YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.

Teacher's Guide to

OUTSMART CYBERTHREATS

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

NATIONAL CRYPTOLOGIC FOUNDATION

Dear Teacher,

Welcome to the Teacher's Guide to Outsmart Cyberthreats! We are excited to present this comprehensive workbook designed specifically for middle and high school students.

In our increasingly digital world, understanding cyber threats and the importance of cybersecurity is essential for empowering our youth to navigate the online landscape safely and responsibly. As educators, you play a vital role in equipping students with the knowledge and skills they need to protect themselves against cyber threats.

This Teacher's Guide explores various topics related to cybersecurity, enabling students to identify potential risks and learn effective strategies for safeguarding their personal information. We also introduce the fascinating realm of artificial intelligence and its implications for cybersecurity. By exploring how AI can be both a tool for protection and a potential source of vulnerabilities, students will gain a well-rounded understanding of the evolving challenges in the digital age.

We encourage you to use this guide as a resource in your classroom discussions and activities. Through engaging exercises, real-world scenarios, and thought-provoking questions, students will develop the critical thinking skills necessary to analyze and respond effectively to cyber threats.

Thank you for your commitment to fostering a safe and informed generation of digital citizens. Together, we can empower our students to embrace technology while remaining vigilant and secure.

Sincerely,

Laura C. Nelson

Laura C. Nelson
President & Chief Executive Officer

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21601
443-795-4498 * booklet@cryptologicfoundation.org * www.cryptologicfoundation.org

WHAT'S INSIDE

WHAT'S INSIDE CONTINUED

Welcome to *Outsmart Cyberthreats*!

Outsmart Cyberthreats is a book meant to teach middle-school students about the importance of safeguarding the personal data they share online. It is also meant to encourage our brightest and best students to consider pathways into careers dedicated to safeguarding the personal data of everyone else sharing it online. After reading the text and completing the accompanying Student Workbook, students will know better how to stay safe online. And they might even have taken their first steps towards a career in one of the most important, rewarding career fields around.

NO TECHNICAL KNOWLEDGE REQUIRED

The *Outsmart Cyberthreats* Teacher's Guide and accompanying Student Workbook help educators and students put the main text to work in the classroom, after school, at summer camp, or anywhere students are learning about cybersecurity topics. Just like *Outsmart Cyberthreats* itself, the guide and workbook assume no prior technical knowledge of information technology security, network administration, or online data systems. Anyone with a basic level of experience using websites, social media platforms, and online communications tools can make a constructive way through the books and gain substantive command of cybersecurity principles and practices.

HOW THE BOOKS WORK

These companion publications follow the structure of *Outsmart Cyberthreats*, with a set of sections corresponding to each of the four parts of the main text. To orient educators to each part, the Teacher's Guide describes a "goal" and an "approach" along with "overview" that summarizes the "activities" that students will complete.

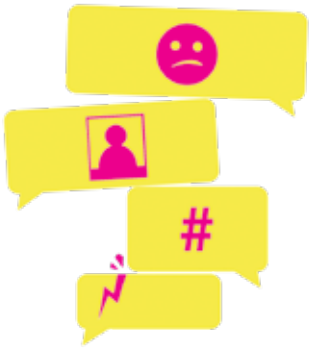
Each part features multiple "sections," along with materials that extend the learning content presented in the book. "Learning objectives" and a "brief background discussion" help users get started with sections, and "key terms," "extensions," and "resources" help fill out and reinforce what students learn. Answers are also provided for activities that have right-or-wrong options, as well as guidance for discussion topics

to develop with open-ended exercises. The resources come with thumbnail guidance in what to expect from reading each item, and educators can judge what, if any, further use to make of them based on their and their students' level of interest or knowledge. Some resources might help educators fill out their own understanding, while others might be appropriate to share with students.

GOOD LUCK AND ENJOY!

We hope you and your students find the whole *Outsmart Cyberthreats* learning experience useful and engaging. It is a flexible program, and you can go through it start to finish or pick and choose the parts that suit your own purposes. Either way, the lessons in cybersecurity can serve both to promote safer individual online behaviors and to encourage kids in the direction of a career that ends up helping make the internet a better place for all of us.

A DAY IN THE LIFE OF YOUR PHONE



GOAL

Provide students a context for understanding how their data gets collected, used, and misused when they go online.

APPROACH

Use smartphones in particular, and kids' online behaviors more generally, to illustrate both legal and illegal uses of personal data they share online.

OVERVIEW

- Students will learn about the great volumes of data that companies collect online and what they do with it all, whether we know about and approve it or not.
- They will learn how artificial intelligence tools can work to gather personal data, attach it to a personal profile, and deliver individualized content meant to influence online behaviors.
- They will also explore the many varieties of criminal behaviors that plague internet users all over the world, along with the staggering sums of money involved.
- Strategies and tactics for defending valuable storehouses of online data conclude this section, with students getting the chance to understand and devise their own approaches to protecting things of value.

SECTIONS

SECTION 1

Companies Do Love to Gather Data

LEARNING OBJECTIVE

Students understand the different kinds of personal data companies can collect about individual users.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Companies collect enormous amounts of data about us when we go online. Much of this data we provide willingly, such as email addresses and other pieces of contact information, payment information, and marketing details like how we learned about a particular website or online service.

However, companies also track and record details about our online behaviors that we might not realize. Not only can companies track what websites we visit, links we click, and where we are in the world when we do these things, they can also track what web browsers we use, our computer and its operating system, how we move the cursor around the screen, and dozens of other surprisingly personal traits and behaviors. AI tools amplify companies' abilities to do all these tasks as well as glean more and deeper insights about us and our preferences. This understanding enables companies to buy ads and market products in highly personalized ways, resulting in more sales revenues and higher prices in the overall marketplace of personal data.

For example, Google and Facebook earn hundreds of billions of dollars per year in ad revenues, targeting users based on AI-enhanced individual profiles. Per user, Google earned $393 and Facebook $271 in 2022. Amazon, Apple, Microsoft, and every other big tech company also make billions of dollars every year doing the same things. While the dollar values can vary across different kinds of internet services, the take-away is clear: **the data we give away for free can add up to a lot of money for the companies that gather it**.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 4-5; 7

SECTION 1 CONTINUED

WARM-UP QUESTIONS

1. How many of the apps named in Part 1 of the book do students themselves use?
2. What kinds of personal data do students think they provide directly to companies that make the apps they use?
3. Which apps do students think collect more data: Amazon Prime or Netflix? YouTube or TikTok? Facebook or X?
4. What kinds of "costs" do students pay for using a free app? Ads that interrupt game play? Requests for more information in exchange for greater access? In-app purchases to advance further into a game or service?

ACTIVITY 1.1.a

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

In this activity, students will analyze the data collection practices of popular social media and video streaming services, as of 2023. The analysis consists of using the included tables showing data collection practices to rank these apps from most to least amounts of collected data. After completing this analysis, they will consider how relevant collected data is to select companies' actual business.

Students will now complete Activity 1.1.a, found on page 6 of their workbook. The activity is replicated with answers on the next three pages of this guide.

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.

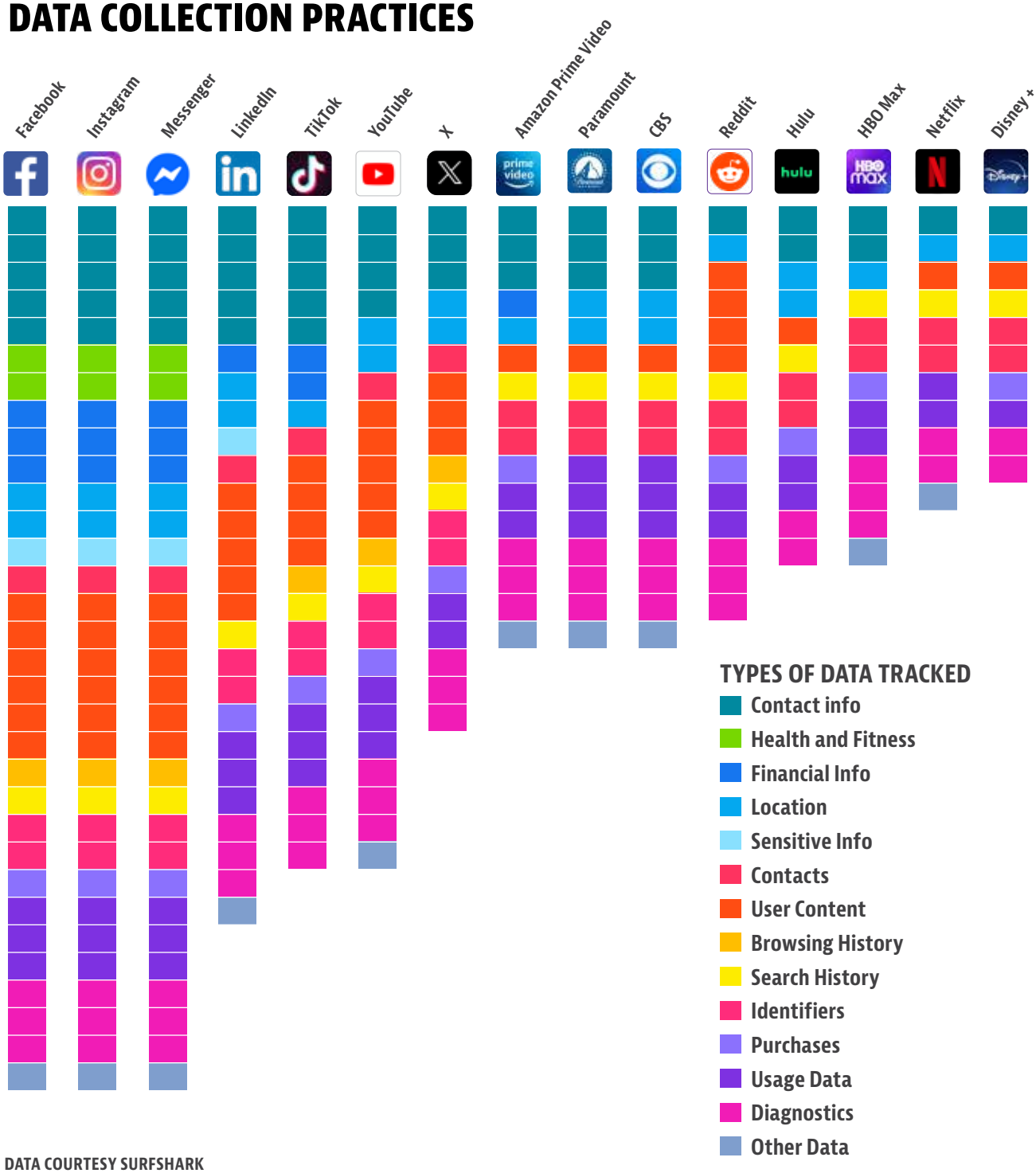
Netflix	1. _____
Amazon Prime Video	2. _____
Disney +	3. _____
YouTube	4. _____
HBO Max	5. _____
Facebook	6. _____
TikTok	7. _____
X	8. _____
Instagram	9. _____
Messenger	10. _____

ANSWERS

1. Facebook (32)
2. Instagram (32)
3. Messenger (32)
4. TikTok (24)
5. YouTube (24)
6. X (19)
7. Amazon Prime Video (16)
8. HBO Max (13)
9. Netflix (11)
10. Disney + (10)

1.1.a (CONTINUED)

DATA COLLECTION PRACTICES



DATA COURTESY SURFSHARK

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?

