

YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.



Student Workbook

OUTSMART CYBERTHREATS

Learn how to take good care of your data.

BONUS: Discover a cool new career in cybersecurity!



NATIONAL CRYPTOLOGIC FOUNDATION
CYBER CENTER FOR EDUCATION & INNOVATION

Fall 2022

Incidents of cyber attacks on individuals in the United States are growing in number daily.

Every time you use your smartphone, tablet, or computer, you share personal data, making you vulnerable to outside, potentially malicious actors. Do you know how to keep your data safe? Do your students? In an increasingly digital world, students must learn about cybersecurity principles in order to protect themselves, their devices, and their futures, and educators play a vital role in facilitating this.

The National Cryptologic Foundation's (NCF) Cyber Center for Education and Innovation (CCEI), a leading expert in K-12 cyber education, in partnership with Start Engineering and Gula Tech Adventures, developed the *Outsmart Cyberthreats* Teacher Guide and Student Workbook so middle and high school educators and students can easily access principles of cybersecurity through the language of Data Care.

The pages that follow detail lessons that teach students not only to understand Data Care principles, but how to put them into practice by using real life examples of cyber threats that students are at risk of every day. We hope this workbook prepares our next generation's workforce to both keep their data safe now, as well as sparks their interest in cybersecurity professions they might one day pursue.

To learn more about the collaborative work that the CCEI is doing amongst many partners in K-12 education, please visit the education program page at cryptologic-foundation.org.

Sincerely,

Laura C. Nelson
President & Chief Executive Officer

TABLE OF CONTENTS

Introduction, p4

PART 1

A Day in the Life of Your Phone p5

Activity 1.1.a: Which Companies Gather the Most Data About You as a User? p6

Activity 1.2.a: The Cost of Cyber Crime, p9

Activity 1.3.a: Harry Potter Is Coming to Town, p11

Activity 1.3.b: Protecting Your School's Grades, p14

PART 2

How Things Go Wrong Online p17

Activity 2.1.a: What Are the Signs of a Bogus Email? p18

Activity 2.1.b: How Good Are You at Spotting Phishing? p20

Activity 2.2.a: Data, Data, Everywhere, p21

Activity 2.2.b: You and Your Data Shadow, p24

Activity 2.3.a: Make an Impossible-to-Crack Password, p27

Activity 2.3.b: How to Manage — and Remember — Your Passwords, p30

PART 3

Control Your Risk Online p32

Activity 3.1.a: Identifying Risks, p33

Activity 3.2.a: How Risky Is Your Phone? p36

Activity 3.3.a: How Likely Is a Cyber Attack in Each Circumstance? p38

PART 4

Explore a Future in Cybersecurity p41

Activity 4.1.a: Riddles and Puzzles to Tickle Your Brain, p43

Reflection on 4.1.a, p48

Activity 4.1.b: Riddles and Puzzles to Tickle Your Brain, as a Group, p49

Activity 4.1.c: Compete in Teams to Solve Riddles and Puzzles, p52

Activity 4.2.a: K-12 Schools Under Threat of Cyber Attack, p55

INTRODUCTION

Welcome to *Outsmart Cyberthreats!*

Outsmart Cyberthreats gives you a full picture of how your personal data gets collected and used — whether you like it or not — when you go online. If *Outsmart Cyberthreats* motivated you to learn how to protect your data on the internet, then this Student Workbook will introduce you to the tools to do so. The information in this book can empower you to employ better online safety practices and direct you towards some of the many different ways you might build a career in the field of cyber.

The activities you will engage in reflect actual cybersecurity challenges that professionals encounter in their everyday work lives. Because the world is evolving and becoming more interconnected through the use of the internet, any future career that you choose will almost certainly require knowing and understanding one or more of the data care concepts presented in the activities in this book. As you complete each section, make note of what captures your attention, or even seems fun to you, as it could be something you might want to explore further after completing this workbook.

Staying safe online comes down to how well we as individuals take care of our own data. If you want to help make the internet a better, safer, and more fun environment for all of us, you can start by learning the data care concepts in this workbook and helping your family and friends to recognize ways that their data is at risk. Then, discover how these concepts are used in professional careers by exploring the vast field of cyber at cryptologicfoundation.org.



PART 1

A DAY IN THE LIFE OF YOUR PHONE

WHAT YOU'LL LEARN

- Companies collect huge amounts of data about us whenever we go online, whether we like or not.
- Criminals lurk in every corner of the internet, and cybercrime adds up to staggering amounts of money.
- Protecting online data involves overlapping, interrelated types of security measures.

WHAT YOU'LL DO

Section 1: Companies Do Love to Gather Data

1.1.a: Which Companies Gather the Most Data About You as a User? p 6

Section 2: The Many Bad Things That People Can Do Online

1.2.a: The Cost of Cybercrime, p 9

Section 3: D-e-f-e-n-s-e, Defense!

1.3.a: Harry Potter Is Coming to Town, p 11

1.3.b: Protecting Your School's Grades, p 14



PART 1: A DAY IN THE LIFE OF YOUR PHONE



1.1.a

Which Companies Gather the Most Data About You as a User?

Below is a list of some of the most popular social media and video streaming services. Use the table on the next page showing data collection practices by these companies to arrange them in order from the most “data-hungry” to the least “data-hungry.” Count the total number of blocks across all the different “types” of data that each service collects, putting the service with most blocks at #1 and the one with fewest at #10, and the rest in between.

