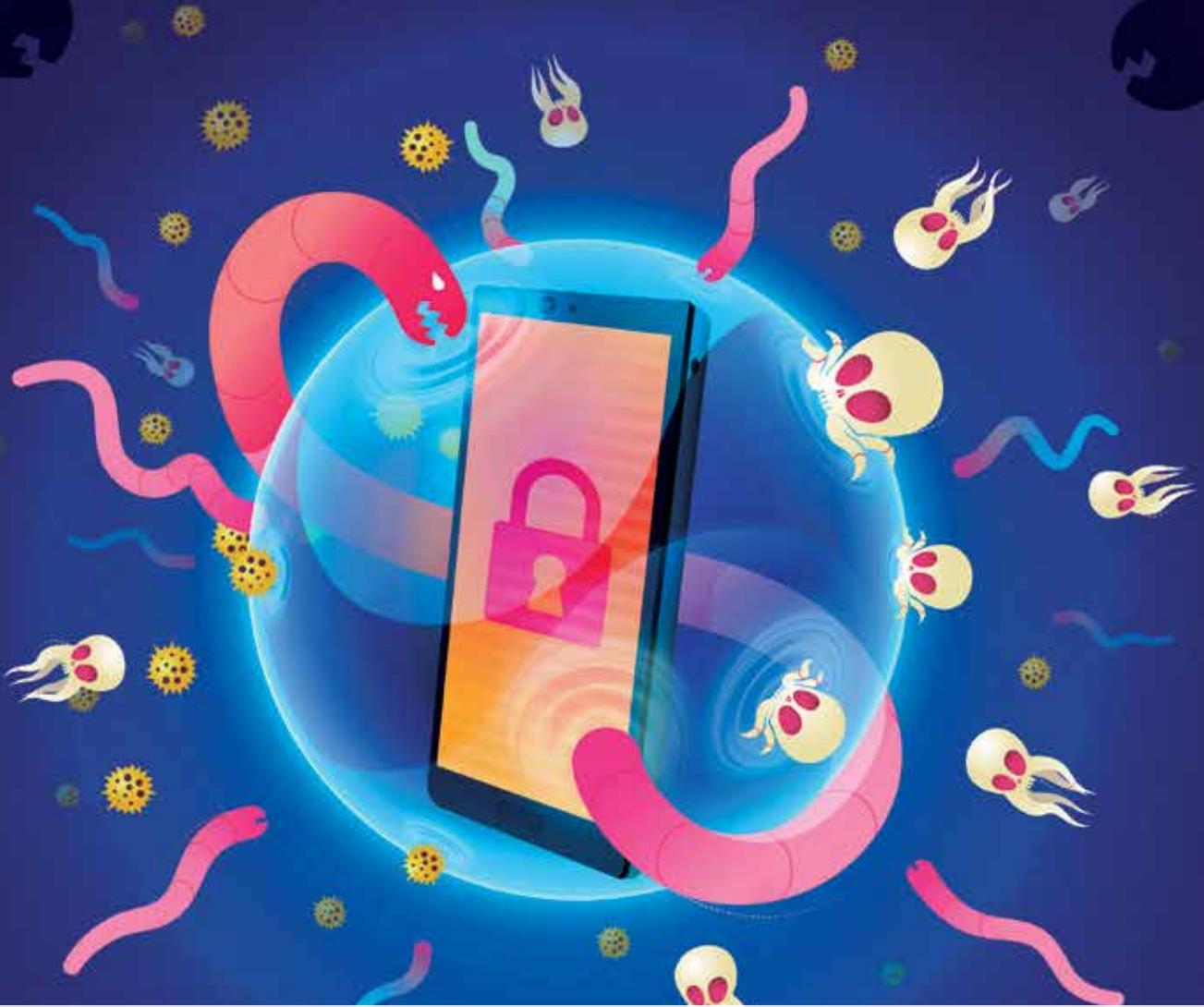YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.

Student Workbook

OUTSMART CYBERTHREATS

**Learn how to protect your data and yourself online.
BONUS: Discover a cool new career in cybersecurity!**

NATIONAL CRYPTOLOGIC FOUNDATION

Dear Student,

Look at your phone. It's not just a device; it's a digital extension of yourself that contains your photos, messages, favorite apps, schoolwork, schedule, and passwords. This makes you a target for cybercriminals.

