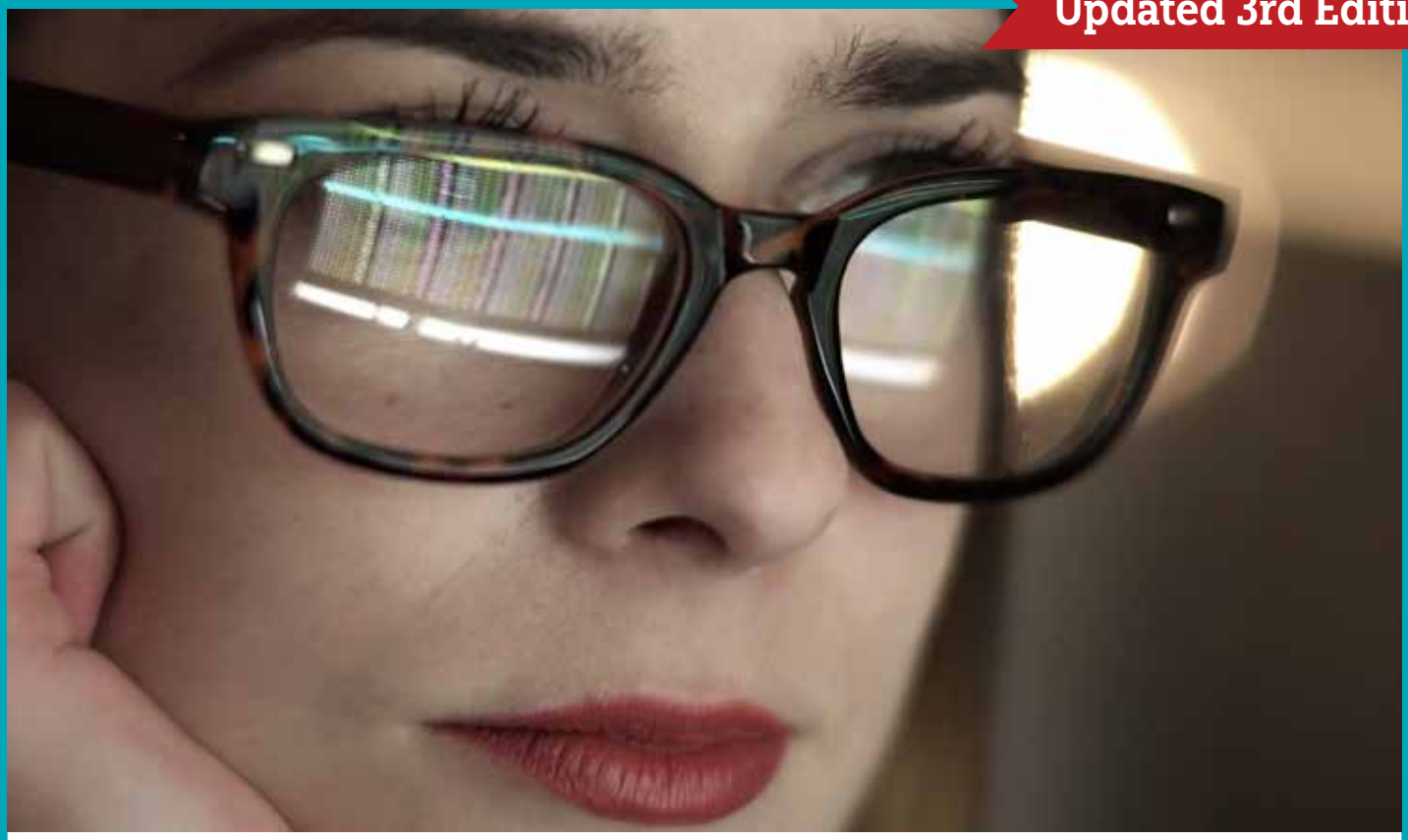
Updated 3rd Edition!



Cybersecurity Career Awareness Program (CyberCAP)

TEACHER'S GUIDE

TEACH YOUR STUDENTS:

What is cybersecurity and why should I care?

What can I do to stay safer online?

How do I know if I like or can do cybersecurity?

How do I figure out if a career in cybersecurity could be right for me?

An easy-to-use way to build cybersecurity career confidence and awareness.

