Updated 3rd Edition!

Cyber 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

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: 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.

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 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.

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 multiply 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 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.

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 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 64 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.