Every time you go online, you leave behind a digital footprint. While this data is often harmless, it can also expose you to serious risks. Cybercriminals are actively seeking vulnerabilities on your phone, within your apps, and in the systems that support schools, hospitals, and businesses. This is where cybersecurity becomes crucial.

This guide is your tool for understanding how cyber threats operate—and how to outsmart them. You will learn practical strategies to protect yourself and others, sharpen your critical thinking skills regarding online content, and recognize how your choices influence the digital landscape.

Whether you aspire to a career in cybersecurity or want to navigate the online world safely and intelligently, this guide is essential. You will also discover career opportunities in this field and meet dedicated professionals who fight against digital threats daily.

From AI-driven attacks to common scams, there is a wealth of knowledge to acquire and an abundance of opportunities for those who know how to identify and respond to danger.

Your phone isn't merely a tool; it's your gateway to the digital world. The more informed you are, the more empowered you become to protect it—and everything connected to it.

You've already taken the first step. Now, let's dive in!

We extend our gratitude to Gula Tech Adventures and Mr. Rand Griffin for providing funding for this critical Data Care project.

Sincerely,

Laura C. Nelson

Laura C. Nelson
President & Chief Executive Officer

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21601

TABLE OF CONTENTS

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

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, as of 2023. 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. _____

X   8. _____

Instagram   9. _____

Messenger   10. _____

DATA COLLECTION PRACTICES

Columns (left to right): Facebook, Instagram, Messenger, LinkedIn, TikTok, YouTube, X, Amazon Prime Video, Paramount, CBS, Reddit, Hulu, HBO Max, Netflix, Disney +

TYPES OF DATA TRACKED

- Contact info
- Health and Fitness
- Financial Info
- Location
- Sensitive Info
- Contacts
- User Content
- Browsing History
- Search History
- Identifiers
- Purchases
- Usage Data
- Diagnostics
- Other Data
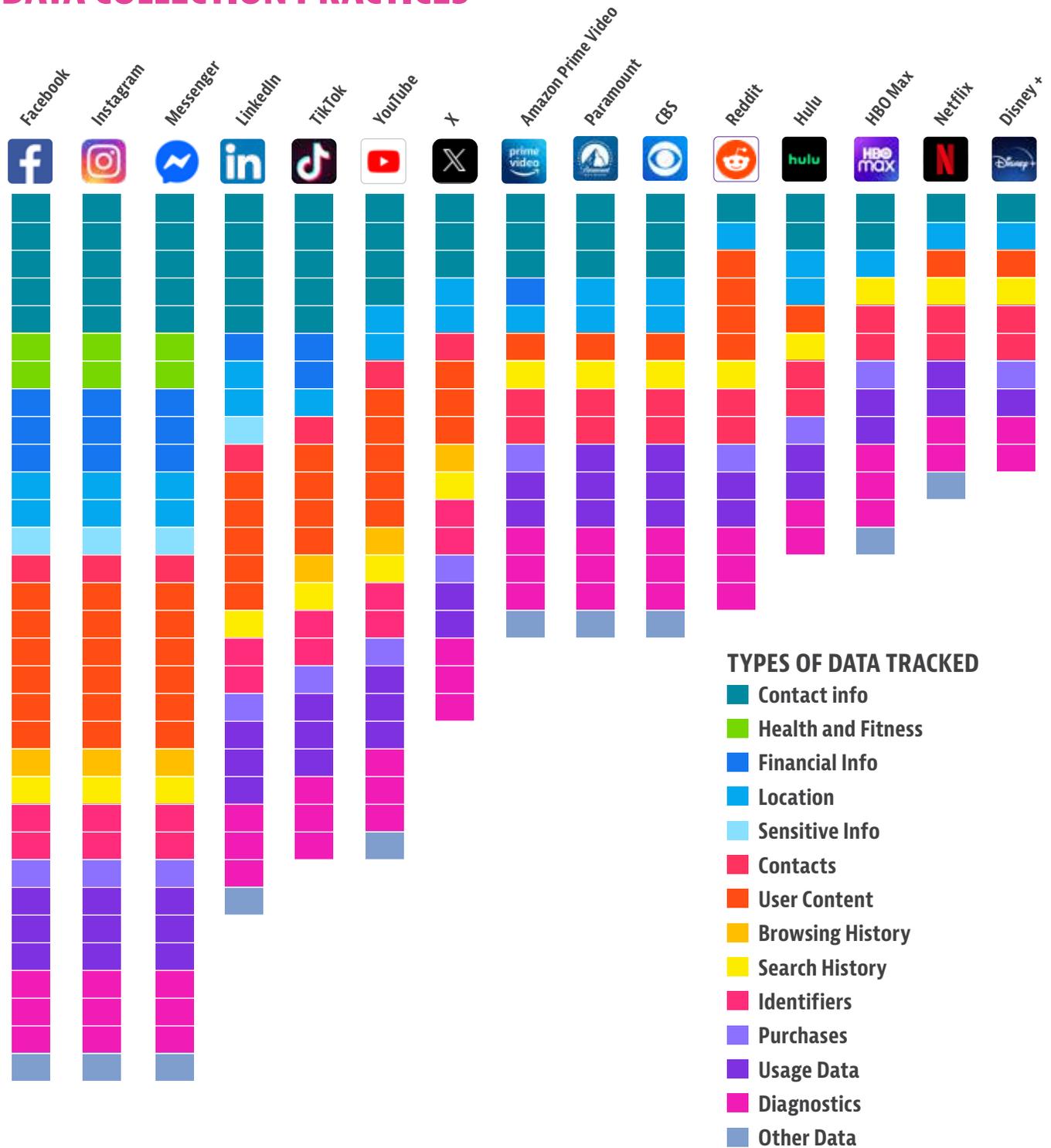
DATA COURTESY SURFSHARK