Netflix 1. _____

Amazon Prime Video 2. _____

Disney + 3. _____

YouTube 4. _____

HBO Max 5. _____

Facebook 6. _____

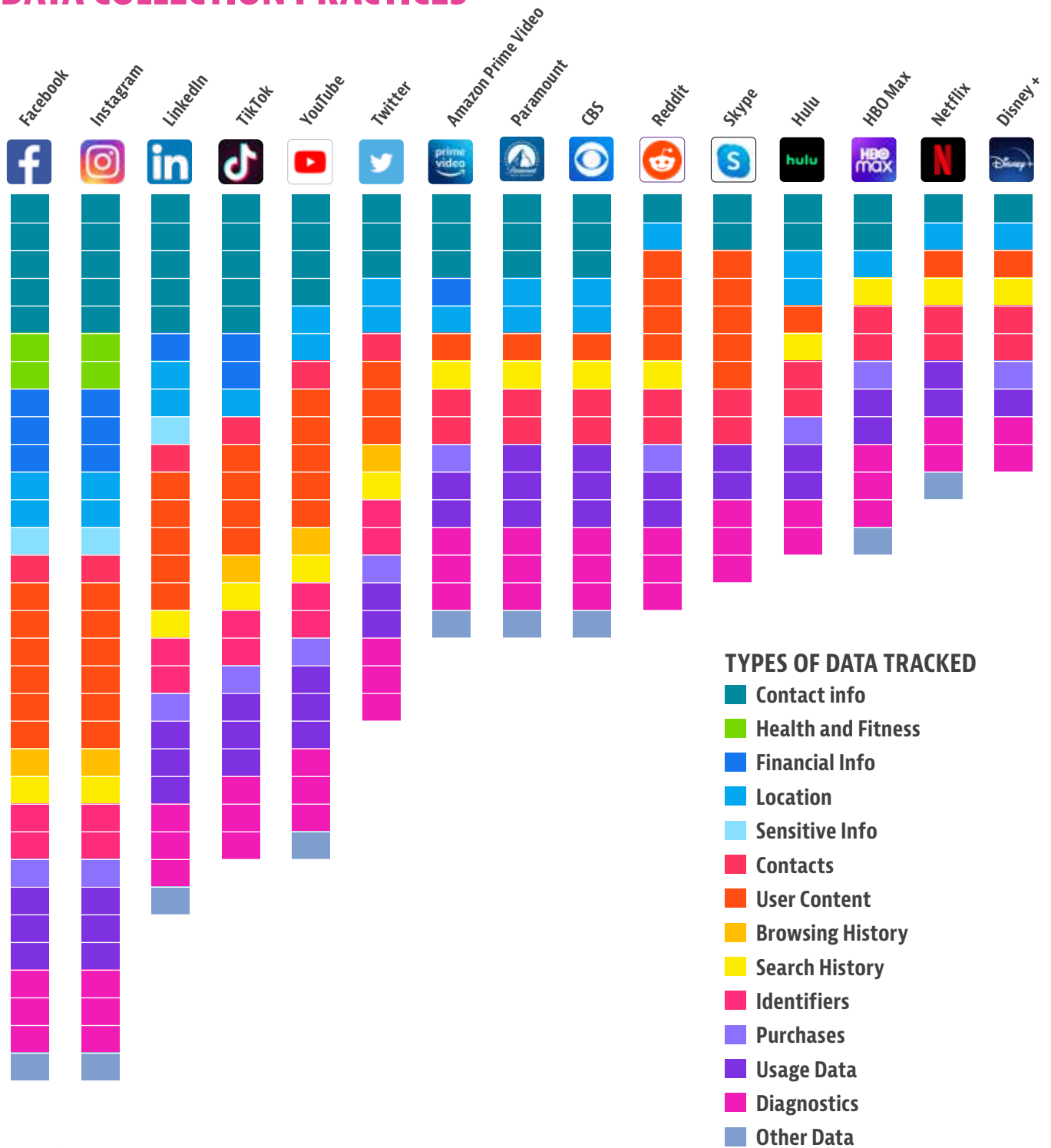
TikTok 7. _____

Twitter 8. _____

Instagram 9. _____

Skype 10. _____

DATA COLLECTION PRACTICES



DATA COURTESY SURFSHARK

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.1.a (CONTINUED)

Look at the types of data that these companies track, identified by the colored boxes displayed below each company's entry in the table.

1. In your opinion, which companies (find 2 or 3) collect data that is most relevant or connected to their business? Why?

2. Which companies collect data that is *least* relevant to their business? Why do you think they collect this kind of data?

PART 1: A DAY IN THE LIFE OF YOUR PHONE

1.2.a

The Cost of Cyber Crime



According to the FBI, the five types of cyber crimes committed most frequently in 2020, with number of victims, were:

- | | |
|-----------------------------|---------|
| 1. Phishing | 241,342 |
| 2. Non-payment/non-delivery | 108,869 |
| 3. Extortion | 76,741 |
| 4. Personal data breach | 45,330 |
| 5. Identity theft | 43,330 |

And the five costliest types of cyber crimes, based on damages in dollar amounts, were:

- | | |
|--|-----------------|
| 1. Fraudulent fund transfers, by email | \$1,866,642,107 |
| 2. Confidence fraud | \$600,249,821 |
| 3. Investment | \$336,469,000 |
| 4. Non-payment/non-delivery | \$265,011,249 |
| 5. Identity theft | \$219,484,699 |

Pick out **ONE** of these types of cyber crimes and do an online search for examples of them getting reported in the news. List three incidents you found, along with brief descriptions of them.

Cyber crime incidents

1. _____

2. _____

3. _____

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.2.a (CONTINUED)

Choose ONE of these three incidents and answer the questions below:

1. How many people were affected by this incident?

2. Who, if anyone, was identified as the perpetrator of the incident?

3. What were the consequences for the people involved?

PART 1: A DAY IN THE LIFE OF YOUR PHONE

1.3.a

Introduction

In this exercise, you will be asked questions involving three different types of security controls, or measures designed to protect valuable resources or spaces related to data networks:

- **Physical controls** prevent access to IT systems with countermeasures such as fencing, locks, guard dogs, closed-circuit TV, etc.
- **Technical controls** are features built into hardware and software systems designed to confirm the identity of a user trying to gain access to a network or data source. Identification, authentication, and authorization are the basic components of technical controls.
- **Administrative controls** include rules, regulations, laws, and policies governing who should and should not have access to data systems. These controls are usually set by governments or organizations that store and own data.

