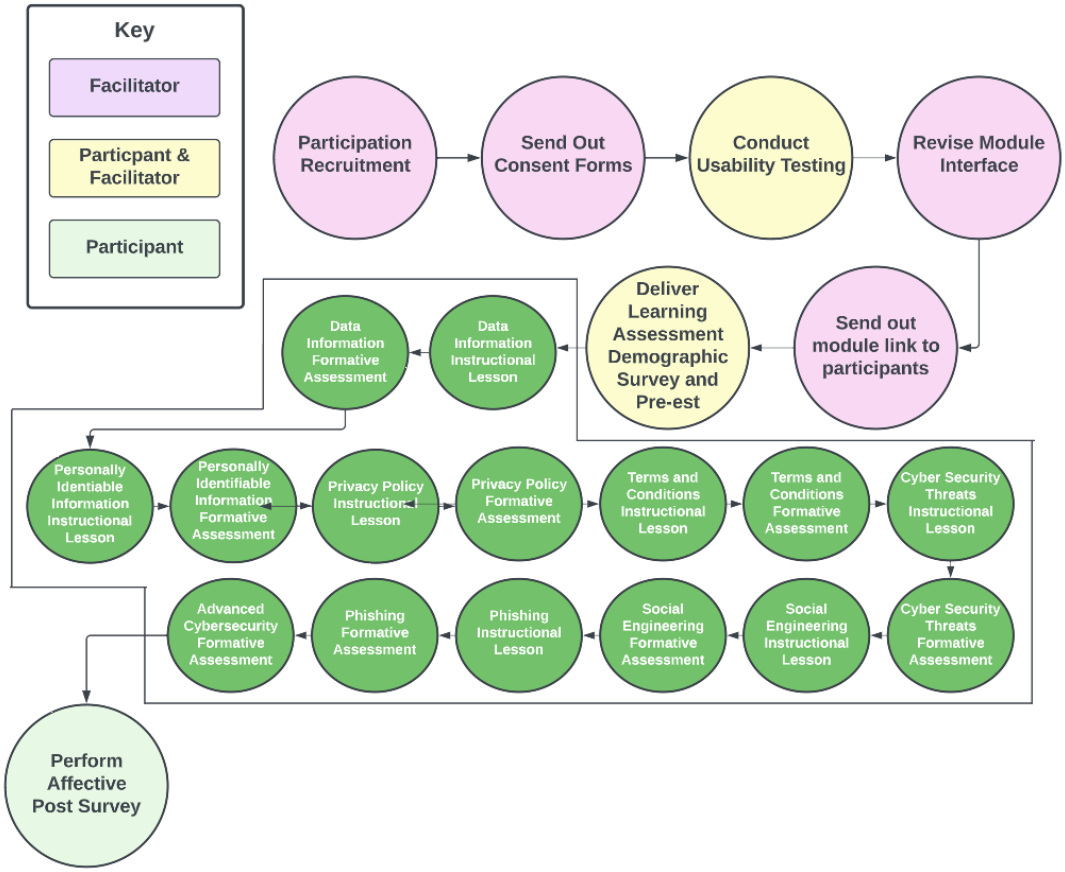
b. Disagree
c. Agree
d. Strongly Agree

9. I am familiar with ‘private policy’ and ‘terms and conditions’ statements.
    a. Strongly Disagree
    b. Disagree
    c. Agree
    d. Strongly Agree

10. I am interested in learning about cybersecurity.
    a. Strongly Disagree
    b. Disagree
    c. Agree
    d. Strongly Agree

Appendix H

Procedure Workflow



Appendix I

Facilitator Script

- ❏ ***START the Meet session by clicking on the "record now"***

Hi, [Name of participant]. My name is Cleve, and I will walk you through this session today. I'm also going to be recording today's usability test session. Is that okay with you? [pause for answer] Thank you!

- ❏ ***ASK participant preliminary questions:***

I'm glad you were able to join this evening. So, what brought you to become a teacher in the Hawaii Department of Education? [listen, respond]

Have you ever been part of a usability study before? [listen] Good to know. This will be great for both of us, and I appreciate your time.

Before we begin, I have some information for you, and I will read it to ensure that I cover everything.

I'm asking people to try using this modified version of a hyperdoc to see whether it works as intended. The session should take about 30 minutes.

The first thing I just want to say right away is that we're testing the training module, not you. You can't do anything wrong here. In fact, this is probably the one place today where you don't have to worry about making mistakes.

As you use the site, I will ask you to think aloud as much as possible. In other words, say what you're looking at, what you're trying to do, and what you're thinking. This will be a big help to us.

Also, please don't worry that you will hurt my feelings. We're doing this to improve the training module, so I want you to talk out loud and hear your honest reactions. Okay? [pause for the yes] Great!

If you have any questions as we go along, just ask them. I may not be able to answer them right away since we're interested in how people do when they don't have someone sitting next to them to help. But if you still have questions, I'll try to answer them when we're done. Fair enough? [pause for answer]

Finally, if you need to take a break at any point, no problem; just let me know. Do you have any questions so far? [pause for answer]

OK, great. We're off to a good start and can start looking at things.