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?

_____

_____

_____

_____

_____

_____

1.1.b

The More You Watch, the More They Make

"Tracking and pervasive personalization" is a form of AI-driven marketing that uses individual online behaviors to generate advertising and sales revenues for companies. Using AI tools, companies gather data about us and then deliver content based on this data that they think will get our attention and make us buy things. An example involves the videos you might watch on TikTok or YouTube. Companies connect data about the topics of these videos to your user profile and then push out ads to you related to the content of these videos. For example, if you watch a lot of videos about unboxing beauty care products, you will find beauty care ads showing up on your phone.

The activity below will help you understand how your online behavior results in you seeing personalized ads that generate revenues for the companies involved.

1. The table below demonstrates the relationship between videos watched and related ads showing up on your screen used by a hypothetical video-hosting and -sharing app.

NUMBER OF VIDEOS WATCHED	NUMBER OF RELATED ADS YOU SEE
9	3
15	5
3	1

What do you notice about the relationship between the number of videos you watch and the number of related ads you see while using the app?

_____

Write an equation that describes this relationship.

_____

2. Applying this understanding of how the app pushes out ads to you based on your video preferences, how many ads from Nike would you see after watching 24 videos about sneakers?

_____

3. For every one of these sneaker ads you watch, Nike pays the app $2.50. In one week, users of the app watch 2,400 sneaker ads. How much money does the app earn in one week from pushing out Nike ads to its users?

_____

1.2.a

The Cost of Cyber Crime

According to the FBI, the five types of cybercrimes committed most frequently in 2023, with number of victims, were:

1. Phishing   298,878
2. Personal data breach   55,851
3. Non-payment/non-delivery   50,523
4. Extortion   48,223
5. Investment   39,570

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

1. Investment $4,570,275,683
2. Business email compromise $2,946,830,270
3. Tech support $924,512,658
4. Personal data breach $744,219,879
5. Confidence fraud $652,544,805

Pick out **ONE** of these types of cybercrimes 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._____

_____

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?

_____

_____

_____

_____

_____

_____

_____

_____

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.

