USING OFFLINE ACTIVITIES TO ENHANCE ONLINE CYBERSECURITY EDUCATION

A Thesis

presented to

the Faculty of California Polytechnic State University,

San Luis Obispo

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

Sarah Padlipsky

December 2018

COMMITTEE MEMBERSHIP

TITLE:	Using Offline Activities to Enhance Online Cybersecurity Education
AUTHOR:	Sarah Padlipsky
DATE SUBMITTED:	December 2018
COMMITTEE CHAIR:	Zachary Peterson, Ph.D. Professor of Computer Science
COMMITTEE MEMBER:	Tim Kearns, Ph.D. Professor of Computer Science
COMMITTEE MEMBER:	Aaron Keen, Ph.D. Professor of Computer Science

ABSTRACT

Using Offline Activities to Enhance Online Cybersecurity Education

Sarah Padlipsky

Since the beginning of the 21st century, the United States has experienced the impact of a technological revolution. One effect of this technological revolution is the creation of entirely new careers related to the field of technology, including cybersecurity. Continued growth in the cybersecurity industry means a greater number of jobs will be created, adding to the existing number of jobs that are challenging an under-educated and under-trained workforce. The goal of this thesis is to increase the effectiveness of cybersecurity education. This thesis studies whether an online course in cybersecurity can be enhanced by offline, in-person activities that mirror traditional classroom methods. To validate the research, two groups of high school students participated in an online course with only one group participating in offline activities. The results showed that the group that participated in both the online and offline portions of the course had a higher percentage of student retention, a more positive mindset towards cybersecurity, and an improved performance in the course.

ACKNOWLEDGMENTS

Thanks to:

- My parents and siblings, for their unconditional support.
- CodeHS (Evelyn Hunter and Lea Sloan), for their help and guidance creating the offline activities.
- Andrew Guenther, for uploading this template.

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

Figure Page

Chapter 1

INTRODUCTION

Since the beginning of the 21st century, the United States has experienced the impact of a technological revolution. One effect of this technological revolution is the creation of entirely new careers related to the field of technology, including cybersecurity. The Information Systems Audit Control Association, a nonprofit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. [32] This global shortage is a result of a growing number of cyber attacks forcing companies to spend more on information security measures. Due to this growing demand, on May 11, 2017 the President of the United States issued Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The order states that the United States must "support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace" [17]. The Secretary of Commerce, Secretary of Homeland Security, and Secretary of Education are tasked with assessing the scope and efforts needed to educate and train the American cybersecurity workforce. This includes cybersecurity related education curricula, training, and apprenticeship programs for primary through higher education.

Because of initiatives like Executive Order 13800, many organizations have been created or have shifted their focus to supporting cybersecurity education. One of these organizations is CodeHS. CodeHS is a comprehensive teaching platform for helping schools teach computer science [15]. CodeHS provides a web-based curriculum, teacher tools and resources, and professional development materials. During the 2018-2019 school year they deployed an Introduction to Cybersecurity course for high school students.

The Introduction to Cybersecurity course is the first blended introduction to cybersecurity course for K-12 education. Blended learning is a term increasingly used to describe the way e-learning is being combined with traditional classroom methods and independent study to create a new, hybrid teaching method.

This thesis explores how blended learning compares to online learning when teaching cybersecurity. Offline activities were made to enhance the online CodeHS course. A control group took the online course and the experiment group took both the online course and the offline activities. This study showed that an online course in cybersecurity can be enhanced by offline, in-person activities that mirror traditional classroom methods.

1.1 Paper Overview

Chapter 2 outlines other approaches researchers are taking to teach cybersecurity and other information on online course and computer science attrition rates. Chapter 3 explains the Introduction to Cybersecurity Course including the standards and concepts taught in the offline activities. Chapter 4 details the offline activities created for the research done in this thesis. Chapter 5 explains the methodology of the research. Chapter 6 evaluates the impact of the offline activities on overall understanding and excitement towards cybersecurity. Chapter 7 analyzes the areas where this project can be developed in the future. Lastly, Chapter 8 provides a summary and concluding remarks about this work.

Chapter 2

RELATED WORKS

There are many efforts to improve cybersecurity education at the K-12 level. All of these efforts aim to reduce attrition rates in the computer science field. These efforts include learning through tabletop games, challenge based learning, and online courses. This chapter provides an overview of computer science attrition rates, other cybersecurity education efforts, online course attrition rates, and the effectiveness of blended learning.

2.1 Computer Science Attrition Rates

Producing sufficient numbers of graduates who are prepared for science, technology, engineering, and mathematics (STEM) occupations has become a national priority in the United States. To attain this goal, some policymakers have targeted reducing STEM attrition in college, arguing that retaining more students in STEM fields in college is a low-cost, fast way to produce the STEM professionals that the nation needs.

The Statistical Analysis Report (SAR) presents an examination of students attrition from STEM fields over the course of 6 years in college using data from the 2004-2009 Beginning Postsecondary Students Longitudinal Study and the associated 2009 Postsecondary Education Transcript Study [24]. In the report, STEM includes mathematics; physical sciences; biological/life sciences; computer and information sciences; engineering and engineering technologies; and science technologies. The term "STEM attrition" refers to enrollment choices that result in potential STEM graduates (i.e., undergraduates who declare a STEM major) moving away from STEM fields by switching majors to non-STEM fields or leaving post-secondary education before earning a degree or certificate.

Among bachelors degree students entering STEM fields between 2003 and 2009, 48% had left these fields by Spring 2009. However, the attrition rate for computer science majors was even higher at 59%.

Due to these numbers, there are many efforts to find the cause of the high attrition rates. A joint effort between University of Colorado, University of California Santa Cruz, and University of Texas aimed to identify which environmental and student factors best predict intention to persist in the computer science major [21]. In this study, student-student interaction was the strongest predictor of intention to major. This suggests that those students who were able to develop peer networks within the major were more likely to remain in the major than those who were less able. This finding, though at the major and not the institution level, is consistent with Astins Theory of Student Involvement [20], which argues that students learn more when they are more involved with both the social and the academic environment of their institution.

2.2 Cybersecurity Education Efforts

The following are two efforts to teach cybersecurity at the K-12 level. Both endeavors have a strong emphasis on collaboration between students.

2.2.1 Security through Play

One cybersecurity education effort focuses on the idea of play as a part of security education [30].Zachary Peterson and Mark Gondree at the US Naval Postgraduate School (NPS) and Tamara Denning at the University of Washington (UW) chose tabletop games as a means for teaching cybersecurity because they have many advantages over digital games.

The first advantage that tabletop games have over digital games is that they are accessible. A student can engage with a tabletop game even if they lack knowledge about computers or computer science. Second, tabletop games are social and allow for student interaction. Cybersecurity has an inaccurate reputation for being an anti-social career. A tabletop game, unlike digital games, correctly depicts cybersecurity as an interactive field. The researchers developed two tabletop games: one card game and one board game.

2.2.1.1 [d0x3d!]

[d0x3d!] is a board game developed by Zachary Peterson and Mark Gondree at NPS where players collaborate as white-hat hackers to infiltrate and navigate an adversarial network, retrieve a set of valuable digital assets, and escape [9]. The game forces a discussion of real ideas in network security. Th developers introduce and use appropriate security terminology such as administrators, intrusion detection, and compromise to cause the discussion to be educationally beneficial.

2.2.1.2 Control-Alt-Hack

Control-Alt-Hack is a card game developed by Tamara Denning [4]. Three to six players act as white-hat hackers in a security consulting game. One by one, each player faces various cybersecurity themed challenges with the end goal of becoming the company's next CEO. Control-Alt-Hack is aimed at raising awareness to the diversity of possible attacks and technologies and the potential opportunities within cybersecurity.

2.2.1.3 Assessment of the Tabletop Games

Initial feedback of [d0x3d!] and Control-Alt-Hack has been positive at the high school, undergraduate, and graduate levels [30]. However, formal assessment of tabletop games is difficult. The current state of evaluation needs improvement before it is possible to decide whether a security game can be used as a pedagogical tool. In further research, they hope to determine the effectiveness of tabletop games.

2.2.2 Challenge Based Learning

Another effort to teach cyber security is Challenge-Based Learning. As proposed by Apple, Challenge-Based Learning (CBL) is a multi-disciplinary approach which encourages students to collaborate with their peers, ask questions, develop a deeper understanding of the subject and take actions in solving real-world challenges [34]. It is made to mirror the 21st century workplace.

The graphic in Figure 2.1 shows a break down of the CBL framework. The first step is to identify the big idea. The big idea should be important on a global scale and deep enough to where students can gain the depth of knowledge required for their

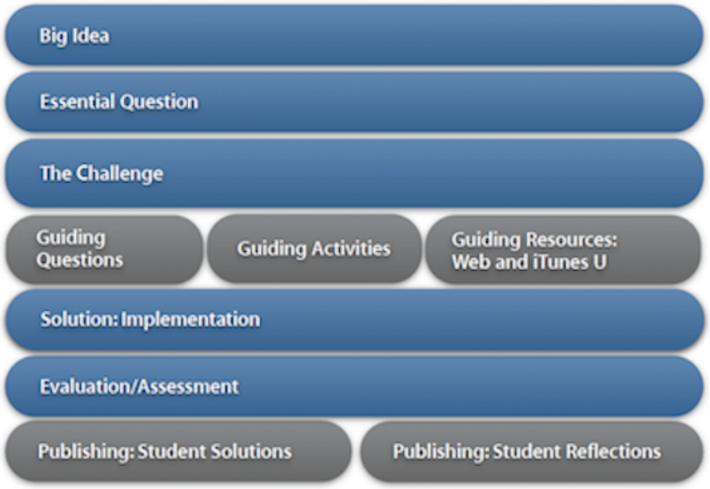


Figure 2.1: Challenge Based Learning Framework as Proposed by Apple

grade level. The next step forces students to identify what they need to know and the resources they need to answer those questions. After generating their questions, students attempt to select a solution through prototyping, experimentation, or other means. Upon deciding on a solution, students fully research, document, and develop that solution and then identify a plan to carry out their implementation. Students then implement their solution and evaluate their success. Lastly, and arguably the most important step, students document their experience and reflect through any medium.

2.2.2.1 CBL Applied to Cybersecurity

Challenge Based Learning has also been applied to the development of cybersecurity skills among high school students. One example is the U.S. Cyber Challenge sponsored by the Center for Strategic and International Studies (CSIS), the SANS Institute, the U.S. Department of Defense (DoD), universities, and private industrial firms. The U.S. Cyber Challenge is both a national cybersecurity talent search and skills development program. High school students compete online in a competition where they learn how to control computer networks and defend computer systems from cyber threats and hackers.

Another example of CBL applied to Cybersecurity Education was constructed at the University of Massachusetts [25]. The students in this study participated in two cybersecurity competitions against their peers. These real-world simulations forced them to work together, think for themselves, and apply their knowledge to defend against cyber attacks. Assessments performed after the two competitions showed an increase in students' computer security skills and interests. As the CBL framework requires, the students also reflected on their experience in presentations to their classmates. These presentations further reinforced the new knowledge the students had gained.

2.2.2.2 Assessment of CBL

Similar to tabletop games, assessment of the CBL Framework is difficult. Assessment currently shows that the CBL framework successfully improves students' computer skills, security knowledge, and interest in cybersecurity. However, it is still undetermined whether Challenge Based Learning can be used in totality as a pedagogical tool due to the lack of evaluation on this framework.

2.3 Online Cybersecurity Courses

Though online computer science courses are abundant, few organizations have created online cybersecurity courses. Most online cybersecurity courses that exist are for students that have already graduated high school. One of the most well-known education technology companies focused on K-12 education is Code.org [3]. Code.org is a non-profit dedicated to expanding access to computer science and increasing participation by women and underrepresented minorities. Code.org is the owner and organizer of the annual Hour of Code campaign which has engaged 10% of all students in the world and provides the leading curriculum for K-12 computer science in the largest school districts in the United States. Code.org provides courses for all ages including fundamental courses for middle and high school, and critical thinking courses for elementary students. However, while Code.org currently follows and helps create the Computer Science Teachers Association K-12 Computer Science Standards, Code.org does not currently mention cybersecurity in any of their online courses. This shows that one of the leading companies in computer science education is lacking this fundamental course.

2.3.1 Online Course Attrition Rates

While online courses are a quick way to reach a larger audience, it is important to consider the attrition rates of online courses. The Distance Education Enrollment Report 2017 reported that 29.7% of all students in higher education are taking at least one distance education course [19]. However, online courses have a 10% to 20% higher failed retention rate than traditional classroom environments [31]. This means that 40% to 80% of online students drop out of online classes [37].

A literature review about retention in online courses recommends one solution to lower the online course attrition rate [22]. The suggestion is to create ways for students to collaborate. Moallem [28] studied the impact of applying an interactive design model for creating an online course that was more structured for collaborative activities, and consequently more amenable to online learning. The results of the study indicated that having cohesive and structured tasks, influences positive interactivity and interaction among students in an online course. By having focused exercises for students to do together, students will have an opportunity to develop peer networks, and ultimately stay enrolled in the course.

2.3.2 Effectiveness of Online and Blended Learning

Due to the high attrition rates of online courses, a lot of research has been done on studying the effectiveness of blended education. An empirical study was done by SRI International [13], an independent, nonprofit research center, to produce a statistical synthesis of studies contrasting learning outcomes for either fully online or blended learning conditions with those of face-to-face classroom instruction [33]. The analysis was conducted using 45 different studies contrasting a fully or partially online condition with a fully face-to-face instructional condition.

The analysis found that, on average, students in online learning conditions performed modestly better than those receiving face-to-face instruction. The advantage over face-to-face classes was significant in those studies contrasting blended learning with traditional face-to-face instruction but not in those studies contrasting purely online with face-to-face conditions. The study mentioned that studies using blended learning tend to involve additional learning time, instructional resources, and course elements that encourage interaction among learners. It was unknown whether one or all of these contributed to the positive outcome for blending learning.

2.3.3 CodeHS Cybersecurity Course

The CodeHS Introduction to Cybersecurity course is another effort to improve cybersecurity education. The Introduction to Cybersecurity course will enhance research on online courses by determining whether an online course can be enhanced through offline activities. The offline activities aim to improve online course attrition rates by adding collaboration between students and additional learning time to mimic the research done on online courses and computer science education.

Chapter 3

CODEHS INTRODUCTION TO CYBERSECURITY COURSE

The Introduction to Cybersecurity provided by CodeHS is the first online blended K12 cybersecurity course [7]. The course is designed for students with some exposure to computer science, but there are no specific course prerequisites. The goal for the course is to prepare students with crucial skills to be responsible citizens in a digital future.

In summary, this section will discuss the Cybersecurity K-12 standards, an overview of the Introduction to Cybersecurity course, and background on cybersecurity topics taught in the offline activities.

3.1 Standards Based Curriculum

Curriculum that is developed by looking at the standards is known as Standards-Based Curriculum. The curriculum should include all knowledge, skills, and learning experiences provided to students within the school program. Standards-based curriculum requires those developing the curriculum to look first at what they want students to accomplish before identifying activities that will help students attain those goals.

There are multiple standards for Computer Science K-12 education because there are many varied opinions about what computer science concepts are most important for the K-12 level. Most Computer Science curriculum pulls from different standards to ensure they are teaching all important concepts. CodeHS follows the CSTA K-12 Computer Science Standards [36] and International Society for Technology in Education (ISTE) [29]. In October 2018, ISTE announced a new initiative called Computational Thinking Standards for All Educators (CT) that represents the first-ever approach to correlate and align the ISTE Standards for Educators, the K12 Computer Science Framework and the Computer Science Teachers Association (CSTA) standards for students [11]. Since the CT Standards were not published by the time the CodeHS Introduction to Cybersecurity course was complete, this thesis focused on using the separate initiatives of the CSTA Standards and ISTE to introduce appropriate concepts to students.

3.1.1 CSTA Standards

Computer Science Teachers Association (CSTA) is a professional association that supports and encourages education in the field of computer science [36]. The CSTA publishes a set of recommended Computer Science Standards for Kindergarten through high school that is created through the core concepts provided by the K-12 Computer Science Framework. The K-12 Computer Science Framework is a "high-level guide for states, districts, and organizations implementing computer science education. Rather than an exhaustive list of computer science topics, the framework represents the essential ideas in computer science for all students" [26]. Utilizing the framework as a guide, the CSTA Standards represents the standards that allow students to master the concepts presented in the K-12 Computer Science Framework.

The CSTA standards are broken up into five different groups: Grades K-2, 3-5, 6-8, 9-10, and 11-12. Recently, the CSTA standards have been expanded to include cybersecurity guidelines. Some examples of the cybersecurity standards include:

- 2-NI-06 - Apply multiple methods of encryption to model the secure transmission of information.

- 3A-NI-08 - Explain trade-offs when selecting and implementing cybersecurity recommendations.

As shown, the standards are given a five or six digit code. The first part determines the age group the standard applies to. For example, 2 is for Grades 6-8, 3A is for grades 9-10, and 3B is for 11-12. The second part of the code applies to the concept category. The concepts include Computing Systems (CS), Networks and the Internet (NI), Data and Analysis (DA), Algorithms and Programming (AP), and Impacts of Computing (IC). The third part is the unique identifier for that standard for a certain age group and concept category.

Since there aren't any national standards, the CSTA Standards provide a guideline in developing K-12 Computer Science curriculum.

3.1.2 International Society for Technology in Education Computer Science Standards

The International Society for Technology in Education (ISTE) Computer Science Standards are a framework for students, administrators, coaches and computer science educators to rethink education and create innovative learning environments [29]. The standards are helping educators worldwide re-invent schools and classrooms for digital age learning.

The ISTE Computer Science Standards are designed to work with a number of learning models and are affiliated with project-based learning, blended learning, and the flipped classroom model. These standards delineate a core set of learning objectives designed to provide the foundation for a complete computer science curriculum.

The ISTE Computer Science Standards contain seven standards:

I. Empowered Learner - Students take an active part in their education. To fulfill this standard, students need to be proficient in learning goals and be able to demonstrate their capability.

II. Digital Citizen - Students are good digital citizens. This means understanding the rights and responsibilities that come with using modern technology by acting ethically, legally, and safely online.

III. Knowledge Constructor - Students understand and contextualize information online. They need to know what reliable information looks like and where they can find it.

IV. Innovative Designer - Students grasp the basics of problem-solving. This requires students to be able to answer open-ended problems, support their design, and refine those designs for the best possible solutions.

V. Computational Thinker - Students must be able to create and employ strategies for solving problems that use technology. This encourages students to break problems down into parts to better understand an issue.

VI. Creative Communicator - Students can express themselves clearly and concisely through digital media.

VII. Global Collaborator - Students understand how their viewpoints are different from others' and work together to achieve a common goal.

CodeHS aligns to and supports the vision of the ISTE Computer Science Student Standards.

3.2 CodeHS Course Overview

The CodeHS Introduction to Cybersecurity is a web-based curriculum made up of a series of learning modules that cover the fundamentals of cybersecurity [7]. The modules are:

I. What is Cybersecurity? - Students are introduced to cybersecurity. They learn why cybersecurity is important, recent threats to cybersecurity, and different careers in the field.