_____

_____

_____

ANSWERS WILL VARY: In both sets of companies, the ones that collect data in fewer categories (i.e., to the right of the table) could be seen as also collecting more relevant data, and vice versa. To push the discussion, though, explore specifically why some of these companies might collect data that seems far from their needs and why individuals might or might not mind such collection practices. For example, why does TikTok collect "financial info" but X does not? Or, how do the big streaming services (Amazon Prime, Hulu, Netflix, Disney+) compare to one another? And how should we feel about YouTube after seeing their approach to data?

ACTIVITY 1.1.b

The More You Watch, the More They Make

In this activity, students will learn about "tracking and pervasive personalization," an online marketing technique driven by AI tools that connect individual users' behaviors with ads related to these behaviors. The activity is meant to illustrate how our online activity can generate significant revenues for companies involved in gathering and selling our personal data.

Students will now complete Activity 1.1.b, found on page 9 of their workbook. The activity is replicated with answers on the next 2 pages of this guide.

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?

Answer: The more videos you watch, the more ads you will see about the topic(s) of these videos.

Write an equation that describes this relationship.

Answer: Number of videos = Number of ads X 3; or Number of ads = Number of videos / 3

1.1.b (CONTINUED)

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?

Answer: 8 ads, or 24 / 3

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?

Answer: The app earns $6,000, or 2,400 X $2.50.

SECTION 1 CONTINUED

KEY TERMS

Personally identifiable information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

Examples include:

- Name
- Address
- Social Security number
- Telephone number
- Email address

Also included in PII are combinations of the following:

- Gender
- Race
- Birth date
- Geographic indicator and other descriptors

Tracking and pervasive personalization: The practice of collecting extensive data about a user's online activity across various platforms and websites, then using that information to deliver highly tailored and targeted content, advertisements, and experiences specifically designed to match users' individual interests and behaviors, often without their full knowledge or consent.

EXTENSIONS

Introduce students to the website, *www.spokeo.com*. Suggest that they search the names of their parent or guardian or even themselves to see an example of how data gathered online can be aggregated and then sold without anyone actually agreeing to the process. Ask for students' reactions to this business model and have a discussion about whether or not it should be allowed or regulated or otherwise constrained.

SECTION 1 CONTINUED

RESOURCES

Broad description of how personal data gets collected, analyzed, and sold by online companies for advertising, marketing, and other purposes. PrivacyEnd, "The Hidden Secrets: How Your Personal Data Is Used Online"; *https://www.privacyend.com/how-personal-data-used-online/*

2023 study of apps across a broad range of categories analyzing degree and type of data being collected. Surfshark, "Uncovering the Apps that Actually Respect Your Privacy"; *https://surfshark.com/apps-that-track-you*

An overview of how online personal data gets collected, used, and sold, along with an interesting history of data collection practices. Wired.com, "The WIRED Guide to Your Personal Data (and Who Is Using It)"; *https://www.wired.com/story/wired-guide-personal-data-collection/*

State-by-state review of consumer privacy laws, with updates on legislative activities in 2023. National Conference of State Legislatures, "2023 Consumer Data Privacy Legislation"; *https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation*

Website of a non-profit organization for "the world's largest and most comprehensive global information privacy community." International Association of Privacy Professionals; *https://iapp.org/about/*

Definition of Personally Identifiable Information, provided by the Department of Labor. "Guidance on the Protection of Personal Identifiable Information," *https://www.dol.gov/general/ppii*

SECTION 2

The Many Bad Things That People Can Do Online

LEARNING OBJECTIVE

Students understand the variety and impact of criminal acts committed through online means.

BRIEF BACKGROUND DISCUSSION OF ISSUE

As noted in the *2024 Cybersecurity Almanac,* published by the online magazine, Cybersecurity Ventures, "If it were measured as a country, then cybercrime – which was predicted to inflict damages totaling $9.5 trillion globally in 2024 – would be the world's third-largest economy after the U.S. and China." This figure represents more than a tripling of damages registered in 2015. And it could well be a significant understatement of reality, since many cybercrimes go unreported, because of embarrassment, reputational harm, or belief that no legal remedy is possible.

The FBI reports that the top three varieties of cybercrime are: phishing scams, personal data breaches, and scams involving non-payment or non-delivery of goods and services. Cyber criminals make rapid adjustments to law enforcement actions taken against cybercrime, relying on large online networks of bad actors sharing software and strategies to make online crime pay.

Especially threatening to us as individuals, online data breaches continue to occur with regularity and in large numbers. 2024 saw 3,158 reported data breaches, according to the Identity Theft Resource Center, a slight decrease from 2023, but over twice the number reported only two years earlier. Headlining the bad news were Ticketmaster, with over 550,000 victims' records getting released, and four other breaches totaling over 100,000 victims each.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 8-9

SECTION 2 CONTINUED

WARM-UP QUESTIONS

1. Have you or has anyone in your family been affected by a data breach or other online crime?

2. What, if any, stories from the news do you remember hearing about cybercrime?

ACTIVITY 1.2.a

The Cost of Cybercrime

Students will explore the frequency and costs associated with different types of cybercrime. Starting with a selection of the "worst" examples of cybercrime, students choose one type of activity for further online research. They will identify three real-world incidents of their chosen type and then pick one such incident for more detailed investigation.

Students will now complete Activity 1.2.a, found on page 11 of their workbook. The activity is replicated on the next two pages of this guide.

1.2.a

The Cost of Cybercrime

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.

Cybercrime incidents

1. _____

2. _____

3. _____

ANSWERS WILL VARY, DEPENDING ON STUDENTS' CHOICES OF EVENT TO INVESTIGATE AND RESULTS OF RESEARCH.

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?

_____

_____

_____

4. Can you determine if AI tools were used in this incident? If so, how were they used?

_____

_____

_____

ANSWERS WILL VARY, DEPENDING ON STUDENTS' CHOICES OF EVENT TO INVESTIGATE AND RESULTS OF RESEARCH.

SECTION 2 CONTINUED

KEY TERMS

Business email compromise: Use of email to impersonate a trusted business contact, such as an executive or familiar vendor, and trick employees into sending money or sensitive information that could be used to access confidential or valuable data.

Confidence fraud: Any scheme in which the criminal pretends to be someone the victim knows and cares about, using personal information and/or emotional appeals to secure money or other things of value under false pretenses.

Extortion: Illegal demands for money based on intimidation or threats to harm someone in any number of ways, such as actual physical harm or public embarrassment.

Fraudulent fund transfers, by email: Scams involving online transfers of money, based on deceptive email exchanges or attacks on email systems allowing criminals to gain access to sensitive financial records or even actual accounts.

Identity theft: Theft enabled by a criminal impersonating someone else by using personally identifiable information stolen from online or physical data sources.

Non-payment/non-delivery: Exchanges of goods or services for money that are never completed, with the criminal either not paying for what they receive or not delivering what they have been paid for.

Phishing: Use of unsolicited emails or other communications purporting to come from legitimate sources to secure sensitive personal data enabling access to financial accounts or other sources of value.

SECTION 2 CONTINUED

EXTENSIONS

Introduce students to the website, *https://haveibeenpwned.com/*. On this site, users can search an enormous database of online accounts that have been hacked, with identifying information like email addresses and passwords made public.

1. Have students enter their email address to see if it has been part of a data breach made public. If they do not have an email address, or if theirs has not been part of a data breach, ask them to use the email address of a parent or guardian, with permission from this person.

2. Review the list of breaches with attention to the kinds of data that were compromised in the breach.

3. Based on the types of compromised data, rank the breaches in order of most to least threatening to, a) the user's online experience and, b) the user's off-line experience. Discuss as a group what would account for answers being different, if they are.

RESOURCES

Wide-ranging collection of data and analysis related to cybersecurity crimes, threats, workforce needs, and trends to be aware of. **Cybersecurity Ventures**, "2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions, and Statistics"; *https://cybersecurityventures.com/cybersecurity-almanac-2024/*

Wide-ranging report on data breaches and consequences and costs for victims. Identity Theft Resource Center, "2024 Annual Data Breach Report"; *https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/*

Federal report on cybercrime, analyzed by type, cost, and other factors, "Federal Bureau of Investigation Internet Crime Report 2023"; *https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf*

SECTION 3

D-e-f-e-n-s-e, Defense!

LEARNING OBJECTIVE

Students understand how multiple, overlapping layers of countermeasures are developed and deployed to provide the greatest level of security possible, as "defense-in-depth" approaches to protecting things of value.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Security controls serve to protect data from inappropriate access. The best security controls systems have multiple, interlocking parts that reinforce each other from different angles of potential attack. These overlapping forms of security controls add up to an approach to data security called "defense in depth." Most defense-in-depth systems deploy controls in three distinct areas: physical, technical, and administrative.

- **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. AI can enhance the strength of such controls by gathering, monitoring, and analyzing users' behaviors as they log into and use these systems.
- **Administrative controls** include rules, regulations, laws, and policies governing who should and should not have access to data systems. These controls are typically set at organizational or governmental levels.

Technical controls are most familiar to internet users in the forms of user IDs and passwords, which constitute the primary means by which individuals can act to enhance (or degrade) the security profile of their individual data stored online. A user

SECTION 3 CONTINUED

ID serves to identify a user, and a password authenticates the user's identity. Once granted access to online data, a user has authorization to do certain things to that data while being prevented from doing other things. Levels of authorization vary, depending on the rules governing access to the data in question.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Page 6

WARM-UP QUESTIONS

1. What kinds of security controls have you encountered in the world trying to go places and do things? Think about doing things like shopping, going to a friend's house, attending a concert or sporting event, getting on airplane, etc. Describe any physical, technical, or administrative controls that you can identify.