- ❏ ***SEND participant website URL through ZOOM chat:***

[Name of participant], I am going to put the URL of the training module into the chat.

[paste the URL into chat:]
I would like for you to click on the URL, and it should automatically open a browser to view the hyperdoc that we will be reviewing tonight. Can you do that for me? [pause for yes]

Let me know when it's up. [let them tell you it's up] Say great job!

- ❏ ***ASK participant to begin the screenshare:***

So now, we're going to see your screen, so I can see what you're seeing, okay? [pause for yes] So look down at the bottom bar to your far right and you will see a "Share Screen" button. Click on it and choose to share your desktop. Do you see that? [pause for yes] Awesome, you're doing great. I want you to click the button and then click on the "A window" and not "your entire screen." I'm just interested in seeing the hyperdoc with you. So let's do that now. [pause]

- ❏ ***ASK participant to narrate their first impression of what the website is about and its overall appearance: [one to two minutes at most]***

So [Name of participant] before we begin I just want to give you the rule you cannot click on anything, just yet. We'll get to that soon but not yet.

First, I'm going to ask you to look at this page and tell me what you make of it: what first impression you have, what strikes you about it, who might be interested in this website, and what's it for. Just look around, and go for it. Just take a look around and do a little narrative. [pause and let them talk]

Thanks for your input to help in this process. That was terrific! (smile)

- ❏ ***SET-UP participant scenario rules to complete a task:***

Now [Name of participant], I'm going to set up a scenario for you (1) of where you work and (2) who you are, for the purposes of the usability study. Okay? [pause for yes]

I'm going to read this out loud, and I'm going to let you click on the buttons now and use the hyperdoc based on what you hear. You can use any features that you see and just go for it. This way, we'll learn a lot more about how well the instructional delivery tool works (or doesn't work).

- ❏ ***EXPLAIN to participant who they are in the scenario and provide <u>first</u> task: [three to five minutes at most]***

You are a middle school teacher.. I'd like to see if you can find something that would be of interest to you?

And again, as much as possible, it will help me if you talk and think out loud as you go along.

Okay? [pause for yes] [watch facial expressions and how they navigate]

Probing question: How might this interest you?

After the first task is completed, direct [Name of participant] to go back to the Homepage for the second part of the study.

- ❏ ***EXPLAIN to participant who they are in the scenario and provide second task: [three to five minutes at most]***

Again, you are a middle school teacher. You want to find information on how to recognize phishing emails. Walk me through how you would find this information and explain to me two ways to spot a phishing email.

Probing question: How do you think this information was useful to you as a teacher?

Allow the user to proceed from one task to the next until you don't feel like it is producing any value or the user becomes very frustrated. Repeat for each task or until time runs out.

Thanks, that was very helpful.

- ❏ ***EXPLAIN to participant who they are in the scenario and provide second task: [three to five minutes at most]***

Again, you are a middle school teacher. You want to reinforce what you know about Personally Identifiable Information. Walk me through how you would find this information as well as the activity to help reinforce your knowledge about PII.

Probing question: Was it to find this information? If so, why or why not?

- ❏ ***Request from the participant that they end their screen share by clicking on the "screen share" link on their left-hand navigation in the window.***

We are done with the main questions, but I have a few more general questions to ask you.

1. On a scale of 1 to 5, with 1 representing very difficult and 5 representing very easy, how would you rate your experience during today's testing? Why?
2. Would you say that the tasks you performed today were easy, somewhat easy, not easy, or difficult? Why?
3. If this website were developed and live, would you recommend it to any of your family or friends that have special needs? Why?

That's the last question. Do you have any questions for me, now that we're done?
I want to thank you for your time and willingness to be a participant in this study. We really appreciate it. We have now completed our time together.

- ❏ ***Stop the air broadcast (Zoom) by clicking on the red button.***

Appendix J

Learning Objectives and Instructional Assessments

1: Define Data
Learning Objective 1: Given the term, the teacher will choose the definition that describes data with 100% accuracy.
Watch: Instructional content on data (video)
Do: Pretest Question #1: Which of the following is the definition of data? A. Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer. B. Facts, information, and skills acquired by a person through experience or education; the theoretical or practical understanding of a subject. C. A number, especially one which forms part of official statistics or relates to a company's financial performance. D. The practice or science of collecting and analyzing numerical data in large quantities, especially to infer proportions in a whole from those in a representative sample. --- Post Test Question #1: Which of the following is the definition of data? A. The practice or science of collecting and analyzing numerical data in large quantities, especially to infer proportions in a whole from those in a representative sample. B. Facts, information, and skills acquired by a person through experience or education; the theoretical or practical understanding of a subject. C. A number, especially one which forms part of official statistics or relates to a company's financial performance. D. Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer.
2: Identify Data
Learning Objective 2: Given a list of words, teachers will be able to identify all choices that could represent the term “data” with 100% accuracy.
Do: Pretest

Question #2: Which of the following are examples of data? (Choose all that apply)

A. Name
B. Birth date
C. Cost
D. Address
E. Email address
F. All of the Above

Post Test
Question #2: Which of the following are examples of data? (Choose all that apply)

A. Name
B. Birth date
C. Cost
D. Address
E. Email address
F. All of the above

3: Define Personally Identifiable Information

Learning Objective 3: Given the term, the teacher will choose the definition that describes personal identifiable information with 100% accuracy.