II. Digital Citizenship and Cyber Hygiene - Students learn Internet etiquette and how to keep themselves safe on the world wide web. Students gain an awareness of the potential effects of their digital footprint, how to protect their information from online risks, and the implications of cyberbullying. Students will also learn how to find and cite quality resources online.

III. Software Security - Students learn what happens when you run a program and how to look inside web apps using developer tools, source code, and more. Students learn about common attacks and recommend solutions for flawed security systems.

IV. The ABCs of Cryptography - Students learn about the history of cryptography systems, the motivation behind using encryption systems, and basic cryptography systems. Students learn how to use cryptography, cryptology, and cryptanalysis to decode a message without the use of a key.

V. Networking Fundamentals - Students learn how the Internet connects computers all over the world. They learn about basic networking protocols, practical networking, and how networks are secured. Students learn about network hacking and the ethics and legality of hacking.

Each module is made up of short video tutorials, example programs, quizzes, programming exercises, challenge problems, and unit tests. Offline activities, like the material made for this thesis, are used to enhance the key concepts away from the computer. To see more information about the course, see Appendix A for the full course Syllabus.

3.3 Cybersecurity Concepts in Offline Activities

The offline activities cover a plethora of topics taught in this course. This section will detail two of the concepts taught in the offline activities that are not widely known: The CIA Triad and Caesar Cipher.

3.3.1 CIA Triad

Confidentiality, integrity and availability, also known as the CIA triad, are considered the three most crucial components of security. It is these three principles that are often exploited by various attacks [16].

Confidentiality is almost equivalent to privacy. Confidentiality ensures that sensitive information can not reach the wrong people, while making sure that the right people can access the sensitive information. An example of confidentiality is an account number or routing number when banking online.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data. This ensures that data can not be changed in transit and that unauthorized people cannot alter the data. Examples of this include file permissions and user access controls.

Availability is the assurance that systems and data are accessible by authorized users when and where needed. It is implemented using methods such as hardware maintenance and software patching.

3.3.2 Caesar Cipher

Encryption is used to support one of the three principles in the CIA Triad, confidentiality. Encryption is a way to send a message as a secret code. The only person who can decode the message is the person who knows the key. The key is how the message was changed. To anyone without the key, the message looks like a random series of characters.

The oldest and simplest form of encrypting a message is known as the Caesar Cipher, or the shift cipher [2]. The Caesar Cipher is a type of substitution encryption where each letter in the original message is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.

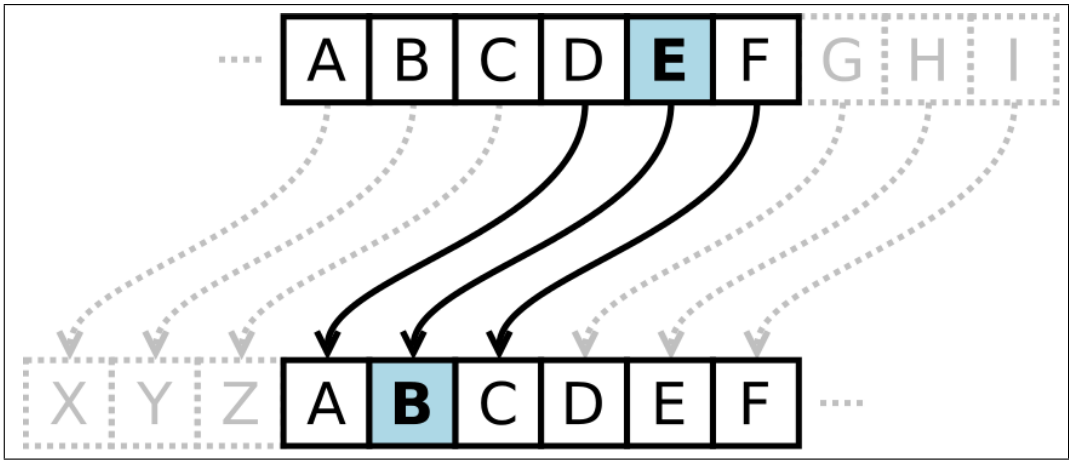


Figure 3.1: Caesar Cipher Example

For each letter of the alphabet, you would take its position in the alphabet and shift it by the key. As Figure 3.1 shows, if the original message was E and the shift was

-3. The encrypted message, as shown below, would be B.

Chapter 4

OFFLINE ACTIVITIES

4.1 What is an offline activity?

CodeHS provides offline activities with their online courses to cover key concepts away from the computer to facilitate blended learning. Blended learning means integrating face-to-face activities with online instruction. These face-to-face activities, called Offline Activities, are collaborative classroom activities that teachers can lead to reinforce concepts and principles learned throughout the curriculum. CodeHS courses come with offline handouts and activities to help teachers run a successful blended classroom that works for all learners.

4.1.1 Offline Activity Structure

Every Offline Activity is structured the same way to allow them to be easily integrated in the lesson plans. Each handout comes with a student version and a teacher version to help the teacher prepare for the activity. The handouts can either be downloaded to edit or printed directly from the website.

Every student handout has the same sections: Corresponding Material, Discussion, Examples, and Class Exercise. Corresponding Material details which section of the course the activity corresponds to. This allows students to be able to reference the course material if they get stuck on the activity. Discussion reminds students of the key concepts that they should know in order to complete this activity. It also may provide some questions to the instructor that can be used to lead a classroom discussion. Examples and Class Exercise contain the work the student should complete. Examples are to be done as a class to illustrate to the students how the Class Exercise should be completed.

The teacher version of the Offline Activity also has a section called Further Discussion. The purpose of this section is to give the teacher background as to why this activity is important and how this activity was intended to be completed (as a class, individually etc.). Teacher handouts also include answers and explanations to all of the exercises that are on the student handout.

4.1.2 Topic Selection

The Offline Activities are meant to be additional resources for the teacher to use, but not essential for understanding of the material. For this reason, we were selective with the Offline Activities we wanted to develop to enforce specific, important concepts.

CodeHS consulted the CSTA K-12 Computer Science Standards and the ISTE Computer Science Standards to create a list of learning objectives they wanted students to achieve through this course. Through these learning objectives, we selected six offline activities that matched up with the goals of the course.

4.2 CodeHS Offline Activities

The Offline Activities that were developed are CIA Triad, Digital Footprint, Do the Right Thing, I've Been Phished, Internet Scavenger Hunt, and Xjhwjy Rjxxflj - Secret Message. The teacher versions of these activities are all included in the Appendix.

CodeHS also made additional Offline Activities to enhance the learning objectives.

These included Create a Privacy Policy, Copyright Licenses, Passing Notes, Telephone Game, Modulo Math, View Page Source Scavenger Hunt, SQL Injection Testing, Establish Firewall Rules, and Reading Logs. For the purpose of this thesis, we will only discuss the activities developedDifital for this thesis.

4.2.1 CIA Triad

The CIA Triad Offline Activity, reinforces the three pillars of the CIA Triad: Confidentiality, Integrity, and Authenticity as shown in Appendix B. It allows students to practice thinking about how the CIA Triad is applied in real-world scenarios. The CIA Triad is a concept that will be applied in every section of the course. Students are first introduced to The CIA Triad in What is Cybersecurity?: CIA Triad in the course.

4.2.1.1 Standards

This activity was selected because it lines up with the CTSA Standards for Grades 6-12:

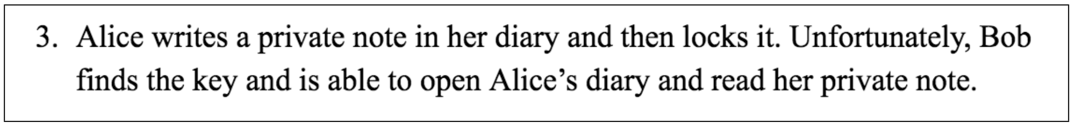
- 3A-NI-08 - Explain trade-offs when selecting and implementing cybersecurity recommendations.
- 3A-NI-06 - Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

These standards detail that students should be able to advocate for security measures given a situation. In order for students to be able to accurately recommend a security measure, they must understand the CIA Triad. CodeHS details that in the following learning objectives for the course:

- Students will be able to (SWBAT) define and apply the CIA triad to well known organizations and networks.
- SWBAT describe the three pillars of securing information and trade-offs between them.

4.2.1.2 Class Exercise

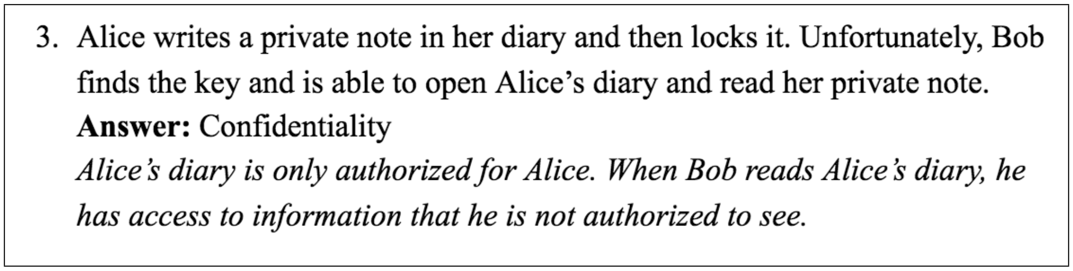
The CIA Triad Offline Activity explains eight real world scenarios and asks the student to determine which pillar of the CIA Triad has been compromised in each one. Teachers are advised to have students work on this activity alone or in small groups and then discuss the answers as a class.



3. Alice writes a private note in her diary and then locks it. Unfortunately, Bob finds the key and is able to open Alice's diary and read her private note.

Figure 4.1: Student Version: CIA Triad Question 3

Figure 4.1 shows Question 3 on the CIA Triad Student Handout. The students are also given a blank space to write whether the scenario presents a breach of confidentiality, integrity, or authenticity.



3. Alice writes a private note in her diary and then locks it. Unfortunately, Bob finds the key and is able to open Alice's diary and read her private note.
Answer: Confidentiality
Alice's diary is only authorized for Alice. When Bob reads Alice's diary, he has access to information that he is not authorized to see.

Figure 4.2: Teacher Version: CIA Triad Handout Question 3

Figure 4.2 shows Question 3 on the CIA Triad Teacher Handout. The teacher handout displays both the question as well as the answer and explanation. This allows the teacher to be able to lead a classroom discussion about the questions and explain why an answer is correct.

As Figure 4.2 explains, since Alice's diary is only authorized for Alice, Bob should not be able to read Alice's diary. Therefore, this is a breach of confidentiality since Bob has access to information that he is not authorized to see.

4.2.2 Digital Footprint

The Digital Footprint Offline Activity is intended to encourage students to think about their digital footprint as shown in Appendix C. College admission committees and future job employers now consider applicants' social media before choosing whether to hire someone. Since the CodeHS cybersecurity course is intended for upperclassmen in high school, it is important for students to consider what reputation they are presenting online.

Teachers are advised to start the discussion by asking students to think about what they would like to do after high school. It is encouraged to have students write down their answer or share it with the class. This exercise can then be done as an in-class activity or as homework. Online reputation is discussed in Digital Citizenship and Cyber Hygiene: Digital Footprint and Reputation.

4.2.2.1 Standards

This activity was selected because it lined up with one of the standards of the International Society for Technology in Education (ISTE) K-12 Computer Science Standards [29], Digital Citizenship.

ISTE states that Digital Citizenship means that students should be able to "recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and act and model in ways that are safe, legal and ethical" [29]. More specifically, Standard 2a states that students should be able to "cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world." By having students think about their digital footprint, students can reflect on their online reputation and learn better ways to remain safe and ethical online.

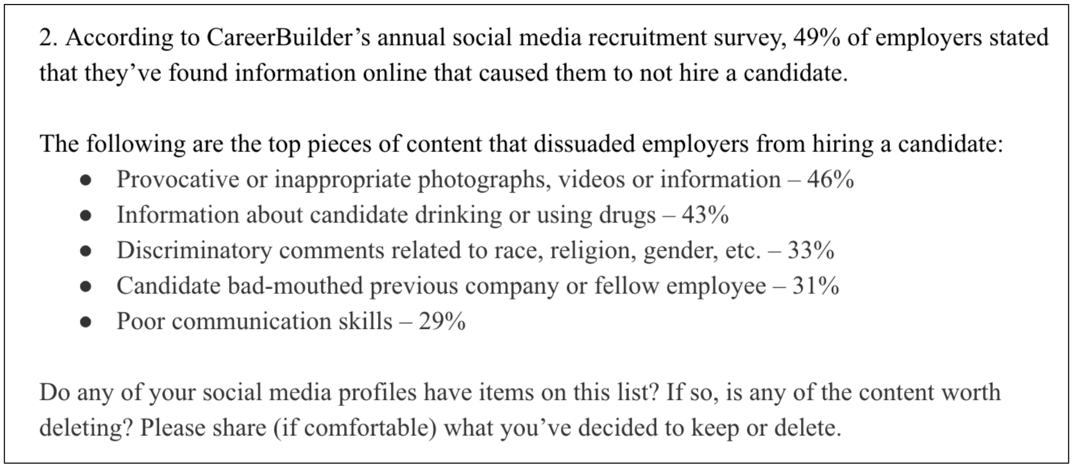
CodeHS created two learning objectives for the course to follow these standards:

- SWBAT reflect on how what they share online will impact themselves and others.
- SWBAT explain the permanence of their digital footprint, and learn to protect their own privacy and respect others privacy.

4.2.2.2 Class Exercise

The Digital Footprint Offline Activity walks students through thinking about their own online reputation and creating a plan to improve their social media presence if necessary.

The activity is split into two sections. The first section walks students through reviewing their online reputation. Students are asked to search their own name on Google and see what information is displayed about them. The handout also explains findings in a survey done by Career Builder [23]. Career Builder's survey determined that over 70% of employers use social media to screen candidates. By using Career Builder's survey, students are introduced to research done by a company other than CodeHS to show how important their online reputation is for their future.



2. According to CareerBuilder's annual social media recruitment survey, 49% of employers stated that they've found information online that caused them to not hire a candidate.

The following are the top pieces of content that dissuaded employers from hiring a candidate:

- Provocative or inappropriate photographs, videos or information – 46%
- Information about candidate drinking or using drugs – 43%
- Discriminatory comments related to race, religion, gender, etc. – 33%
- Candidate bad-mouthed previous company or fellow employee – 31%
- Poor communication skills – 29%

Do any of your social media profiles have items on this list? If so, is any of the content worth deleting? Please share (if comfortable) what you've decided to keep or delete.

Figure 4.3: Digital Footprint Question 2

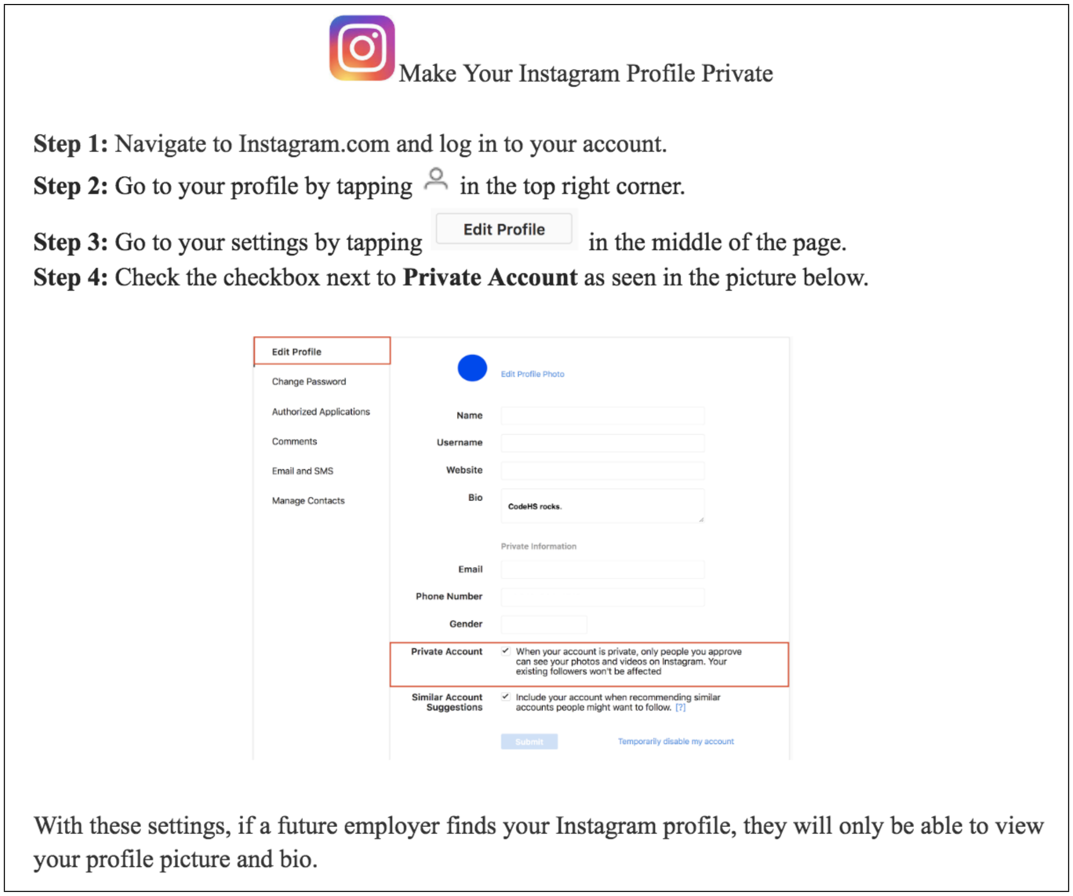
Figure 4.3 shows Question 2 on the Digital Footprint Offline Activity. The question highlights the social media content the survey found to be harmful when applying for a job. After providing factual information to the students, the activity asks students to actively think and change their online presence.

The second part of the activity provides tutorials on how to make accounts on popular social media websites private. The tutorials include Facebook, Twitter, and Instagram and then challenges students to find online tutorials for other social media websites they use.

Figure 4.4 shows one of the tutorials that details how to make an Instagram profile private. The activity convinces students to improve their online presence instead of privatizing it. However, if students think that is the smartest choice, resources have been supplied so they can do so.

4.2.3 Do the Right Thing

The Do the Right Thing Offline Activity educates students on cyberbullying and tools to handle the situation if faced with it. Due to the sensitive nature of the material, it



Make Your Instagram Profile Private

Step 1: Navigate to Instagram.com and log in to your account.
Step 2: Go to your profile by tapping in the top right corner.
Step 3: Go to your settings by tapping Edit Profile in the middle of the page.
Step 4: Check the checkbox next to **Private Account** as seen in the picture below.

Name

Username

Website

Bio: CodeHS rocks.

Private Information

Email

Phone Number

Gender

Private Account ☑ When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected

Similar Account Suggestions ☑ Include your account when recommending similar accounts people might want to follow. [?]

With these settings, if a future employer finds your Instagram profile, they will only be able to view your profile picture and bio.

Figure 4.4: Digital Footprint Instagram Tutorial

is recommended that teachers review the material ahead of time and lead the activity as a classroom discussion to mediate the conversation. The full activity is included in Appendix D and discussed in Digital Citizenship and Cyber Hygiene: Cyberbullying.