2. What kinds of proof of identity do you know of? What kinds do you yourself actually have or use?

3. Where are some places in the world where you have to show proof of identity?

ACTIVITIES

1.3.a: Mr. Beast Is Coming to Town
1.3.b: Protecting Your School's Grades

This activity features two parts, each one a scenario-based exercise in learning about the three different types of security controls that go into defense-in-depth security systems. In the first exercise, students will simply identify different types of controls that are mentioned in the scenario. In the second exercise, they will develop their own ideas of what controls might be used in each category, based on classroom discussion, review of the first scenario, and any reference to resources identified below or from other sources teachers might bring into use.

Students will now complete Activities 1.3.a and 1.3.b found on pages 13 and 16 of their workbook. The activities are replicated with answers on the next three pages of this guide.

1.3.a

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. **ANSWERS COULD INCLUDE: checkpoints; traffic barriers; guard dogs; National Guard Members; identification cards**

2. Technical controls. **ANSWERS COULD INCLUDE: userid and password systems; encryption to limit password access**

3. Administrative controls. **ANSWERS COULD INCLUDE: current enrollment in school; teaching or administrative position in school**

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.

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._____

ANSWERS COULD INCLUDE: locks on doors where computers are kept; surveillance devices such as cameras or motion sensors; locating sensitive data in off-site data storage facilities, etc.

2. Technical controls — and why

a._____

b._____

c._____

ANSWERS COULD INCLUDE: identification/userids and authentication/passwords uniquely generated for system access; authorization/access to data aligned with user roles; built-in system monitoring for unauthorized data incursions; key card/security fob for multi-factor authentication systems; etc.

3. Administrative controls — and why

a._____

b._____

c._____

ANSWERS COULD INCLUDE: variable levels of authorized access for different kinds of users; schedules for opening and closing access to writing/reading data; requirements for multi-factor authentication; training in internet/data security for users; rules about security for different types of data and/or users; etc.

SECTION 3 CONTINUED

KEY TERMS

Administrative controls: Rules, regulations, laws, and policies governing who should and should not have access to data systems.

Authentication: A process for proving that the identity of a user is actually what the user represents as real and reliably true.

Authorization: The set of privileges an authenticated user enjoys to view, alter, or otherwise access data within a larger system of stored information.

Defense in depth: A multi-layered approach to defending valuable assets that employs redundant, interlocking protective measures and can withstand security breaches or failures at one or more layers.

Identification: A label or tag that establishes who a user is within an online data environment, often in the form an email address or other name-based user ID.

Physical controls: Objects, tools, or other material resources that limit or prevent access in the real world to data systems and storage locations.

Technical controls: Hardware and/or software designed to limit or prevent access to online data, according to governing rules or principles put in place by system owners and stakeholders.

SECTION 3 CONTINUED

EXTENSIONS

Ask students to do internet searches on "defense in depth" and keep track of how many different types of environments or activities come up in results attached to the term. The concept applies to defensive measures in all kinds of settings, but with different emphases and meanings.

1. Identify 3-5 different settings in which "defense in depth" appears as a relevant concept. For example, different settings might be the military, information security, and nuclear energy.

2. Ask students to pick two different settings in which "defense in depth" is used and make a list of similarities and differences in the two settings.

3. Ask students to identify their favorite or most valuable possession. Explain that the wiliest, most devious burglar in town has decided to try and steal it. Students must develop a "defense-in-depth" approach, the strongest they can devise, to keep their possession safe and secure. As a follow-up topic, students can present their defense strategy to the group and see if others can identify weaknesses in it.

4. AI tools can be used to enhance various features of a "defense in depth" system. Ask students to imagine how they might strengthen each of the three areas of controls discussed in above: physical, technical, and administrative. In which of these areas would AI help the most? In which the least?

SECTION 3 CONTINUED

RESOURCES

Brief discussion of "defense in depth" as related to information technology systems. **Wikipedia**, "Defense in depth (computing)"; *https://en.wikipedia.org/wiki/Defense_in_depth_(computing)*

Blog post about protecting data stored in online data networks from one of the foremost experts on the topic of protecting public resources and information on the internet. **Schneier on Security**, "Security in the Cloud"; *https://www.schneier.com/blog/archives/2006/02/security_in_the.html*

Summaries of academic, technical resources examining "defense in depth" from various angles. **ScienceDirect**, "Defense in Depth"; *https://www.sciencedirect.com/topics/computer-science/defense-in-depth*

How the U.S.'s Cybersecurity and Infrastructure Security Agency use AI tools to defend its own systems,
"CISA Artificial Intelligence Use Cases"*; https://www.cisa.gov/ai/cisa-use-cases*

PART 2

HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT

GOAL

Identify and give instruction in basic approaches to safeguarding individual data online.

APPROACH

1. Show how individual choices and behaviors can strengthen or degrade security of online data.
2. Explain practices and tools that can protect personal data and make internet use safer.

OVERVIEW

- Students will learn about tactics people use to gain unlawful access to online data, what the damage can look like, and actions they can take to protect their data by building and using strong passwords.
- All these themes fall generally into the area of how difficult it is to establish and maintain online trust among individuals and the companies and organizations that store their personal data online.
- Students will also learn how AI tools have made it easier for malicious hackers to carry out criminal activities, including phishing campaigns, attacks on data stores, and identity theft.

SECTIONS

SECTION 1

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

LEARNING OBJECTIVES

- Students understand the scope of phishing scams as an online risk.
- Students learn to identify indicators of an email used as part of a phishing scam and what to do when they think they receive one.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Con artists have worked long and hard to perfect the art of telling stories to trick and swindle. Designed to persuade people to part with money or other items of value, these stories play on emotion, especially fear, greed, temptation, and other states of mind that move us to make bad decisions. Such "social engineering" has been a part of human exchanges nearly forever.

Digital communications platforms have only amplified the reach and force of these kinds of stories. In fact, we might just be living in a golden age of scams and hoaxes, aided and abetted by readily available AI tools that make these schemes both cheaper and easier to execute as well as more realistic and persuasive. From fake PayPal invoices to QR codes that lead to fraudulent websites to deceptive notices of phantom account suspensions, emails by the dozen as well as texts and phone calls arrive every week with "urgent" messages like these.

"Phishing" is the catch-all term for these kinds of scams. The goal of a phishing campaign is to persuade people to cough up personally identifying information that allows malicious hackers to get into data stores and networks that should be off-limits to them. With such access, they insert malware, launch ransomware operations, steal troves of data to sell on the dark web, or commit other kinds of cybercrimes that cost businesses and individuals billions of dollars every year. →

SECTION 1 CONTINUED

Phishing is an ongoing, online disaster, and the full scope of activity and damage is almost impossible to calculate. In general:

1. Phishing is by far the most common form of cybercrime, by almost a 5:1 margin, according to the FBI.
2. Businesses are the most common target, with financial institutions, social media companies, and webmail services (Gmail, Hotmail, etc.) suffering the greatest number of attacks.
3. Alarmingly high percentages of people fall for scams – by one count, over 20 percent of recipients open phishing messages, and two-thirds of these click on links they contain.
4. One large study found that 95 percent of data breaches result from human error, with the vast majority resulting from successful phishing campaigns.
5. Cybercriminals use AI tools to make phishing emails even more realistic and hard to detect by incorporating individualized content, graphics that almost perfectly resemble those used by real companies, and persuasive, natural language.

The best defense against phishing is teaching people how to recognize the signs of digital messages meant to defraud, to avoid clicking on suspicious links or downloads, and to remain vigilant and cautious with any request for personal data.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 16-17

SECTION 1 CONTINUED

WARM-UP QUESTIONS

1. Have any students — or anyone they know — received phishing messages? What did they look like? What was their goal?
2. What kinds of appeals or offers might be most likely to trick students into falling for a phishing scam? Free sneakers? Concert tickets? A new phone?
3. How do students think they might protect themselves from phishing campaigns?

ACTIVITIES

2.1.a: What Are the Signs of a Bogus Email? and **2.1.b: How Good Are You at Spotting Phishing?**

In this activity, students will try their hand at identifying the telltale signs of bogus phishing emails, build further knowledge of what goes into a message meant to deceive people by taking several online phishing quizzes, and then develop recommendations for other people about how to identify emails that could be part of scams to deceive and steal.

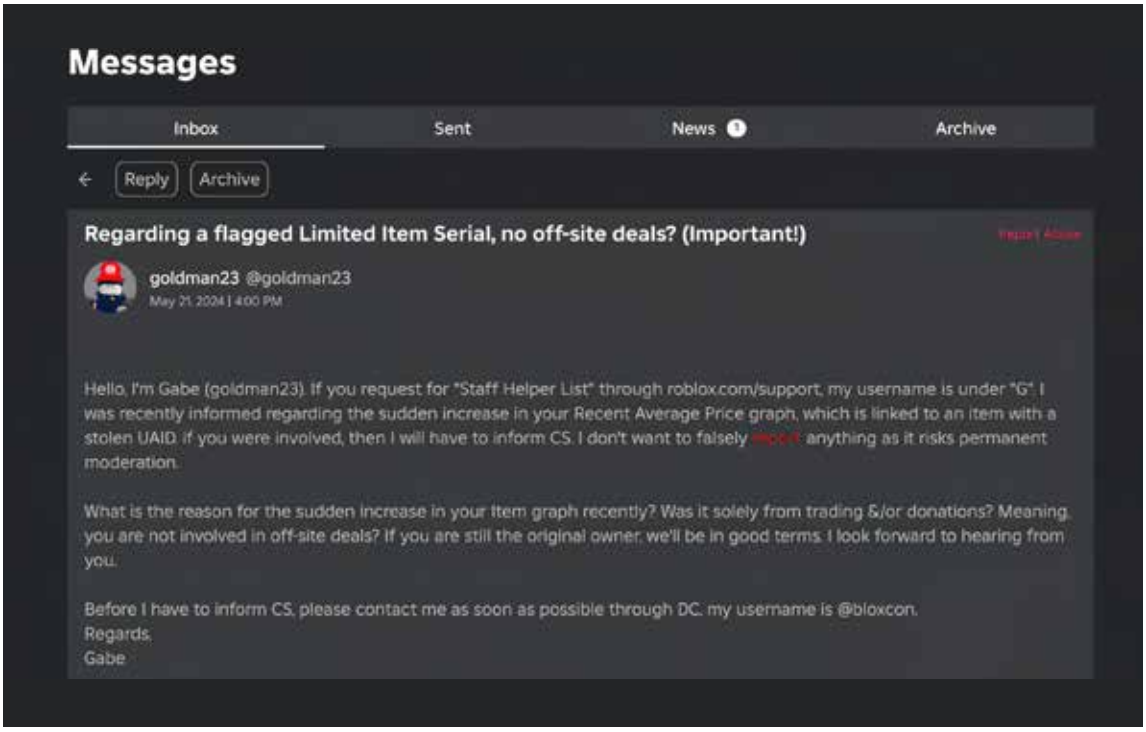
Students will now complete Activities 2.1.a and 2.1.b, found on pages 20 and 24 of their workbook. The activities are replicated with answers on the next five pages of this guide.