Mr. Beast Is Coming to Town

Incredible news! Mr. Beast, king of the YouTube influencers, is stepping out of his YouTube channel and coming to your school for an assembly, a one-time-only event to include shooting part of a new video and a discussion of his amazing journey to online superstardom. 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.

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 his or her 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 Mr. Beast scenario above, identify the security controls that belong in each of the three categories below:

1. Physical controls

_____

_____

_____

_____

_____

2. Technical controls

_____

_____

_____

_____

_____

_____

_____

3. Administrative controls

_____

_____

_____

_____

_____

_____

_____

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 or guardians 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, guardians) gets access to the data they are supposed to see, and other kinds of controls that might be needed.

Turn the page.

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._____

_____

_____

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

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, invitations to communicate in some kind of alternate, private form, or absent or invented information related to the person receiving the email.

The message below is a real-world example of a phishing email sent through Roblox's user-to-user messaging platform. See how many clues you can find that show it is part of a scam. Try to identify at least **four** clues.
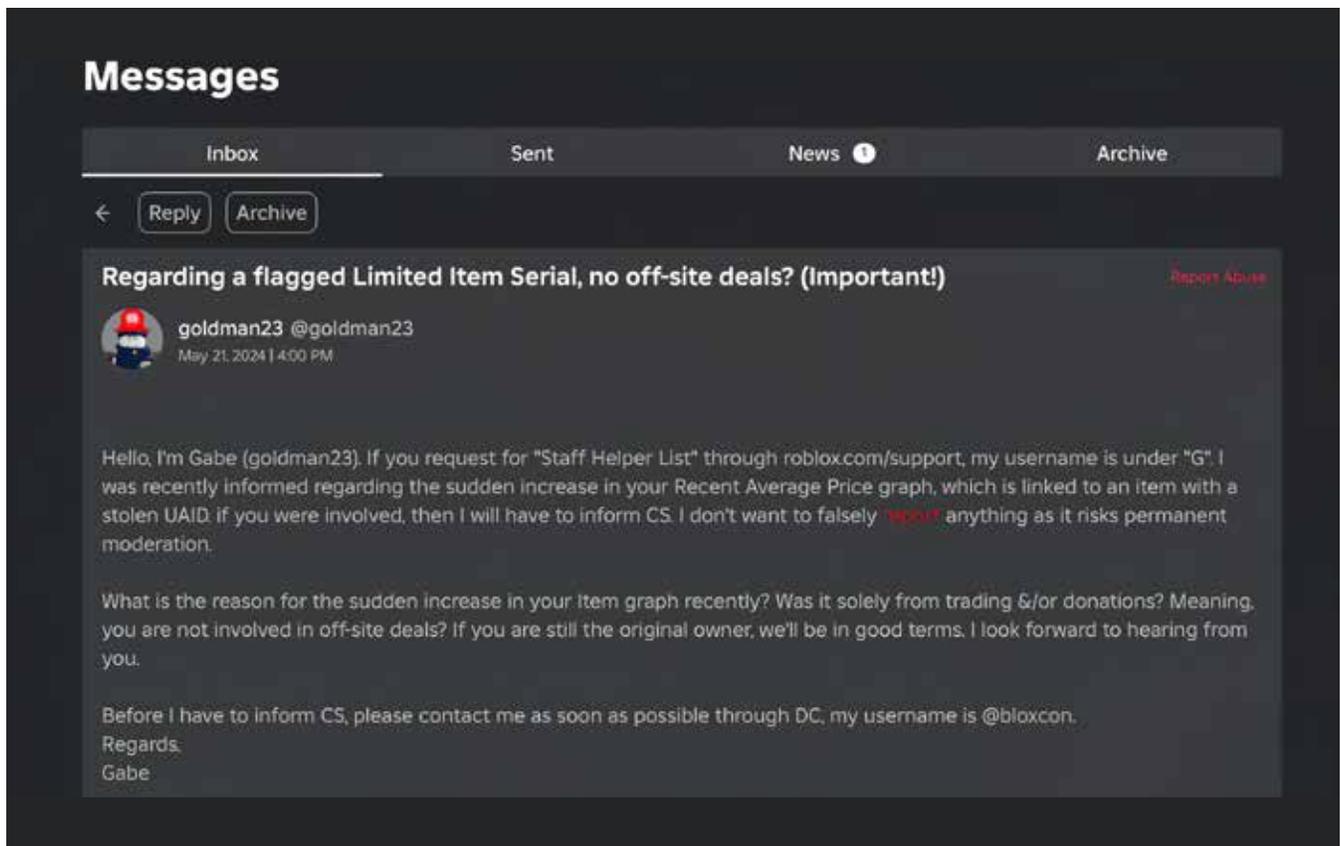
PART 2: HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT

CLUES:

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

BONUS, CAN YOU FIND ANY MORE?