4.2.3.1 Standards

Though this activity lines up with standards and learning objectives, Do The Right Thing was created to help fight the growing cyberbullying problem. i-SAFE Inc., a non-profit foundation whose mission is to educate and empower youth to make their Internet experiences safe and responsible, conducted a survey on 1,500 students grades 4-8 [6]. They found that 42% of kids have been bullied online and 53% of kids admit to having said something mean or hurtful to another person online. Another anti-bullying organization, StopBullying.gov, provides information from various government agencies on what bullying is, what cyberbullying is, who is at risk, and how you can prevent and respond to bullying [14]. They reported that 15% of high school students (grades 9-12) were electronically bullied in the past year.

Both studies show a significant amount of students are affected by cyberbullying. In a course that encourages extra time online, it is imperative to focus on positive and healthy behavior.

As discussed previously, ISTE K-12 Computer Science Standards include Digital Citizenship (Standard 2), which mirrors this effort [29]. Standard 2b states that "Students [should] engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices." This standard has two motives. First, students need to think about the effects any cyberbullying they partake in may have on others. Students then also need to consider what to do when faced with cyberbullying both aimed at themselves and at those around them.

CodeHS created two learning objectives for the course to follow this standard:

- SWBAT explain steps to take if they are involved in a cyberbullying situation.
- SWBAT reflect on the impact that cyberbullying can have on individuals and communities

These learning objectives line up with the previously mentioned motives of the ISTE standard.

4.2.3.2 Class Exercise

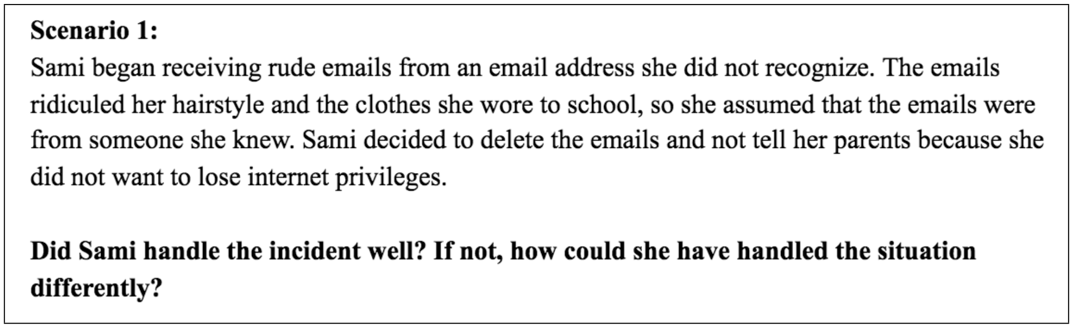
The Do The Right Thing Offline Activity starts by defining cyberbullying. The Discussion then gives tips on what to do if students encounter cyberbullying. This information will hopefully introduce them to new solutions and help them prepare for the activity. The teacher version also provides further discussion questions including:

- What is cyberbullying?
- How is cyberbullying different from other forms of bullying? Why do you think some people bully others online?
- Why do you think it is hard sometimes for someone to speak up when they are being bullied?
- What is one thing you could do today (right now!) to help stop or prevent cyber bullying?

Teachers are instructed to lead a classroom discussion on cyberbullying using these questions. By talking openly about cyberbullying, students will become more comfortable discussing this issue.

The activity then asks students to read a few scenarios in which cyberbullying has occurred. For each scenario, they are asked to discuss with a classmate how well they think the person in each story handled the situation. Students should also reflect on how they might have handled it differently.

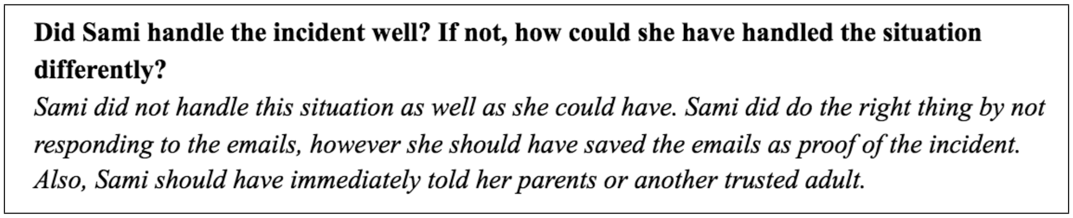
Figure 4.5 shows Scenario 1 as displayed to the students. Using the new options discussed on how to handle cyberbullying, students should brainstorm as a class on how to handle these tough situations better.



Scenario 1:
Sami began receiving rude emails from an email address she did not recognize. The emails ridiculed her hairstyle and the clothes she wore to school, so she assumed that the emails were from someone she knew. Sami decided to delete the emails and not tell her parents because she did not want to lose internet privileges.

Did Sami handle the incident well? If not, how could she have handled the situation differently?

Figure 4.5: Student Version: Do The Right Thing Scenario 1



Did Sami handle the incident well? If not, how could she have handled the situation differently?
Sami did not handle this situation as well as she could have. Sami did do the right thing by not responding to the emails, however she should have saved the emails as proof of the incident. Also, Sami should have immediately told her parents or another trusted adult.

Figure 4.6: Teacher Version: Do The Right Thing Scenario 1

Teachers are also provided with an answer as shown in Figure 4.6. For this example, it is made clear that Sami did not handle the situation well. The answer discusses that though Sami did do the right thing by not responding to the emails, she should have saved them as proof of the incident instead of deleting them and told a trusted adult about the situation. Students' answers may vary, however the provided answer supplies a starting point for the conversation if students cannot come up with answer themselves.

4.2.4 Internet Scavenger Hunt

The Internet Scavenger Hunt Offline Activity is a fun task that allows students to practice their skills in Information Literacy. The full activity is shown in Appendix F. Information Literacy is the set of skills required to identify, retrieve, organize, and analyze information. Since students rarely use an encyclopedia or other books to look up information, it is important to be literate on the Internet. Though the Internet is a quick source to retrieve information, anyone can publish content for others to access. This means that there is a lot of incorrect information to sort through when performing research.

This activity should be done as a competition. Students will race to see who can find the information online first. Teachers are advised to stress the significance of taking time to evaluate the website before treating the information as fact. Information Literacy is discussed in Digital Citizenship and Cyber Hygiene: Information Literacy.

4.2.4.1 Standards

This activity was selected because it lined up with the third ISTE K-12 Computer Science Standards, Knowledge Constructor [29]. ISTE states that Knowledge Constructor means that students should be able to "critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts and make meaningful learning experiences for themselves and others." More specifically, Standard 3b states that "Students [should] evaluate the accuracy, perspective, credibility and relevance of information, media, data or other resources." Furthermore, Standard 3c states that students should be able to "curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions." This activity forces students to search the internet for information, but consider the source for credibility and accuracy prior to coming to a conclusion.

CodeHS created a learning objective for the course to follow this standard:

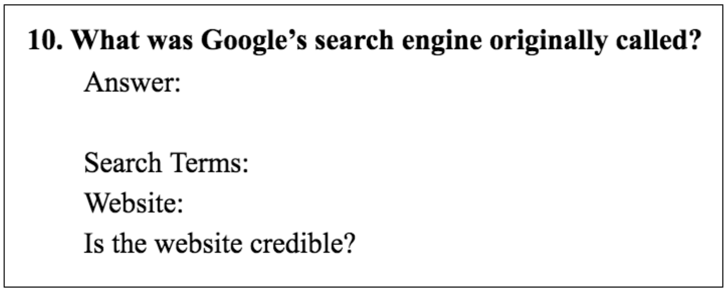
- SWBAT evaluate the quality, credibility and validity of websites and give proper credit.

4.2.4.2 Class Exercise

The Internet Scavenger Hunt Offline Activity starts by defining information literacy. The Discussion then gives tips on what to consider when determining the credibility of a website. Students are advised to consider the following:

- How recently was this article published?
- Are scholarly sources cited?
- Is the site .edu or .gov? If not, who is the author? Is this a credible source?
- Is the site well-designed?
- Does this site follow spelling and grammar rules?

The activity then turns into a scavenger hunt to see who can search the internet and find correct and reliable information the fastest. For each question listed, students must search for the answer using a search engine of their choice. Once they find the answer, they record the answer, what the search terms were, the website in which they found the answer, and a decision of whether or not the website is credible.

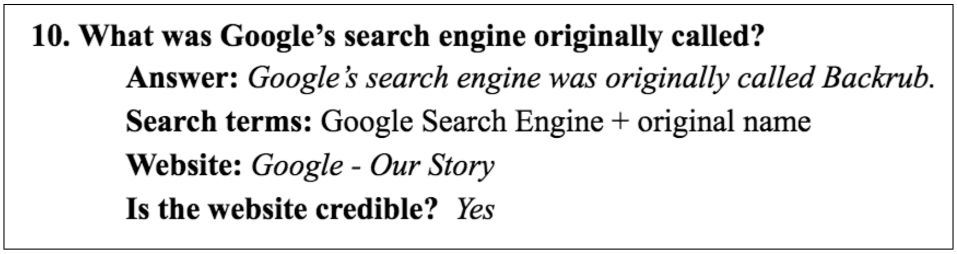


10. What was Google's search engine originally called?
Answer:

Search Terms:
Website:
Is the website credible?

Figure 4.7: Internet Scavenger Hunt Question 1

Figure 4.7 shows Question 10 as displayed to the students. Some questions, such as this one, are computer science related, and others are completely random. Other questions ask “How tall is the Statue of Liberty?”, “What are the high and low temperatures tomorrow in your city tomorrow?” or “Who is the father of computer science?”



10. What was Google’s search engine originally called?

Answer: *Google’s search engine was originally called Backrub.*

Search terms: Google Search Engine + original name

Website: *Google - Our Story*

Is the website credible? *Yes*

Figure 4.8: Internet Scavenger Hunt Teacher Question 1

Figure 4.8 shows Question 10 as displayed to the teachers. Teachers receive one possible solution to each question, though student answers may vary. As shown in 4.8, one possible way to find the original name for Google’s search engine is by searching ”Google Search Engine + original name”. The answer can be found on the credible website Google - Our Story and the answer is Backrub.

4.2.5 I’ve Been Phished

The I’ve Been Phished Offline Activity introduces students to another important internet security concept, phishing. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The goal is to trick the email recipient into believing that the message is something they want or need so that they will click a link or download an attachment.

This activity can be done as an individual worksheet or as a class discussion. Phishing is discussed in Digital Citizenship and Cyber Hygiene: Privacy and Security.

4.2.5.1 Standards

This activity was selected because it lined up with the third ISTE K-12 Computer Science Standard, Knowledge Constructor [29]. Standard 3b states that "Students [should] evaluate the accuracy, perspective, credibility and relevance of information, media, data or other resources." Though the Internet Scavenger Hunt Offline Activity also helps students solidify this standard, this standard can be depicted many different ways. This standard can either describe being able to find credible sources for research purposes, as solidified in The Internet Scavenger Hunt Offline Activity, or for protection against attacks, as mastered in this offline activity.

As stated previously, CodeHS created a learning objective for the course to follow this standard:

- SWBAT evaluate the quality, credibility and validity of websites and give proper credit.

4.2.5.2 Class Exercise

The I've Been Phished Offline Activity reminds students of phishing and what the perpetrator aims to do by phishing another person. Students are advised to identify phishing by looking for:

- Generic greeting - Phishing emails are sent in large quantities in hopes that a percentage of recipients will not realize it is fraudulent. Do a quick check of how the sender addressed you!
- Generic body - Phishing emails normally tend to have a generic body in the email. By keeping the information nonspecific, the internet criminals hope that

the user believes that at least some of the information applies to them. Take a quick moment to assess whether the information is actually about you!

- Incorrect Company Information - Many phishing emails do not send the email from an email address with the correct domain (i.e. from the correct company). Some sender emails will try to trick you by having the correct sub-domain, but not the correct domain (i.e. @am.amazon.com instead of @amazon.com)

- Request for personal information - Companies do not request personal information over email since email is insecure. If an email is asking for personal information, it is most likely a phishing email.

- Sense of urgency - Internet criminals want to get your personal information now so they can move on to another victim. To do this, phishing emails normally make you think that something needs to happen fast to fix the situation. If an email is asking you to act fast, don't! Slow down and assess the situation.

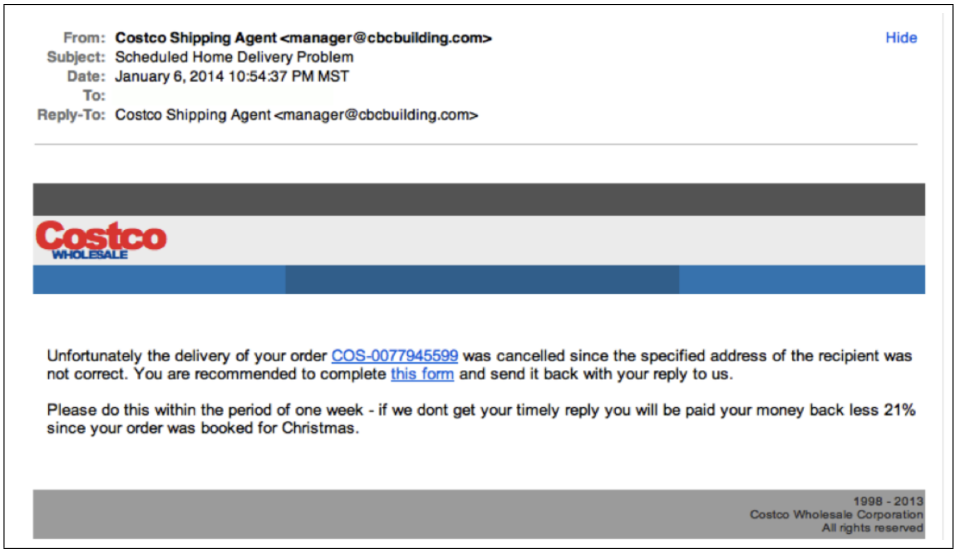
- Poor grammar - An email from a legitimate organization should be well written. Any email with poor grammar should be enough to cause you to pause and evaluate the email.

- Still can not tell? Call the company and ask!

Students are also advised on what to do if they've been phished or if they've fallen for a phish. See Appendix E for advice given to the students.

The activity then asks students to observe 3 different real-world examples of phishing emails. For each example, students explain how they can tell that it is a fraudulent email.

Figure 4.9 shows one example of a Costco real-world phishing attempt. Teachers are



From: **Costco Shipping Agent <manager@cbcbuilding.com>**
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

Figure 4.9: Costco Phishing Example

also provided with notes on how students should notice that this is a phishing attack. For this particular example, these include:

- Generic greeting - This email has a generic greeting and does not address the recipient by name.

- Generic body - This email has a very generic body. It is does not reveal the name of the recipient or any information about the order.

- Incorrect company information - The sender email address is not from a Costco affiliated domain (cbcbuilding). Also, the Costco logo is close to the actual logo, but not quite correct. Look it up!

- Sense of urgency - The email is stating that the user needs to complete a form within one week or a full refund is not possible. Note that the email does not state the actual date that this order will be non-refundable.

- Poor grammar - The grammar in this email is far from professional. A lack of commas and apostrophes should be a warning.

Teachers are provided this list to facilitate student learning as they complete this activity. By the completion of this activity, students should be able to notice emails as fraudulent in the real-world. Hopefully this will save them from falling for any phishing attacks.

4.2.6 Xjhqjy Rjxxflj - Secret Message

The Xjhqjy Rjxxflj - Secret Message Offline Activity enforces the concept of the Caesar Cipher. Through the activity, students will experience how much more difficult and time consuming it is to decode a message that has an encryption scheme applied, even one as simple as the Caesar Cipher. Caesar Cipher is discussed in The ABCs of Cryptography: Basic Crypto Systems - Caesar Cipher. The full activity is shown in Appendix G.

4.2.6.1 Standards

This activity lines up with one of the CTSA Standards for Grades 6-12:

- 2-NI-06 - Apply multiple methods of encryption to model the secure transmission of information.

The CTSA Standards clearly state that encryption should be taught. CodeHS details that in the following learning objectives for the course:

- SWBAT simulate the effect of encrypted and unencrypted personal data in a shared classroom setting
- SWBAT create their own encrypted message using a unique cryptographic key

These standards and learning objectives also connect to those provided about The CIA Triad, as Encryption is one way to provide Confidentiality.

4.2.6.2 Class Exercise

The Xjhqjy Rjxxflj - Secret Message Offline Activity Discussion reminds students of the Caesar Cipher and how to create a decoded message using this encryption method. Teachers are instructed to split the class into groups of 3 and assign each student a letter (A, B, or C). The teachers are also given an example to go over to show how to apply the Caesar Cipher in case students forgot.

Students then complete two tasks as a group of 3. Task 1 is to pass a note without any encryption applied to the note. The steps include:

I. Person A writes a short message on a sheet of paper.

II. Person C intercepts the message as Person A passes it to Person B. As soon as Person C sees the message, write down the start time.

III. Once Person C is done figuring out the message (should not take long), record the stop time and pass the note on to Person B.

IV. Person B decodes the message.

Task 2 is to pass a note with the Caesar Cipher encryption scheme applied to the note. The steps include:

I. Person A and Person B step away from Person C and decide what the shift, or key, is going to be for this message. Examples are +5, -10, +23.

II. Person A writes a short encrypted message on a separate sheet of paper using the caesar cipher.

III. Person C intercepts the message as Person A passes it to Person B. As soon as Person C sees the message, write down the start time.

IV. Once Person C is done figuring out the message, record the stop time and pass the note on to Person B.

V. Person B decodes the message.

Students should notice that Task 2 took a lot more time and effort to complete than Task 1. This will help solidify the importance of encryption in real-world security systems.

Chapter 5

METHODOLOGY

To study whether an online course in cybersecurity is enhanced by offline activities, we surveyed two classrooms of high school students; one class participated in both the online course and the offline activities and the second class participated in just the online course. The surveys revealed how interested students are in cybersecurity and how much information they had gained before and after the course.

The methodology outlined below was evaluated and approved by Cal Poly Institutional Review Board (IRB) [10]. The necessary parental consent forms were signed and collected by all participants and the study follows normal educational practices.

5.1 Participants

Computer science classes from two schools participated in the research for this paper: Mission College Preparatory Catholic High School [12] and Coast Union High School [1].

5.1.1 Coast Union High School

Coast Union High School (Coast Union) is located on the Central Coast of California in the community of Cambria [1]. The school is a traditional 9-12 high school with approximately 250 students enrolled. The District also serves the communities of San Simeon to the north and Cayucos to the south (grades 9-12) as well as surrounding rural areas.

Coast Union High School offers a cyber class to all grades. This course aims to get students interested and involved in technology and computer science. 11 students are enrolled in the course ranging from 9th grade to 12th grade. They meet either two or three times a week for 90 minutes each session.

5.1.2 Mission College Preparatory Catholic High School

Mission College Preparatory Catholic High School (Mission Prep) is a Catholic, coeducational, college-preparatory, secondary school in the Diocese of Monterey, striving to be an extension of family and church [12]. The school serves grades 9-12 with approximately 350 students enrolled. The school is located on the Central Coast of California in the town of San Luis Obispo. Approximately half of the students come from three area Catholic grammar schools, while the other students come from 26 other schools locally, regionally, nationally, and internationally.

Mission Prep offers AP Computer Science Principles to juniors (11th grade) and seniors (12th grade). AP Computer Science Principles introduces students to the foundational concepts of the field and challenges them to explore how computing and technology can impact the world.[18]. 7 students are enrolled in this course: 3 juniors and 4 seniors during the 2018-2019 school year. They meet either two or three times a week for 80 minutes each session.