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.



2.1.a (CONTINUED)

Clue 1: _____

Clue 2: _____

Clue 3: _____

Clue 4: _____

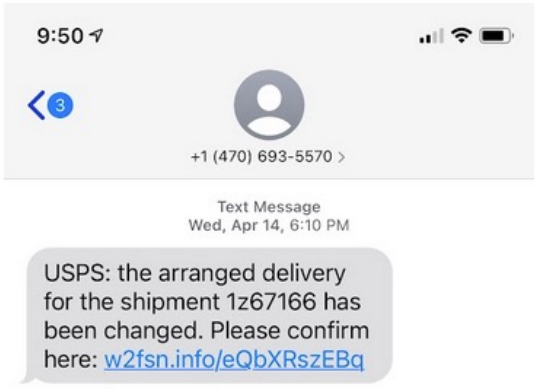
Phishing clues ANSWERS

1. **The subject line conveys urgency and importance, trying to get the recipient to act quickly and with less care than would be appropriate.**
2. **Awkward construction in the 2nd and 3rd sentences of the first paragraph.**
3. **The 4th sentence starts with a lower-case letter.**
4. **The first paragraph ends with a threat to the recipient, raising the emotional intensity of the message.**
5. **In the second paragraph, 1st sentence, the word "Item" is capitalized for no reason.**
6. **The 2nd and 3rd sentences of the second paragraph are awkwardly constructed in a tone that seems wrong for the kind of message being sent.**
7. **The 4th sentence in the second paragraph says "in good terms" instead of "on good terms."**
8. **The message ends with an appeal to communicate on a different platform, outside of the Roblox environment: "DC" is shorthand for Discord, a different communications platform outside of Roblox.**

2.1.a (CONTINUED)

1. 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!



2.1.a (CONTINUED)

Clue 1: _____

Clue 2: _____

Clue 3: _____

Clue 4: _____

Clue 5: _____

Phishing clues **ANSWERS**

1. **The texts come from unknown numbers.**
2. **The punctuation and structure of the first sentence are awkward.**
3. **The texts reference events – a raffle and a shipment – that the recipient did not initiate or expect.**
4. **The urls to click look "unofficial."**
5. **The messages are coming out of the blue and asking for prompt responses, always an indication of something fishy.**

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?

   _____

   _____

Answers will vary, depending on the results of students' quizzes.

SECTION 1 CONTINUED

KEY TERMS

Phishing: The use of emails that seem to come from a trusted site or person seeking to trick the recipient into giving up sensitive personal data, usually meant to gain access to restricted data networks and records.

Smishing: The use of simple text messages, or texting, to accomplish the same goals as phishing.

URL: Uniform Resource Locator, or the name of a website usually built to describe the contents or identify the organization associated with the website itself.

Vishing: The use of voice messages to accomplish the same goals as phishing.

EXTENSIONS

Ask students to develop a phishing campaign designed to elicit personal data that would enable access to a protected data storehouse or network. The elements of the campaign should address the following questions, among others:

1. What source of data are you trying to break into? For example, a bank? Google Classroom? A social media platform? A shopping rewards program?
2. Who is the target recipient of your phishing campaign? What kind of user of the data source is the recipient? In the case of Google Classroom, for example, is it a student? A teacher? An administrator?
3. What kind of data are you trying to acquire? User ID? Password? Account numbers? Other items?
4. What would the headline of the phishing email be? How would it capture a recipient's attention and motivate him or her to open it?
5. What "problem" or situation would the email describe as motivation for the recipient to provide personal data as part of the solution? An outdated password? A need to reconfirm a user's authorization to access data? Perhaps an urgent, special offer of something valuable?
6. Imagine access to all-powerful AI tools that can locate details of recipients' personal lives. What kinds of details would you include in your phishing campaign to make it more persuasive and compelling for people to open?

SECTION 1 CONTINUED

RESOURCES

Website for organization promoting education, awareness, and public-private partnerships in support of greater online security and protections from cybercrime.
National Cybersecurity Alliance
https://staysafeonline.org/

Website for SafeSearchKids, presenting tips for helping kids avoid falling for online scams.
https://www.safesearchkids.com/protecting-against-online-scams-phishing-smishing-vishing/

Guidance from the federal government in staying safe from phishing scams.
Federal Trade Commission, "How to Recognize and Avoid Phishing Scams";
https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

Report from FBI about actions taken and information gathered in response to reports of cybercrimes.
FBI Internet Complaint Center, "Annual Report 2023";
https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Data and further information about phishing from security.org.
https://www.security.org/resources/something-smells-phishy/.

Scholarly article describing how AI-powered phishing campaigns work, written by leading experts in cybersecurity.
Heiding, Fredrik, et al. (2024). IEEE Explore, "Devising and Detecting Phishing Emails Using Large Language Models"; *https://ieeexplore.ieee.org/document/10466545*

Magazine article about generative AI tools making phishing campaigns more numerous and dangerous.
Heiding, Fredrik, et al., (May 30, 2024). Harvard Business Review, "AI Will Increase the Quantity — and Quality — of Phishing Scams";
https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

SECTION 2

The Many Faces of Data

LEARNING OBJECTIVES

- Students understand that data comes in many forms and is used in different ways by different kinds of people.
- Students understand the three main components of data security: confidentiality, integrity, and availability.

BRIEF BACKGROUND DISCUSSION OF ISSUE

We talk about data being stored online, but what do we actually mean by this? Where does data go and how does it get there, when it gets "stored online?"

One answer is that data is stored in the "cloud." But "cloud" is a deceptively simple word for an extremely complicated system of servers, software programs, processors, controls, buildings, energy sources, procedures, rules, wires, switches, and much else. And installations of such systems exist in enormous, rapidly growing numbers all over the world. Our personal technology devices are connected to these systems nearly all the time, transmitting and receiving data in the background and foreground of all the things we do online, like shopping, emailing and texting, reading and watching, paying bills, and much else.

The complexity of cloud computing, however, also introduces challenges to cybersecurity. Indeed, all the possible vectors of attack make "defense in depth" (see Part 1, Section 3) all the more relevant. Redundant, mutually reinforcing layers of protection need to be in place to give reliable protection to the many, intersecting components of a cloud-based data system. Because AI systems rely so heavily on cloud computing systems, they present unique risk scenarios. AI systems "learn" about the world by digesting often enormous sets of training data that serve as the foundation for what they "know" about the world. These systems compare new pieces of data to the contents of the training data to find patterns, infer connections, and generate responses about what the new pieces of data represent. Training data often resides in the cloud, and malicious actions to alter, or "poison," the data can corrupt the reliability and integrity of the AI sys-

SECTION 2 CONTINUED

tem and its outputs. This kind of cyberattack is called "adversarial machine learning." It takes place almost invisibly, and users might well have no way of knowing when an operation like this is at work to manipulate or degrade the outputs of an AI system.

Cloud-based networks, then, and AI tools in particular, need to be secured from end to end. But they must be more than just secure. They must also be usable. And the framework for incorporating both security and usability starts with confidentiality, integrity, and availability, or the CIA triad. At this point, for the purposes of both background knowledge and classroom discussion, it will be useful to review the presentation of the CIA triad in Outsmart Cyberthreats on page 18.

A fully conceptualized strategy for protecting data “in depth” will address all three elements of the CIA triad.

- **Confidentiality** might be preserved with authentication measures, like passwords, biometrics, PINs, and security questions. Encryption would be a key tool for protecting identification and authentication measures from unauthorized access.
- **Integrity** would be protected by protocols governing access to data and operations as well as monitoring tools designed to identify unauthorized or inappropriate a lterations to data.
- **Availability** would rely on resources that keep systems up and running even when internal components fail or in the face of problems like power outages, natural disaster, or attacks on operations.

Cyberattacks can target the confidentiality, integrity, or availability of data from any direction at any time, but the security system must be designed to preserve all three facets at all times. As noted above, data poisoning attacks can especially undermine the integrity of an online data system that uses AI tools, often in ways that might not be obvious. This asymmetry makes cybersecurity a more difficult enterprise than cybercrime. Cloud computing, it turns out, allows for revolutionary innovations and efficiencies in the ways that both society and attacks on society can work.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Page 18

SECTION 2 CONTINUED

WARM-UP QUESTIONS

1. Where do students have their data stored online? What kinds of services or apps hold personal information of theirs? Remind students that any website that requires a user ID and password has gathered and stored their data.

2. What kinds of problems have students ever encountered getting access to their data? Problems could run from difficulty or delays logging in to a website to a website outage to actual data breaches or compromised online identity. In any such instances, ask students to identify which of the three CIA principles they would attach to the problems.

ACTIVITIES

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

In Activity 2.2.a, students will practice applying their understanding of confidentiality, integrity, and availability. First, students will read brief accounts of recent, high-profile data breaches and answer questions about the impact and nature of these incidents. Then, working with more familiar, school-related data types in an imaginary online data system, they will step into the role of data security system designer to address questions about access and status of data type. In Activity 2.2.b, students imagine all the data that their school likely has about them.

Students will now complete Activity 2.2.a, found on page 25 of their workbook, and Activity 2.2.b, found on page 30 of their workbook. The activities are replicated with possible answers on the next four pages of this guide.

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.

Another 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.

2.2.a (CONTINUED)

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: **Hackers broke into the PlayStation network and gained access to about 77 million users' personal accounts. The attack prevented users from accessing online gaming services and also exposed personal information to possible public exposure.**

Target: **The attackers stole credit card data belonging to about 40 million customers, and personal data of 70 million other people, by loading malware into the registers customers used in Target stores to pay for merchandise.**

Office of Personnel Management: **Theft of sensitive personal information belonging to over 21 million people who applied for or held federal government jobs. Records included social security numbers, background investigations, and even fingerprints.**

2.2.a (CONTINUED)

National Public Data: Attackers gained unauthorized access to an online storage database containing records of personal data to be used by the company's clients making background checks on people. Types of information included names, phone numbers, email addresses, Social Security Numbers, and names of family members.

Tay: Twitter users tweeted large numbers of inflammatory phrases and messages at Tay, and the chatbot learned from these tweets how to respond in kind with other examples of hate speech and inappropriate content. Microsoft removed the Tay account from Twitter within 16 hours of its initial release.