6. _____

_____

7. _____

_____

2. Since the release of ChatGPT and other generative AI tools in the early 2020's, phishing campaigns have become more numerous and sophisticated. The volume and variety of phishing activities have increased dramatically, and AI-generated campaigns have spread quickly to text messaging and other platforms used by kids. These shorter-form messages can be even more convincing than emails because there are fewer things for spammers to get "wrong" and users tend to respond more quickly and carelessly to them. Gone are the obvious errors in punctuation, grammar, and formatting. In their place are simpler, more direct appeals to click on a link or do something else to reveal compromising, personal information.

The text messages below were generated with the help of an AI phishing tool. What about these messages might make you suspicious of them as being parts of a scam? Try to find **five** phishing clues!

9:51

+1 (631) 690-5738 >
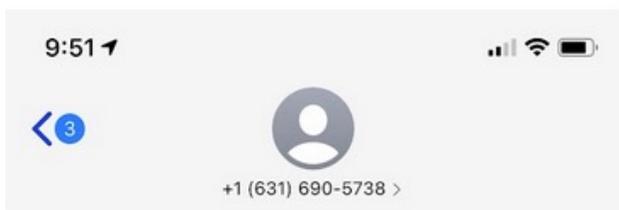
Text Message
Tue, Mar 9, 5:05 AM

Amazon: Congratulations Aashish, you came in 1st in this week's Amazon Earpods raffle! Click the link to arrange shipment: u5fxc.info/ZEJTTzmY3Z

9:50

+1 (470) 693-5570 >
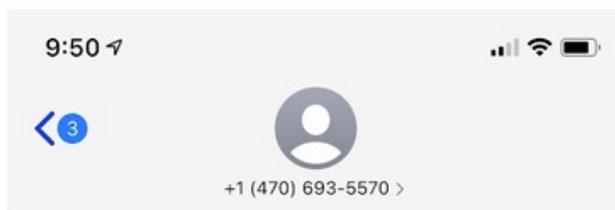
Text Message
Wed, Apr 14, 6:10 PM

USPS: the arranged delivery for the shipment 1z67166 has been changed. Please confirm here: w2fsn.info/eQbXRszEBq

CLUES:

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

5. _____

_____

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?

_____

_____

_____

2.2.a

Data, Data, Everywhere

As long as they have been gathering personal data, both companies and governments have had a hard time keeping it safe and secure. Data breaches have occurred often and everywhere, and there's little sign of things getting better.

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.

Since then, the pace of data breaches has remained high. Every year, hundreds of millions of internet users' records get exposed in data breaches, with the average cost of each incident totaling over $4 million. In 2024, for example, a data brokerage company called National Public Data suffered a data breach exposing 2.9 billion records, including contact information, Social Security Numbers, and names and addresses of individuals and family members. By the end of the year, the company had filed for bankruptcy.

A fourth incident illustrated problems related to data as it can be used to power AI tools. In 2016, Microsoft released an AI chatbot on Twitter (now called X) called Tay, presented in the persona of a teenage girl and designed to interact with other Twitter users. These interactions would serve as training data for Tay to learn how to conduct exchanges on the social media platform. Other Twitter users quickly realized that feeding Tay racist, bigoted messages would teach it to respond in similar terms, and within 16 hours Tay's Twitter presence had become fully contaminated with hate speech. A highly public example of "data poisoning," the incident highlights how the nature and quality, or integrity, of data coming OUT of an AI system depends on the integrity of data going INTO it.