Watch: Instructional content on personally identifiable information (video)

Do:
Pretest
Question #3: Which of the following is the definition of personally identifiable information?

A. Information such as business phone numbers and race, religion, gender, workplace, and job titles.
B. Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
C. Student information such as grade level, dates of attendance, photographs, and addresses.
D. None of the above.

Post Test
Question #3: Which of the following is the definition of personally identifiable information?

A. Information such as business phone numbers and race, religion, gender, workplace, and job titles.
B. Student information such as grade level, dates of attendance, photographs, and addresses.
C. Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
D. None of the above.

4: Identify Personally Identifiable Information

Learning Objective 4: Given a list of words, teachers will be able to identify all choices that represent the term "personally identifiable information" with 100% accuracy.

Do:
Pretest
Question 4: Which of the following represents personally identifiable information? (Choose all that apply)

A. Name
B. Phone number
C. Business phone number
D. Race
E. Social security
F. Driver's licence number
G. Graduation date
H. Medical information
I. Job title

Post Test
Question 4: Which of the following represents personally identifiable information? (Choose all that apply)

A. Social security
B. Job title
C. Phone number
D. Name
E. Graduation date
F. Driver's licence number
G. Race
H. Business phone number
I. Medical information

5: Define a Privacy Policy Statement

Learning Objective 5: Given the term, teachers will be able to select the correct definition that applies to a “privacy policy” with 100% accuracy.

Watch: Instructional content on privacy policy (video)

Do:
Pretest
Question 5: Which of the following best describes a privacy policy?

A. A statement or a legal document that discloses information about how a party gathers, uses, discloses, and manages a customer or client's data.
B. Simple statements from a website making users aware of the site's liability limitations.
C. A political science tool used to study how government programs are managed.
D. None of the above.

Do:
Post Test
Question 5: Which of the following best describes a privacy policy?

A. Simple statements from a website making users aware of the site's liability limitations.
B. A political science tool used to study how government programs are managed.
C. A statement or a legal document that discloses information about how a party gathers, uses, discloses, and manages a customer or client's data.
D. None of the above.

6: Define Terms of Condition

Learning Objective 6: Given the term, teachers will be able to select the correct definition that applies to a “privacy policy” with 100% accuracy.

Do:
Pretest
Question 6: Which of the following best describes ‘terms and conditions?’

A. An agreement that sets the rules and guidelines that users must agree to and follow to use and access another party’s website or mobile app.
B. An agreement that businesses use to protect themselves from lawsuits
C. A handshake agreement
D. An agreement between the user and other users.

Post Test
Question 6: Which of the following definitions best describes ‘terms and conditions?’

A. An agreement between the user and other users.
B. An agreement that businesses use to protect themselves from lawsuits
C. An agreement that sets the rules and guidelines that users must agree to and follow to use and access another party's website or mobile app.
D. A handshake agreement

7: Identify phrases that edtech companies may use in their privacy policy statements.

Learning Objective 7: Given an edtech company's privacy policy, teachers will be able to examine phrases that could put online data at risk with 100% accuracy.

Do:
Pretest
Question 5: View the following privacy policy statement:

> *Employees may access file metadata (e.g., file names and locations) when they have a legitimate reason, like providing technical support. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so).*
>
> *These and other features may require our systems to access, store and scan Your Stuff. You give us permission to do those things, and this permission extends to trusted third parties we work with.*

What is wrong with this written privacy policy?

A. "Employees may access file metadata."
B. "Your Stuff" is an ambiguous term."
C. "…this permission extends to trusted third parties we work with."
D. All of the above

Post Test
Question 5: View the following privacy policy statement:

> *Employees may access file metadata (e.g., file names and locations) when they have a legitimate reason, like providing technical support. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so).*
>
> *These and other features may require our systems to access, store and scan Your Stuff. You give us permission to do those things, and this permission extends to trusted third parties we work with.*

What is wrong with this written privacy policy?

A. "…this permission extends to trusted third parties we work with."
B. "Employees may access file metadata."
C. "Your Stuff" is an ambiguous term."
D. All of the above

8: Explain which privacy policy and terms of condition statements are problematic

Learning Objective 8: Given several privacy policies and terms of condition statements from different edtech companies, the teacher will be able to explain why each one may be problematic with 100% accuracy.

Do:
Pretest
Question 8: Why are the following privacy policy and terms of condition statements problematic?

1) *"Our automated systems analyze your content (including emails) to provide you with personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."*

   Correct answer: The statement means that the company can analyze all of your sent, received, and stored data.