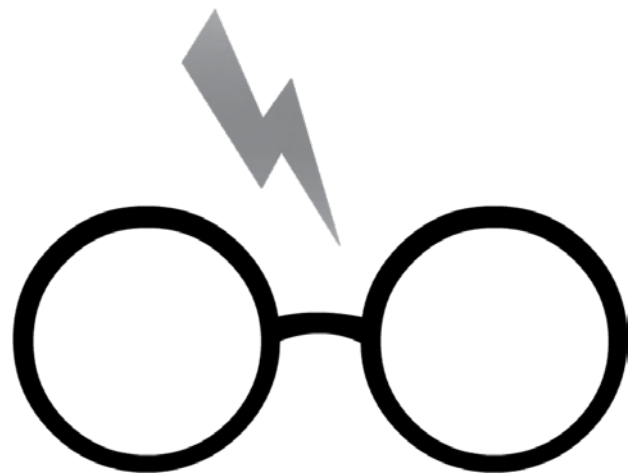
As elements of a multidimensional security system, these controls overlap in an approach to protecting data called “defense in depth.” Sets of controls reinforce one another so that if any one set fails, the other controls remain in place as security measures. These two related concepts — “security controls” and “defense in depth” — are fundamental aspects of data care. The exercises that follow will show you in more detail how all of these features and approaches to security can fit together.

Harry Potter Is Coming to Town

Incredible news! Harry Potter, the wizard of Hogwarts, has stepped out of the movies and into real life. He is coming to your school for an assembly, a one-time-only event to include a demonstration of magic and discussion of the story behind his final triumph over the dark lord himself, Voldemort. Everyone in the world wants to come, but he has made it completely clear: Only students, teachers, and administrators in your school are allowed to attend.

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.3.a (CONTINUED)

To control who is allowed into the event, your school is bringing in the National Guard. Members of the Guard will set up checkpoints around the perimeter of the school property, with traffic barriers and guard dogs at each one. They will be checking identification credentials to ensure only you and your schoolmates can pass through.



To get through the checkpoints, each student will have to show their school identification card as well as provide a special password to be distributed through the school email system. The password will be given out in code, and the key for cracking the code will be handed out in social studies class the day before the assembly.

Everyone is excited beyond words. Now, if only you could find that dang ID card you got on the first day of school and immediately put ...

In the Harry Potter scenario above, identify the security controls that belong in each of the three categories below:

1. Physical controls

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.3.a (CONTINUED)

2. Technical controls

3. Administrative controls

PART 1: A DAY IN THE LIFE OF YOUR PHONE

1.3.b

Protecting Your School's Grades

For years, your school has struggled with gathering, calculating, recording, and reporting grades for students at the end of the term. All the teachers have had to manage their own individual systems for grading, doing it all on paper or their own computers and then submitting students' grades in triplicate on a hard-copy form that administrators then had to enter into a computer in the conference room next to the principal's office, with paper files stored in a locked cabinet in a closet down the hall. Some years it took until July for students' final grades to arrive!



But this year, everything will be different. A new computer system will allow teachers to log in to one, centralized data system and enter grades for each and every assignment as the year goes on. Every student will have a profile in the system containing all their personal and academic data, not only from the current school year but every prior year of their academic history, as well. Students' parents will also get login credentials and be able to see real-time grading data.

At the end of each term, the system will automatically calculate final grades as soon as teachers complete their assessments of each student's last assignments. Report cards will then be generated, and email notices will go out to students and their families with instructions about how to access them.

Everyone is really excited about this new system, except for, well, the students. Great, your friends are saying, more ways for my parents to bug me about homework.

Your school's new grading system will need robust, reliable security controls. What kinds of protections would you build into a "defense-in-depth" data security system to keep it safe? Think about how to protect grading data from being entered falsely or changed after entry, how and where the machines can be best protected, how to make sure each user group (administrators, teachers, students, parents) gets access to the data they are supposed to see, and other kinds of controls that might be needed.

Turn the page.

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.3.b (CONTINUED)

In each of the three categories below, identify the kinds of controls you would build into your school's "defense-in-depth" data security system, along with a brief explanation of why. Provide at least three examples of controls in each category.

1. Physical controls — and why

a. _____

b. _____

c. _____

2. Technical controls — and why

a. _____

b. _____

PART 1: A DAY IN THE LIFE OF YOUR PHONE, 1.3.b (CONTINUED)

c. _____

3. Administrative controls — and why

a. _____

b. _____

c. _____

PART 2

HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT

WHAT YOU'LL LEARN

- All about phishing emails and how to identify them.
- Data takes many forms – making it safe AND accessible can be tricky.
- How to build and manage strong passwords, the first, best defense against threats to your data.

WHAT YOU'LL DO

Section 1: Let's (Not) Go Phishing and How to Stay Safe While Doing So

- 2.1.a: What Are the Signs of a Bogus Email? p18
- 2.1.b: How Good Are You at Spotting Phishing? p20

Section 2: The Many Faces of Data

- 2.2.a: Data, Data, Everywhere, p21
- 2.2.b: You and Your Data Shadow, p24

Section 3: Building and Managing Passwords for Security and Convenience

- 2.3.a: Make an Impossible-to-Crack Password, p27
- 2.3.b: How to Manage — and Remember — Your Passwords, p30



PART 2: HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT


2.1.a

What Are the Signs of a Bogus Email?

Most phishing emails will reveal themselves as fake when you look at them closely. Telltale signs of a phishing email include things like spelling and punctuation errors, awkward formatting, constructions of language that do not really make sense, URLs that do not contain the name of the company behind the message, and absent or invented information related to the person receiving the email.

Look at the email below and see how many clues you can find that reveal it as part of a phishing campaign. Try to identify at least **five** clues within the email.

From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM



Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | [Privacy Policy](#) | [Terms of Service](#)

PART 2: HOW THINGS GO WRONG ONLINE, 2.1.a (CONTINUED)

1. _____

2. _____

3. _____

4. _____

5. _____

BONUS, CAN YOU FIND ANY MORE?

6. _____

7. _____



2.1.b

How Good Are You at Spotting Phishing?

Below are links to some online phishing quizzes. You can also find other quizzes by searching for "online phishing quiz." Pick out 2-4 quizzes to take, record the results in the table, and then answer the questions below.