Read the brief articles at the websites on the next page 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: "Office of Personnel Management data breach"
https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

National Public Data: "2024 National Public Data breach"
https://en.wikipedia.org/wiki/2024_National_Public_Data_breach

Microsoft AI chatbot Tay
https://en.wikipedia.org/wiki/Tay_(chatbot)

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

Sony PlayStation _____

_____

_____

_____

_____

Target _____

_____

_____

_____

_____

Office of Personnel Management: _____

_____

_____

_____

National Public Data: _____

_____

_____

_____

Tay _____

_____

_____

_____

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

Sony PlayStation _____

_____

_____

_____

Target _____

_____

_____

_____

Office of Personnel Management: _____

_____

_____

_____

National Public Data: _____

_____

_____

_____

_____

Tay _____

_____

_____

_____

_____

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 or guardians 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._____

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.

3. Which data types did you rank first and last for each aspect of CIA? Explain why you ranked each one first or last.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

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.	

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. How would you advise someone to build the **strongest possible** password?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

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.	

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 "aiR19nIke64" 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: "aiR19nIke64Goo!" 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, "aiR19nIke64", 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 39

Section 2: Know Risk, Not "No" Risk: Smartphones and AI Tools

3.2.a: How Risky Is Your Phone? p 42

3.2.b: AI: It's All In How You Use It p 44

Section 3: Assessing Risk Across Different Fields of Activity

3.3.a: How Likely Is a Cyber Attack in Each Circumstance? p 48

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. _____

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

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 out-line 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

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		

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: _____

_____ _____

_____

3.2.b

AI: It's All In How You Use It

AI tools can offer incredible time-saving efficiencies as well as present risks that range from the obvious to the unexpected. In this exercise, students consider a classroom-based scenario involving ChatGPT as a way to start thinking about both potential benefits and drawbacks of using AI as an aid to schoolwork.

EXERCISE

Taylor's History class is finishing up the term with a unit on the Civil War. For several weeks, his class has been reading, watching videos, and talking about the years before, during, and after the war. His teacher has assigned a 750-word essay on the causes of the Civil War as a final project.

Everyone is pretty nervous about writing such a long paper. Taylor hasn't been paying very close attention in class, and he's feeling really nervous. That night, everyone must turn in their paper by 11:59 PM. As the evening drags on, and he has no words to show for his efforts, Taylor panics. Until, an idea – ChatGPT! A matter of moments after asking for a "750-word essay on the causes of the Civil War," Taylor has a polished, detailed, well-organized account of why the Civil War took place. Change a few words, copy it into his online History classroom page, and all done!

A few days later, his teacher hands out grades and Taylor gets a big, fat zero, along with instruction to come back after school for a conference. His teacher recognized the writing as different from Taylor's past work and used AI detection software to flag it as produced by a chatbot.

"That's plagiarism, Taylor," says his teacher, "a serious problem. And worse than that, you haven't actually learned the material. Could you explain what caused the Civil War right now, in your own words?"

"Um, not really," Taylor admitted. His stomach was in his shoes, as he imagined all the trouble he was in. A teacher who doesn't trust him, angry parents/guardians, a failing grade.

His teacher, however, understands that AI is a new, complicated part of the online world. Instead of just flunking Taylor, he gives him a new assignment: an essay on the

effects of the Civil War. With ChatGPT as a starting point for research, Taylor will use books from the classroom to confirm and extend what AI tells him. And he will come after school every day the following week to write another essay using his own words and really learn the material. Combined with a review of his first paper, Taylor will end up knowing about both the causes and effects of the Civil War as well as how to use ChatGPT to extend his learning, not replace it.

With the understanding of vulnerability, threat, and attack that you have developed in this part of *Outsmart Cyberthreats*, identify elements of Taylor's story that fit each of these three risk factors. Remember, a vulnerability is the weakness or circumstance that creates an environment for bad things to happen; the threat is the potential danger(s) that can result from the vulnerability; and the attack is the actual bad thing(s) that happen. Then pick one risk factor from each category and describe a mitigation strategy to reduce the risk of bad things happening.