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

Sony PlayStation:
Confidentiality – personal account data;
Availability – access to online services was denied.

Target:
Confidentiality – personal and credit card data;
Integrity – data systems were exposed and subject to change;
Availability – canceled credit/debit cards would prevent access to accounts.

Office of Personnel Management:
Confidentiality – sensitive personal data was stolen;
Integrity – possible alteration of data within the system and misuse in other online locations.

National Public Data:
Confidentiality – contact information, Social Security Numbers, dates of birth, phone numbers.

Microsoft:
Integrity – "data poisoning" in the form of hate speech trained an AI tool to produce and distribute similarly offensive language in social media exchanges.

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 parent or guardian 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.

MULTIPLE POSSIBLE ANSWERS:

1. name, age, grade
2. class schedule, class assignments
3. test scores, homework grades
4. lunch purchases, bus riding information
5. sports team memberships, club participation
6. musical instrument, theater participation
7. hallway camera footage, attendance, late arrivals,
8. siblings' names and grade level
9. names of parents or guardians
10. immunization records, medical records, etc

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.

2.2.b (CONTINUED)

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

SECTION 2 CONTINUED

EXTENSION

Different kinds of users put data in a system to different kinds of uses. They read, share, edit, delete, lock down, move, export, import, and do other things, as well, depending on the type of data, user, and organization, among other variables. This exercise asks students to think about uses of data and how to control who gets access to what and for what purposes. In other words, it asks them to think about users, authentication, and authorization.

Ask students to pick out 3-5 types of data from their work in 2.2.b and complete the table below. Follow-up discussion can involve students sharing different ideas about who uses data for what reasons as well as how and why system administrators would treat different data types in different ways.

DATA TYPE	USERS	AUTHENTICATION	AUTHORIZATION
1.	1.	1.	1.
2.	2.	2.	2.
3.	3.	3.	3.
4.	4.	4.	4.
5.	5.	5.	5.

POSSIBLE ANSWERS:

User(s): students, teachers, parents or guardians, principal, nurse, coaches, meal administrators, transportation department, attendance monitor, et al.

Authentication: none, username, password, two-factor authentication code, fingerprint scan, keycard, etc

Authorization: read, view, edit, copy, etc.

SECTION 2 CONTINUED

KEY TERMS

Adversarial machine learning: Introducing data into an AI system's training set that is meant to deceive or mislead a learning model into producing incorrect, unreliable results.

Availability: The need for data and the system in which it is stored to be accessible and functional at all times needed for users' and owners' business purposes.

Cloud computing: A network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

Confidentiality: The condition of data being disclosed only to those who are authorized to view it.

Controls: A set of devices or procedures that govern how a machine operates, with inputs from a user, a software program, or other source.

Data poisoning: Intentionally feeding misleading, harmful, or generally corrupted data into an AI system to make it produce biased, inaccurate results. An example of "adversarial machine learning."

Integrity: Assurance that data stored online remains accurate and whole, corresponding to off-line realities and/or the owner's understanding of its complete-ness and correct-ness.

User privileges: Authorization given to users that enables them to access specific resources on the network and perform defined operations on them, such as view, edit, delete, etc.

User ID: The identity or label by which a person is known on a computer system or network.

SECTION 2 CONTINUED

RESOURCES

Magazine article about cyberattack against Target.
Constantin, Lucian. (January 13, 2014). "Target's point-of-sale terminals were infected with malware." **Computer World**;
https://www.computerworld.com/article/1519447/target-s-point-of-sale-terminals-were-infected-with-malware.html

Background information about confidentiality, integrity, and availability concepts.
Project Ares (Circadence; video file), "What's the CIA Triad?";
https://youtu.be/rwigKjEsdTc

Description of cyberattack against Office of Personnel Management. "Office of Personnel Management data breach";
https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

Description of cyberattack against online Sony PlayStation network.
Wikipedia, "2011 PlayStation Network Outage";
https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage

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

Magazine article about Tay chatbot and hate speech.
Schwartz, Oscar (November 19, 2019). **IEEE Explore**, "In 2016, Microsoft's racist chatbot revealed the dangers of online conversation.";
https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation

Federal government review of "adversarial machine learning" tactics.
National Institute of Standards and Technology. "NIST identifies types of cyberattacks that manipulate behavior of AI systems."
https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

SECTION 3

Building and Managing Passwords for Security and Convenience

LEARNING OBJECTIVE

Students understand how to build and manage strong, unique passwords.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Online security systems rely on the capacity to authenticate, reliably and repeatedly, a user's real-life identity when he or she logs into an account. The online password is the primary mechanism for this authentication operation. And a strong password, used once and only once, provides powerful protection against unauthorized access to online data.

Unfortunately, passwords — in both construction and handling — prove difficult for people to use properly. Too many of us, all too often, build simple, easily cracked passwords, use them for multiple accounts, share them with other people, or give them up to phishing campaigns. However, it is easy to learn good password safety practices, and making them habitual is nearly a civic duty. Sloppy, careless handling of passwords can put not only our individual data at risk, but also everyone else's data stored in virtual proximity.

In a properly built and administered online data network, even network operators do not have direct access to passwords. Automated encryption systems translate our passwords into lengthy, seemingly random strings of characters, or "hashes." This hash is then saved in the system for comparison to the password we use next time we log in. Encrypted or hashed again, the password must match the established value for our user identity to be authenticated.

But hashes, if leaked, can still be deciphered when passwords are poorly built. And the rampant frequency of data breaches should remind us to put little trust in the overall security of online data networks. AI tools only exacerbate these problems,

SECTION 3 CONTINUED

making it easier for cybercriminals to crack passwords and break into storehouses of sensitive data. Even when they lack access to actual password files, hashed or not, hackers can crack passwords with brute force, using raw computing power to cycle through variations of letters, numbers, and special characters until some combination clicks as a real password.

They can also use sophisticated software that brings the capacities of artificial intelligence or machine learning into the mix. One way such programs work is to scan the web for bits of personal information connected to people's names on social media profiles, public databases, or other such online locations. They then plug these bits of data – birthdays, pets' names, vacation spots, favorite songs, etc. – into possible password constructions to try and break into personal online accounts. **For this reason, students — and everyone — should never incorporate personal information they share online into passwords they use to protect online accounts**.

As AI systems grow in sophistication and capability, so too do AI password cracking tools. In a 2023 study, an AI-driven tool called PassGAN took only one month to crack over 80 percent of passwords in a set of 15 million passwords stolen in a 2009 data breach. Even simple passwords up to 12 characters long fell in only three weeks. However, complex passwords involving numbers, upper- and lower-case letters, and special symbols remained effective. At 12 characters, such constructions would take 30,000 years for PassGAN to crack. And longer complex passwords took much more time to crack, running to the millions of years and beyond.

Note: Any passwords that students use in a classroom exercise are immediately compromised and unusable as actual passwords in their personal lives. They should always keep their actual passwords private and known only to themselves. It is important to remind students of this fact throughout any exercises involving password building and management.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Page 11

SECTION 3 CONTINUED

WARM-UP QUESTIONS

1. How many passwords do students themselves use? How do they remember and keep track of them?
2. Do students share their passwords? With whom? Do they know other people's passwords? If so, whose?
3. Are students aware of any stories from the news about passwords and other personal data getting leaked online? If so, which ones? Do they think their personal data might have ever been leaked online?

ACTIVITIES

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

In these exercises, students will learn how to build a strong, complex password. Exercises will give them practice in several different approaches to this important online safety skill. In addition to building passwords, students will learn about managing them. Keeping track of passwords can be done in different ways, and students will be asked to consider several, as well as propose approaches of their own devising.

Students will now complete Activities 2.3.a and 2.3.b, found on pages 33 and 36 of their workbook. The activities are replicated on the next five pages of this guide.

Be sure to remind students, repeatedly, that any passwords they develop in this activity should NOT be considered for actual use in their personal lives. Once a password is used in a learning activity, it is compromised and public.

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.

2.3.a (CONTINUED)

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?

_____

_____

_____

2.3.a (CONTINUED)

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.	

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 "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.

SECTION 3 CONTINUED

KEY TERMS

Encryption: A translation of language in plain, conventional text into ciphered text requiring a key to decode and make legible.

Hash: Data or language transformed by a formula to generate a string of random characters of defined length, requiring a decryption key to make comprehensible.

Password manager: A tool for managing and/or generating unique online passwords that stores and automatically enters a user's authentication credentials needed to gain access to an account.

EXTENSIONS

Developing strong, memorable passwords is one thing. Keeping track of them is another. Every approach to tracking passwords carries some risk. Writing them down in a notebook means you could lose the notebook, someone could take a peek, or your dog could chew it up. Putting them in a file on your computer could make them accessible to someone able to hack into your machine. A password manager can work well, but you still must remember the main password for the account.

Ask students to develop two or three different systems for recording and tracking passwords. Starting this exercise with an internet search can be useful, especially for getting acquainted with how different kinds of password managers work.

Then ask them to recommend a particular approach to a) a grandparent and b) a friend, along with a brief explanation about why they recommend the particular approach they choose. Students can be advised as well to choose a system for themselves. But in keeping with best privacy practices, they should not explain their system to anyone else.

SECTION 3 CONTINUED

RESOURCES

Password guidance from a leading expert on online security topics for individuals and organizations.

Krebs, Brian. "Password do's and don'ts";
https://krebsonsecurity.com/password-dos-and-donts/

Password guidance from another leading expert in the field.

Schneier, Bruce. "Choosing secure passwords";
https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Magazine article about how AI tools can crack passwords.

Yee, Alaina (April 11, 2023). **PC World**, "AI can crack most passwords faster than you can read this article";
https://www.pcworld.com/article/1782671/ai-can-crack-most-passwords-faster-than-you-can-read-this-article.html

Guidance on how to build strong passwords from cybersecurity non-profit.

Identity Theft Resource Center, "The Evolution of Password Advice";
https://www.idtheftcenter.org/post/the-evolution-of-password-advice/

CONTROL YOUR RISK ONLINE

GOAL

Show students how to identify and assess risk factors in both real-world and online environments, as well as encourage students to reflect on what kinds of cybersecurity career fields might align with their own interests.

APPROACH

1. Explore the components of risk: vulnerabilities, threats, and attacks.
2. Introduce a basic procedure for assessing risk, involving the likelihood and degree of damage associated with an attack.
3. Introduce types of career fields in cybersecurity and encourage students to consider how their own interests and abilities might lend themselves to contributions in the field.