PHISHING QUIZ	HOW I DID
1. opendns.com/phishing-quiz/	1.
2. sonicwall.com/en-us/phishing-iq-test	2.
3. phishingquiz.withgoogle.com/	3.
4. phishingbox.com/phishing-test	4.

1. What kinds of indicators of bogus emails did you learn about from taking the quizzes? Name at least three.

2. Compare the results of your quizzes. Were they different? If so, why do you think they differed?

3. If you were teaching someone else about identifying a phishing email, what three things would you identify as most important for them to remember or look out for?

PART 2: HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT



2.2.a

Data, Data, Everywhere

Three landmark data breaches that raised the profile of risks to personal data stored in online systems were the Sony PlayStation hack of 2011, the theft of credit card data from Target in 2013, and the break-in against the federal government’s Office of Personnel Management in 2015. Each affecting millions of people, these large-scale data breaches illustrate how attacks on data systems can target the confidentiality, integrity, and availability of personal information.

Read the brief articles at the websites shown below and then answer the questions that follow addressing details of the incidents.

Sony PlayStation: “2011 PlayStation Network Outage”
https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage

Target: “Target’s point-of-sale terminals were infected with malware.” Computer World; <https://www.computerworld.com/article/2487643/target-s-point-of-sale-terminals-were-infected-with-malware.html>

Office of Personnel Management: “Cybersecurity Incidents”
<https://www.opm.gov/cybersecurity/cybersecurity-incidents/>

1. In brief terms, describe what happened with each attack?

Sony PlayStation _____

PART 2: HOW THINGS GO WRONG ONLINE, 2.2.a (CONTINUED)

Target _____

Office of Personnel Management _____

2. What part or parts of the CIA triad were harmed in the attack? Identify all that apply and explain briefly.

Sony PlayStation _____

PART 2: HOW THINGS GO WRONG ONLINE, 2.2.a (CONTINUED)

Target _____

Office of Personnel Management _____

PART 2: HOW THINGS GO WRONG ONLINE

2.2.b

You and Your Data Shadow

As a student, you – and all the things you do – generate large volumes of data for your school to collect. From your parents enrolling you in school to your schedule of classes and all the grades you get in them to all the other things you do during the school year, your school keeps track of many different types of data related to who you are and what you do.

1. What specific types of data can you imagine your school gathering about you?

Think about both online and in-person activities as well as all the different places you go and things you do throughout the whole school year. Name as many different kinds of data as you can, with a goal of at least 10 items.

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

PART 2: HOW THINGS GO WRONG ONLINE 2.2.b (CONTINUED)

2. How important is it to maintain the confidentiality, integrity, and availability of the data types? Rank the 10 data types you listed in question 1 in order of most to least important for each aspect of CIA. Remember:

Confidentiality means keeping data visible and accessible only to people with proper authorization.

Integrity means keeping data accurate and consistent across storage locations.

Availability means making sure data is accessible when and where users need it.

If you came up with more than 10 items in number 1, pick out just 10 to use in this exercise.

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
6.	6.	6.
7.	7.	7.
8.	8.	8.
9.	9.	9.
10.	10.	10.



2.3.a

Make an Impossible-to-Crack Password

People are generally careless and uninformed when it comes to building passwords. The single most important action individuals can take to protect themselves online results, all too often, in epic failure. The most commonly used passwords include obvious, simple constructions like "123456," "qwerty," and "password." Cracked by a computer in nanoseconds and guessed by hackers almost as quickly, passwords such as these represent open invitations to data theft. If any of your passwords look anything like these, stop reading and go change them. Now.

A good password is long, varied, memorable, and unique. In this exercise, you will test out passwords of different lengths and forms to learn what strong and weak passwords actually look like. NOTE: Any password you build for use in this exercise is automatically and immediately unusable as a password in your personal life. You should always keep your passwords private, just for your use and knowledge.

First, make up passwords of three different lengths: 6, 9, and 12 characters.

- 1. _____
- 2. _____
- 3. _____

Then, go to <https://www.security.org/how-secure-is-my-password/> and enter the three passwords you made up. Record how long it would take to crack each one.

PASSWORDS	CRACKING TIME
1.	
2.	
3.	

PART 2: HOW THINGS GO WRONG ONLINE, 2.3.a (CONTINUED)

Next, make your passwords more complex by varying the types of characters used in them. Include upper- and lower-case letters, numbers, and special symbols (&%\$#), but still use 6, 9, and 12 characters to test your passwords.

What is the hardest-to-crack password you can develop at each length?
How long would it take to crack it? Try it now.

PASSWORDS	CRACKING TIME
1.	
2.	
3.	

Compare the cracking times across the different password lengths.

1. What do you think is most important to include in a password if you want to make it hard to crack? Length? Varied characters? Some combination?

2.3.b

How to Manage — and Remember — Your Passwords

Now that you know how to build a strong password, you need to develop a system to help you manage and remember it. Or actually, manage them. Because you should never use a password – however strong it might be – more than once. The exercises below show you different approaches to building passwords. NOTE! Any password you write down in this workbook is compromised and public. **Never use any passwords from these exercises for actual online accounts.**

Make them mean something

Choose a personally meaningful phrase or a book title or words from a song. And then twist it into something nobody would guess, with special characters, first letters only, or some other alteration:

- “My pet flerken” → “(myP3tf13rk3n)”
- “Avengers, assemble!” → “Av3ng3rzA\$\$3mbLe*”
- “I am Iron Man” → “eYeAm1ronM@n”

What memorable phrases, titles, song lyrics, or other combinations of words would you choose? Build three different, strong passwords using this approach and test out how long it would take to crack them, using the “How secure is my password?” website. Remember! Never test real passwords in any online tool for checking password security.

PASSWORDS	CRACKING TIME
1.	
2.	
3.	

PART 2: HOW THINGS GO WRONG ONLINE, 2.3.b (CONTINUED)

Next, make your passwords more complex by varying the types of characters used in them. Include upper- and lower-case letters, numbers, and special symbols (&%\$#), but still use 6, 9, and 12 characters to test your passwords.

PASSWORDS	CRACKING TIME
1.	
2.	
3.	