1. Vulnerabilities:

_____

_____

_____

*Mitigation strategy*_____

2. Threats:

_____

_____

_____

Mitigation strategy_____

3. Attacks:

_____

_____

_____

Mitigation strategy_____

REFLECTIONS:

Have you ever used ChatGPT or other AI tools for help with schoolwork? Which ones? How did your experience with AI go?

_____

_____

_____

_____

Do your teachers or other people at school ever discuss with students safe and responsible ways to use AI tools? If so, what do they say?

_____

_____

_____

_____

_____

_____

Imagine you are invited to be the student representative on a teacher-student committee that will be developing guidelines for safe use of AI tools in the classroom. What are three important topics or suggestions you would want to include in these guidelines?

_____

_____

_____

_____

_____

_____

_____

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? _____

    _____

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? _____

_____

_____

3. Pick one of the scenarios described above and explain the plan you would recommend to the principal to reduce the risk of the attack succeeding. Think about the computer or data systems involved, the human behaviors to be considered, and the physical environment in which the attack could take place. A full plan to reduce risk should address all three of these dimensions. Remember, we want to build "defense-in-depth" security systems.

_____

_____

_____

_____

_____

_____

_____

_____

_____

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

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

Cyber Defender or AI Creator?

For the following three questions, circle the answer that best matches what you would do.

1. You find an old, locked treasure chest in your attic. What do you do?

   A. Look for clues on the lock, test different keyholes with a screwdriver, and try to figure out how to open it.

   B. Wonder how the chest was designed and whether you could build a better lock.

2. You're playing a board game, and your friend Tyler makes a strange move. How do you react?

   A. You review Tyler's previous moves, looking for patterns and trying to predict what he might do next.

   B. You wonder if the game could be improved by adding rules related to his strange move.

3. Your friend Alana is having a problem with her trombone case. Someone keeps moving it around the Band Room on days the band practices. How do you try to help?

   A. Set up a plan to catch the person, plotting out how you're going to interrogate suspects.

   B. Look for patterns in how and where the trombone case gets moved, like solving a puzzle.

TURN THE PAGE

REFLECTION

Now go back and look at your answers. If you chose more A's, you think like a cyberse-curity pro. Solving mysteries, getting to answers, and keeping things safe matter to you. If you chose more B's, you might be more of an AI type. Recognizing patterns, improving systems, and making this work better capture your interest. If you chose some of both, maybe using AI tools to make the internet safer is for you. The next set of activities will help you understand more about what your interests are and how they might point you in the direction of a career in the field.

4.1.b

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 re-sponsibilities 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

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

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?

   KKKKKKKKKKKXXXXKXKKXXXXXKKKKKX
   XXXXXKKKXXKXXXXXKXKKKKKXKXXXXK
   KKKKKXXXKXKXXXXXYKKKKXXXKKKKXXXXK
   XKKXXXKKKKXKKKKXXXXXKKKKXXKXXXXXX

   _____

Programmer

9. Divide 40 by ½ 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.

Now go back to the table on page 51 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].

    _____

    _____

_____

_____

_____

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.b

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?

    _____

    _____

    _____

    _____

4.1.c

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?

   _____

   _____

   _____

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!
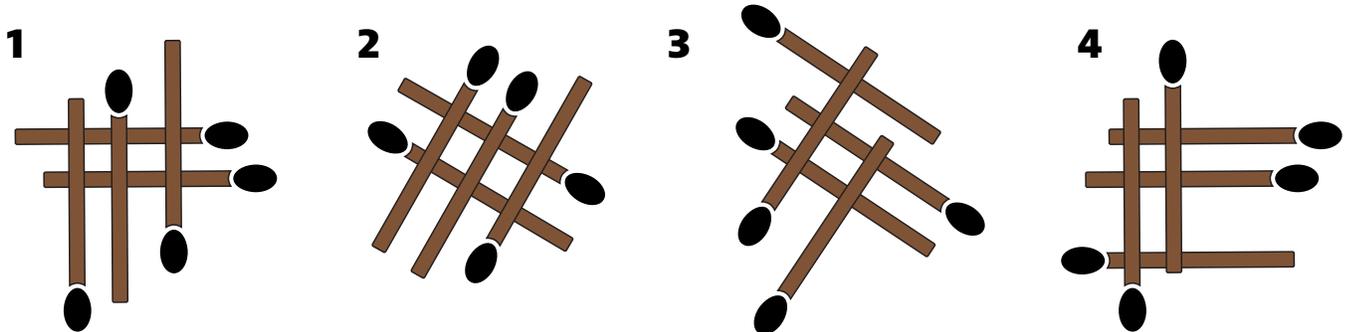
    _____