OVERVIEW

- Students will learn the basic components of risk and how to identify them within both real-world and online scenarios.
- They will also learn to apply a procedure for assessing risk and then follow up by considering how different areas of the cybersecurity field require different approaches to applying this procedure.

SECTIONS

SECTION 1
Risky Business

LEARNING OBJECTIVES

- Understand and differentiate among components of risk.
- Use risk analysis to formulate plans to mitigate risk.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Risk is always all around us. It is embedded in the world almost everywhere, in ways both hidden and surprising as well as obvious and predictable. One of the jobs of a cybersecurity professional, not to mention a person in general, is to learn to identify the components of risk and adopt activities and behaviors that reduce the likelihood of risk turning into actual harm.

Risk can be analyzed through a sequence of three phenomena: vulnerabilities, threats, and attacks. These terms are defined in the text on page 28, and this section challenges students to think about all three phenomena as things unto themselves as well things connected to each other that add up to potentially harmful events. Students practice identifying these components of risk in a familiar environment: their neighborhood swimming pool. This activity is meant not to scare them but to demonstrate that learning to identify risk starts with learning to see familiar, seemingly safe environments through a different kind of lens from the one they use every day. They will start to see things as risk analysts, able to work back and forth through the vulnerability-attack-sequence to identify ways to reduce risk. NOTE: If students cannot relate to the swimming pool scenario, any other environment familiar to them can be used instead.

For cybersecurity professionals, this aptitude is often called "thinking like an adversary." It means getting into the mindset of a cyber criminal and seeing how data systems and technology devices and user behaviors combine to expose individuals to potentially damaging digital attacks. Both as individual users of the internet as well →

as possible future professionals in the field, students will lead safer, more constructive lives online if they can develop the ability to "think like an adversary" in all the ways they use the internet.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Page 28

WARM-UP QUESTIONS

1. What kinds of things or ideas do students associate with the words "vulnerability," "threat," and "attack"?
2. In what sequence of occurrence would students arrange these three phenomena?
3. What kinds of vulnerabilities, threats, and attacks can students think of that would present risks — of any kind — to a school building? To the school's computer systems, e.g., Google Classroom or the school's online grading system?

ACTIVITY

3.1.a: Identifying Risks

In this activity, students will learn about vulnerabilities, threats, and attacks by thinking through how these three risk factors might be relevant to a familiar environment: a swimming pool. They will begin a "risk analysis" by considering seemingly mundane, innocuous features of a swimming pool as potential sources of risk. Then they will start to learn to "think like an adversary," imagining different kinds of attacks to work backwards towards a deeper understanding of threats and vulnerabilities.

Students will now complete Activity 3.1.a, found on page 39 of their workbook. The activity is replicated with possible answers on the next three pages of this guide.

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:

POSSIBLE ANSWERS

1. **Poolside activities, like a slide or diving board.**
2. **Pool-cleaning chemicals beyond their expiration date or not locked up.**
3. **The deep end.**
4. **Lifeguards not paying attention and/or not certified in CPR.**
5. **Pool computers used near water hazards.**
6. **Crowds of people moving in many different directions at the same time.**
7. **Running kids and wet slippery surfaces.**
8. **Night-time security measures.**
9. **Hard surfaces near swimming areas, like the bottom of the pool, corners, or edges.**
10. **Guest Wi-Fi network with no password.**
11. **Poolside seats in full sun.**
12. **Old, unstable seats for guests.**
13. **Trash receptables.**

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

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

Possible answers will vary enormously, depending on what students come up with as vulnerabilities or attacks to start with. In any case, discussion of how they connect all three elements of risk will be useful to illustrate the concepts.

SECTION 1 CONTINUED

KEY TERMS

Attack: Activity that causes damage or harm to people or resources. Attacks can include both intentional acts committed by people to cause harm as well as acts of nature that do the same, such as natural disasters, extreme weather conditions, or other events that harm people or property.

Risk analysis: Identifying and breaking out the different factors that add up to a risk: vulnerabilities, threats, and attacks.

Threat: A device, pathway, action, or actor that can combine with a vulnerability to inflict damage of any kind on a resource. A threat can be intentionally constructed to harm or result from unlucky combinations of circumstance with no underlying malicious intent.

Vulnerability: A weakness in a system, environment, or structure that can be exploited by an outside force to cause damage to people or resources of value.

EXTENSION

Ask students to extend their analyses of risks at a swimming pool to other familiar environments, like stores, restaurants, sporting events, etc. The more practice students get applying risk analysis to environments that might not seem risky in the first place, the more they will be honing their developing abilities to discern risk in their lived experiences.

RESOURCE

General information from the federal government about risk assessment related to natural and manmade hazards.
https://www.ready.gov/risk-assessment.

SECTION 2

Know Risk, not "No" Risk: Smartphones and Artificial Intelligence Tools

LEARNING OBJECTIVES

- Understand the nature of vulnerabilities, threats, and attacks that could pose a risk to smartphone users.
- Apply principles of analyzing and mitigating risk to using a smartphone as well as AI tools.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Smartphones are a security nightmare, in many different ways. The obvious ways, as suggested in the text, have to do with threats to personal data and digital resources we rely on to live our online lives. But that is only the beginning, and a healthy awareness of the risk vector that smartphones represent is important for students to develop.

Risks to smartphones – and the personal data they store or provide access to – start with loss or theft and extend to malicious downloads or sketchy links we might expose our phones to with careless use. These latter scenarios should be familiar to students, but they represent such a huge portion of real-life risk to smartphone users that dwelling on the potential for harm is worthwhile. The speed with which new apps hit the market and the appetite for data tracking that drives the mobile marketplace combine to make it almost impossible to regulate or even understand threats to the data of mobile users. The best defense is founded on teaching and encouraging kids to make informed, risk-reducing choices about the devices and tools they use in their online lives.

The explosion of AI tools in nearly every sphere of online life has not failed to register on K-12 education. Accessible in supervised, intentional ways in the classroom as well as in unsupervised ways everywhere else, AI tools present choices to students that an

SECTION 2 CONTINUED

understanding of risk can help them navigate. From their own actions to the outputs they get from the tools themselves, engaging with AI tools requires students to recognize and avoid risk in various ways. Falling afoul of AI risks can jeopardize students' standing in school, undermine learning, and damage important personal relationships.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 26-28

WARM-UP QUESTIONS

1. Looking at all the events from Parts 1-3, do students recognize any of their own behaviors or experiences in what happens to the main character? Which ones?
2. What would students do differently from the main character?

ACTIVITIES

3.2.a: How Risky Is Your Phone? and
3.2.b: AI: It's All In How You Use It

Students apply the learning about vulnerabilities, threats, and attacks in general to the use of smartphones and AI tools in this activity. They will parse the events in *Outsmart Cyberthreats* to do with the main character's smartphone misadventures to tease out the different risk factors in evidence. Then they will develop possible approaches to mitigation strategies that could prevent or minimize harm from actually occurring. In the second exercise, they will examine risks to do with using generative AI tools for schoolwork. Just as choices and behaviors about using smartphones can expose us to risk, so too can choices and behaviors about using AI.

Students will now complete Activities 3.2.a and 3.2.b, found on pages 42 and 44 of their workbook. The activities are replicated with possible answers on the next 5 pages of this guide.

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.

Possible answers in purple

RISK FACTORS	IN THE TEXT	IN GENERAL USAGE
Vulnerabilities	careless user behavior, access to contacts across apps, apps that gather data	out-of-date software, on-device settings that allow too much access to stored data, improper password behaviors, inappropriate sharing of personal information
Threats	malware downloaded onto phone	physical damage from water, cold/heat, mishandling; malicious hacking activities; unpaid bills
Attacks	social engineering scam text message, demand for ransom	phishing, spam, theft, intentional damage, carrier terminating service, parents/guardians or other authorities taking away phone for misuse

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:_____

_____

Possible answers will depend on items chosen by students.

Follow-up discussion can include other students' assessments of how well proposed mitigation strategies might work and/or suggestions for different approaches to risk mitigation.

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, a failing grade.

3.2.b (CONTINUED)

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. Identify at least 3 possible risk elements in each category, and then describe a mitigation strategy that would reduce the risk of 1 of these elements from happening.

Possible answers in purple, with mitigations dependent on students' choices.

1. Vulnerabilities:

- **Not paying attention in class**
- **Waiting until the last minute**
- **Easy access to ChatGPT**
- **Unsupervised task at home**
- **Doing the paper all at one time, instead of developing drafts over time with the teacher reviewing them**

2. Threats:

- **ChatGPT seems to present an easy solution**
- **ChatGPT can get things wrong**
- **Relying on AI alone risks exposing lack of understanding**
- **Detection software can identify products of AI writing**

3.2.b (CONTINUED)

3. Attack:

- **Taylor submitting the essay as his own**
- **Getting caught cheating**
- **Damaging relationship of trust with his teacher**
- **Not learning the material**
- **Angry parents or guardians**
- **Bad grade**

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?

Answers will vary for all questions, depending on the direction of students' interests and thoughts or that of classroom discussions.

SECTION 2 CONTINUED

KEY TERM

Mitigation: Actions taken to reduce the possibility or extent of damage that a risky set of circumstances can present.

EXTENSION

Share the articles shown in the Resources section with students. Ask them to read the articles and develop a list of the five biggest threats to privacy that using a smartphone can present. They should provide brief explanations of why they selected these items as the riskiest. Then ask students to develop recommendations for how to reduce the threats to privacy associated with these apps. As a class, teachers and students can compile their recommendations to develop something like a guide to smartphone privacy for possible use in their own school or even more broadly in their community.

SECTION 2 CONTINUED

RESOURCES

Federal government guidance about using apps and sharing data safely.
Federal Trade Commission, "How Websites and Apps Collect and Use Your Information";
https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

Educator-oriented discussion of how smartphones can put private data at risk, both via intentional and unintentional sharing behaviors.
Temming, Maria. (January 30, 2018). "Smartphones put your privacy at risk";
Science News for Students,
https://www.sciencenewsforstudents.org/article/smartphones-put-your-privacy-risk

Summary-level overview of risks to privacy that smartphones can pose.
DeMuro, Jonas. (September 8, 2023). "8 reasons why smartphones are privacy nightmare"; TechRadar,
https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare

Full newspaper-style account of how location data is gathered from phones, attached to individuals, and used for disclosed and undisclosed purposes.
Klosowski, Thorin. (September 29, 2022). "How Mobile Phones Became a Privacy Battleground–and How to Protect Yourself." The New York Times.
https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/

Broad discussion of how educators can think about and put to use AI tools in the classroom.
Elgersma, Christina. (March 6, 2024). "ChatGPT and Beyond: How to Handle AI in Schools." Common Sense Media.
https://www.commonsense.org/education/articles/chatgpt-and-beyond-how-to-handle-ai-in-schools

Teachers organization presents different aspects of using and controlling AI tools in educational settings.
Blose, Abreanna. (April 12, 2023). "As ChatGPT Enters the Classroom, Teachers Weigh Pros and Cons." neaToday.
https://www.nea.org/nea-today/all-news-articles/chatgpt-enters-classroom-teachers-weigh-pros-and-cons

SECTION 3

Assessing Risk Across Different Fields of Activity

LEARNING OBJECTIVES

- Understand and apply a basic procedure for conducting risk assessment.
- Connect approaches to mitigating risk with each of the three fields that make up the cybersecurity career landscape: the logical field, the social field, and the physical field.