---

2) *"You grant CompanyXYZ a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicensable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to CompanyXYZ, including, but not limited to, any user-generated content, ideas, concepts, techniques and/or data to the services, you submit to CompanyXYZ, without any further consent, notice and/or compensation to you or to any third parties."*

   Correct answer: Your data is owned by CompanyXYZ and can do whatever they want with it.

---

3) *"CompanyABC or its agents will review content to resolve the issue. This is in addition to the uses described in this Agreement and the Privacy Statements."*

Correct answer: CompanyABC and its partners can review all your data.

Post Test
Question 8: Why are the following privacy policy and terms of condition statements problematic?

1) *"Our automated systems analyze your content (including emails) to provide you with personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."*

   Correct answer: The statement means that the company can analyze all of your sent, received, and stored data.

2) *You grant CompanyXYZ a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicensable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to CompanyXYZ, including, but not limited to, any user-generated content, ideas, concepts, techniques and/or data to the services, you submit to CompanyXYZ, without any further consent, notice and/or compensation to you or to any third parties."*

   Correct answer: Your data is owned by CompanyXYZ and can do whatever they want with it.

---

3) *"CompanyABC or its agents will review content to resolve the issue. This is in addition to the uses described in this Agreement and the Privacy Statements."*

   Correct answer: CompanyABC and its partners can review all your data.

9: Identify Cybersecurity Threats

Learning Objective 9: Given a list of different cybersecurity threats, the teacher will be able to match the threat with its definition with 100% accuracy.

Watch: Instructional content on cybersecurity threats (video)

Do:
Pretest
Question 9: Match the cybersecurity threat with its definition

I. Macro Malware	a. a program that disguises itself as a useful application but when installed, establishes a back door that can be exploited by attackers.
II. Ransomware	b. an attack launched by a large number of other machines preventing a server from responding to service requests.
III. Trojan horse	c. a type of malware that blocks access by encrypting the victim's data until a ransom is paid.
IV. Virus	d. a computer bug that attaches itself to an application and replicates itself to infect other its host or other network devices.
V. Distributed Denial of Service (DDOS)	e. unwanted commands targeting a Microsoft file that is installed in your system without your consent.

Do:
Post Test
Question 9: Match the cybersecurity threat with its defintion

VI. Macro Malware	a. a program that disguises itself as a useful application but when installed, establishes a back door that can be exploited by attackers.
VII. Ransomware	b. an attack launched by a large number of other machines preventing a server from responding to service requests.
VIII. Trojan horse	c. a type of malware that blocks access by encrypting the victim's data until a ransom is paid.
IX. Virus	d. a computer bug that attaches itself to an application and replicates itself to infect other its host or other network devices.
X. Distributed Denial of Service (DDOS)	e. unwanted commands targeting a Microsoft file that is installed in your system without your consent.

10: Identify ways to protect devices

Learning Objectives 10: Given a list of choices, the teacher will be able to identify ways to protect devices by selecting all options that apply with 100% accuracy.

Watch: Instructional content on ways to protect devices (video)

Do:
Pretest
Question 10: Fill in the blank with the correct word.

1. Keep your computer hardware and software updated.
2. Install a trusted anti-virus software such as Norton or McAfee.
3. Do not click on any suspicious links.
4. Do not open any email attachments from random people.

Pretest
Question 10: Fill in the blank with the correct word.

5. Keep your computer hardware and software u_____.
6. Install a trusted a_____ software such as Norton or McAfee.
7. Do not click on any suspicious l_____.
8. Do not open any email a_____ from random people.

11: Identify social engineering techniques

Learning Objective 11: Given a list of different social engineering terms, the teacher will be able to identify social engineering terms by the techniques with its correct definition with 100% accuracy.

Watch: Instructional content of social engineering techniques (video)

Do:
Pretest
Question 11: Match the following social engineering terms to its description.

I. Phishing
II. Scareware
III. Watering Hole
IV. Baiting

a. a cybersecurity tactic used by an attacker to persuade a user into believing an update, application, extension, or other resources are useful. An attacker may also install a malicious program onto a USB drive, placing it in a discreet location hoping an unsuspecting person will plug it into their device.
b. a tactic used by cyber criminals by downloading malicious code onto a high-traffic website allowing them to steal personal information from visitors.
c. a cybersecurity tactic where an attacker scares a user into navigating to a harmful website or installing a malicious application onto their device with the intent of stealing personal information such as credentials and passwords.

d. a cybersecurity tactic where an attacker sends out malicious email (or text) designed to trick a user into responding to the email or opening up a link or attachment.

Do:
Post Test
Question 11: Match the following social engineering terms to its description.

I. Phishing
II. Scareware
III. Watering Hole
IV. Baiting

a. a cybersecurity tactic used by an attacker to persuade a user into believing an update, application, extension, or other resources are useful. An attacker may also install a malicious program onto a USB drive, placing it in a discreet location hoping an unsuspecting person will plug it into their device.
b. a tactic used by cyber criminals by downloading malicious code onto a high-traffic website allowing them to steal personal information from visitors.
c. a cybersecurity tactic where an attacker scares a user into navigating to a harmful website or installing a malicious application onto their device with the intent of stealing personal information such as credentials and passwords.
d. a cybersecurity tactic where an attacker sends out malicious email (or text) designed to trick a user into responding to the email or opening up a link or attachment.