    _____

    _____

Protector

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

    Can you find the
    the **mistake**?
    1 2 3 4 5 6 7 8 9

    _____

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

1 **2** **3** **4**

_____

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 = ??

_____

4.1.d

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.

    _____

Analyst

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

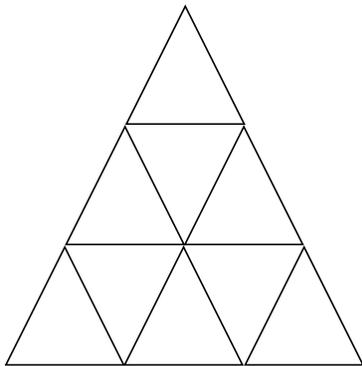   a. irfa/rwae _____

    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	Block 2	Block 3	Block 4
192.168.1.3	10.10.0.3	14.17.1.1	10.10.16.4
192.168.2.7	10.1.6.4	192.1.5.1	192.168.4.3
192.1.4.9	254.250.1.1	192.192.1.4	172.16.9.8
172.16.4.3	200.1.3.1.1	221.122.1.4	4.4.4.8

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

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

_____

_____

_____

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. _____
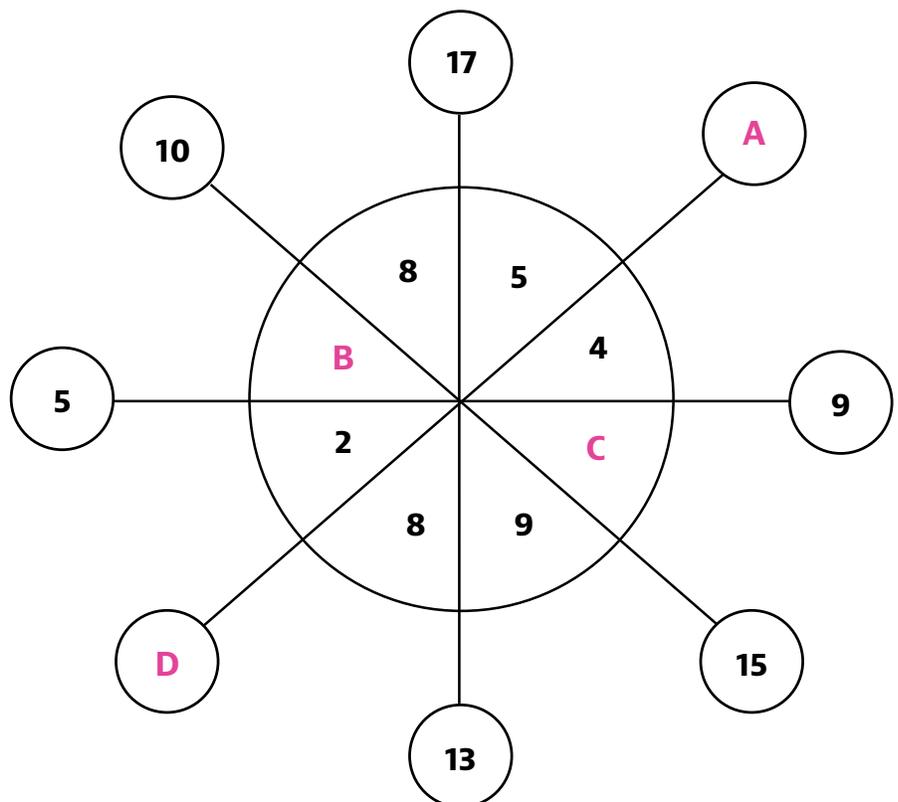
4.2.a

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?

_____

_____

_____

_____

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.

    _____

    _____

    _____

    _____

    _____

    _____