BRIEF BACKGROUND DISCUSSION OF ISSUE

Assessing risk can be understood as the starting point for almost any online security enterprise. The ability to assess, respond to, and reduce risk is a fundamental requirement for almost any cybersecurity job, something professionals in the field must do before, during, and after a cybersecurity event. This section extends students' abilities to assess risk by considering a different set of variables from those considered in previous sections: the likelihood of an event occurring and the damage an event would incur if it did take place.

The section also grounds students in real-world scenarios, asking them to think about risk in terms of the three different cybersecurity "fields" identified in the text: the logical field, social field, and physical field. Assessing risk in each field involves a consistent form of logic but would represent applications of different bodies of knowledge:

- In the **logical** field, a programmer or analyst might review code or a networked system of computers to identify possible avenues of illicit access and develop a software patch or modify the architecture of a system to remedy the weakness. AI tools greatly enhance technical security measures by identifying more online threats earlier, faster, and more accurately.

- In the **social** field, a psychologist or trainer might study the kinds of phishing messages that trick the greatest numbers of recipients into opening or clicking

SECTION 3 CONTINUED

when they should not. To reduce risk, he or she might develop teaching materials to educate users about how to identify the signs of deceptive, malicious digital messages, with careful attention to the greater persuasiveness and deceptiveness that AI tools can bring to them.

- In the **physical** field, an engineer or technician might work to ensure a building or physical structure housing computer assets is secure and able to withstand break-in attempts or other efforts to gain access to sensitive hardware.

In all these cases, cybersecurity professionals are applying similar principles of risk assessment, within their own areas of expertise, to promote a safer environment for online data. A central lesson of *Outsmart Cyberthreats* is the diversity of skill sets and interest areas students can bring to a career in cybersecurity. The job of securing our personal data online involves so many different facets and so many different types of environments that it truly does require a whole-of-society effort.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 26-27

SECTION 3 CONTINUED

WARM-UP QUESTIONS

1. Ask students to assess the "riskiness" of some simple, even silly, scenarios. For example, what carries more risk – sharing a toothbrush or sharing a pencil? Why? What could go wrong?
2. What do students think are the three riskiest things they do in daily life? Why are they risky? Which is the most and which is the least risky?

ACTIVITY

3.3.a: How Likely Is a Cyberattack in Each Circumstance?

In this activity, students apply a basic procedure for conducting a risk assessment. They will try to estimate or quantify the likelihood of an attack occurring as well as the damage an attack might cause. Combining these two variables into an overall assessment of risk is the first part of the exercise. The second part asks students to develop a comprehensive plan to mitigate risk, taking into account protective measures related to the logical, social, and physical fields of cybersecurity described in the text of *Outsmart Cyberthreats* on page 29.

Students will now complete Activity 3.3.a, found on page 48 of their workbook. The activity is replicated with possible answers on the next two pages of this guide.

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.

Possible answers in purple.

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: **2**
   Why? **The likelihood could be low because access to scoreboard controls is limited and the type of activity is unique to this particular environment and set of machines.**

   Damage: **3**
   Why? **The damage would be real to any individual targeted this way, but limited to one person and not necessarily involving more than hurt feelings.**

   Overall risk: **2**
   Why? **The overall risk seems low, given the combination of these two factors.**

3.3.a (CONTINUED)

2. A hacking group is targeting school nurses' offices with a phishing campaign designed to get user ID 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: **5**
   Why? **Because the attack has already occurred in other schools, the likelihood of it happening in this school must be seen as high.**

   Damage: **4**
   Why? **The damage is high, as well, because medical records are sensitive, and the number of people involved could be large.**

   Overall risk: **5**
   Why? **The risk would be high both because of the potential for abuse of sensitive data as well as the ruptures in trust that would ensue within the school community at large.**

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.

Possible answers will vary. Whatever students come up with, follow-up discussion can include students' responses to each other's answers and/or collaborative efforts to improve upon or extend assessments of risk and approaches to mitigation.

SECTION 3 CONTINUED

KEY TERMS

Cyber domain: The interdependent network of connected computers and information technology infrastructure through which people communicate, conduct transactions of varied natures, represent themselves in virtual forms, and engage in ever-multiplying range of interactions of an individual and collective nature.

Logical field: All the programmable and computer-driven devices that connect and comprise an information technology network as well as the programming itself required to make the devices work.

Physical field: The hardware and infrastructure that comprise information technology networks as well as the actual building sites where hardware is located.

Social field: The human factors, both real and virtual, that are manifest in the behaviors and exchanges that people engage in through information technology networks.

EXTENSION

Review page 29 of *Outsmart Cyberthreats* with the students, with careful attention to the three fields of cybersecurity careers: the logical field, the social field, and the physical field. Ask students to react to and expand on the kinds of activities they understand to fit into each of the three fields.

Then lead a discussion about academic experiences that might prepare students for work in each of the three cybersecurity career fields. Upon completion of such an exercise, ask students to rank order these academic experiences according to their own preferences or abilities. This activity can help students imagine what possible pathway into a cybersecurity career might be suitable for them as individuals.

SECTION 3 CONTINUED

RESOURCES

General approach to teaching risk assessment, with some useful resources and graphics to illustrate details and variables and sequences of questions to consider.
https://www.plt.org/activity-resources/focus-on-risk-activity-4-risk-assessment/

Overview of risk assessment terms and methods, especially in relation to classroom environments.
https://www.twinkl.com/teaching-wiki/risk-assessment

Background materials on various layers of the "cyber domain."
https://www.hoover.org/research/cybersecurity-introduction

EXPLORE A FUTURE IN CYBERSECURITY

GOAL

Help students self-assess their own inclinations and abilities related to possible success in the cybersecurity field.

APPROACH

1. Connect cybersecurity job functions to underlying skills and interests that students can identify and practice.
2. Encourage students to identify skills and interests of theirs that could indicate suitability or aptitude for work in cybersecurity.

OVERVIEW

- Students will complete challenges and puzzles, on their own and in teams, as a way to explore possible aptitudes for work in cybersecurity jobs. Reflection on their experiences with these exercises can help them understand how their particular preferences and abilities might point them towards a pathway into the field.
- Students will study the threat environment in which K-12 schools operate and apply this learning to an analysis of their own school district's security profile. This exercise gives them hands-on experience with "real" cybersecurity analysis and operations.

SECTIONS

SECTION 1

Puzzles, Riddles, and Brain Teasers as Pathways Into Cybersecurity

LEARNING OBJECTIVES

- Identify skills and interests related to cybersecurity professionals' job functions.
- Understand possible aptitude for work in cybersecurity field.

BRIEF BACKGROUND DISCUSSION OF ISSUE

The question of skills and interests that indicate a potential for success in cybersecurity matters greatly to people trying to address the large shortfall in candidates ready to enter the field as new workers. One challenge is that jobs in the field require an unusual combination of technical skills and soft skills, such as imaginative problem-solving, abilities to communicate and work in teams, and continuous learning and exploration. But a general consensus exists that while technical skills can be taught, the soft skills are harder to find and develop among candidates for pathways into cybersecurity jobs.

As artificial intelligence utilities become a bigger part of the cybersecurity toolkit, the desirable sets of both technical and soft skills are evolving, as well. In both domains, logic and problem-solving, systems thinking, pattern recognition, and data analysis underlie many professional roles and functions. However, subtle differences in purpose distinguish endeavors in cybersecurity and artificial intelligence. AI systems are designed to learn from data and make predictions; cybersecurity systems protect against and react to specific threats and attacks. Skills associated with using and developing AI can run more towards creativity, experimentation, and a broad grasp of language uses and social behaviors. Cybersecurity focuses more on discipline and protocol, preventing harm, and understanding people's malicious intentions. In combination, though, AI systems complement and extend the capacities of cybersecurity systems to accomplish security goals. Predicting threats, identifying anomalous patterns, learning from attack

SECTION 1 CONTINUED

data — AI delivers a boost to efforts along these and numerous other vital lines of cybersecurity defense strategies.

The exercises in this section should challenge but also entertain students. 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 first activity introduces students to the idea that cybersecurity and AI are related areas of activity, suggesting where they resemble as well as differ from each other. The next three activities are aligned with the "Types of Cyber Jobs" table on page 35 of Outsmart Cyberthreats. As students tackle different kinds of puzzles, they 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 students 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.

SECTION 1 CONTINUED

Help students find their future in cybersecurity

Students can pick from many paths to pursue a cybersecurity career. From certificates to community college and university programs there's a suitable starting point for every student.