Start Engineering

INTRODUCTION

Welcome to the Start Engineering Cyber Career Awareness Program, or CyberCAP, our program to build awareness and inspire confidence among middle and high school students about pursuing cybersecurity as a field of study and work. Everyone knows cybersecurity is big. And getting bigger. As both a problem and an opportunity, cybersecurity is becoming only more important in only more ways to all of us in both our online and offline lives.

Our CyberCAP program can help educators get students thinking in newly meaningful, actionable ways about cybersecurity as both a problem and opportunity. Whether in the classroom or after-school, at summer camp, in the library, or at home, kids will learn lessons about cybersecurity that apply both to their present online lives as well as the possible futures they might build by studying or working in the field.

TWO NEEDS: ONLINE SAFETY AND FUTURE WORKFORCE DEVELOPMENT

A constant stream of news items about data breaches and improper disclosures of sensitive, personal data repeatedly drives home the fact that we all need to learn and practice appropriate online behaviors. The imperatives of online safety are evolving rapidly. Starting as early as elementary school, individuals need to learn and practice appropriate online behaviors in order to have the internet continue to serve their needs at home, work, and play. This is why the principles and practices of good online safety form one of the dominant themes of this program.

At the same time, the opportunities for study and work in cybersecurity hold enormous promise for students of all backgrounds and interests. A strategic necessity for any organization that uses the inter-

net is a workforce with robust cybersecurity awareness and current, applicable skills. Such a workforce is vital to managing critical data, enabling growth, and even just staying operationally viable.

Because of a great, persistent disparity between this workforce need and the number of people prepared to fill it, students with cybersecurity skills will find an incredible range of career opportunities awaiting them upon graduation. And they have increasingly varied educational pathways available for charting a course towards the competencies in cybersecurity that will set them up for success in their work lives. From certificate programs to two- and four-year degrees, learning options exist to enable almost any kind of student interested in cybersecurity to gain the expertise and credentials he or she needs to enter the field and make it a rewarding career. For this reason, instilling awareness and confidence about pursuing a career in cybersecurity is the second dominant theme of this program.

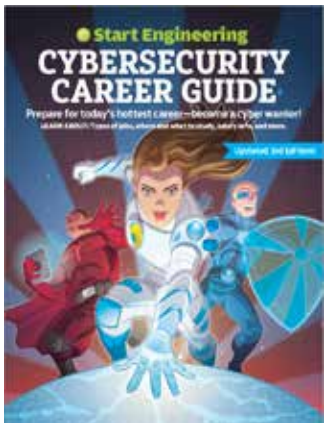
ACCESSIBLE, IMMEDIATE HELP FOR EDUCATORS GETTING STARTED WITH CYBERSECURITY

Notwithstanding the importance of online safety and the rich career prospects in cybersecurity, it can be a challenge to get students started with cybersecurity learning and awareness. It is infrequently taught in school, seen as frighteningly technical and difficult, or deemed something just not right for most students.

Our program is designed to make cybersecurity – as both a personal priority and a career opportunity – accessible and engaging for educators and students of all kinds. It can inspire confidence in both students and educators to start a rewarding journey in cybersecurity learning and even future work. The program also supports Computer Science Teachers Association learning standards related to cybersecurity. Completing the program will introduce students to the core content areas identified by CSTA as integral to cybersecurity studies.

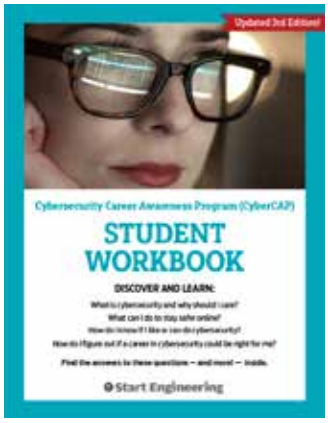
Start Engineering's CyberCAP Program

Our program has three components:



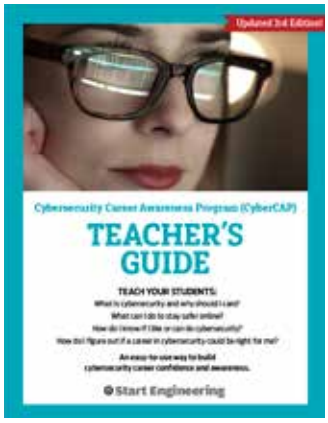
1. Cybersecurity Career Guide

Explains what cybersecurity is, covers the wide range of career opportunities in the field, describes varied educational pathways, and offers employer and salary data.