12: Identify different types of phishing attacks

Learning Objective 12: Given several emails, the teacher will be able to correctly identify the different types of phishing attacks with 100% accuracy.

Watch: Instructional content of phishing attacks (video)

Do:
Pretest
Question 12: Match the following phishing terms to its description.

I. Spearfishing	a. a type of phishing technique where an attacker targets a specific user that has access to privileged or sensitive information.
II. Whaling	b. a type of phishing technique where an attacker uses the phone to gain sensitive information from the user. Also known as vishing.
III. Email Phishing	c. a type of phishing technique where an attacker targets a specific user into sharing his/her information and credentials.
IV. Voice Phising	d. a cybersecurity tactic where an attacker sends out malicious email designed to trick a user into responding to the email or opening up a link or attachment.

Post Test
Question 12: Match the following phishing terms to its description.

V. Spearfishing	e. a type of phishing technique where an attacker targets a specific user that has access to privileged or sensitive information.
VI. Whaling	f. a type of phishing technique where an attacker uses the phone to gain sensitive information from the user. Also known as vishing.
VII. Email Phishing	g. a type of phishing technique where an attacker targets a specific user into sharing his/her information and credentials.
VIII. Voice Phising	h. a cybersecurity tactic where an attacker sends out malicious email designed to trick a user into responding to the email or opening up a link or attachment.

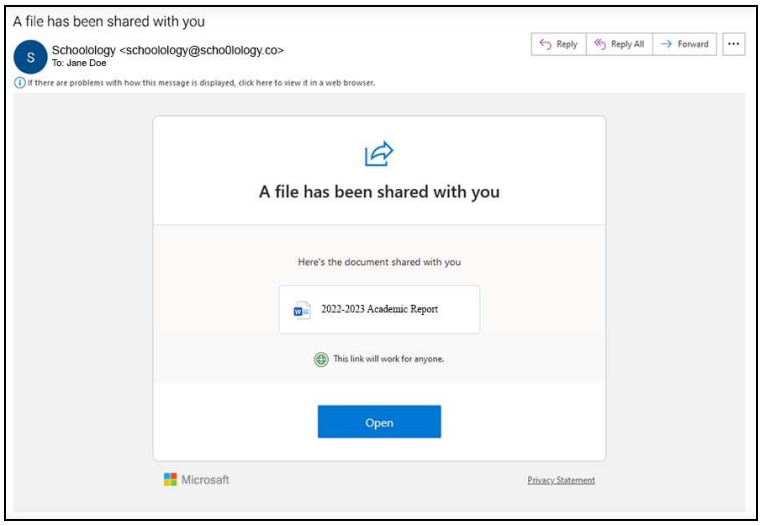
13: Discriminate between a phishing and an authentic email

Learning Objective 13: Given several emails, the teacher will be able to discriminate between a phishing and an authentic email.

Watch: Instructional content of what to look for in phishing emails. (video)

Do:
Pretest
Question 13: Given the following sample emails, which ones could be a phishing email and which ones are legitimate? Write the reason for your answer.

I. Sample #1

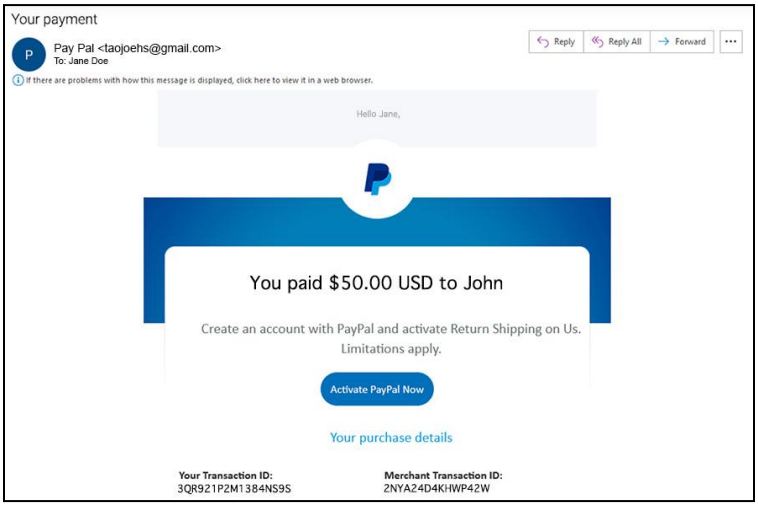


Is this a phishing email or a legitimate email?

a. Phishing
b. Legitimate

Why? Schoology email address reads 'school0gy.' Microsoft is mispelled (Microsaft).