5.2 Experiment

The research was conducted as A/B Testing. For the purpose of this paper, Group A represents the students from Coast Union High School and Group B represents the students from Mission College Preparatory Catholic High School. Group A participated in the online cybersecurity course and Group B participated in both the online cybersecurity course and the offline activities.

5.2.1 Introduction to Cybersecurity Pilot

The Introduction to Cybersecurity Pilot is a 3 hour subset of the year-long Introduction to Cybersecurity course. The material in The Introduction to Cybersecurity Pilot is the following:

I. What is Cybersecurity? (1 hour)

  A. What is cybersecurity?

  B. Famous Cybersecurity Attacks

  C. Cybersecurity and Autonomous Vehicles

  D. Threat Map

  E. Why learn about cybersecurity?

  F. Impact of cybersecurity

  G. CIA Triad

  H. Offline Activity (Group B): CIA Triad

II. The ABCs of Cryptography (1 hour)

  A. What is cryptography?

  B. History of cyrptography

  C. Why encrypt?

  D. Basic Encryption Systems:

    i. Caesar Cipher

ii. Vigenere Cipher

E. Offline Activity (Group B): Xjhwjy Rjxxflj - Secret Message

III. Other Cybersecurity Topics (1 hour)

A. Data Privacy and Security

i. What is Data Privacy and Security?

ii. Privacy and Security Quiz

iii. How strong is your password?

iv. Offline Activity (Group B): I've Been Phished

B. Information Literacy

i. Information Literacy

ii. Effective Internet Searches

iii. Hero Pig?

iv. Offline Activity (Group B): Internet Scavenger Hunt

5.2.2 Surveys

Before and after the students participated in the pilot course, students took two surveys to track their growth through the course. The Mindset Survey tested the students' interest and excitement towards cybersecurity and computer science. The Knowledge and Skills Survey directly evaluated the students' understanding of the material taught in the course.

5.2.2.1 Mindset Survey

The Mindset Survey was conducted online as part of the course both before and after. The Mindset Survey asked students to rate how much they agree or disagree with the following statements, from 1 (strongly disagree) to 10 (strongly agree). The questions they were asked were:

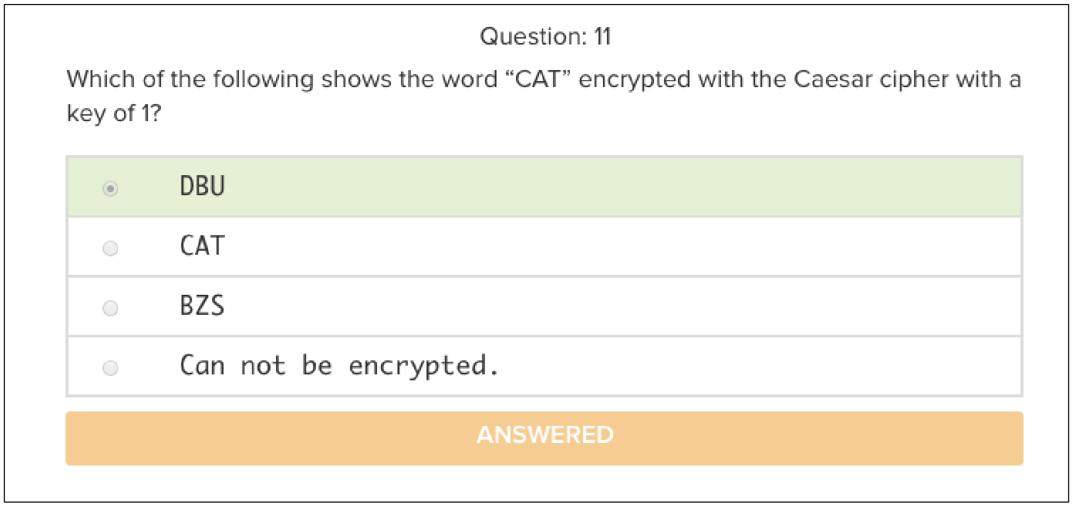
- I think cybersecurity is interesting.
- I am confident I can use computer science to solve problems.
- I hope that I will use coding and computer science in my future career.
- I think computer science is interesting.
- After this class, I hope to take another computer science course.
- I am considering studying computer science in college.

A printed version of this survey can be seen in Appendix H.

5.2.2.2 The Introduction to Cybersecurity Knowledge and Skills Survey

The Introduction to Cybersecurity Knowledge and Skills Survey tested students' understanding of the material taught in the online material and offline activities. This survey was conducted by paper for the pre-test and online for the post-test. A version of this survey is attached in Appendix I.

Students answered 15 questions about the CIA Triad, information literacy, password security, encryption, and more. Figure 5.1 shows an example of a question on both the Pre-Test and Post-Test Knowledge and Skills Survey. Caesar cipher, and all other topics tested in this survey, are taught on both the online platform and in an offline activity. This allows the survey to reveal if the offline activities enhanced student learning.



Question: 11

Which of the following shows the word “CAT” encrypted with the Caesar cipher with a key of 1?

- ● DBU
- ○ CAT
- ○ BZS
- ○ Can not be encrypted.

Figure 5.1: Post-Test Knowledge and Skills Survey Question 11

As shown in Figure 5.1, students are asked to select the correct answer given four choices. After students select their answer for the post-test, they are shown the correct answer.

5.3 Caveats With Experimental Design

There are a few caveats in this experiment to consider when determining the validity of the results. First, the sample size of the two groups is too small to have conclusive results. It was a challenge to find high school computer science classrooms that had more than 10 students. The sample size will provide a proof of concept, however more research will need to be done to solidify the results. Secondly, due to the difficulty of finding large computer science courses, the students from the two groups are from different schools. Therefore, the two groups have different educational backgrounds, live in different areas, and may have other unknown differences.

In this study we recognize that there may be a bias due to the test groups chosen. As a result the data collected in the two surveys is suspect and can not be trusted entirely.

However, efforts were made to create a non-biased results, such as not comparing the two groups directly, but instead comparing each group to themselves before and after taking the course. This allows us to draw some conclusions from the results in an effort to get closer to understanding how cybersecurity can be effectively taught to students.

Chapter 6

RESULTS

In this chapter, we discuss the results gathered from the pilot course which includes three different evaluation measures: student retention, Mindset survey results, and Knowledge and Skills survey results.

6.1 Student Retention Rate

Before discussing the results of the surveys conducted during the course, it is important to discuss student retention over the duration of the course.

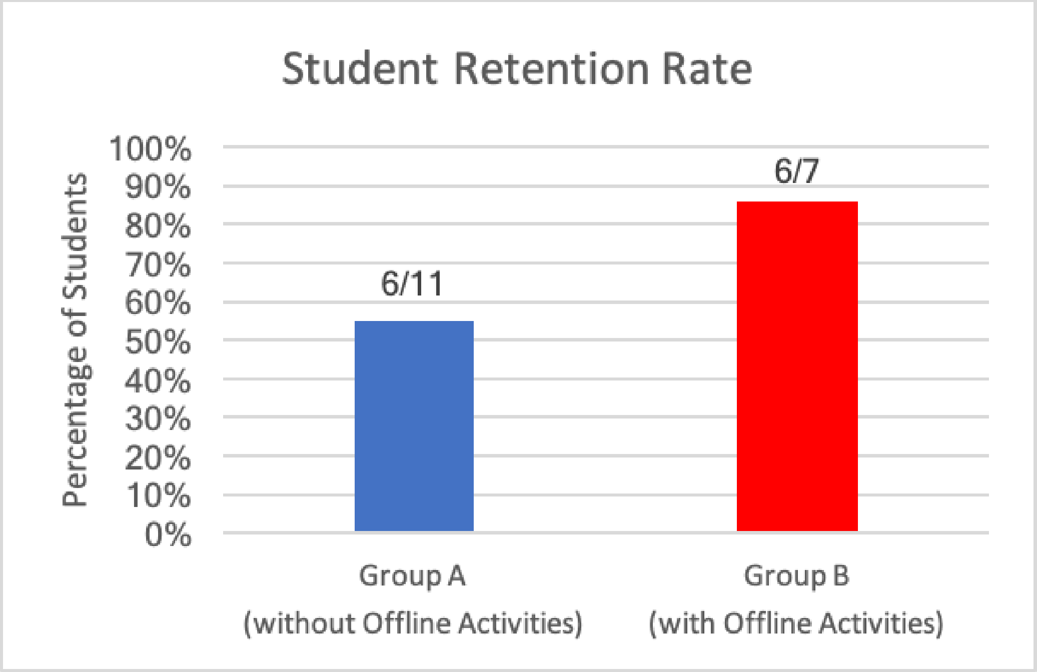


Figure 6.1: Student Retention Rate

Originally, it was expected that all students participating would finish every activity, exercise, and test even though students were voluntarily participating in the course. In reality, Group A initially started with 11 students enrolled in the course, but only 6 students completed the course. Group B started with 7 students in the course and 6 students completed the course entirely. As shown in Figure 6.1, this means that 54.5% of students in Group A and 85.7% of students in Group B finished the course.

As discussed earlier, the retention rates for computer science and online courses are 52% and 20-60% respectively. The retention rates for Group A, were aligned with these numbers at 55%. However, the retention rates were significantly better for students who participated in the offline activities (Group B) at 85.7%.

6.2 Mindset Survey

As discussed earlier, the Mindset Survey tested the students' interest and excitement towards cybersecurity and computer science. Only students who completed the Mindset Survey before and after the course, were included in the data which included 6 students from Group A and 6 students from Group B.

Figure 6.2 shows the improvement on the post-test from the original scores on the post-test for each school, out of 10 points. For example, for Question 3 (Q3), both Group A's and Group B's post-Test average was 0.1667 points higher than the pre-test. As a reminder, the following are the questions as they correspond to the graph:

- **Q1:** I think cybersecurity is interesting.
- **Q2:** I am confident I can use computer science to solve problems.
- **Q3:**I hope that I will use coding and computer science in my future career.
- **Q4:** I think computer science is interesting.

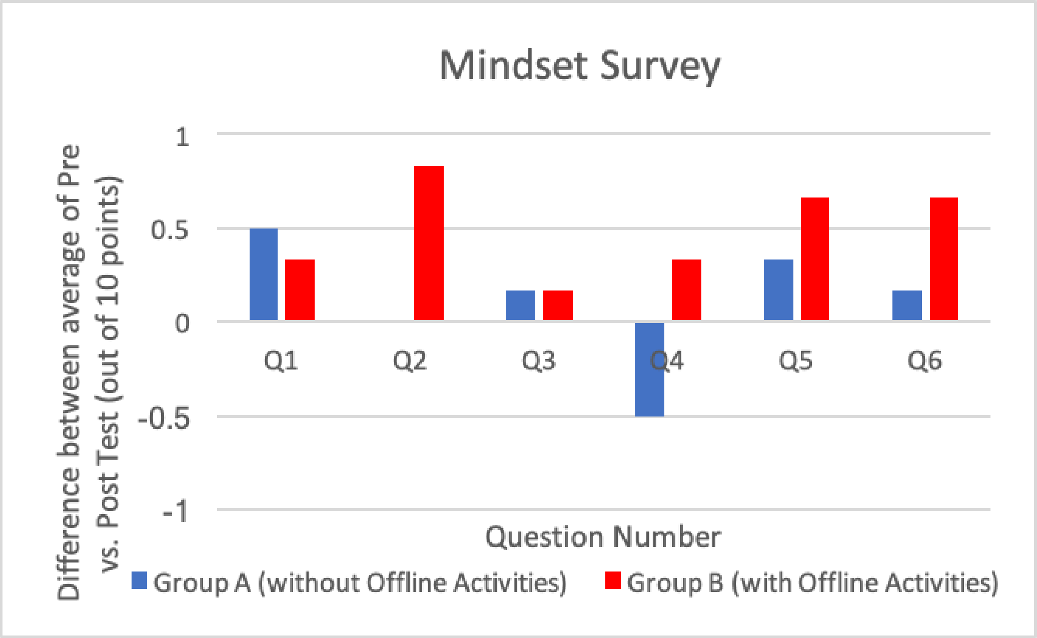


Figure 6.2: Mindset Survey Results By Question

- **Q5:** After this class, I hope to take another computer science course.
- **Q6:** I am considering studying computer science in college.

The Mindset Survey reflected a similar pattern as the retention rates. After being more engaged in the course, Group B's mindset towards computer science and cybersecurity improved more than Group A. Even so, it is important to note that mindset changes in both groups were minimal since neither group improved more than 1 point in any given question, as shown in Figure 6.3. This was expected as the students only engaged in the course for a few hours. It is possible that with the full length course, these numbers would be more dramatic.

6.3 Knowledge and Skills Survey

The Knowledge and Skills Survey evaluated the students' understanding of the material taught in the course. Like the Mindset Survey, only students who completed the

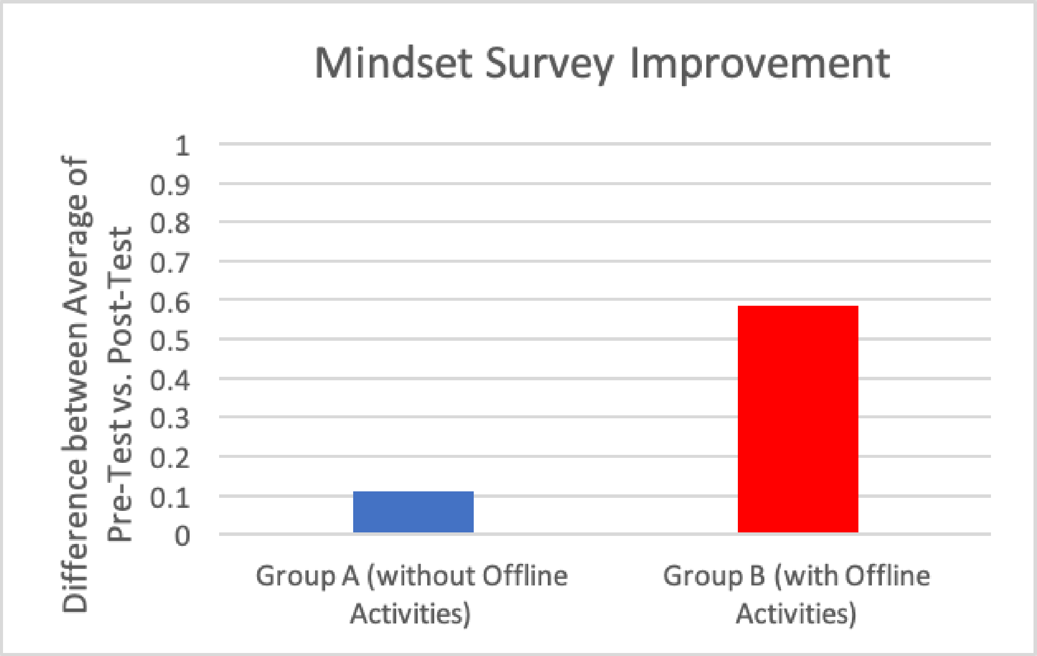


Figure 6.3: Mindset Survey Improvement

Knowledge and Skills Survey before and after the course, were included in the data.

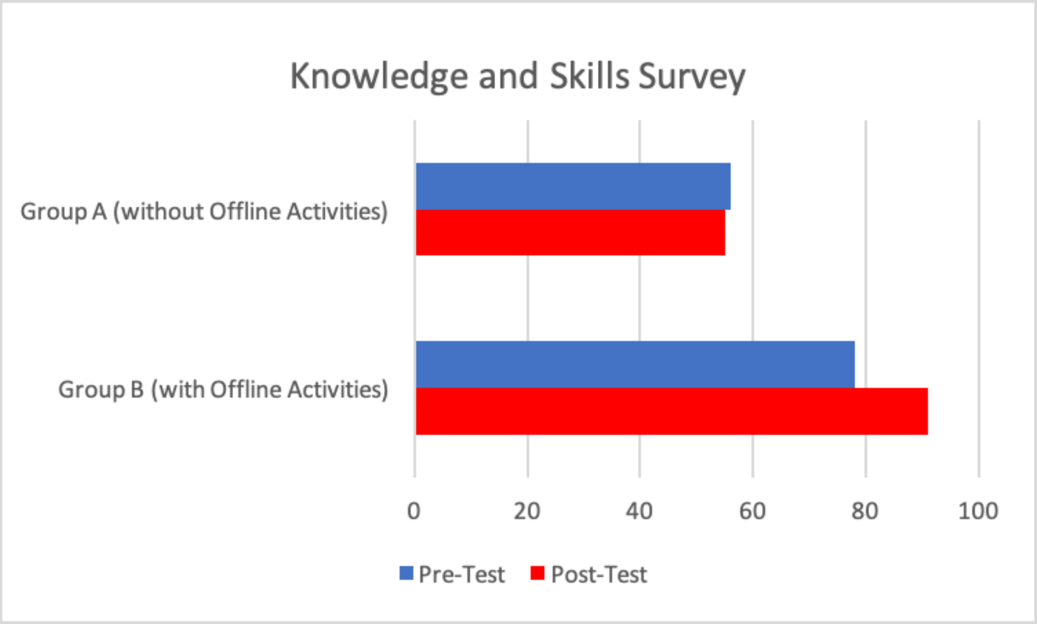


Figure 6.4: Knowledge and Skills Survey Results

Figure 6.4 shows the average of the pre and post-test for each Group. Group A got an average of 56% on the pre-test and 55% on the post-test. Group B got an average of 77.77% on the pre-test and 91.11% on the post-test. More explicitly, Figure 6.5 shows that Group A's average decreased by 1% and Group B's average improved by 13.34%.

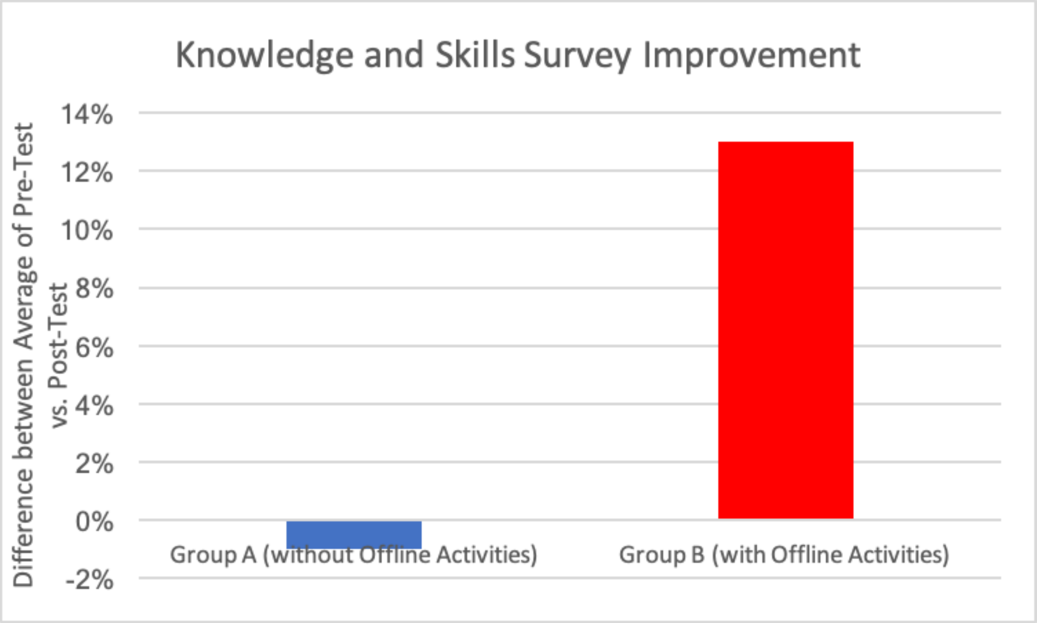


Figure 6.5: Knowledge and Skills Survey Improvement

6.4 Qualitative Feedback from Group B

After completing the course, Group B was asked to fill out a feedback form detailing their favorite activities, least favorite activities, and whether or not they enjoyed partaking in the offline activities.