Use a same-body/different-tail approach. Start with a base combination of characters that you will easily remember and then add an ending unique to whatever account you are using. For example, if you really love your Air Jordan sneakers, and you know Nike was founded in 1964, you could start with "aiR19nlke64" as the base.

Then to make a password for, say, your Google Classroom account, you could add "Goo!" as the ending. The resulting password would be: "aiR19nlke64Goo!" For other accounts, you would take the first three letters of the company or service, add an exclamation point, and add the combination to the same base, "aiR19nlke64", to make a unique, strong, and memorable password.

Now you try it. First, build a base or body to use as a repeated element in your password develop system. Then build password endings for accounts with imaginary companies called Unicorn, Zero5, and Books4All. Add these endings to your base to make full, unique passwords. Then test on the password checker website. For any real online accounts, though, avoid online password checkers, and just keep your passwords private.

PART 3

CONTROL YOUR RISK ONLINE

WHAT YOU'LL LEARN

- The components of risk — vulnerability, threat, and attack — and how to identify them.
- The types of risk involved with using smartphones and how to reduce them.
- Approaches to assessing risk and how to prevent it from doing its worst.

WHAT YOU'LL DO

Section 1: Risky Business

3.1.a: Identifying Risks, p 33

Section 2: The Many Facets of Smartphone Risk

3.2.a: How Risky Is Your Phone? p 36

Section 3: Assessing Risk Across Different Fields of Activity

3.3.a: How Likely Is a Cyber Attack in Each Circumstance? p 38



PART 3: CONTROL YOUR RISK ONLINE



3.1.a

Identifying Risks

Identifying and analyzing risk of the places we go and things we do in our lives requires taking a different perspective. Think about a swimming pool, for example. What kinds of risk to pool-goers can you imagine in and around a pool? Go back to the “Big Idea” on page 28 in *Outsmart Cyberthreats* and study the three factors that add up to risk: vulnerabilities, threats, and attacks.

Then imagine what kinds of pool-related vulnerabilities might expose people who work and visit there to risk. Vulnerabilities can relate to any kind of harm, coming from weather, burglary, digital attack, activities of people in the area, etc. For example, the Snack Shack sitting just in front of that big, beautiful shade tree could be vulnerable to branches that fall off the tree during a strong summer thunderstorm, resulting in damage to the building, loss of property inside, or even injury to people nearby.

What vulnerabilities are there at a swimming pool? Try to think of at least 7-10 different vulnerabilities and list them below:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

PART 3: CONTROL YOUR RISK ONLINE, 3.1.a (CONTINUED)

Now think about what kinds of threats and attacks might combine with a vulnerability to produce actual harm. Pick out 3 vulnerabilities and describe possible threats and attacks for each that would all add up to a risk of harm or damage at a swimming pool. In the scenario above, for example, the Snack Shack location is the “vulnerability,” the tree is the “threat,” and falling branches are the “attack.”

VULNERABILITY	THREAT	ATTACK

A key trait of cybersecurity professionals is “thinking like an adversary,” that is, imagining an attack and then backtracking through the system or environment under attack to understand threats and identify vulnerabilities. In this exercise, do the opposite of what you did above: Think up 3 kinds of attacks that might cause harm at a swimming pool — different from those you have already imagined — and work backwards to define a threat and pinpoint a vulnerability.

ATTACK	THREAT	VULNERABILITY

PART 3: CONTROL YOUR RISK ONLINE, 3.1.a (CONTINUED)

Once you have identified a vulnerability for each of the 3 attacks, consider if and how you would mitigate the vulnerability. The first question asks you to weigh reasons for and against doing anything to mitigate the vulnerability. It could happen, for example, that the tree above the snack shack is too useful and beautiful to take down, and you decide just to live with the vulnerability. Or not. The second question asks you to outline a mitigation strategy, that is, describe briefly what you would do to reduce the risk of the attack connected to the vulnerability from actually happening.

Identify reasons for and against removing or reducing the vulnerability:

VULNERABILITY	FOR	AGAINST

Briefly describe a mitigation strategy for each vulnerability:

VULNERABILITY	MITIGATION STRATEGY

PART 3: CONTROL YOUR RISK ONLINE

3.2.a

How Risky Is Your Phone?

Cybersecurity professionals concern themselves with risks to the personal technologies and data networks that we all use to conduct our online lives. *Outsmart Cyberthreats* describes in detail how these risks can present themselves to anyone who uses a phone. Review the details of the story on pages 24-25 in *Outsmart Cyberthreats* about what happens with the main character’s phone. As you read, identify the vulnerabilities, threats, and attacks. Then think about phones in general and see how many more vulnerabilities, threats, and attacks you can come up with in each category.

RISK FACTORS	IN THE TEXT	IN GENERAL USAGE
Vulnerabilities		
Threats		
Attacks		

PART 3: CONTROL YOUR RISK ONLINE, 3.2.a (CONTINUED)

Pick out one vulnerability, one attack, and one threat from the list you identified above. Describe how you would mitigate the risk associated with each one — meaning, what would you do to prevent the vulnerability, threat, or attack from resulting in actual harm to the phone and/or the personal data it contains?

Vulnerability: _____

Mitigation strategy: _____

Threat: _____

Mitigation strategy: _____

Attack: _____

Mitigation strategy: _____

PART 3: CONTROL YOUR RISK ONLINE

3.3.a

How Likely Is a Cyber Attack in Each Circumstance?

Assessing risk involves considering both the likelihood an event might occur and the damage the event would cause if it did occur. In combination, these two factors — likelihood and damage — can yield an overall assessment of risk associated with a particular scenario. Our responses to risk online — and to risk as we face it in real-world life — should take into full account both these dimensions.

Imagine you are a cybersecurity professional at your school and you get advanced word of plans in motion to carry out the “attacks” described below. Your job is to assess the risk, considering the likelihood of the event and the damage it might cause, and explain your reasoning to your boss, the principal of the school. Use your imagination and any actual experience you have from your own school to come up with your risk assessments. Use a scale of 1 – 5, with 1 being the lowest and 5 the highest value of likelihood, damage, and risk.