II. Sample #2

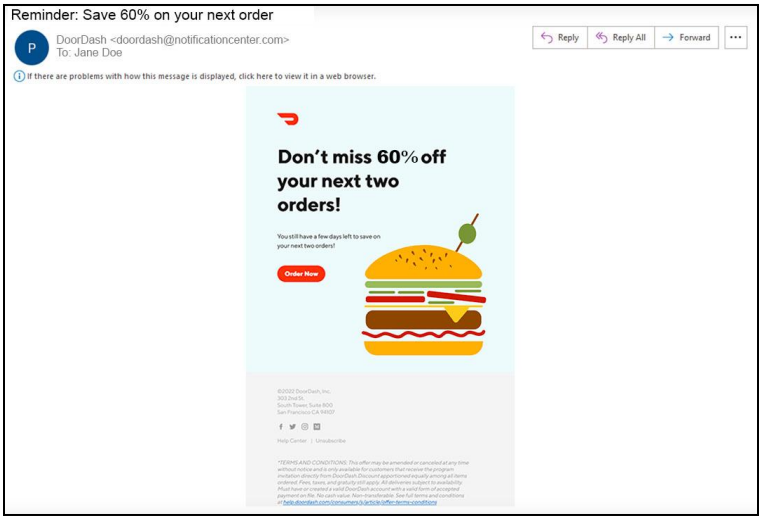


Is this a phishing email or a legitimate email?

a. Phishing
b. Legitimate

Why? Paypal email is ‘gmail.com.’

III. Sample #3

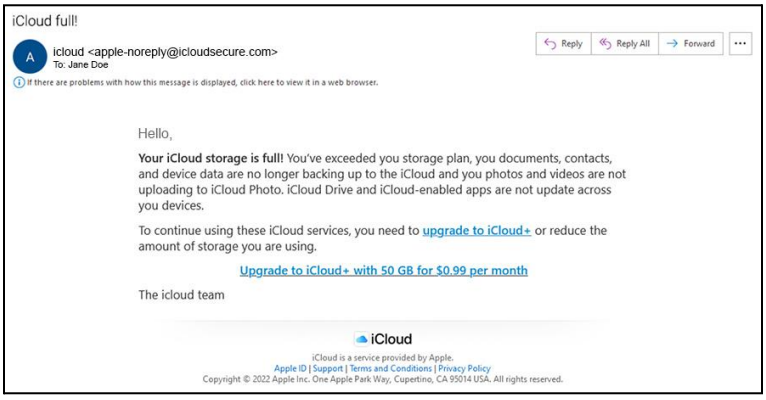


Is this a phishing email or a legitimate email?

a. Phishing
b. Legitimate

Why? Nothing suspicious to note.

IV. Sample #4



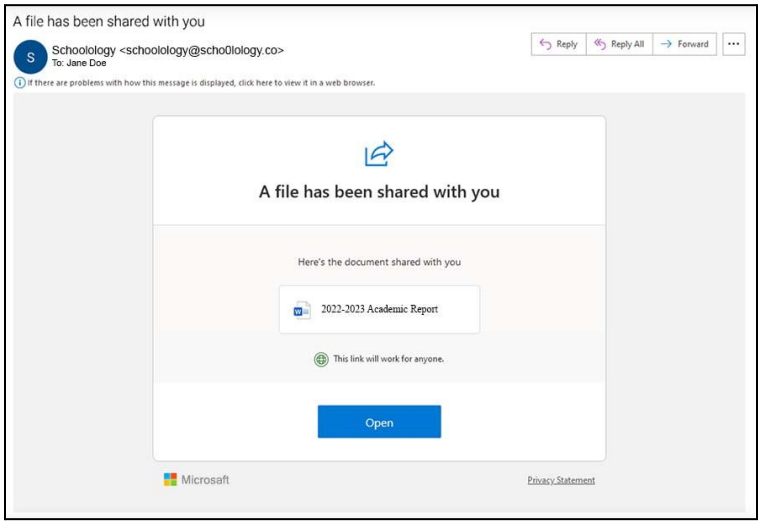
Is this a phishing email or a legitimate email?

a. Phishing
b. Legitimate

Why? No salutation. Spelling and grammar errors.

Do:
Pretest
Question 13: Given the following sample emails, which ones could be a phishing email and which ones are legitimate? Write the reason for your answer.

I. Sample #1

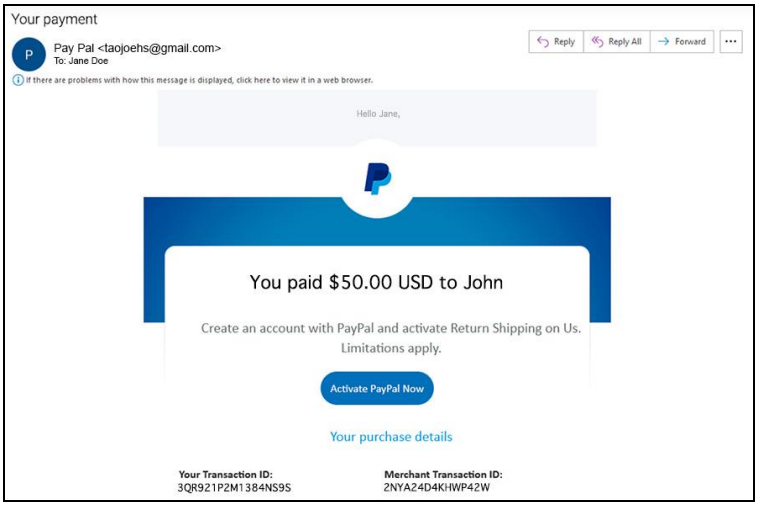


Is this a phishing email or a legitimate email?

c. Phishing
d. Legitimate

Why? Schoology email address reads 'school0gy.' Microsoft is mispelled (Microsaft).