Unanimously, the students enjoyed the offline activities that encouraged them to work together or in small groups. These activities included Xjhqjy Rjxxflj - Secret Message and I've Been Phished. In addition, most students mentioned that their least favorite offline activities were activities done alone, mostly Internet Scavenger Hunt, because it was done as a single person race.

Students' general reflections on the importance of the offline activities lined up with their interest in having interactive offline activities. Almost all of the students stated that interacting with others helps them learn concepts faster and generate new excitement towards the topic. Other students stated that the offline activities helped them connect the new information to relateable, real-world scenarios.

Overall, the students' reflections mimic what was shown in the quantitative results; the offline activities encouraged students to get more excited about the material and retain information.

6.5 Discussion

Due to the small population size, there are a few conclusions that are worth mentioning, but can not be confirmed as results. As discussed, Group B had more favorable results for student retention, their mindset, and the knowledge they gained from the course. This suggests that the offline activities allowed students to be more engaged in the course, excited about the material, and retain more of the information. There are a few factors that may have caused these results.

First, the offline activities allowed students who were less engaged in the material to be re-engaged once every hour. For example, one student in Group B had stopped participating in the second online portion of the course, the cryptography section. However, the offline activity that was next was Xjhqjy Rjxxflj - Secret Message, which helped the student re-engage in the course and learn a bit of the material he had missed by not participating. This student then finished the last portion of the online course and performed better on the post-test compared to the pre-test. In comparison, students in Group A that stopped participating early on, continued to not participate through the end. This may be because there was no way to re-engage them in the course.

Secondly, I observed that once students stopped participating in the course, they caused other students to also stop. It appeared that most students had a friend or a group of friends in the class. For example, there was a group of 3 students in Group A that were working closely together and mentioned to me that they had known each other for over 10 years. On the first day these three students completed all online portions they were asked to complete. However, on the second day, one student never participated in any online portions of the course. The other two began to work on the course, but quickly got distracted due to the other student not participating. It is unknown why the first student stopped participating in the class.

Lastly, it appears that student retention may have had an effect on student mindsets and the amount of knowledge retained. Once students in Group B stopped participating in the course, even students who continued to participated were less motivated to do so. The majority of the classroom in Group A was talking and helping students with other assignments, unlike Group B. Group B was focused and not distracting others. It is possible that this had an effect on the results as students who were less focused, may have paid less attention to the material, therefore scoring worse on the Knowledge and Skills post-test and the Mindset survey.

To re-iterate, further research needs to be done using more participants to be able to make any conclusions. However, these observations pose as a starting place for future research and studies.

Chapter 7

FUTURE WORK

This chapter discusses the improvements that can be made to this thesis and the possibilities for future work.. The opportunities for improvement include creating more interactive offline activities, adjusting the experiment to include less caveats, and doing the same test using multiple online courses.

7.1 Adding More Interactive Offline Activities

While leading the offline activities, it became apparent that the most effective offline activities were activities that allowed for interaction between the students. In the experiment, this included the Internet Scavenger Hunt and the Xjhqjy Rjxxflj - Secret Message activities. Students shared that the interactive activities provided a balance against the solo online portion of the class. I believe that the results may have been more dramatic had all of the activities been interactive instead of worksheet based.

There is an opportunity to add more activities to the existing course as well as incorporate offline activities into other online courses. A possible additional interactive activity could be to have students play the Memory/Concentration game using vocabulary learned in the course. Students can work together to create the cards for the game. Another activity that can be added is an additional encryption activity where students use different forms of encryption learned in the course to see how difficult they are to crack without a computer. Students can race against each other to crack different ciphers and solidify their understanding of different encryption methods. Besides these activities, there are many other interactive activities that could be created that may enhance the results of this thesis.

7.2 Experiment Adjustments

As stated, this experiment is a proof of concept, however more work can be done to provide verifiable results including testing the full course and having larger experimental groups.

The experiment was done using a 3 hour piloted version of the course. However, the full course includes 180 hours of instruction including more offline activities, online course work, and unit projects. To understand the effect of the offline activities on the full course, it is imperative that a study be done using the full course and all offline activities.

It is also important to have larger experimental groups to get rid of any unknown biases. This can simply be done by doing research at more schools to create a bigger sample size. If classes are bigger, you can also split every classroom in half and put one half in Group A and one half in Group B. This will also help eliminate any inherent biases between the two groups.

7.3 Additional Experiments

As discussed, this experiment was conducted using only material form the CodeHS Introduction to Cybersecurity course. Because of this, it is not possible to make conclusions about in-person activities helping/hindering all forms of online education for cybersecurity. In order to do so, the offline activities would have to be added to many K12 cybersecurity courses. However, as of the end of 2018, there are no such courses beside the one used.

Once other K12 cybersecurity courses exist, this experiment can be repeated with every course. In doing so, the results would show the effect of offline activities on online cybersecurity education.

Chapter 8

CONCLUSION

With the increasing number of unfilled jobs in cybersecurity, educating the upcoming workforce is important. By 2021, there will be as many as 3.5 million unfilled cybersecurity positions in the industry [27]. This gap can be lessened by adding cybersecurity to K-12 education.

A lot of research has been done on how to incorporate computer science education, and more specifically cybersecurity education, into grade schools. Researchers have looked into increasing excitement towards cybersecurity through games, group work, and online education. Since online coursework struggles to retain students compared to traditional classroom methods, many researchers have focused on blended education methods. Blended education has more positive outcomes due to additional learning time, instructional resources, and course elements that encourage interaction among learners.

This work applied blended education to an online cybersecurity course and concluded that online cybersecurity education can be enhanced through blended education, like many other subjects. Two groups of high school students partook in a online cybersecurity course provided by CodeHS [15]. One of the groups also partook in offline activities that mirrored a blended education. Students were evaluated on their attitude towards cybersecurity and the knowledge gained in the course. The results showed that the group that participated in both the online and offline portions of the course had a higher percentage in student retention, a more positive mindset towards cybersecurity, and an increase in the amount of knowledge gained through the course.

We hope this work helps educators continue to integrate cybersecurity and computer science education into their curriculum. We also hope that our work can be expanded upon in the future to test more offline activities and on a larger participant pool to allow for further conclusions.

BIBLIOGRAPHY

[1] About Us Coast USD. http://www.coastusd.org/index.php/about.

[2] Caesar Cipher. https://learncryptography.com/classical-encryption/caesar-cipher.

[3] Code.org. https://code.org/.

[4] Control-Alt-Hack. http://www.controlalthack.com/.

[5] CSforALL. https://www.csforall.org/about/.

[6] Cyber Bullying: Statistics and Tips. https://www.isafe.org/outreach/media/media_cyber_bullying.

[7] Cybersecurity. https://codehs.com/info/curriculum/cybersecurity.

[8] Cyberseek. https://www.cyberseek.org.

[9] [d0x3d!], A Network Security Game. http://d0x3d.com/d0x3d/welcome.html.

[10] Human Subjects – Procedures and Guidelines. https://research.calpoly.edu/HS-guidelines.

[11] ISTE Announces New Computational Thinking Standards for All Educators. https://www.iste.org/explore/articleDetail?articleid=2286&category=Press-Releases&article=.

[12] Mission College Preparatory Catholic High School Home. https://www.missionprep.org/.

[13] SRI International - About Us. https://www.sri.com/about.

[14] StopBullying.gov. https://www.stopbullying.gov/.

[15] What is CodeHS? https://codehs.com/info/.

[16] What is Confidentiality, Integrity, and Availability (CIA Triad)? https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[17] Executive Order 13800. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/, 2017.

[18] AP Computer Science Principles — AP Central The College Board. https://apcentral.collegeboard.org/courses/ap-computer-science-principles, Sep 2018.

[19] S. J. Allen, E. I. Distance Education Enrollment Report 2017. In *Digital Learning Compass*, 2017.

[20] A. W. Astin. Student Involvement: A Developmental Theory For Higher Education. *Journal of college student personnel*, 25(4):297–308, 1984.

[21] L. J. Barker, C. E. McDowell, and K. Kalahar. Exploring Factors That Influence Computer Science Introductory Course Students to Persist in the Major. In *SIGCSE*, 2009.

[22] P. Bawa. Retention in Online Courses: Exploring Issues and Solutions : A Literature Review. *SAGE Open*, 6(1):2158244015621777, 2016.

[23] CareerBuilder. Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study. https://www.prnewswire.com/news-releases/number-of-employers-

`using-social-media-to-screen-candidates-at-all-time-high-finds-latest-careerbuilder-study-300474228.html`, Jun 2017.

[24] X. Chen and M. Soldner. STEM Attrition: College Students' Paths Into and Out of STEM fields, January 2014.

[25] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia. Challenge Based Learning in Cybersecurity Education. Proceedings of the 2011 International Conference on Security & Management, 2011.

[26] K.-. C. S. F. S. Committee. K-12 Computer Science Framework. Technical report, New York, NY, USA, 2016.

[27] Cybercrimemag. Cybersecurity Jobs Report 2018-2021. `https://cybersecurityventures.com/jobs/`, Jun 2018.

[28] D. DiMatteo-Gibson. Interactive Online Course Development. In T. Bastiaens and G. Marks, editors, *Proceedings of E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2013*, pages 71–73, Las Vegas, NV, USA, October 2013. Association for the Advancement of Computing in Education (AACE).

[29] I. S. for Technology in Education. ISTE national educational technology standards (nets). 2000.

[30] M. Gondree, Z. N. Peterson, and T. Denning. Security Through Play. *IEEE Security & Privacy*, 11(3):64–67, 2013.

[31] M. Herbert. Staying the Course: A Study in Online Student Satisfaction and Retention. Online Journal of Distance Learning Administration, 2006.

[32] J. Kauflin. The Fast-Growing Job With A Huge Skills Gap: Cyber Security. *Forbes*, March 2017.

[33] B. Means, Y. Toyama, R. Murphy, and M. Baki. The Effectiveness of Online and Blended Learning: A Meta-analysis of the Empirical Literature. *Teachers College Record*, 115(3):1–47, 2013.

[34] C. K. Nichols, Mark H. Challenge Based Learning White Paper. Technical report, Apple Inc., Cupertino, California, 2008.

[35] PwC. *Turnaround and Transformation in Cybersecurity*. The Global State of Information Security. 2017.

[36] D. Seehorn, S. Carey, B. Fuschetto, I. Lee, D. Moix, D. O'Grady-Cunniff, B. B. Owens, C. Stephenson, and A. Verno. CSTA K–12 Computer Science Standards: Revised 2017. Technical report, New York, NY, USA, 2017. 104111.

[37] B. G. Smith. *E-learning Technologies: A Comparative Study of Adult Learners Enrolled on Blended and Online Campuses Engaging in a Virtual Classroom*. Doctor of philosophy (thesis), Capella University.

APPENDICES

Appendix A

INTRODUCTION TO CYBERSECURITY SYLLABUS

CodeHS

Introduction to Cybersecurity Syllabus
Vigenère: One Year for High School (155 contact hours)

Course Overview and Goals

As our world becomes increasingly dependent on technology, cybersecurity is a topic of growing importance. It is crucial that companies and individuals take precautions to protect themselves from the growing threat of cyber attacks. This course prepares students with crucial skills to be responsible citizens in a digital future.

The Introduction to Cybersecurity is the first online blended K12 cybersecurity course. The Vigenère year-long version is designed for students with some exposure to computer science, but there are no specific course prerequisites. Students will learn foundational cybersecurity topics including digital citizenship and cyber hygiene, the basics of cryptography, software security, networking fundamentals, and basic system administration and all through the CodeHS web-based platform. Students will complete projects at the end of each module, and a culminating course project where they will complete a simulated hack walkthrough. This is not a coding intensive course, but students will learn basic SQL, and will utilize basic HTML and JavaScript within specific contexts and will be provided supports within those contexts.

Learning Environment: The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Students will modify existing code and run it in the browser, investigate cyber related topics and reflect on them and discuss them, create digital presentations, and engage in in-person collaborative exercises with classmates. Teachers utilize tools and resources provided by CodeHS to leverage time in the classroom and give focused 1-on-1 attention to students.

Programming Environment: Students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in HTML, JavaScript and SQL (sand shell commands in the supplementary module). Students will also participate in simulated cyber attacks on safe sites in order to learn how to mitigate cyber attacks. Students will be able to document their processes and discusses best practices for preventing cyber attacks.

Quizzes: Each lesson includes at least one formative short multiple choice quiz. At the end of each module, students take a summative multiple choice quiz that assesses their knowledge of the concepts covered in the module.

Prerequisites: The Introduction to Cybersecurity course is designed for beginners to intermediate computer science students with at least some knowledge and interest in computer science. The course is highly visual, dynamic, and interactive, making it engaging for those new to computer science.

More information: Browse the content of this course at https://codehs.com/course/3433

Course Breakdown

Module 1: What is Cybersecurity? (4 weeks/20 hours)
This module gives an introduction to cybersecurity. It focuses on why cybersecurity is important, recent threats to cybersecurity, and different careers in the field.
Browse the full content of this module at https://codehs.com/library/course/3433/module/4858

Objectives / Topics Covered	● Course Overview ● What is Cybersecurity? ● Impact of Cybersecurity ● The CIA Triad
Example Assignments / Labs	● Course Overview ○ Do you use the Internet? ○ How do you use the Internet? ○ What kinds of information are at risk? ○ What are some different CS career fields? ○ Coding as the new literacy ○ What is this course about? ○ Example activity: ■ Lists steps to take to protect yourself on the Internet ■ What is something you want to know or make by the end of the course? ● What is Cybersecurity? ○ Cybersecurity defined ○ Why is cybersecurity important? ○ Cybersecurity in the news ○ Cybersecurity and IoT (Internet of Things) ○ How do we prevent cyber attacks? ○ Example activities: ■ Summarize and discuss recent cyber attacks ■ Explore a threat map to see where cyber attacks are coming from and which countries are being targeted ● Impact of Cybersecurity ○ Why do we care about cybersecurity? ○ What information is at risk? ○ What are the impacts of cyber attacks?

	■ Financial impact ○ Cybersecurity workforce ○ What are current cybersecurity career? ○ Example activities: ■ Review resources and reflect on or discuss ● What information do cyber criminals steal? ● What do cyber criminals do with stolen information? ● The CIA Triad ○ What is the CIA triad? (confidentiality, integrity, availability) ○ What are “secure systems?” ○ What do confidentiality, integrity, and availability mean in cybersecurity? ○ Example activities: ■ Determine where scenarios break part of the CIA Triad

Module 2: Digital Citizenship and Cyber Hygiene (10 weeks/50 hours)

This module includes topics on Internet etiquette and how to stay safe on the world wide web. We will also look at the potential effects of our digital footprints, how to protect information from online risks, and the implications of cyberbullying. Finally, the module includes how to find and cite quality resources online.

Browse the full content of this module at https://codehs.com/library/course/3433/module/4859

Objectives / Topics Covered	● Digital Footprint and Reputation ● Cyberbullying ● Internet Safety ● Privacy and Security ● Information Literacy ● Creative Credit and Copyright ● Hacking Ethics
Example Assignments / Labs	● Digital Footprint and Reputation ○ What is a digital footprint? ○ What is ***your*** digital footprint and reputation? ○ What does it mean that the internet is public and permanent? ○ Who looks at your digital footprint and reputation? ○ What are some recommended social media guideline? ○ How can you maintain your digital footprint? ○ What does your digital footprint say about you? ○ Example activities: ■ What is your digital footprint? ■ Are you going to make any changes in what

	you post on social media? ● Cyberbullying ○ What is cyberbullying? ○ What are the impacts of cyberbullying? ○ Are there cyberbullying roles? ○ What do you do if you are being bullied? ○ What do you do if you see bullying? ○ How can you be an upstander? ○ Example activities: ■ Explore cyberbullying scenarios: What would you do? ● Internet Safety ○ What are some ways to stay safe online? ○ What are some online safety guidelines? ○ Example activities: ■ Explore Internet safety scenarios: What would you do? ● Privacy and Security ○ What are data privacy and security? ○ How can you keep personal data secure and private? ○ What can happen if you data is stolen and what can you do about it? ○ Example activities: ■ Test out various passwords on a site ■ Explore Google's privacy policy: What do they know about you? ● Information Literacy ○ What is information literacy? ○ How can you do effective internet searches? ○ What are some techniques for judging source legitimacy and identifying misinformation? ○ Example activities: ■ Create and test search queries ■ Explore evidence for using sources ● Creative Credit and Copyright ○ What is copyright? ○ What are the different types of copyright licenses ○ Example activities: ■ Create citations for sources ■ Explore image search tools ● Hacking Ethics ○ What are hackers? H ○ Are there different kinds of hackers? (white, black, grey) ○ What are bug bounty programs? ○ Is hacking always illegal? ○ What are the consequences of illegal hacking?

	○ Example activities: ■ Explore what penetration testing is ■ Sign ethical hacker agreement ● Final project: Create a Public Service Announcement ○ Create a Public Service Announcement (PSA) to teach your peers about your selected topic in digital citizenship and cyber hygiene. You can select any of the topics covered in this module. Be creative and make it fun! You could make a video, song, poster, or slideshow.

Module 3: The ABCs of Cryptography (7 weeks/35 hours)
In this module, we will dive into the history of cryptography systems, the motivation behind using encryption systems, and basic cryptography systems. Additionally, we will explore topics on how to use cryptography, cryptology, and cryptanalysis to decode a message without the use of a key. Finally, we will look into more advanced cryptographic topics like public key cryptography and hash functions.
Browse the full content of this module at https://codehs.com/library/course/3433/module/4860

Objectives / Topics Covered	● Cryptography, Cryptology, Cryptanalysis ● History of Cryptography ● Why do we Need to Encrypt Data? ● Basic Cryptography Systems: Caesar Cipher ● Basic Cryptography Systems: Cracking the Caesar Cipher ● Basic Cryptography Systems: Vigenère Cipher ● Advanced Cryptography ● Hash Functions ● Hash Function Development
Example Assignments / Labs	● Cryptography, Cryptology, Cryptanalysis ○ Why do we need some secrecy in our transparent information age? ○ Explain general encryption with data, keys ○ Example activities: ■ Video and discussion on securing the cloud ■ Passing notes in class (offline activity) ● History of Cryptography ○ Why do we encrypt? ○ What are some classic encryption techniques? ○ What is the flaw in substitution ciphers? ○ What was The Enigma during WW2? ○ What is modern cryptography and how has cryptography changed over time? ○ What is 256-bit key encryption and how does this help cryptography overall? ○ Example activities:

	■ How did the Enigma work? ● Why do we Need to Encrypt Data? ○ Explore the CIA Triad and encryption ○ Example activities: ■ Telephone game with math (offline) ■ Modulo math activity sheet ● Basic Cryptography Systems: Caesar Cipher ○ Explore examples of the Caesar cipher ○ Example activities: ■ Practice with a Caesar Cipher JavaScript program ■ Modify the program to create the decrypting Caesar program ● Basic Cryptography Systems: Cracking the Caesar Cipher ○ How do we solve the Caesar Cipher with brute force and using letter frequency analysis? ○ Example activities: ■ Practice cracking Caesar Cipher with brute force ■ Practice cracking Caesar Cipher with letter frequency ● Basic Cryptography Systems: Vigenère Cipher ○ Explore examples of the Vigenère Cipher ○ Example activities: ■ Practice with a Vigenère Cipher JavaScript program ● Advanced Cryptography ○ What are the problems with Caesar cipher? (History recap) ○ What does today's cryptography look like? ○ What does "hard vs. easy problems to crack" mean? ○ What kinds of encryption are there? (symmetric, asymmetric, public key) ○ Example activities: ■ Discuss resources related to public key cryptography ● Hash Functions ○ What is cryptographic hashing? ○ How is hashing used? ○ What is a hash function?n Why are hash functions used? ○ What does the ideal hash function do? ○ How do attackers try to crack a hashing algorithm? ○ Example activities: ■ Use a hash generator to create hashes for various input ● Hash Function Development ○ How can we preventing hash function cracking?