1. At halftime of the next home basketball game, a message on the digital scoreboard will be displayed that contains insulting language and personally revealing information about one of the players.

Likelihood: _____

Why? _____

Damage: _____

Why? _____

Overall risk: _____

Why? _____

PART 3: CONTROL YOUR RISK ONLINE, 3.3.a (CONTINUED)

2. A hacking group is targeting school nurses' offices with a phishing campaign designed to get userid and password information that will then be used to break into students' personal medical records. Several schools in your area have reported receiving these emails but nobody in your own building has got one ... as far as you know.

Likelihood: _____

Why? _____

Damage: _____

Why? _____

Overall risk: _____

Why? _____

PART 4

EXPLORE A FUTURE IN CYBERSECURITY

WHAT YOU'LL LEARN

- Skills and interests of yours that might mean a career in cybersecurity could work for you.
- Different kinds of roles and responsibilities that cybersecurity professionals can assume.
- What kinds of threats and attacks are most common in K-12 schools.

WHAT YOU'LL DO

Section 1: Puzzles, Riddles, and Brain Teasers as Pathways Into Data Care

4.1.a: Riddles and Puzzles to Tickle Your Brain, p 43

Reflection on 4.1.a, p 48

4.1.b: Riddles and Puzzles to Tickle Your Brain, as a Group, p 49

4.1.c: Compete in Teams to Solve Riddles and Puzzles, p 52

Section 2: Cyber Threats Close to Home: K-12 School Districts at Risk

4.2.a: K-12 Schools Under Threat of Cyber Attack, p 55



PART 4: EXPLORE A FUTURE IN CYBERSECURITY

The exercises in this section should challenge but also entertain you. They are brain teasers, puzzles, and riddles, involving numbers, words, lateral thinking, and a bit of silliness, as well.

In addition, they are designed to illustrate some of the skills and abilities that help cybersecurity professionals do their jobs. The puzzles are aligned with the "Types of Cyber Jobs" table on page 35 of *Outsmart Cyberthreats*. As you tackle different kinds of puzzles, you will be trying out different ways to reason and analyze and solve problems. These different thought processes are linked to cyber job types in the table below and can help guide you in both attempting and reflecting on the exercises.

TYPES OF CYBER JOBS	ASSOCIATED THOUGHT PROCESSES
Investigator	Solve problems with imagination and logic; synthesize and apply knowledge or understanding from different realms.
Analyst	Gather and study information to identify patterns and make meaning; sift out distractions and irrelevant information to home in on the key issue or problem.
Protector	Find the weak points or vulnerabilities of a system; identify flaws or mistakes and point towards solutions.
Programmer	Use abstract reasoning or logic to answer questions or build solutions; a grasp of mathematical and spatial relations helps greatly.
Manager	Organize tasks, connect specific problems to larger contexts of security needs, coordinate and lead teams.



4.1.a

Riddles and Puzzles to Tickle Your Brain

The riddles and puzzles below require no advanced knowledge or expert command of reading or math. They just take some patience, imagination, attention to detail, and often the ability to see what is right in front of you from just a slightly different angle than what might seem normal or familiar. The exercises are associated with different types of cyber jobs to show you what kind of thought processes you might use as a professional in the field with responsibilities in the area in question.

Investigator

1. A man was walking home in the rain through a field with no trees or anything else overhead. He didn't have a coat or umbrella, and his clothes got completely soaked before he made it back to his house. But not a single hair on his head got wet. How can this be?

2. Your neighbor has 18 chickens in her backyard chicken coop. And they wake you up every morning. Aagh. One night a big storm damages the chicken coop, and all but three chickens run away. How many chickens does your neighbor have left?

3. What 3-letter word can be inserted into all five lines below to form complete words?

- a. I _ _ _ E
 - b. W _ _ _ H
 - c. C A _ _ _
 - d. C _ _ _ E R
 - e. _ _ _ I O
-

PART 4: EXPLORE A FUTURE IN CYBERSECURITY ACTIVITY 4.1.a (CONTINUED)

Analyst

4. Maria’s mother had five children. The first was named Lala, the second was named Lele, the third Lili, and the fourth was named Lolo. What was the fifth child named?

5. Which of the following is the correct sentence?

- a. The yolk of the egg is white.
 - b. the yolk of the egg is white.
-

6. You can find this in Mercury, Earth, Mars, Jupiter, Saturn, and Uranus, but not in Venus or Neptune. What is it?

Protector

7. In a computer program, valid combinations of data are five characters long and must start AND finish with a letter. In between, letters OR numbers may be used. Which, if any, of the lines below break this pattern?

- a. A123B C546D m874a M938A v847F
 - b. x82aC D546j z834A L421N y9358 k142q
 - c. A123b Ca46D m474a P411N Mj38A v8b7F
 - d. x82aC D566j z8f4A h4x1N y93aB k122q
-

PART 4: EXPLORE A FUTURE IN CYBERSECURITY ACTIVITY 4.1.a (CONTINUED)

8. One of the rows of repeated figures below has a mistake in it: a single instance of a letter that does not belong. What row has a mistake in it, and what is the mistake?

KKKKKKKKKKKKKXXXXKXKKKXXXXKKKKKX
XXXXXKKKKXXKXXXXXKXKKKKKXKXXXXXK
KKKKKXXXKXKXXXXXYKKKKXXXKKKKXXXXK
XKKXXXKKKKXKKKKKXXXXXKKKKXXKXXXXX

Programmer

9. Divide 40 by $\frac{1}{2}$ and add 10. What do you get?

10. You planted magic flower seeds in your back yard. Every day, the number of flowers appearing in your back yard doubles. If it takes 27 days for the flowers to fill your back yard, how many days does it take to fill half your back yard?

11. How many times can you subtract 10 from 100?

Turn the page.

PART 4: EXPLORE A FUTURE IN CYBERSECURITY ACTIVITY 4.1.a (CONTINUED)

Now go back to the table on page 42 of the Student Workbook. Review the “associated thought processes” for each type of cyber job and use the terms and concepts connected to each type of job to write a brief description of how you reached answers to questions for each of the job types. If you did not get the answers yourself, you can still describe how these thought processes could lead you to an answer. The point of the exercise is to recognize what it feels like for you yourself to be thinking the way people do in each of these types of jobs.