2. Cybersecurity Student Workbook

Shows students why cybersecurity is relevant to them, teaches online safety basics, and helps students assess how well cybersecurity might suit their future study and work plans.



3. Cybersecurity Teacher's Guide

Prepares educators – even with no training in the field – to help students make sense of cybersecurity as an individual imperative and future career option.

More about the Cybersecurity Teacher's Guide

This guide helps educators get the most out of the learning opportunities presented in the *Cybersecurity Student Workbook*. The workbook encourages learning in three general directions:

1. Grasp of online safety principles and practices.
2. Identifying and developing individual aptitudes for cybersecurity.
3. Understandingwhat careers in the field are all about.

See the Appendix at the end for selected learning resources in each of these areas.

The Teacher's Guide includes technical support for both the learning content and exercises featured in the workbook. Brief explanations of goals and approaches introduce each chapter, along with student learning objectives. Getting the most out of exercises is made easier with tips for leading activities, time estimates, and answer keys. Users will also find cross-references to CSTA learning standards to do with cybersecurity, available for review online at www.csteachers.org/page/standards.

Throughout the student workbook and the teacher's guide, substantive, topical content combines with engaging lessons and activities to make cybersecurity a viable, accessible learning topic in all kinds of educational settings. Even with no training in the field, educators should be able to use this guide to help students become more knowledgeable and confident about staying safer online and judging cybersecurity as a future option for study and work.

CHAPTER ONE

What Is Cybersecurity and Why Should I Care?

GOAL

Build understanding of the risk of putting personally identifiable information, or PII, online.

- Risks are pervasive and unpredictable online, coming from any direction.
- We are **all** probably more exposed than we imagine.
- Identifying particular types of risks: phishing, social engineering, malware.

APPROACH

Make online risks understandable, relevant, and personal to middle and high school students.

- Kids their age have been compromised.
- Families and schools are at risk.
- Familiar activities like email, social media, and online gaming can all involve risk.
- There are many ways for devices and accounts to become compromised.

STUDENT LEARNING OBJECTIVES

- Understand how any and all information online is at risk of disclosure or compromise.
- Understand just some of the many ways that cyber criminals work to steal data and break into systems.

ACTIVITY 1: Getting to Know Your Networks

THE POINT: Taking stock of how many networks students and their families are already part of should highlight how widely available their PII could be online.

TIPS:

- Try to get students to build as long a list as possible of the networks they are part of. It might be useful or necessary to start off with a group discussion of what networks are and brainstorm examples together.
- The whole activity can be a take-home exercise for students to do with their families.
- It can be interesting to examine how many of the same networks students and their families belong to, compared to how many different networks they are in.
- Using news reports to identify online networks that have experienced data breaches in recent times can underscore how vulnerable online repositories of our PII actually are.
- If students use the website, www.haveibeenpwned.com, be aware that the results might be sensitive or private and not appropriate for sharing with a group.

TIME ESTIMATES:

Introductory discussion ..... 15 minutes
Cataloguing networks ..... 15 minutes
Investigating possible breaches ..... 10 minutes
Describing breach responses ..... 10 minutes
Review and reflection ..... 10 minutes
Total ..... **60 minutes**

ANSWER KEY:

Students' specific answers will all vary, of course. But there will almost certainly be a set of the same networks that show up in many students' answers – Amazon, Verizon/AT&T/T-Mobile, Apple, utilities, etc. – which can serve to illustrate the larger point about how attractive these troves of concentrated data are to cyber criminals.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

ACTIVITY 2: Identify Deceptive Online Communications

THE POINT: It can be hard to recognize deceptive online communications, like phishing emails, but with some amount of practice, it gets a lot easier.

TIPS:

- Doing a quiz or two together will help students identify the tell-tale indicators of a bogus email.
- Encourage students to think critically about all online communications they receive; almost anything that seems weird or that comes out of the blue should be approached with caution and skepticism.
- Students might overestimate their abilities to detect bogus communications; real-world examples of teen-agers falling for scams can be powerful.
- As students take quizzes, encourage them to make notes of what questions they get wrong; in review, these notes might reveal a pattern for them to be aware of.