	○ Why is modulo math so important for hash programs? ○ Example activities: ■ Practice module math problems (offline) ■ Test a simple hash program ● Final project: Develop a hash program ○ Modify a hash function program with new math to create different hashes for the same inputs. Explain how your new program works and show before and after results for 3 different input strings that the new hash function changed the hash created.

Module 4: Software Security (9 weeks/45 hours)

In this module, we will learn what happens when running a web application and how to look inside web apps using developer tools, source code, and more. We will learn basic SQL so we can learn about common attacks like SQLi and XSS. and recommend solutions for flawed security systems.

Browse the full content of this module at https://codehs.com/library/course/3433/module/4895

Objectives / Topics Covered	● Inside Web Applications ● Developer Tools ● SQL Overview ○ What is SQL? ○ Structuring Data in SQL ○ Basic Querying in SQL ○ Filtering Queries in SQL ● Clients, Servers, Databases ● Common Security Problems ● SQL Injection ○ SQLi Overview ○ Types of SQLi ○ Preventing SQLi ● Cross-Site Scripting (XSS) ○ XSS Overview ○ Types of XSS ○ Preventing XSS ● Data Exposure
Example Assignments / Labs	● Inside Web Applications ○ View page source (images, navigation and page layout, stylesheets, JavaScript, minified code ○ Example activities: ■ View page source scavenger hunt ■ Getting started with OWASP ● Developer Tools ○ Use the inspect tools to look more deeply inside of

	web apps ○ How does view page source compare to inspect in terms of information about the site / app? ○ Example activities: ■ Practice using the Chrome developer tools ■ Change a favorite site using the Chrome developer tools on your end only. Take a screenshot of your change. ● SQL Overview ○ What is SQL? ○ How do we structuring data using SQL? ○ How do we query databases using SQL? ○ Example activities: ■ Use the SELECT statement to query a database ■ Use the WHERE clause to query a database ● Clients, Servers, Databases ● Common Security Problems ○ What is the “Fortification Principle”? ○ What are some tips about HTTP vs. HTTPS, password fields and CAPTCHA that can help us to navigate more securely on the Web? ● SQL Injection ○ SQLi Overview ■ What is SQLi? ■ Why is SQLi a problem? ■ What happens during a SQLi attack? ■ What is the the fallout of a SQLi attack? ■ How does SQLi work? ■ How do hackers use SQL in a SQLi? ○ What are the types of SQLi (error-based, union-based, blind) ■ What is the underlying SQL behind the scenes that hackers may be trying to hack? ○ How to we mitigate or prevent SQLi? ■ What are the OWASP recommendations? ■ How can we tell if our code is vulnerable? ○ Example activities: ■ Discuss the Equifax SQL injection attack ■ Practice basic SQLi on a safe site ■ Research SQLi prevention ● Cross-Site Scripting (XSS) ○ XSS Overview ■ What is XSS? ■ Why is XSS a problem? ■ What happens during an XSS attack? ■ What is the fallout of a XSS attack? ■ How does XSS works

	■ How do hackers use JavaScript in a XSS attack? ○ What are the types of XSS (reflected XSS, stored or persistent, DOM) ■ What is the vulnerable JavaScript behind the scenes? ○ How do we prevent or mitigate XSS? ■ What are the OWASP recommendations? ■ How can we tell if our code is vulnerable? ○ Example activities: ■ Discuss the XSS bug in Yahoo email attack ■ Practice basic XSS on a safe site ■ Research XSS prevention ● Data Exposure ● Final project: Hack Walkthrough ○ Students will be given a series of SQLi and XSS attacks that they need to perform on the site http://hackyourselffirst.troyhunt.com/ . Students will then reflect on classifying the vulnerabilities that they exploited and how they would mitigate the various attacks.

Module 5: Networking Fundamentals (6 weeks/30 hours)

This module explores the structure and design of the internet and networks, and how this design affects the reliability of network communication, the security of data, and personal privacy. We will learn how the Internet connects computers all over the world. Finally, we will explore basic networking protocols, practical networking, and how networks are secured.
Browse the full content of this module at https://codehs.com/library/course/3433/module/4894

Objectives / Topics Covered	● Introduction to the Internet ● Internet Hardware ● Internet Addresses ● Domain Name System (DNS) ● Routing ● Packets and Protocols ● The Internet and Cybersecurity ● Impact of the Internet ● Network Hacks ● Securing a Network
Example Assignments / Labs	● Introduction to the internet ○ What is the Internet? How does it work? What have been its impact on society? ○ Why do we need protocols for the Internet? ○ Example Activity

	■ Explore the different levels of the internet. ● Internet hardware ○ Vocabulary: bandwidth, bitrate, latency ○ Why are protocols so important? ○ How do we send data over the Internet? ○ Example Activities ■ Explore how data is able to be transmitted across the ocean by using underwater cables ■ Explore the role of simple and complex networks and routers ● Internet Addresses ○ Vocabulary: Internet Protocol (IP) ○ How do IP addresses compare to postal addresses? ○ How IP addresses work? ○ Example Activities ■ Explore the differences between IPv4 and IPv6. Why are we running out of addresses? ■ Trace a website request from the server, through the network, and to your computer ● Domain Name System (DNS) ○ How does DNS help with sending digital information and IP addresses? ○ Example Activities ■ Explore the process of how requesting a web resource works ● Routing ○ How is routing used to send messages / data? ○ Why is redundancy a good thing for the Internet? (fault tolerant) ● Packets and Protocols ○ How data is transmitted? ○ How are internet packets able to find their way to your computer? ○ Example Activities: ■ Explain in your own words how a request from your computer travels through the various levels of servers to reach and return the correct webpage and resources? ■ As a class, create a protocol that will allow one classmate to send another classmate a note, without the need for talking to each other. ○ What are the standard protocols for the Internet and how do they work? (TCP/IP, HTTP) ● The Internet and Cybersecurity ○ What are cybercrime and cyberwarfare? ○ How do we network attacks? (certificate authorities, public key encryption)

	● Network Hacks ○ What are common network attacks? ○ Explain common network attacks and how they happen. (DNS spoofing, DoS/DDoS, Waterhole attacks, fake WAP, eavesdropping) ● Securing a Network ○ How can we detect intrusions? (checking logs, firewall rules, intrusion detection systems - IDS) ○ What are some recommended approaches for mitigating or preventing network attacks? ● Final Project ○ Create a basic network configuration simulation that is optimized for security via the following site: http://malkiah.github.io/NetworkSimulator/simulator01.html# ● Final course Project / Challenge: ○ Walk through a simulated attack from the attacker and defender perspectives and incorporate all techniques and recommendations garnered from the course.

Appendix B

UNDERSTANDING THE CIA TRIAD

Understanding the CIA Triad
(Teacher Version)

Corresponding Material

What is Cybersecurity?: CIA Triad

Discussion

The CIA Triad is a widely-accepted security measure that should be guaranteed in every secure system. It stands for Confidentiality, Integrity, and Availability.

- Confidentiality is the protection of information from people who are not authorized to view it.
- Integrity aims at ensuring that information is protected from unauthorized or unintentional alteration.
- Availability is the assurance that systems and data are accessible by authorized users when and where needed.

It is these three principles that are often exploited by various attacks.

Further Discussion

This activity is intended to let students practice thinking about how the CIA Triad is applied in real-world scenarios. The CIA Triad is a concept that will be applied in every section. It is important for students to understand the concept as applied to everyday situations before applying it the cybersecurity concepts.

Examples

The following are three examples to share with the class before they work on the rest of the handout in pairs or alone.

1. Bob wants to watch the new episode of his favorite show on Hulu. However, the website will not load due to an attack.
   Answer: Availability

Bob is not able to access his favorite show because the website is down when he needed it.

2. Alice has a website that she sells computer parts on. However, Bob has gotten ahold of her website and is able to alter the prices of the parts prior to purchasing anything.
   Answer: Integrity
   As a customer, Bob is not authorized to alter the price of the product. Since an unauthorized party is able to change information, this is a breach of integrity.
3. Alice went to her doctor to get an x-ray of her leg. Unfortunately, when the doctor called Alice, the doctor did not realize he was talking to Mallory and told Mallory the results of the x-ray.
   Answer: Confidentiality
   Due to laws that doctors must follow (HIPPA), doctors are only allowed to share medical information with the patient it concerns. By giving Mallory medical information about Alice, the doctor has given Mallory information she is not authorized to know.

Class Exercise

Decide which of the CIA (Confidentiality, Integrity, or Availability) triad was broken in each scenario.

1. Alice and Bob are students. Alice copies Bob's homework.
   Answer: Confidentiality
   This is a violation of plagiarism. Homework should only be viewed by the student who wrote it and the teacher. Since Alice is not authorized to view Bob's homework, this is a violation of confidentiality.

2. Alice and Bob play computer games. Right as Alice is about to slay Bob's character with a +10 spell, Bob yanks her Ethernet cable.

Answer: Availability
Alice was not able to slay Bob's character because the system was not accessible when it was needed. This is because Bob unplugged the Ethernet cable.

3. Alice writes a private note in her diary and then locks it. Unfortunately, Bob finds the key and is able to open Alice's diary and read her private note.
Answer: Confidentiality
Alice's diary is only authorized for Alice. When Bob reads Alice's diary, he has access to information that he is not authorized to see.

4. Bob sends Alice a check for $10. She then adds a "0" to the amount so now Bob has sent Alice a check for $100.
Answer: Integrity
Alice is able to alter the value of the check even though Bob was the only party authorized.

5. Alice has online homework due at 2:00 PM and she is rushing to finish it. Right before she is about to submit, her power cuts out and Alice is no longer able to submit her homework by the due date.
Answer: Availability
Alice was not able to turn in her homework on time because the power cut out. This caused the system to be inaccessible to her when she needed it.

6. Alice and Bob are trying to pass notes in class, but Mallory is sitting in between them. In order for Alice to get a note to Bob, Alice must pass it to Mallory and then Mallory must pass the note to Bob. One time, Bob needed help with

Appendix C

DIGITAL FOOTPRINT

Digital Footprint
(Teacher Version)

Corresponding Material

Digital Citizenship and Cyber Hygiene: Digital Footprint and Reputation

Discussion

Most of us use the Internet as a way to connect with friends, explore topics, or study for school. Many are connected to multiple social media platforms including Facebook, Twitter, and Instagram. We share various pieces of our lives online, from our weekend plans to photos of the last food we ate. While it appears that you're just keeping your friends updated on the important (and unimportant) events in your life, you are actually creating the foundation for your online reputation. That means that anything you have posted online is creating a digital trail that can last a lifetime.

If the digital footprint you are creating lasts a lifetime, is it one you'll be proud to share? Even more immediate, is your online reputation one you're willing to share with college admissions or future employers?

Further Discussion

This activity is intended to encourage students to think about their digital footprint. Start the discussion by asking students to think about what they would like to do after high school. Encourage some of them to share it with the class or write it down. This exercise can then be done as an in-class activity or as homework.

Class Exercise
Today you will view your own online reputation and create a plan to improve your online reputation (if necessary).

1. Search your full name on google.com. Does any information about you appear in the search results? If so, what information displayed is positive? What information displayed is negative? If not, try searching for your name and your school or your name and your city. For example, search for "John Doe Los Angeles" or "John Doe Alan Turing High School".

2. According to CareerBuilder's annual social media recruitment survey, 49% of employers stated that they've found information online about that caused them to not hire a candidate.

The following are the top pieces of content that dissuaded employers from hiring a candidate:

- Provocative or inappropriate photographs, videos or information – 46%
- Information about candidate drinking or using drugs – 43%
- Discriminatory comments related to race, religion, gender, etc. – 33%
- Candidate bad-mouthed previous company or fellow employee – 31%
- Poor communication skills – 29%

Do any of your social media profiles have items on this list? If so, is any of the content worth deleting? Please share (if comfortable) what you've decided to keep or delete.

3. According to the same annual social media recruitment survey done by CareerBuilder, 32% of employers have found information that caused them to hire a candidate.

The following are the top pieces of content that convinced employers to hire a candidate:

- Candidate’s background information supported job qualifications – 44%
- Candidate’s site conveyed a professional image – 44%
- Candidate’s personality came across as a good fit with company culture – 43%
- Candidate was well-rounded, showed a wide range of interests – 40%
- Candidate had great communication skills – 36%

Thinking about your future prospects, do your social media platforms contain any of the content above? Consider: Do you post about your hobbies or interests? Do you use proper grammar and punctuation? Do you maintain a professional presence online at all times?

Are there any you can start implementing today?

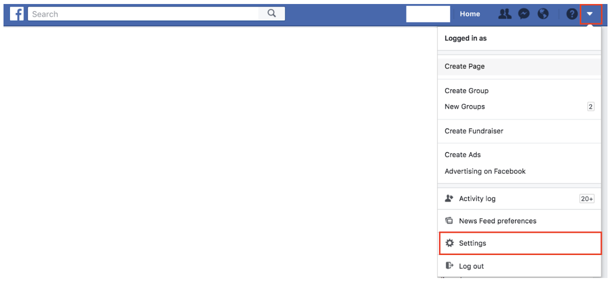
4. 41% of employers say they are less likely to interview job candidates if they are unable to find information about that person online. So, it is a better idea to make your online reputation positive rather than non-existent. However, you should limit the amount of information the public has access to using the guides on the next page. Discuss what changes you made to your existing profiles.

5. Are there any other social media accounts you use? If so, look up how to make these services more private. Write about what you found below.

Make Your Facebook Profile More Private

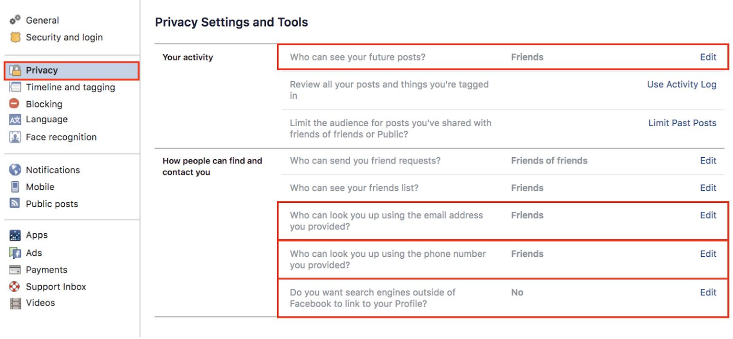
Step 1: Navigate to Facebook.com on a browser and log in.

Step 2: Click the down arrow in the right corner and select **Settings.**



Step 3: In the panel on the left side, click **Privacy** and fix your settings to match the picture below by following these steps:

1. Set "Who can see your future posts?" to **Friends.**
2. Set "Who can look you up using the email address you provided" to **Friends.**
3. Set "Who can look you up using the phone number you provided" to **Friends.**
4. Set "Do you want search engines out of Facebook to link to your Profile?" to **No.**

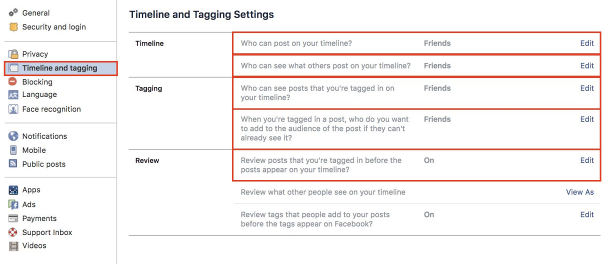


Privacy Settings and Tools

Your activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How people can find and contact you	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Friends	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit

Step 4: In the panel on the left side, click **Timeline and tagging.** Fix your settings to match the picture below by following these steps:

1. Set "Who can post on your timeline?" to **Friends.**
2. Set "Who can see what others post on your timeline? to **Friends.**
3. Set "Who can see posts that you're tagged in on your timeline?" to **Friends.**
4. Set "When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?" to **Friends.**
5. Set "Review posts that you're tagged in before the posts appear on your timeline?" to **On.**
   Note: This allows you to ensure that posts made by friends are appropriate for your timeline.

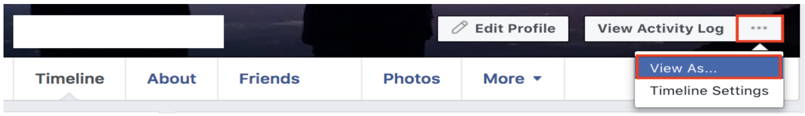


Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
Tagging	Who can see posts that you're tagged in on your timeline?	Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	Edit
Review	Review posts that you're tagged in before the posts appear on your timeline?	On	Edit
	Review what other people see on your timeline		View As
	Review tags that people add to your posts before the tags appear on Facebook?	On	Edit

Step 5: Once you have updated these settings, navigate to your profile by clicking your profile picture on the blue bar at the top.

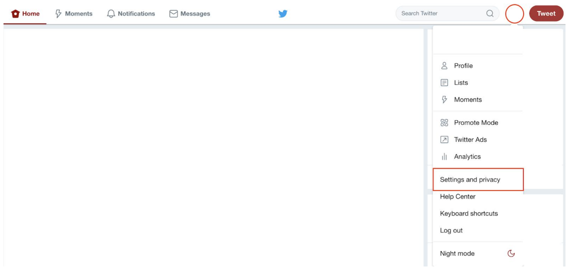
Step 6: Click the three horizontal dots in the top right corner of your profile and select **View As...** Once selected, your profile will display how it appears to the public.



Make Your Twitter Profile Private

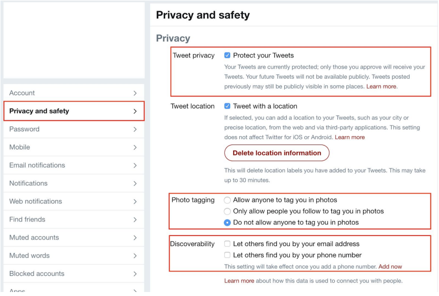
Step 1: Navigate to Twitter.com on a browser and log in to your account.