Example:

To answer Investigator Question 1, I **imagined** the scene in my head, including the man soaking wet from head to toe. One **logical** way his hair would not get wet is if he had no hair to get wet in the first place.

1. To answer **Investigator** Question No. [1, 2, and/or 3] , I [use terms or concepts from “associated thought processes” to describe arriving at a solution].

2. To answer **Analyst** Question No. [4, 5, and/or 6] , I [use terms or concepts from “associated thought processes” to describe arriving at a solution].

PART 4: EXPLORE A FUTURE IN CYBERSECURITY ACTIVITY 4.1.a (CONTINUED)

3. To answer **Protector** Question No. [7 and/or 8] , I [use terms or concepts from "associated thought processes" to describe arriving at a solution].

4. To answer **Programmer** Question No. [9, 10, and/or 11] , I [use terms or concepts from "associated thought processes" to describe arriving at a solution].

Reflection on 4.1.a

Think for a few moments about how you experienced all these activities, connected to the four types of cyber jobs: Investigator, Analyst, Protector, and Programmer. To guide your reflection, answer the questions below:

1. Did any set of job-based questions seem easier, more fun, or more interesting to you than the others? Which one and why?

2. Did any set of questions seem harder or less enjoyable? Which one? Why?

PART 4: EXPLORE A FUTURE IN CYBERSECURITY

4.1.b

Riddles and Puzzles to Tickle Your Brain, as a Group

Within your group, each member should pick one of the four types of cyber jobs and try to solve the problems associated with it. After making a full effort at solving your assigned problems, work with other group members to complete any that remain unanswered. Once your group has done what you can to answer all the problems, share your thought processes that enabled you to find the answers. For any unanswered problems, discuss the challenges you faced and work with your class as a whole to reach a solution.

Investigator

1. The light bulb problem: There are three light switches on a wall outside of a room, labeled 1, 2, and 3. The door to the room is closed, no light gets in or out, and you can't see anything on the inside from outside the room. All bulbs are incandescent, and all three switches are turned off. Your job is to figure out which switch belongs to which bulb. You can flip the switches any way you want, but you can only enter the room one time. How do you figure out which bulb belongs to which switch?

2. You start with six eggs. You break two, cook two, and eat two. But you still have eggs left over. How can this be? And how many eggs do you still have?

PART 4: EXPLORE A FUTURE IN CYBERSECURITY 4.1.b (CONTINUED)

Analyst

- 3. A clerk at the butcher shop is six feet tall and wears size 10 shoes. What does he weigh?

- 4. Read the paragraph below and identify what is "unusual" about it.

This is an unusual paragraph. I'm curious as to just how quickly you find out what is so unusual about it. It looks so ordinary and plain that you would think nothing was wrong with it. In fact, nothing is wrong with it! It is highly unusual, though. Study it and think about it, but you still may not find anything odd. But if you work at it a bit, you might find out. Try to do so without any coaching!

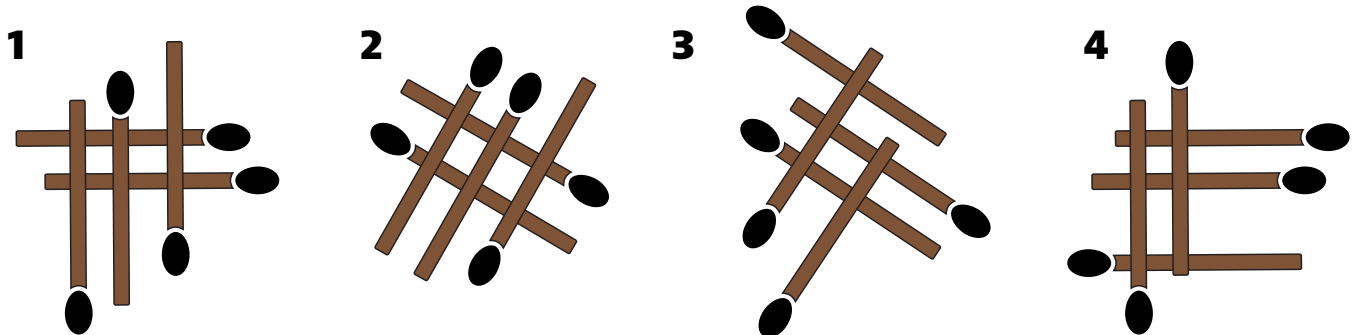
Protector

- 5. Look at the picture below and try to answer the question it contains.



PART 4: EXPLORE A FUTURE IN CYBERSECURITY 4.1.b (CONTINUED)

6. Take a look at the four matchstick patterns below. Can you identify which one of these is the odd one out?



Programmer

7. You have exactly 12 white socks and 12 black socks in your sock drawer. How many times do you have reach into your drawer and pull out socks one at a time to make sure you have a matching pair?

8. Look at the pattern of answers in the equations below and solve the last one:

- a. $2 + 2 = 44$
- b. $3 + 3 = 96$
- c. $4 + 4 = 168$
- d. $5 + 5 = 2510$
- e. $6 + 6 = ??$

PART 4: EXPLORE A FUTURE IN CYBERSECURITY

4.1.c

Compete in Teams to Solve Riddles and Puzzles

Solve the problems below in collaboration with other team members. You can either divide up problems by type of job, as in 4.1.b, or work together as a group, one problem at a time. Or try some other arrangement altogether. It's your group to organize as you wish! Use your preparation time to come up with the best uses of your group members' individual talents and become the best team you can.

Investigator

1. A farmer is traveling with a fox, a goose, and a bag of beans. During her journey, she comes across a river with a boat available for use in crossing it. The farmer can fit only thing in the boat with her at a time. If left alone together, the fox will eat the goose, or the goose will eat the beans. How does the farmer get all three things across the river safely?

2. Which of the following statements is/are true?
 1. Exactly one statement on this list is false.
 2. Exactly two statements on this list are false.
 3. Exactly three statements on this list are false.
 4. Exactly four statements on this list are false.
 5. Exactly five statements on this list are false.