II. Sample #2

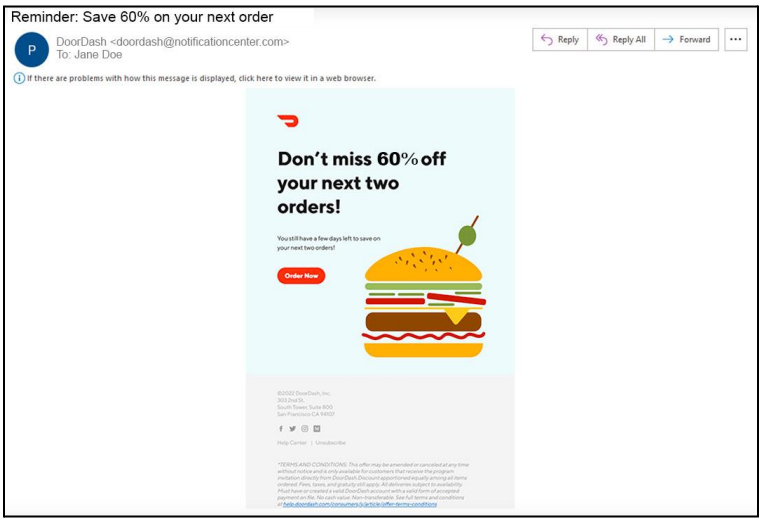


Is this a phishing email or a legitimate email?

c. Phishing
d. Legitimate

Why? Paypal email is ‘gmail.com.’

III. Sample #3

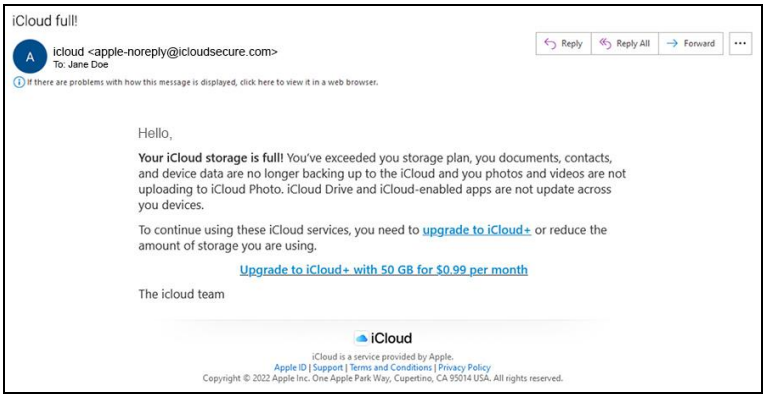


Is this a phishing email or a legitimate email?

c. Phishing
d. Legitimate

Why? Nothing suspicious to note.

IV. Sample #4



Is this a phishing email or a legitimate email?

c. Phishing
d. Legitimate

Why? The greeting doesn't address anyone. Spelling and grammar errors.

14: Evaluate security threats

Learning Objective 14: Given a scenario that describes a cybersecurity threat, the teacher will be able to evaluate the types of threats and their potential.

Watch: Instructional content on evaluating cybersecurity threats. (video)

Do:
Pretest
Question 14: Given the following scenarios, what type of cyber threat is being addressed?

Scenario 1:
Good Afternoon Jane:
This is Principal John. Do you have a minute to talk? Do you have a phone number I can reach you at?

Thank you,
Principal John Doe

This is an example of:

A. Baiting
B. Ransomware
C. Spearfishing
D. None of the above

Scenario 2:
You get the following after downloading an attachment:

This is an example of:

A. Baiting
B. Ransomware
C. Spearfishing
D. None of the above

Scenario 3:
You find a USB drive in your mailbox with a label that reads, “Academic Plan.” You open it and it wipes out your computer.

This is an example of:

A. Baiting
B. Ransomware
C. Spearfishing
D. None of the above

Do:
Post Test
Question 14: Given the following scenarios, what type of cyber threat is being addressed?

Scenario 1:
Good Afternoon Jane:
This is Principal John. Do you have a minute to talk? Do you have a phone number I can reach you at?

Thank you,
Principal John Doe

This is an example of:

A. Baiting
B. Ransomware
C. Spearfishing
D. None of the above

Scenario 2:
You get the following after downloading an attachment:

This is an example of:

E. Baiting

F. Ransomware
G. Spearfishing
H. None of the above

Scenario 3:
You find a USB drive in your mailbox with a label that reads, "Academic Plan." You open it and it wipes out your computer.