TIME ESTIMATES:

Taking 3 quizzes..... 30 minutes
Recording scores and reflection..... 15 minutes
Total..... **45 minutes**

ANSWER KEY:

Each quiz will provide its own set of answers and summary results.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

ACTIVITY 3: Engineering Your Own Scam

THE POINT: Thinking like the enemy is a key part of defensive preparedness. This exercise encourages students to step into the mind of a cyber criminal and assess online behaviors for vulnerabilities to attack. In cybersecurity, this activity is what "red teams" do to test the security of an organization's systems.

TIPS:

- Students might start by thinking of any personal experiences they've had getting fooled, or almost fooled, by online communications.
- The results of online phishing quizzes can be a source of effective tactics to include in an online scam.
- It might help students to start thinking about their social engineering scam from back to front; the ultimate goal or outcome can shape the earlier stages.
- In discussing tips students offer, be sure to address the benefits and drawbacks, including feasibility, efficiency, and resulting tradeoffs between security and accessibility of information.
- This exercise could also work as a small-group exercise, with 2-3 per group.

TIME ESTIMATES:

Developing scam..... 30 minutes
Thinking of 3 tips..... 15 minutes
Total..... **45 minutes**

ANSWER KEY:

Individual answers will vary, according to students' inventiveness and effort. The chapter provides much information about how scams work, which should provide a basis for assessing students' efforts.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-06: Explain how physical and digital security measures protect electronic information.

3A-NI-06: Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-08: Explain tradeoffs when selecting and implementing cybersecurity recommendations.

ACTIVITY 4: Research Malware

THE POINT: The more we understand about the tactics and weapons that cyber criminals have at their disposal, the better prepared we are to defend ourselves against them.

TIPS:

- In a group setting, having students cover as many different possible topics would help everyone learn more about malware. Assigning topics to students might be useful towards this end.
- Students might need help with online research; setting up a clear sequence of concrete, related questions for them to answer in their research can help keep them on track.

TIME ESTIMATES:

Researching malware.....1 - 2 hours
Reporting out to group.....30 minutes
Total.....**1½ - 2½ hours**

ANSWER KEY:

Results will vary, according to students' topic and research efforts. Professionals in the field spend enormous amounts of time and effort on understanding malware; any basic, coherent assessments of malware that students can produce would represent success.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05: Explain how physical and digital security measures protect electronic information.

3A-NI-06: Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-08: Explain tradeoffs when selecting and implementing cybersecurity recommendations.

CHAPTER TWO

What Can I Do to Stay Safer Online?

GOAL

Build understanding of some of the many ways people can act and make choices to enhance their levels of online safety.

- Consciously tending to online safety measures is a necessary, ongoing part of our digital lives.
- Most cybersecurity failures start with individuals' bad choices, whether unintentional or conscious.
- Online safety is a function of both general habits of thought and behavior as well as technical understanding of online safety tools, such as passwords.

APPROACH

Illustrate a variety of ways for students to modify or initiate behaviors that will help them stay safer online.

- Encourage students to apply a general appreciation for safety measures to their online lives.
- From general ethical principles to specific strategies for passwords, students have many ways to protect themselves.
- Knowing what kind of information cyber criminals want is key to online safety.

STUDENT LEARNING OBJECTIVES

- Understand ethical issues related to using computers and online resources.
- Understand how to build and manage strong passwords.

ACTIVITY 1: Cyberethics

THE POINT: Applying ethical reasoning to how we use computers can help to reframe students' understanding of their own behaviors in digital realms. It also helps develop students' own agency and control over their online selves.

TIPS:

- The scenarios work well as combined individual/group exercises; the questions can serve as the basis for debates among students.
- An extension exercise could include asking students to volunteer any personal experiences they might have had with ethically challenging or ambiguous circumstances to do with computers.
- Discussing the full range of possible infractions of the code of computer ethics that students identify can generate good discussions about how people can see ethical issues in different ways.
- Discussing the possible outcomes of the scenarios can be done effectively as a group exercise, especially if the first two questions are done individually.
- Inviting debate and even devil's-advocate approaches to ethical issues can lead to good discussions of both what we gain and lose as computer users; there are always tradeoffs, with real questions about costs associated with them.