Step 2: Click your profile picture in the top right corner and select **Settings and Privacy.**



Step 3: In the left panel, select **Privacy and Safety.**

1. Select the checkbox next to **Protect your Tweets.**
2. Under **Photo Tagging,** select "Do not allow anyone to tag you in photos".
   Note: This will ensure that photos of you on Twitter that are posted by others will not be linked to your social media account in case they are inappropriate.
3. Under **Discoverability,** make sure that both "Let others find you by your email address" and "Let others find you by your phone number" are deselected.



Privacy and safety

Privacy

Tweet privacy ☑ Protect your Tweets

Your Tweets are currently protected; only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location ☑ Tweet with a location

If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more

Delete location information

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging ○ Allow anyone to tag you in photos
○ Only allow people you follow to tag you in photos
● Do not allow anyone to tag you in photos

Discoverability □ Let others find you by your email address
□ Let others find you by your phone number

This setting will take effect once you add a phone number. Add now

Learn more about how this data is used to connect you with people.

With these settings, if a future employer finds your twitter profile, they will only be able to view your profile picture and bio.

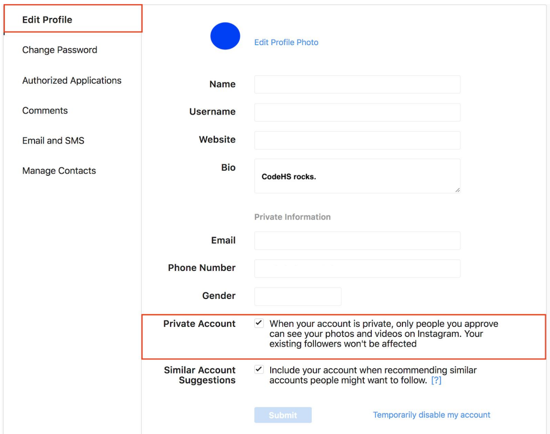
Make Your Instagram Profile Private

Step 1: Navigate to Instagram.com and log in to your account.

Step 2: Go to your profile by tapping 👤 in the top right corner.

Step 3: Go to your settings by tapping Edit Profile in the middle of the page.

Step 4: Check the checkbox next to **Private Account** as seen in the picture below.



Name

Username

Website

Bio: CodeHS rocks.

Private Information

Email

Phone Number

Gender

Private Account ☑ When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected

Similar Account Suggestions ☑ Include your account when recommending similar accounts people might want to follow. [?]

With these settings, if a future employer finds your Instagram profile, they will only be able to view your profile picture and bio.

Appendix D

DO THE RIGHT THING

Do the Right Thing
(Teacher Version)

Corresponding Material

Digital Citizenship and Cyber Hygiene: Cyberbullying

Discussion

The internet has provided tremendous value. It provides a potential for learning, socializing, and leisure. However, with these advancements, also comes new problems, including cyberbullying. Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. It is the most common online risk for teenagers, and can occur to any young person online. Unlike bullying, there are no common risk factors. It really can happen to anyone.

What to do if you encounter cyberbullying:

- Tell a trusted adult (i.e. a parent or a teacher)
- Contact host/website provides if inappropriate material is being posted on their website.
- Save all evidence if bullying is taking place online.
- Do not respond to rude messages. This only encourages the bully.
- If the cyberbullying is directed at another person, stand up for the victim!

Further Discussion

This activity is intended to cause students to reflect about different cyberbullying situations and how they would personally react. Before reading the case studies, lead a discussion about cyberbullying using the questions below as a guide.

1. What is cyberbullying?
2. How is cyberbullying different from other forms of bullying? Why do you think some people bully others online?
3. Why do you think it is hard sometimes for someone to speak up when they are being bullied?
4. What is one thing you could do today (right now!) to help stop or prevent cyber bullying?

NOTE: Please review this activity before using it in class because some of the case studies have mature themes.

Class Exercise

Read each scenario below. For each scenario, discuss with a classmate how well you think the person in each story below handled cyberbullying and how you might have handled it differently.

Scenario 1:
Sami began receiving rude emails from an email address she did not recognize. The emails ridiculed her hairstyle and the clothes she wore to school, so she assumed that the emails were from someone she knew. Sami decided to delete the emails and not tell her parents because she did not want to lose internet privileges.

Did Sami handle the incident well? If not, how could she have handled the situation differently?
Sami did not handle this situation as well as she could have. Sami did do the right thing by not responding to the emails, however she should have saved the emails as proof of the incident. Also, Sami should have immediately told her parents or another trusted adult.

Scenario 2:
David received a friend request from Charlie. He had met Charlie once or twice, but did not know him very well. To add to his growing number of friends, David accepted the friend request. Soon after, Charlie started posting strange photographs on David's timeline. David quickly consulted his parents who advised him to send Charlie a private message asking him to stop. When Charlie continued to post these photos on David's timeline, David "unfriended" Charlie on Facebook and blocked Charlie from seeing his Facebook account. He then reported the photographs Charlie had posted to Facebook.

Did Charlie handle the incident well? If not, how could he have handled the situation differently?
Charlie handled the incident well. He saved the emails, told a trusted adult, and also reported the photographs to Facebook administration.

Scenario 3:
Patricia Brown received an Instagram follow from Fatricia Brown, a fake Instagram account aimed at making fun of Patricia. Patricia began to scroll through the photos and cry. Instantly she became enraged. She had been having an ongoing problem with Mary, a girl at school, and realized right away Mary was the one behind the fake Instagram account. To get back at Mary, Patricia made a fake Instagram named Hairy Mary and started posting photos of Mary. This only escalated the problem and both fake accounts continued to post horrible photos.

Did Patricia handle the incident well? If not, how could she have handled the situation differently?
Patricia did not handle the incident well. Patricia should have told an adult right away. She also should not have "responded" to the bully. By creating another fake Instagram account, Patricia became a bully as well which only encouraged Mary to continue.

Scenario 4:
Kyle and Mark were really great friends. They had a non-stop group chat where they texted all day long. One day, Kyle had an argument with another student in his class named Ryan. Kyle was pretty annoyed with Ryan and texted Mark mean comments about Ryan. Since Mark was good friends with Ryan, Mark chose not to respond and finally Kyle stopped making rude remarks.

Did Mark handle the incident well? If not, how could he have handled the situation differently?
Mark could have handled the situation better. While the bullying was not directed at Mark, Mark had the opportunity to stop the comments and stand up for Ryan. Though Mark did not engage with Kyle any further, he definitely could have made it known that the comments being made were not okay.

Appendix E

I’VE BEEN PHISHED

I’ve Been Phished!
(Teacher Version)

Corresponding Material

Digital Citizenship and Cyber Hygiene: Privacy and Security

Discussion

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The goal is to trick the email recipient into believing that the message is something they want or need so that they will click a link or download an attachment. Phishing is a play on the word “fishing”, as it is a way of “throwing out bait” to see who bites. The best way to protect yourself from phishing is to learn how to recognize it.

How to identify phishing scams:

1. **Generic greeting -** Phishing emails are sent in large quantities in hopes that a percentage of recipients will not realize it is fraudulent. Do a quick check of how the sender addressed you!
2. **Generic body -** Phishing emails normally tend to have a generic body in the email. By keeping the information nonspecific, the internet criminals hope that the user believes that at least some of the information applies to them. Take a quick moment to assess whether the information is actually about you!
3. **Incorrect Company Information -** Many phishing emails do not send the email from an email address with the correct domain (i.e. from the correct company). Some sender emails will try to trick you by having the correct subdomain, but not the correct domain (i.e. @am.amazon.com instead of @amazon.com)

4. **Request for personal information -** Companies do not request personal information over email since it email is insecure. If an email is asking for personal information, it is most likely a phishing email.
5. **Sense of urgency -** Internet criminals want to get your personal information now so they can move on to another victim. To do this, phishing emails normally make you think that something needs to happen fast to fix the situation. If an email is asking you to act fast, don't! Slow down and assess the situation.
6. **Poor grammar -** Internet criminals are not dumb. They prey on the uneducated because they are easier targets. An email from a legitimate organization should be well written. Any email with poor grammar should be enough to cause you to pause and evaluate the email.
7. **Still can't tell?** Call the company and ask!

I've been phished! Now what?

- Do not click on any links or open attachments.
- Do not reply to the sender.
- Report the scam (forward the email to the FTC - spam@uce.gov)
- If you do legitimate business with the spoofed company, you may inform the company of the phishing email in circulation.
- Delete the email.

Uh oh. I fell for a phish! What now?

- Don't panic!
- Change passwords to any website you have logged into since the phish.
- Scan your computer for viruses.
- Contact the company who has been spoofed so they can alert other people!

- If this happened on a school computer, let an administrator know as soon as possible.

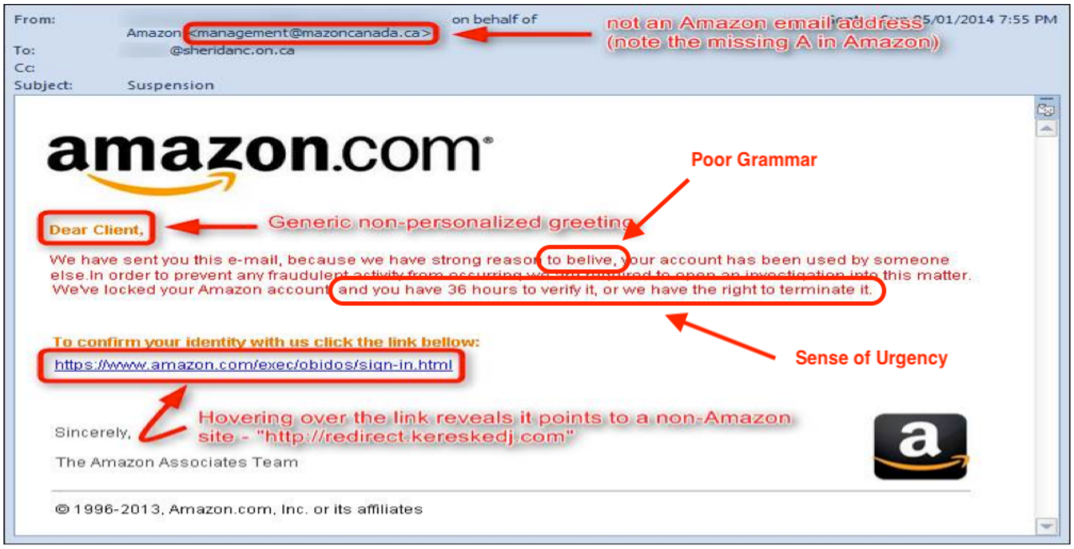
Further Discussion

This activity is intended to introduce students to another important internet security concept, phishing. It is important for students to be able to protect themselves everywhere on the internet, including their email. This activity can be done as an individual worksheet or as a class discussion.

Class Exercise

Observe the following real-world phishing examples. For each example, explain how you can tell that it is a fraudulent email.

Example:



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>

5/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

Dear Client,

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

not an Amazon email address (note the missing A in Amazon)

Poor Grammar

Generic non-personalized greeting

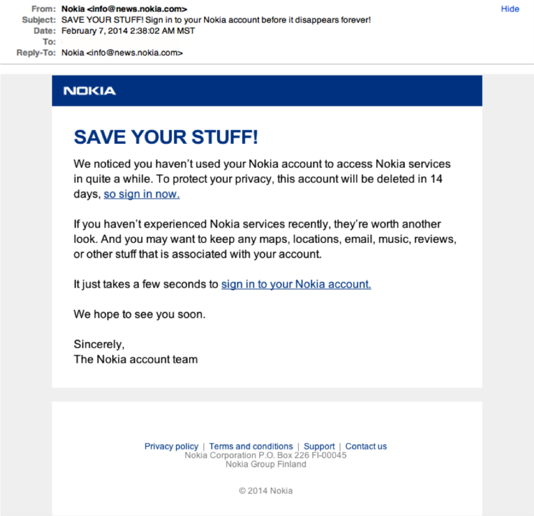
Sense of Urgency

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Notes:

- Generic greeting - This email has a generic greeting and does not address the recipient by name.
- Incorrect company information - This email address is missing an "A" and says "mazon", so is clearly not from an Amazon employee. Also, the link reveals that it points to a non-Amazon site, which should not be the case if this was a legitimate email.
- Sense of urgency - The email is stating that the user needs to click a link in the next 36 hours or else their Amazon account will be terminated.
- Poor grammar - The grammar is not professional. The misspelling of "believe" should be a red flag.

Email #1:



From: Nokia <info@news.nokia.com>
Subject: SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To:
Reply-To: Nokia <info@news.nokia.com>

SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, so sign in now.

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to sign in to your Nokia account.

We hope to see you soon.

Sincerely,
The Nokia account team

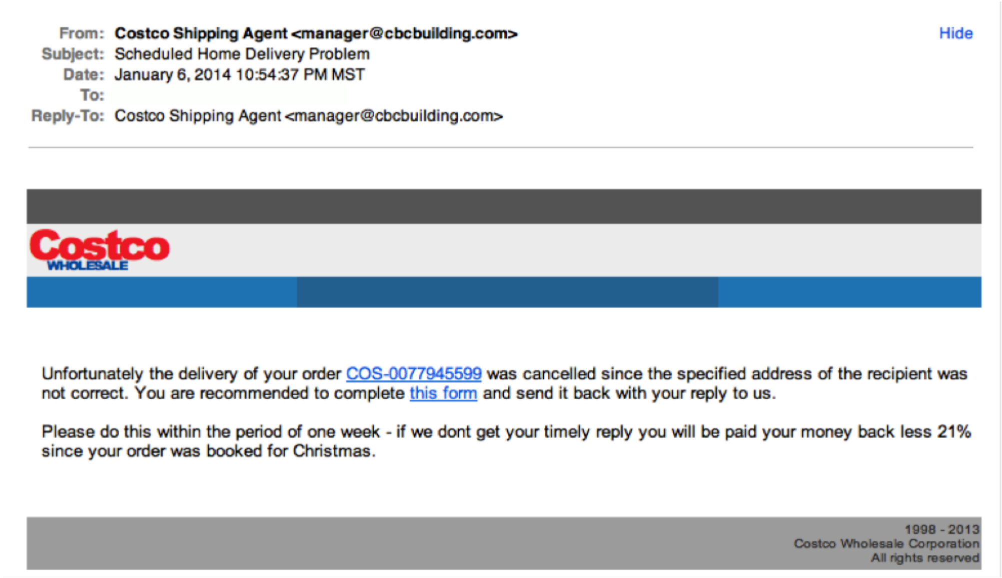
Privacy policy | Terms and conditions | Support | Contact us
Nokia Corporation P.O. Box 226 FI-00045
Nokia Group Finland

© 2014 Nokia

Notes:

- *Generic greeting - This email has a generic greeting and does not address the recipient by name.*
- *Generic body - This email has a very generic body. It states that your Nokia account is going to be revoked but also states that if you do not have a Nokia account, it's worth looking into. The user should realize that the sender of this email does not know whether he/she has a Nokia account. This is definitely a red flag.*
- *Incorrect company information - This email address may or may not be an actual Nokia email address. Normally emails from companies are @company.com, so the "news" in the email address definitely is of concern.*
- *Sense of urgency - The email is stating that the user needs to click a link in the next 14 days or else their Nokia account will be deleted.*

Email #2:



From: **Costco Shipping Agent <manager@cbcbuilding.com>**
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

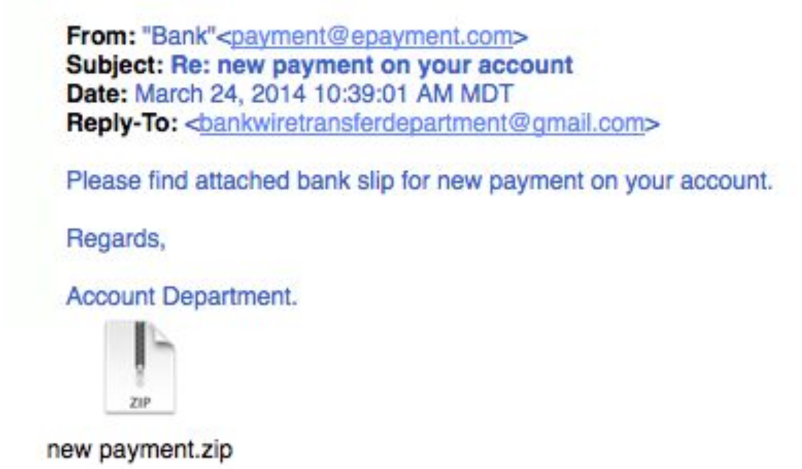
Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

Notes:

- *Generic greeting - This email has a generic greeting and does not address the recipient by name.*
- *Generic body - This email has a very generic body. It is does not reveal the name of the recipient or any information about the order.*
- *Incorrect company information - The sender email address is not from a Costco affiliated domain (cbcbuilding). Also, the Costco logo is close to the actual logo, but not quite correct. Look it up!*
- *Sense of urgency - The email is stating that the user needs to complete a form within one week or a full refund is not possible. Note that the email does not state the actual date that this order will be non-refundable.*
- *Poor grammar - The grammar in this email is far from professional. A lack of commas and apostrophes should be a warning.*

Email #3:



From: "Bank"<payment@epayment.com>
Subject: **Re: new payment on your account**
Date: March 24, 2014 10:39:01 AM MDT
Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

Account Department.

new payment.zip

Notes:

- *Generic greeting - This email has a generic greeting and does not address the recipient by name.*
- *Generic body - This email has a very generic body. It is does not reveal the name of your bank.*
- *Lack of company information - A lack of company information is just as much of a warning as incorrect company information.*
- *Poor grammar - While the grammar of this email is fine, it is not very professional as a normal bank statement would be.*

Appendix F

INTERNET SCAVENGER HUNT

Internet Scavenger Hunt
(Teacher Version)

Corresponding Material

Digital Citizenship and Cyber Hygiene: Information Literacy

Discussion

Information Literacy is the set of skills required to identify, retrieve, organize, and analyze information. Since students no longer go to an encyclopedia or others books at the library to look up information, it is important to be literate on the Internet. Though the internet is a quick source to retrieve information, anyone can publish content for others to access. This means that there is a lot of incorrect information to sort through when performing research.

When looking at a website, consider the following questions:

- How recently was this article published?
- Are scholarly sources cited?
- Is the site .edu or .gov? If not, who is the author? Is this a credible source?
- Is the site well-designed?
- Does this site follow spelling and grammar rules?

Further Discussion

This activity is intended to be a fun task that allows students to practice finding reliable information. This activity should be done as a competition. Students will race to see who can find the information online first. It is important to stress the significance of taking time to evaluate the website before treating the information as fact.

Class Exercise

You are about to partake in a scavenger hunt to see who can search the internet and find correct and reliable information the fastest. For each question listed below, you must search for the answer using a search engine of your choice. Once you find the answer, record it, what the search terms were, the website in which you found the answer, and a decision of whether or not the website is credible.

Example:

Which university in the United States was the first to establish a computer science department?
Answer: Purdue University
Search Terms: first computer science department + U.S.
Website: Purdue's University Website (https://www.cs.purdue.edu/history/)
Is the website credible? *Yes*

Race:

Note: Answers may vary.