This is an example of:

E. Baiting
F. Ransomware
G. Spearfishing
H. None of the above

15: Perform the device protection strategies to avoid data being compromised

Learning Objective 15: Given several cybersecurity threat scenarios, the teacher will be able to perform strategies to help avoid having their device and data compromised.

Do:
Pretest
Question 15: Choose the answer (A, B, or C) that best solves the given scenario.

Scenario 1:
Your co-worker tells you that she will be absent tomorrow and asks you to log into her account with her user-ID and password so you can print out lesson plans for her substitute. What should you do? (Choose all that apply)

A. Ignore the request and tell her you forgot.
B. If your co-worker trusts you, then it's fine.
C. Tell her to share it with your @k12.hi.us account as long as there isn't any personally identifiable information.
D. Decline the request.

Reason: You could do your co-worker a favor by printing it out if it is shared with your @k12.hi.us account. You could also decline the request and tell her that she should not share her user-IDs and passwords with anyone.

Scenario 2:
You receive the following email:

Good Morning!

You are receiving this from the DOE Help Desk. We are currently updating our directory. Please provide us with the following:

*Name (first and last):
*Email Login:
*Password:
*Date of birth:
*Alternate email:

Please contact the Help Desk with any questions. Thank you for your immediate attention.

What should you do?

A. It seems like a phishing email to me. Do not respond and forward the message to the Office of Information Technology Services Branch.
B. Forward the email to others.
C. It's from the DOE Help Desk, it's okay to respond with the information.

Reason: This is an example of a phishing email. Do not send login information through email.

Scenario 3:
A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card.

What should you do?

A. Delete it.
B. It's okay to open it because it's from someone you know.

Reason: Emails can be faked. Attachments can contain malicious code or can direct you to a malicious site that could harm your device and access your data.

Scenario 4:
Which of the following passwords is considered the strongest?

A. @#$)*&^%
B. akHGksmLN

C. A2Dc0cE4Evr!
D. Password1

Reason: A strong password should contain at least 12 characters, upper and lowercase letters, numbers, and symbols.

Do:
Post Test
Question 15: Choose the answer(s) that best solves the given scenario.

Scenario 1:
Your co-worker tells you that she will be absent tomorrow and asks you to log into her account with her user-ID and password so you can print out lesson plans for her substitute. What should you do? (Choose all that apply)

A. Ignore the request and tell her you forgot.
B. If your co-worker trusts you, then it's fine.
C. Tell her to share it with your @k12.hi.us account as long as there isn't any personally identifiable information.
D. Decline the request.

Reason: You could do your co-worker a favor by printing it out if it is shared with your @k12.hi.us account. You could also decline the request and tell her that she should not share her user-IDs and passwords with anyone.

Scenario 2:
You receive the following email:

Good Morning!

You are receiving this from the DOE Help Desk. We are currently updating our directory. Please provide us with the following:

*Name (first and last):
*Email Login:
*Password:
*Date of birth:
*Alternate email:

Please contact the Help Desk with any questions. Thank you for your immediate attention.

What should you do?

A. It seems like a phishing email to me. Do not respond and forward the message to the Office of Information Technology Services Branch.
B. Forward the email to others.
C. It's from the DOE Help Desk, it's okay to respond with the information.

Reason: This is an example of a phishing email. Do not send login information through email.

Scenario 3:
A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card.

What should you do?

A. Delete it.
B. It's okay to open it because it's from someone you know.

Reason: Emails can be faked. Attachments can contain malicious code or can direct you to a malicious site that could harm your device and access your data.

Scenario 4:
Which of the following passwords is considered the strongest?

A. @#$)*&^%
B. akHGksmLN
C. A2Dc0cE4Evr!
D. Password1

Reason: A strong password should contain at least 12 characters, upper and lowercase letters, numbers, and symbols.

Appendix K

Participant Post-Survey

1. I found this 'Cybersecurity for Middle School Teachers' training module useful.
    a. Strongly Disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly Agree

2. I found this training module engaging.
    a. Strongly Disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly Agree

3. The videos in the training module provided enough information to feel confident about that lesson's topic.
    a. Strongly Disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly Agree

4. The learning activities (e.g., multiple-choice questions, matching questions, and scenario-based problems) challenged me.
    a. Strongly Disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly Agree

5. After going through the lessons in this module, I am more aware of cybersecurity threats and keeping online data safe.
    a. Strongly Disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly Agree

6. After going through the lessons in this module, I will practice safe online habits to protect online data and devices.
    a. Strongly Disagree
    b. Disagree
    c. Neutral

   d. Agree
   e. Strongly Agree

7. I would recommend this training to all my colleagues.
   a. Strongly Disagree
   b. Disagree
   c. Neutral
   d. Agree
   e. Strongly Agree

8. What were some of the positive experiences you had while going through the training module?

9. What were some of the negative experiences you had while going through this training module?

10. What suggestions could you make to improve the unit if version two was to be created in the future?

11. Any other suggestions or comments you would like to make.