TIME ESTIMATES:

Single scenario as individual exercise.....20 minutes
Single scenario as group exercise.....40 minutes

ANSWER KEY:

Each scenario describes infractions of the code of computer ethics. Students should be able to identify at least one in every instance. The possible outcomes will vary, according to students' imaginations and level of effort.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

3A-NI-06: Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

ACTIVITY 2: Staying Safer Online

THE POINT: Learning basic online safety behaviors is vital and also easy to do. Command of even just basic approaches helps eliminate much of the risk students will face in their online lives.

TIPS:

- To encourage fuller engagement with the content, ask students to rank their tips in order of importance or effectiveness.
- To extend the exercise, ask students to find other online sources of information about their chosen topics and compare the recommendations they find.

TIME ESTIMATES:

Researching tips.....15 minutes
Presentations.....5 minutes/group

ANSWER KEY:

Answers will vary, depending on students' areas of emphasis and interpretation.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05: Explain how physical and digital security measures protect electronic information.

ACTIVITY 3: Building Passwords

THE POINT: Passwords are at once the first line of protection for PII as well as something we have a great deal of control over. Developing the habit of building strong passwords is a fundamental tool in our online safety kit.

TIPS:

- Start off demonstrating the different ways to build passwords of different lengths, or do it as a group exercise.
- Model how to estimate "cracking time" in a way that correlates to password length.
- The impact of this exercise relies on students doing each part fully and thoughtfully, before moving on to next steps.

TIME ESTIMATES:

Building passwords of varying lengths ..... 10 minutes
Testing passwords online ..... 5 minutes
Comparing and reflecting on results: ..... 15 minutes
Total ..... **30 minutes**

ANSWER KEY:

Answers will vary, but the end result should be a healthy disdain for simple, carelessly constructed passwords.

CSTA LEARNING STANDARDS:

1A-NI-04: Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05: Explain how physical and digital security measures protect electronic information.

ACTIVITY 4: A Personal Password Management System

THE POINT: Passwords are only as useful as the systems we use to build and manage them. There are many ways to build and manage a strong password system, and we all need to settle on one that works for us.

TIPS:

- Avoid doing this exercise in groups or in public, if students plan to implement an approach developed in this activity.
- Any discussions of what students might actually adopt as their own practices should be confidential.

TIME ESTIMATES:

Evaluating password systems ..... 15 minutes
Developing a password system ..... 15 minutes
Total ..... **30 minutes**

ANSWER KEY:

Answers will vary, and students should be cautioned against sharing their approaches with classmates, if they plan on putting them to actual use.

CSTA LEARNING STANDARDS:

1A-NI-04: Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05: Explain how physical and digital security measures protect electronic information.

ACTIVITY 5: Password Cracking Challenge

THE POINT: Thinking like a hacker can give students insights into how to protect themselves from real-life cyber criminals in their own online lives.

TIPS:

- Works well as an individual or group exercise.
- Give out bonus points for anyone who recognizes the scenario as coming from Toy Story 3.
- It might be hard for students to guess each other's actual passwords. It can help to limit a round of guessing to a certain number of questions, and then see how close students can get to a correct guess

TIME ESTIMATES:

Building passwords for Andy.....15 minutes
Guessing others' passwords.....30 minutes
Total.....**45 minutes**

ANSWER KEY:

Answers will vary.

CSTA LEARNING STANDARDS:

1A-NI-04: Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05: Explain how physical and digital security measures protect electronic information.

CHAPTER THREE

How Do I Know if I Like or Can Do Cybersecurity?

GOAL

Guide students in identifying and exploring already-developed aptitudes and interests that are related to cognitive capacities associated with success in cybersecurity occupations.

- Imaginative problem-solving, teamwork, and systems thinking are more important than technical knowledge per se.

APPROACH

Provide a variety of activities, both quantitative and qualitative, that draw on some of the skills and faculties useful in cybersecurity work.

STUDENT LEARNING OBJECTIVES

- Understand that cybersecurity draws on varied, interrelated intellectual abilities.
- Understand their own inclinations and abilities in modes of thinking related to cybersecurity success.

ACTIVITY 1: Numbers, Numbers, Numbers

THE POINT: Identifying patterns and relationships among numbers outside of those based on addition, subtraction, multiplication, and division requires the kind of imagination and alternative perspectives on seemingly familiar things that cybersecurity professionals need.