1. **What are the high and low temperatures tomorrow in your city tomorrow?**
   Answer: *Tomorrow in San Francisco, CA, the high temperature is 62° and the low temperature is 53°.*
   Search Terms: *San Francisco, CA + weather*
   Website: *weather.com*
   Is the website credible? *Yes*

2. **What does the word *pandiculation* mean?**
   Answer: *Pandiculation is the act of stretching and yawning, especially on waking.*
   Search terms: *pandiculation definition*
   Website: *dictionary.com*

Is the website credible?: *Yes*

3. **If you purchased a "ordinateur" from a french store, what would you have just purchased?**
   Answer: *You would have purchased a computer.*
   Search terms: *ordinateur in english*
   Website: *Google Translate*
   Is the website credible? *Yes*

4. **Who is considered to be the "father of Computer Science"?**
   Answer: *The father of Computer Science is Alan Turing.*
   Search terms: father of computer science
   Website: *Britannica*
   Is the website credible? *Yes*

5. **Research one famous computer scientist. What did they contribute to the field?**
   Answer: *Grace Hopper helped develop a compiler that was a precursor to the widely used COBOL.*
   Search terms: famous computer scientists
   Website: *Biography*
   Is the website credible? *Yes*

6. **What does CLI (computer term) stand for? What is the purpose of it?**
   Answer: *CLI is the Command Line Interface. It is a text-based interface to interact with the operating system.*
   Search terms: CLI computer term
   Website: *LINFO (Linux Information Project)*
   Is the website credible? *Yes*

7. **How tall is the Statue of Liberty?**
   Answer: *The Statue of Liberty is 151 feet and 1 inch.*
   Search terms: "Statue of Liberty" + height
   Website: *National Park Service - Statue of Liberty*
   Is the website credible? *Yes*

8. **Whose inauguration was the first to be nationally radio broadcasted?**
   Answer: *Calvin Coolidge's inauguration was the first national radio broadcast of an inauguration.*
   Search terms: first inauguration + radio broadcasted
   Website: *History, Art, and Archives - U.S. House of Representatives*
   Is the website credible? *Yes*

9. **What is a *netizen?***
   Answer: *A netizen is a user of the internet.*
   Search terms: *netizen definition*
   Website: *dictionary.com*
   Is the website credible? *Yes*

10. **What was Google's search engine originally called?**
    Answer: *Google's search engine was originally called Backrub.*
    Search terms: Google Search Engine + original name
    Website: *Google - Our Story*
    Is the website credible? *Yes*

Appendix G

XJHWJY RJXXFLJ - SECRET MESSAGE

Xjhwjy Rjxxflj
Secret Message
(Teacher Version)

Corresponding Material

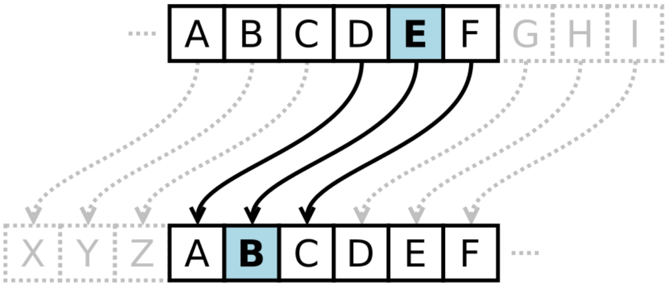
The ABCs of Cryptography: Basic Crypto Systems - Caesar Cipher

Discussion

Encryption is used to support one of the three principles in the CIA Triad, confidentiality. Encryption is a way to send a message as a secret code. The only person who can decode the message is the person who knows the "key", or how the message was changed. To anyone without the key, the message looks like a random series of characters.

The oldest and simplest form of encrypting a message is known as the Caesar Cipher, or the shift cipher. The Caesar Cipher is a type of substitution encryption where each letter in the original message is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.

For each letter of the alphabet, you would take its position in the alphabet and shift it by the key. For example, let's say our original message was "E" and our shift was -3. The encrypted message, as shown below, would be "B".



Further Discussion

Split the class into groups of 3. If there is not enough students to make even groups of 3, have two students be the eavesdropper (Person C).

Before the class starts the exercise, go over an example of how to encrypt a message using the Caesar Cipher.

Given the plaintext message "Cybersecurity is cool!" with a key of +5, the encrypted message would be "Hdgjwxjhzwnyd nx httq!". This is because 5 letters after C, is H. 5 letters after y, is d. 5 letters after b, is g, etc.

Class Exercise

Get into a group of 3 and decide who is going to be Person A, Person B, and Person C. For each task, make sure to time how long it took the eavesdropper to decode the message. After completing the exercise, answer the discussion questions with your group.

Task 1: No Encryption (Person C is eavesdropper)

Step 1: Person A writes a short message on a sheet of paper.

Step 2: Person C intercepts the message as Person A passes it to Person B. As soon as Person C sees the message, write down the start time.

Step 3: Once Person C is done figuring out the message (should not take long), record the stop time and pass the note on to Person B.

Step 4: Person B decodes the message.

Start Time:

End Time:

Total Decode Time (seconds):

Task 2: Caesar Cipher (Person C is eavesdropper)

Step 1: Person A and B steps away from Person C and decides what the “shift”, or key, is going to be for this message. Examples are +5, -10, +23.

Step 2: Person A writes a short encrypted message on a separate sheet of paper using the caesar cipher.

Step 3: Person C intercepts the message as Person A passes it to Person B. As soon as Person C sees the message, write down the start time.

Step 4: Once Person C is done figuring out the message, record the stop time and pass the note on to Person B.

Step 5: Person B decodes the message.

Start Time:

End Time:

Total Decode Time (seconds):

Repeat Task 1 and Task 2, two more times, rotating who becomes the eavesdropper. Use the blanks below to fill out the start/end time.

Task 1: No Encryption (Person A is eavesdropper)
Start Time:
End Time:
Total Decode Time (seconds):

Task 2: Caesar Cipher (Person A is eavesdropper)
Start Time:
End Time:
Total Decode Time (seconds):

Task 1: No Encryption (Person B is eavesdropper)
Start Time:
End Time:
Total Decode Time (seconds):

Task 2: Caesar Cipher (Person B is eavesdropper)
Start Time:
End Time:
Total Decode Time (seconds):

Discussion Questions:

How long did it take an eavesdropper to decode a message when it was not encrypted?
Answers may vary. However, the eavesdropper should have been able to decode the message immediately because it was not encrypted.

How long did it take an eavesdropper to decode a message when it was encrypted with the Caesar Cipher?
Answers may vary. However, the eavesdropper should have taken longer to decode this message than the message written in plaintext.

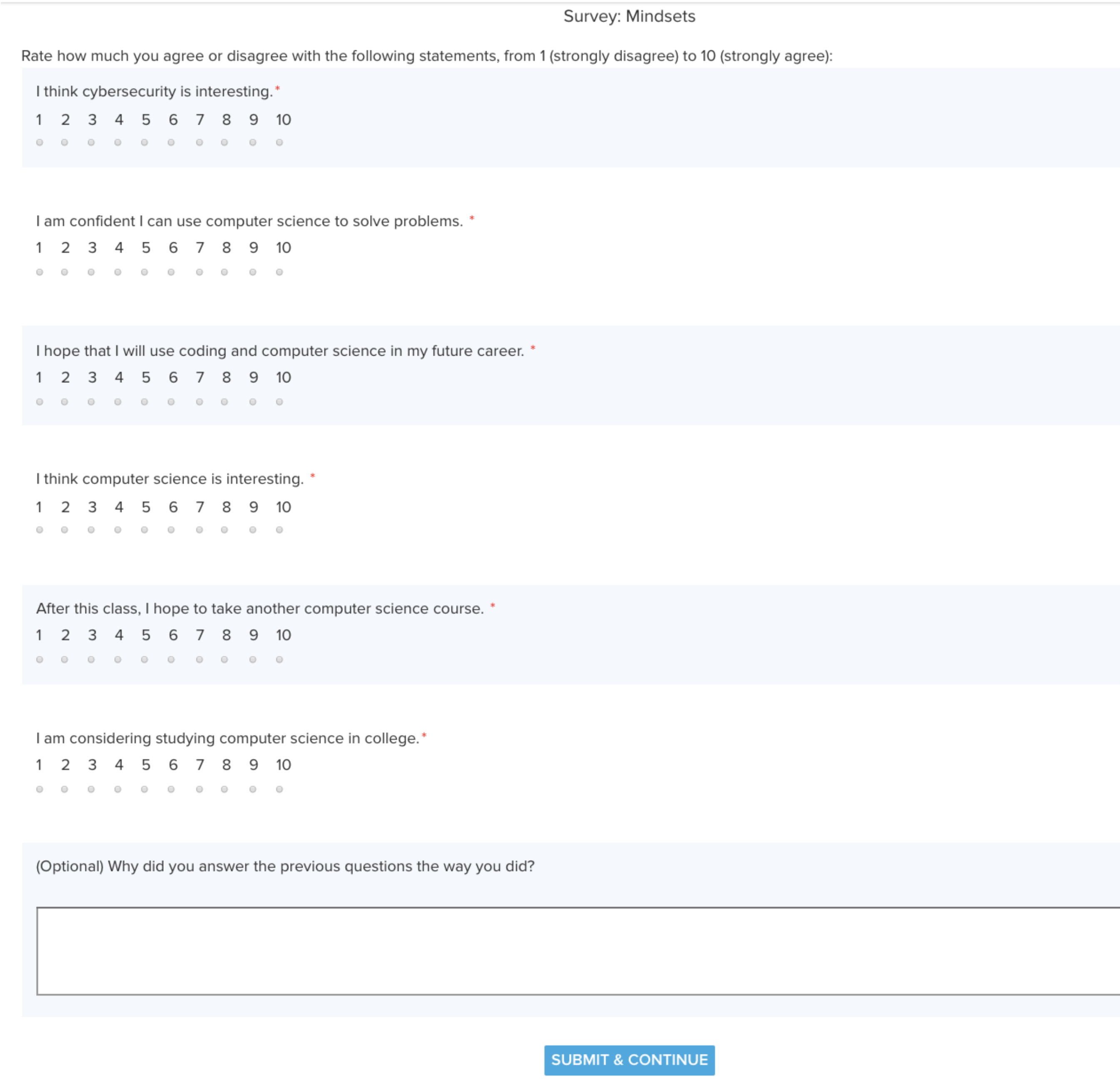
What is the benefit to encrypting a message?
A working (non-broken) encryption scheme makes it impossible for an eavesdropper to read a message if they were not the intended recipient.

What is the drawback to encrypting a message?
There are two drawbacks to encrypting a message. The first is that the sender and the recipient (Person A and Person B in this exercise), have to decide beforehand how they are going to encrypt the message. The second drawback is that is takes Person B a longer time to decode the message than if the message was not encrypted.

Is Caesar Cipher a working encryption scheme? Why or why not?
The Caesar Cipher is a broken encryption scheme because it is possible for the eavesdropper to decode the message as there are only 26 possible keys (1-26).

Appendix H

MINDSET SURVEY



Survey: Mindsets

Rate how much you agree or disagree with the following statements, from 1 (strongly disagree) to 10 (strongly agree):

I think cybersecurity is interesting.*

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

I am confident I can use computer science to solve problems. *

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

I hope that I will use coding and computer science in my future career. *

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

I think computer science is interesting. *

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

After this class, I hope to take another computer science course. *

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

I am considering studying computer science in college.*

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

(Optional) Why did you answer the previous questions the way you did?

Appendix I

KNOWLEDGE AND SKILLS SURVEY

Name: ____________________

Date: ____________________

Class: ____________________

Introduction to Cybersecurity Knowledge & Skills

1. **Which of the following is considered an unethical use of computer resources?**

   A. Downloading file sharing software on your home computer

   B. Searching online for the answers to CodeHS exercises and quizzes

   C. Purchasing an app from an app store and downloading it directly to a mobile device

   D. Searching online for an electronic version of a textbook

2. **Which of the following are characteristics of a credible source online?**
   I. The domain is .edu or .gov
   II. Multiple scholarly sources are cited
   III. The author is anonymous
   IV. The site has multiple spelling errors

   A. I only

   B. I and II

   C. I, II, and III

   D. I, II, III, and IV (all)

3. **Blake logs into the website for his math class and realizes that he has access to the upcoming midterm exam—even though his teacher said the exam questions would not be released until the day of the exam.**
   Which part of the CIA Triad has been compromised?
   I. Confidentiality
   II. Integrity
   III. Availability

   A. I and II

   B. I only

   C. III only

   D. I, II, and III

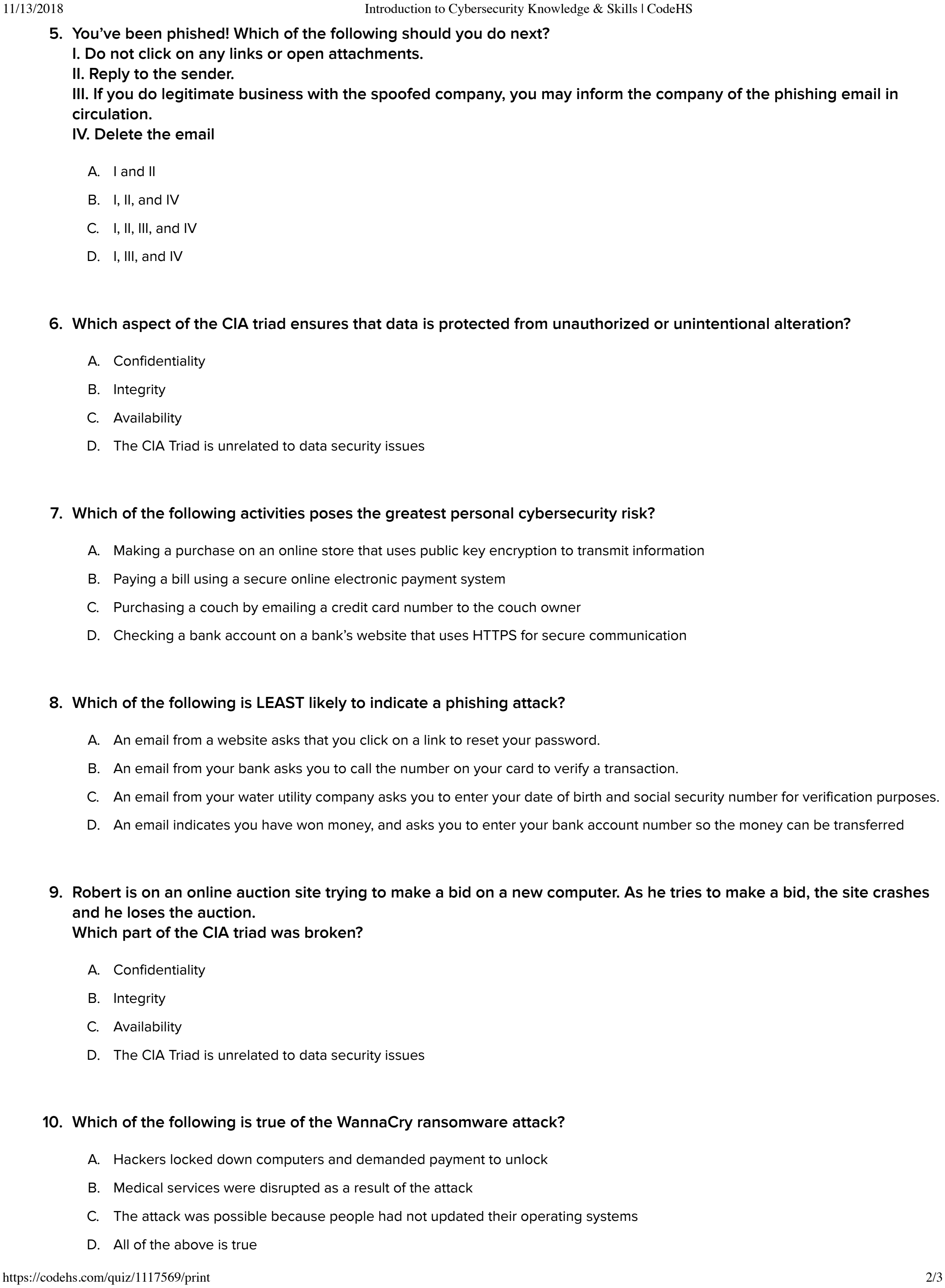
4. **Which of the following are best practices for keeping secure passwords?**
   I. Create passwords that are long in length
   II. Use the same password for multiple accounts
   III. Use a password manager
   IV. Don’t use personal information like your name or birthdate in your passwords

   A. I only

   B. I and II

   C. I, III, and IV

   D. I, II, III, and IV



5. **You've been phished! Which of the following should you do next?**
   I. Do not click on any links or open attachments.
   II. Reply to the sender.
   III. If you do legitimate business with the spoofed company, you may inform the company of the phishing email in circulation.
   IV. Delete the email

   A. I and II
   B. I, II, and IV
   C. I, II, III, and IV
   D. I, III, and IV

6. **Which aspect of the CIA triad ensures that data is protected from unauthorized or unintentional alteration?**

   A. Confidentiality
   B. Integrity
   C. Availability
   D. The CIA Triad is unrelated to data security issues

7. **Which of the following activities poses the greatest personal cybersecurity risk?**

   A. Making a purchase on an online store that uses public key encryption to transmit information
   B. Paying a bill using a secure online electronic payment system
   C. Purchasing a couch by emailing a credit card number to the couch owner
   D. Checking a bank account on a bank's website that uses HTTPS for secure communication

8. **Which of the following is LEAST likely to indicate a phishing attack?**

   A. An email from a website asks that you click on a link to reset your password.
   B. An email from your bank asks you to call the number on your card to verify a transaction.
   C. An email from your water utility company asks you to enter your date of birth and social security number for verification purposes.
   D. An email indicates you have won money, and asks you to enter your bank account number so the money can be transferred

9. **Robert is on an online auction site trying to make a bid on a new computer. As he tries to make a bid, the site crashes and he loses the auction.**
   Which part of the CIA triad was broken?

   A. Confidentiality
   B. Integrity
   C. Availability
   D. The CIA Triad is unrelated to data security issues

10. **Which of the following is true of the WannaCry ransomware attack?**

    A. Hackers locked down computers and demanded payment to unlock
    B. Medical services were disrupted as a result of the attack
    C. The attack was possible because people had not updated their operating systems
    D. All of the above is true

11. **Which of the following shows the word “CAT” encrypted with the Caesar cipher with a key of 1?**

   A. DBU

   B. CAT

   C. BZS

   D. Can not be encrypted.

12. **An encryption method that uses a series of interwoven Caesar ciphers based on the letters of a keyword is called**

   A. hashing

   B. the Vigenère Cipher

   C. the symmetric key

   D. public key encryption

13. **Encrypted information is only viewable by authorized users who have the correct key to decrypt. This describes which aspect of the CIA triad?**

   A. Confidentiality

   B. Integrity

   C. Availability

   D. Collisions

14. **By checking the box on a privacy policy page, a company can legally use your data and information in all the ways disclosed, no matter what.**

   A. True. This is always the case.

   B. True. Changing your settings does not affect the privacy policy.

   C. False. It depends if the privacy policy allows you to opt in or out of sharing data.

   D. False. Companies do not give you the option to update your settings.

15. **Felipe is trying to find information on wind power in Germany. Which of the following would be the most effective search query for this?**

   A. wind + power

   B. “wind” + Germany

   C. “wind power” - Spain

   D. “wind power” + Germany