PART 4: EXPLORE A FUTURE IN CYBERSECURITY 4.1.c (CONTINUED)

Analyst

3. Unscramble the letters below to come up with pairs of words that rhyme:

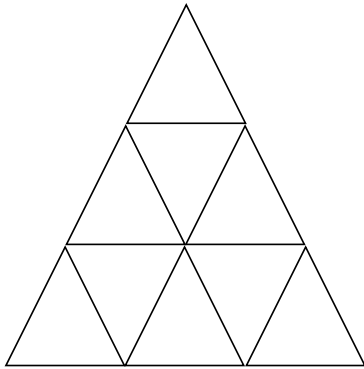
a. irfa/rwae _____

b. ertgrae/hterfrgei _____

c. ugohtth/hatugc _____

d. meyhr/blcmi _____

4. How many triangles can you find in the picture below?



Protector

5. On a computer network, each computer has a unique label or identity called an IP address. A valid address must take the form [0-255]. [0-255]. [0-255]. [0-255]. For example, a valid IP address could be "192.168.13.2." Look at the blocks of IP addresses below. Which block, if any, contains an INVALID IP address?

Block 1

- 192.168.1.3
- 192.168.2.7
- 192.1.4.9
- 172.16.4.3

Block 2

- 10.10.0.3
- 10.1.6.4
- 254.250.1.1
- 200.1.3.1.1

Block 3

- 14.17.1.1
- 192.1.5.1
- 192.192.1.4
- 221.122.1.4

Block 4

- 10.10.16.4
- 192.168.4.3
- 172.16.9.8
- 4.4.4.8

PART 4: EXPLORE A FUTURE IN CYBERSECURITY 4.1.c (CONTINUED)

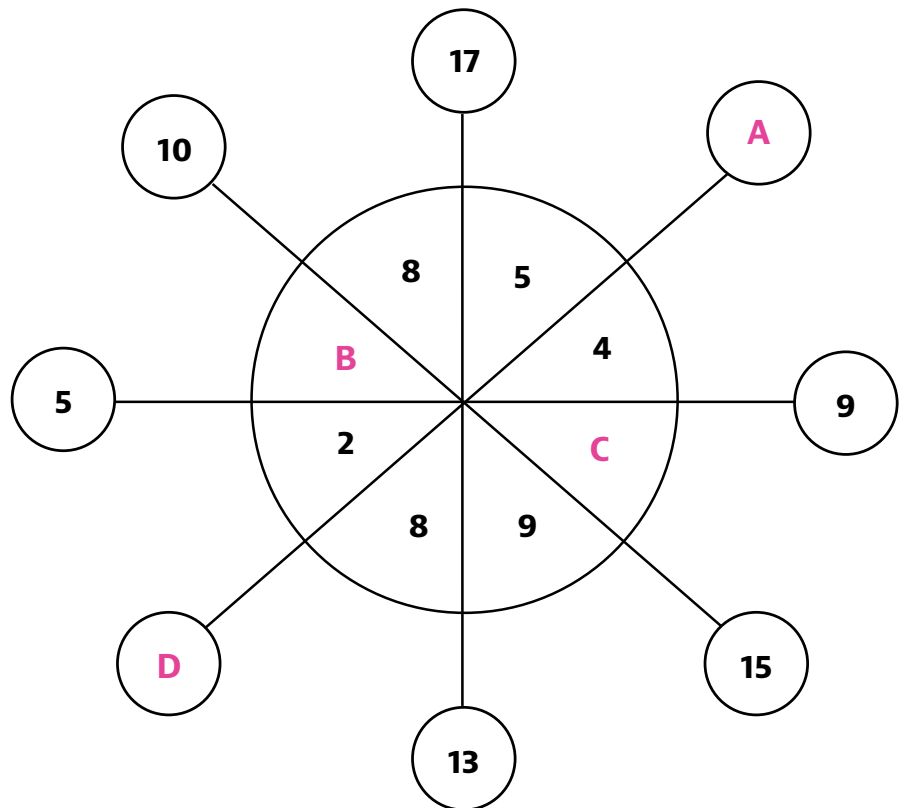
6. Read the statement below and try to solve the problem it poses.

There are five things wrong with this sentence; only geniuses will be able to spot all of the mistakes

Programmer

7. Ramona is 12, and her father is 38. When Ramona is half her father's age, how old will he be?

8. Solve the puzzle below by finding the value for the numbers missing from the circle.



A. _____

B. _____

C. _____

D. _____

PART 4: EXPLORE A FUTURE IN CYBERSECURITY



4.2.a

K-12 Schools Under Threat of Cyber Attack

K-12 school districts have become increasingly popular targets for cyber criminals. Even before Covid drove schools to expand enormously their use of online teaching and learning tools, K-12 IT systems provided ripe targets for digital attacks. In this activity, you will learn some of the reasons that school districts have been vulnerable to cyber attacks and what kinds of bad things have happened as a result. Then you will be asked to connect these topics to circumstances in your own school, as you step into questions and problems that cybersecurity professionals might confront in their real-life work situations.

The source text for this activity is "The State of K-12 Cybersecurity: 2020 Year in Review." The main part of the report is 15 pages long, with added materials at the end explaining how it was produced and providing reference materials. Read the main part and then answer the questions below. The report can be found online at the bottom of this webpage: <https://www.k12six.org/the-report>

1. What is the "only truly secure system" for IT at a school? Can such a system actually be built? Why or why not?

2. What kinds of school districts are at the greatest risk of suffering a cyberattack? Describe the traits these school districts tend to share. Why are such school districts most susceptible to attack?

PART 4: EXPLORE A FUTURE IN CYBERSECURITY 4.2.a (CONTINUED)

3. What are the four most common types of cyber attacks launched against K-12 school districts? See pages 3-11, then identify each one and briefly describe it.

1.

2.

3.

4.

4. Go to the incident map located at this website: <https://www.k12six.org/map>. Find 3 incidents on the map located near your school or at least in your state and briefly describe them.