TIPS:

- Encourage students to look beyond the format and appearance of these exercises; solving the problems requires seeing things from new and different angles.
- The problems work well as small-group exercises.
- All these exercises relate to skills used in encryption: learning to see things as other than what they seem to be at first blush. Finding patterns or filling in missing but implied pieces of information will help students see how information can be hidden in many ways, even when it's in plain sight.

TIME ESTIMATES:

Problems A – C ..... 10 minutes
Problems D – G ..... 15 minutes
Problems H – J ..... 20 minutes
Total ..... **45 minutes**

ANSWER KEY:

A) **25.** *You add the digits of each number, then multiple the result, to get (1+4) x (4+1) or 5 x 5..*

B) **28.** *Each number increases by the difference of the previous two numbers plus 1; 3(+3), 6(+4), 10(+5), 15(+6), 21(+7).*

C) **1113122112.** *Each successive number "describes" the prior number; 132112 becomes: one (1)1, one (1)3, one (1)2, two (2)1's, and one(1)2, or 1113122112.*

D) **56** *Starting with 1, the numbers double from left to right: 1, 2, 4, 8, 16, 32, 64, 128, 256.*

E) **((8 + 2) x 5) – 7 = 43**

F) **7 – (6 / (1 + 1)) = 4**

G) **((6 + 3) x 9) – 1 = 80**

H) **4 x (9 – (7 / 7)) = 32**

I) **A = 5; B = 1; C = 4; D = 2; E = 3**

J) **A = 1; B = 4; C = 3; D = 5; E = 2**

K) **A = 1; B = 3; C = 2; D = 5; E = 4**

CSTA LEARNING STANDARDS:

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

ACTIVITY 2: Words, Words, Words

THE POINT: As with the numbers exercises, these word-based exercises encourage students to look at things from new angles. Finding patterns, filling in missing information, and getting out of established habits of mind is key to solving cybersecurity problems.

TIPS:

- Exercises work well in groups or individually.
- Students can make up their own exercises along similar lines, once they get the hang of these examples.
- Have students reflect on which set of exercises — the numbers or the words — seemed more fun or easier or more interesting.

TIME ESTIMATES:

Each exercise.....5 minutes
Total.....**20 minutes**

ANSWER KEY:

A) dove; nice; army; vine; then

B) book crook; long song; small ball; high fly; low blow

C) Herb, Job, Nice, Polish, and Differently(!)

D) That that is, is. That that is not, is not. Is not that it? It is.

CSTA LEARNING STANDARDS:

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

ACTIVITY 3: Reasoning

THE POINT: Creative reasoning is a go-to skill for cybersecurity professionals. These exercises challenge students to pay attention to details, see beneath the surface, and be imaginative.

TIPS:

- The answers are often right in front of students, on the page. Trying out one together can help them get the hang of how to think about the others.
- Putting a time limit on individual attempts to solve problems might be necessary; solving them as a group after a certain period still works well.

TIME ESTIMATES:

Exercises A - E ..... 2 - 3 minutes each
Exercises F - J ..... 10 - 15 minutes each

ANSWER KEY:

A) **9.** 2 parents, 6 daughters, and the same 1 brother for all.

B) **3 minutes.** If it takes 3 minutes for 1 cat to catch 1 mouse, it doesn't matter how many cats are catching how many mice, as long as they are all catching just 1. It will always take 3 minutes.

C) The letters can be used to spell "one word."

D) 7.

E) 60 minutes. Pill 1 at 0:00; pill 2 at 0:30; pill 3 at 0:60.

F) Take a piece of fruit from the box marked "apples and oranges." Suppose the fruit you take is an apple. Then that box must be the box containing just apples. Therefore, the box marked "oranges" can't be the box containing just apples, and it can't be the box containing just oranges either — so it must be the box containing apples and oranges. The remaining box is therefore the box containing just oranges.

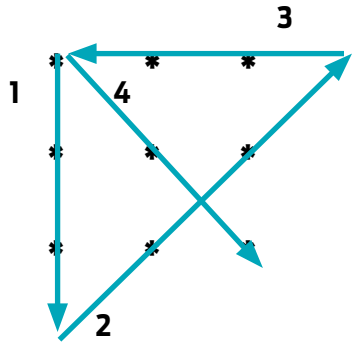
If the fruit you take out is an orange, the solution is derived in a similar fashion: the box marked "apples and oranges" is the box containing just oranges; the box marked "apples" is the box containing both apples and oranges; and the box marked "oranges" is the one containing just apples.

G) Two half-full barrels are dumped into one of the empty barrels. Two more half-full barrels are dumped into another one of the empty barrels. This results in nine full barrels, three half-full barrels, and nine empty barrels. Each son gets three full barrels, one half-full barrel, and three empty barrels.

H) There were two little girls and a boy, their parents, and their father's parents, totaling seven people.

I) Light one fuse at both ends and, at the same time, light the second fuse at one end. When the first fuse has completely burned, you know that a half hour has elapsed, and, more relevantly, that the second fuse has a half hour left to go. At this time, light the second fuse from the other end. This will cause it to burn out in 15 more minutes. At that point, exactly 45 minutes will have elapsed.

J.



CSTA LEARNING STANDARDS:

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

ACTIVITY 4: Algorithms

THE POINT: Algorithms underlie an incredible range of digital experiences we have, from following directions on our phones to picking out new movies on Netflix to generating Google search results. Understanding the basic logic enabling all these phenomena is necessary for being digitally literate.

TIPS:

- Spend some time expanding students' grasp of what algorithms are and how they work.
- Students should easily be able to identify other processes for which algorithms could be written after completing the exercise.
- Testing out students' algorithms is more than half the fun of this exercise.

TIME ESTIMATES:

Developing algorithm ..... 10 minutes
Testing out students' work ..... 20 minutes
Total ..... **30 minutes**

ANSWER KEY:

Answers will vary, but putting students' algorithms to the test by having them follow each others' steps will demonstrate which ones work and which ones need fixing.

CSTA LEARNING STANDARDS:

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

ACTIVITIES 5-8: Cryptography

THE POINT: Cryptography is a linchpin of cybersecurity technologies. These examples are all vastly simpler than systems professionals use, but the principles remain the same.

TIPS:

- All these exercises lend themselves to students using the models of cryptography they present to words and/or messages of their own devising, which they can exchange with others.
- Looking at all the methods as a whole, students should be able to make comparisons and judgments about relative effectiveness, complexity, secretiveness, etc.

TIME ESTIMATES:

Each individual activity.....15 minutes

ANSWER KEY:

Activity 5: Party at Nate's house tonight at eight.

Activity 7: Pop quiz in math class today.

Activity 8:

1. Racecar
2. Stamp
3. Map
4. Heroine
5. Towel
6. Footsteps

CSTA LEARNING STANDARDS:

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

ACTIVITY 9: Crossword Puzzle—Vocabulary Review

THE POINT: Active review of new words and concepts reinforces the learning students have gained from the workbook so far.

TIPS:

- Have students try the puzzle first without going back to review any previous parts of the book.

TIME ESTIMATES:

Complete entire puzzle.....15 minutes

ANSWER KEY:

ACROSS	DOWN
1. PII	1. Phishing
5. Algorithm	2. Password manager
7. Virus	3. Trojan horse
8. Worm	4. Https
9. Ransomware	6. Malware
10. Spyware	
11. Cipher	

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

CHAPTER FOUR

How Do I Figure Out if a Career in Cybersecurity Could Be Right for Me?

GOAL

Help students identify the general area of cybersecurity that might be a good fit for them and start making plans for further education that will move them towards work in the field.

- Cybersecurity offers many different kinds of career paths, demanding various forms of expertise; there is something in the field for students of all backgrounds and interests.

APPROACH

Project students as actors into real-world incidents of cyber attacks to help them imagine working in the field. Then guide students through a career self-assessment exercise to help them identify the area(s) of the field that might suit their abilities and interests.

STUDENT LEARNING OBJECTIVES

- Understand how widely and deeply cybersecurity threats affect industries and organizations.
- Understand the general landscape of the cybersecurity work world.
- Understand what role(s) in cybersecurity could be a good fit.

ACTIVITY 1: Cybersecurity in Action

THE POINT: Real-world cyber attacks make regular news but understanding the impact or consequences can be hard. Researching details and projecting themselves into attacks as investigators and responders helps students make their own assessments of cyber threats in general as well as what kind of work in the field might be interesting for them.

TIPS:

- These exercises are long and involve many parts. Breaking them up into individual and group activities and spreading them out over days will help.
- Cyber attacks make lots of news and generate extensive technical analysis. Extending research efforts can enrich understanding but it can also become overwhelming. The goal here is as much to exercise students' imaginations as their research skills.
- The exercise asks students to examine three different scenarios; limiting the scope to one or even two scenarios might feel more manageable for both teachers and students.
- Students might want to revise or revisit their answers after discussions or reports of others' answers.
- In discussion, important themes to emphasize include both the benefits and the costs of improving security; tradeoffs in cybersecurity measures are very important to acknowledge and account for in implementation decisions.

TIME ESTIMATES:

One scenario, questions 1 – 7 ..... 40 minutes
Discussion time ..... 20 minutes
Questions 8 – 10 ..... 75 minutes
Discussion time ..... 45 minutes
Total ..... **180 minutes**

ANSWER KEY:

Answers will vary widely.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

3A-NI-06: Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-08: Explain tradeoffs when selecting and implementing cybersecurity recommendations.

ACTIVITY 2: Career Exploration

THE POINT: Cybersecurity work involves so many different, interrelated topics that opportunities in the field exist for students of nearly all backgrounds and interests. Introducing them to the wide, diverse landscape of work options in the cybersecurity field is the first step in helping them plot a pathway into the career that fits them best.

TIPS:

- The NICE career framework often uses abstract language and technical terms that can be confusing and vague. Developing workable, student-led definitions of the career roles can help everyone make sense of the exercise.
- The "work roles" exercises on page 63 take some tricky website navigation. Getting students to the right materials and helping them review the information might be best done as a group, or with full, individual guidance.
- Students might have trouble coming up with related classes or subjects in the final exercise. Again, guidance and group discussions can help.

TIME ESTIMATES:

Ranking career categories	10 minutes
Exploring Pro's and Con's	20 minutes
Reflection and review	10 minutes
Identifying work roles	15 minutes
Analyzing work role components	15 minutes
Connecting to school options	15 minutes
Total	**85 minutes**

ANSWER KEY:

Answers will vary widely.

CSTA LEARNING STANDARDS:

1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected.

Appendix

The CyberCAP program focuses on three main areas of learning related to cybersecurity, both as an individual imperative and potential career pathway:

- Grasp of online safety principles and practices.
- Identifying and developing individual aptitudes for cybersecurity.
- Understanding what careers in the field are all about.

Select resources appear below that can provide sources of materials for further learning in each of these areas.

Grasp of online safety principles and practices

National Cybersecurity Alliance – online safety tips and resources, presented under the Stay Safe Online banner.
https://staysafeonline.org/stay-safe-online/

Common Sense Media Digital Citizenship – ready-to-teach lessons in all facets of online safety and awareness for all levels of K-12.
https://www.commonsense.org/education/digital-citizenship

Federal Trade Commission – guidance for adults and kids in staying safe while exploring a wide variety on online activities
https://www.consumer.ftc.gov/topics/protecting-kids-online

Connect Safely – high-quality tips, advice, guidance, and news about online safety from a long-running Silicon Valley nonprofit organization.
https://www.connectsafely.org/

Identifying and developing individual aptitudes for cybersecurity

Cyberstart – cybersecurity training brought to life through real-world hacking challenges and puzzles, accompanied by a rich blog.
https://cyberstart.com/

NOVA Labs cybersecurity – an online cybersecurity simulation from PBS that offers lots of resources to support educators using the tool.
https://www.pbs.org/wgbh/nova/labs/lab/cyber/

TeachCyber – a high school cybersecurity education curriculum framework developed by some of the leading experts in the field.
https://teachcyber.org/

Appendix continued

Understanding what careers in the field are all about

Life Hackers – a documentary film from RoadTrip Nation, with three aspiring cybersecurity professionals exploring new and surprising directions people are going in the field.
https://roadtripnation.com/roadtrip/cybersecurity-documentary

Palo Alto Networks Career Guide – In their own words, stories from scores of cybersecurity professionals about how they got started in the field.
https://www.paloaltonetworks.com/resources/ebooks/cybersecurity-career-guide

NICE Career Framework – Schematic overview of the different roles and functions that people fill in the field of cybersecurity.
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

CyberSeek – Detailed, interactive data about jobs and career trends in cybersecurity, with background information for educators and students.
https://www.cyberseek.org/