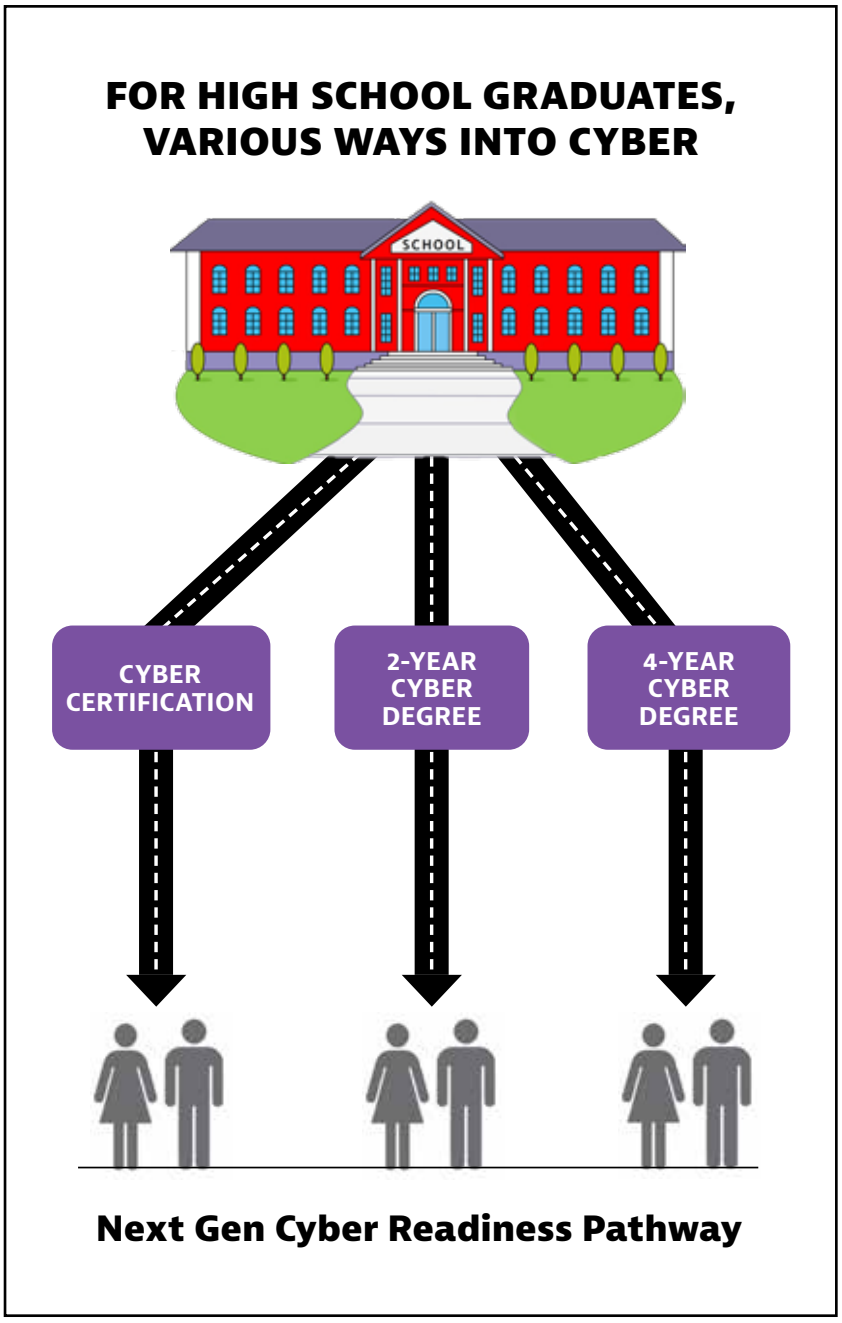
Classroom Tips

1. **"There's more than one way in."** Show how different options can all lead to rewarding cybersecurity careers.

2. **"What's your path?"** Have students pick a route and map out what steps they'd take — making the idea real and personal.

3. **"It takes all kinds to make cybersecurity work."** Emphasize how many different kinds of skills and interests are needed in the field — problem-solving, curiosity, and communication all matter. It's not just for "techies.

4. **"Let's explore real programs near us."** Look up local certificate, community college, or university programs. Make the next step feel real and reachable.



SECTION 1 CONTINUED

ACTIVITY

4.1.a Cyber Defender or AI Creator?

In this short activity, students answer pairs of questions to get a sense of which side of the cybersecurity-AI coin they might lean most comfortably towards.

Students will now complete Activity 4.1.a on page 53 of their workbook. The activity is replicated on the next two pages of this guide.

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.

REFLECTION

Now go back and look at your answers. If you chose more A's, you think like a cybersecurity pro. Solving mysteries, getting to answers, and keeping things

4.1.a (CONTINUED)

safe matter to you. If you chose more B's, you might be more of an AI type. Recognizing patterns, improving systems, and making things 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.

SECTION 1 CONTINUED

ACTIVITIES

4.1.b: Riddles and Puzzles to Tickle Your Brain
4.1.c: Riddles and Puzzles to Tickle Your Brain, as a Group, and
4.1.d: Compete in Teams to Solve Riddles and Puzzles

Activity 4.1.b consists of individual exercises, in which students will step into four of the five Types of Cyber Jobs: Investigator, Analyst, Protector, and Programmer. The Manager job type is handled separately in the Extension.

Activity 4.1.c asks students to work collaboratively, preferably in groups of four, with each group member taking primary responsibility for exercises aligned with the four types of jobs named above.

Activity 4.1.d combines collaboration with competition, pitting teams against one another in races to reach the right answers first.

The exercises in all three Activities are associated with the four types of cyber jobs, to give students a framework for understanding which kind of thought processes they are putting to work in which kinds of exercises. (See table on page 90.) These associations can also serve as the basis for guided reflections and discussions with students about what types of cyber jobs might suit them, if they pursue further studies and activities in the area of cybersecurity.

Students will now complete Activity 4.1.b on page 55 of their workbook. The activity is replicated with answers on the next four pages of this guide.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 32-33

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 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?
   The man was bald, with no hair to get wet in the first place.

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?
   Three. The rest have run away.

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

   RAT

4.1.b 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? **Maria.**

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.
   Neither. The yolk of an egg is yellow

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

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
   Line b: y9358 breaks the pattern

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?

   KKKKKKKKKKKXXXXKKXKKKXXXXXKKKKKX
   XXXXXKKKKXXKXXXXXKXXKKKKKXKXXXXXK
   KKKKKXXXKXKXXXXXYKKKXXXKKKKXXXXK
   XKKXXXKKKXKKKKXXXXXKKKKXXKXXXXX

   Line 3 has a Y right in the middle.

4.1.b (CONTINUED)

Programmer

9. Divide 40 by ½ and add 10. What do you get?
   90. 40 / ½ is the same as 40 x 2, or 80. 80 + 10 = 90

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?
    26 days, since the prior day is one-half of the day that follows.

11. How many times can you subtract 10 from 100?
    One time. After that, you are subtracting 10 from 90, then 80, and so on.

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].

4.1.b (CONTINUED)

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 EXERCISE ON ACTIVITY 4.1.b

This exercise asks students to use the terms and concepts introduced as "associated thought processes" on page 52 of their student workbook (page 90 of this guide) in descriptions of their own approaches to answering, or attempting to answer, the 11 preceding questions in Activity 4.1.b.

Encouraging students to think about their thinking should help them learn to identify inclinations, even strengths, that might serve them well in a cybersecurity career. Even the opposite result – finding little or no inclination towards work in cybersecurity – can still help them develop meta-cognitive self-awareness, better and fuller understanding of how they think and feel.

NOTE: Before asking students to complete the reflection, it will be useful to provide answers to the 11 questions in 4.1.b and, if possible, lead a group discussion of how students succeeded or struggled in finding answers.

Students will now complete Reflection on Activity 4.1.b, found on page 60 of their workbook. The activity is replicated on the next page of this guide.

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?

ACTIVITY

4.1.c: Riddles and Puzzles to Tickle Your Brain, as a Group

These exercises give students a chance to work together on challenges. Collaborating with people who bring different perspectives can help teach active listening and patience as well as open up a student's mind to new ways of seeing things. For this reason, diversity on a team is valuable; the solutions originating with a team of people coming from different perspectives and experiences are almost always better than the solutions from a team of people who all think alike.

Students will now complete Activity 4.1.c, found on page 61 of their workbook. The activity is replicated with answers on the next three pages of this guide.

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?
   Turn on switch 1 and leave it on. Turn on switch 2, keep it on for a few minutes. Then turn it off. Leave switch 3 off. Then go into the room. The lit bulb connects to switch 1. Check to see which of the other two bulbs is hot and which is cold. The hot bulb connects to switch 2, the cold one to switch 3.

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?
   Four. You break, cook, and eat the same two eggs. You could also end up with two eggs, if breaking, cooking, and eating involved two sets of two eggs.

4.1.c (CONTINUED)

Analyst

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

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!

   This paragraph has no instances of the letter "e" in it, even though it is the most commonly used letter in English.

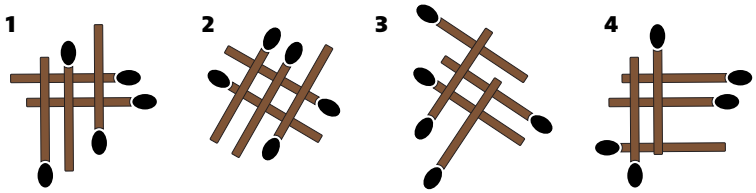
Protector

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

The word "the" is repeated.

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



All the criss-crossing matchsticks result in two finished rectangles inside the pattern, EXCEPT for number 3.

4.1.c (CONTINUED)

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? **Three times. If you pull out a white sock and a black sock the first two times, you will pull out one or the other on the third try and be guaranteed of having a matched 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 = ??

3612. The "answers" show first the product of the two numbers, then the sum of them. 6 x 6 = 36; 6 + 6 = 12.

ACTIVITY

4.1.d: Compete in Teams to Solve Riddles and Puzzles

Working under pressure in collaboration is often part of a cybersecurity professional's job description. These exercises ask students to work together in teams in competition with other teams to get to the right answers first. Divide students into small teams and pit them against each other, either one on one or every team on its own against everyone else. Or time how long it takes teams to come up with their answers, and then compare the results they all come up with. It can be helpful to give teams a few moments to talk about plans or approaches to problem-solving before kicking off the competitions.

Students will now complete Activity 4.1.d, found on page at 64 of their workbook. The activity is replicated with answers on the next three pages of this guide.

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.c, 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?

   Trip 1: Take the goose across the river; return with nothing.
   Trip 2: Take the beans across the river; return with the goose.
   Trip 3: Take the fox across the river, leaving the goose; return with nothing.
   Trip 4: Take the goose across the river (again!).

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.

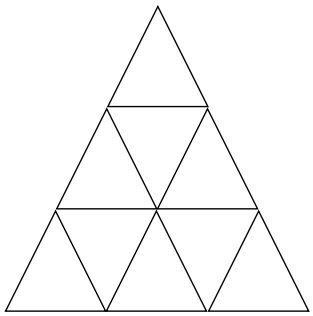
   Number 4 is true. The easiest way to answer this question is to restate each line as a true statement, rather than a false statement. Consider number 1: if it's true that one statement is false, that means that four are true. Likewise, if two are false, then three are true, and so on. So now it should become clear that only one statement can be true, since if more than one were true, the statements would contradict each other. Number 4 is the only statement that "truly" answer the question, since it is correct to say that the other four statements are false, except for Number 4, are all false.

4.1.d (CONTINUED)

Analyst

3. Unscramble the letters below to come up with pairs of words that rhyme:
   a. irfa/rwae **fair / wear**
   b. ertgrae/hterfrgei **greater / freighter**
   c. ugohtth/hatugc **thought / caught**
   d. meyhr/blcmi **rhyme / climb**

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



13; 9 simple triangles, 3 overlapping triangles made up of 4 simple triangles each, and the 1 large triangle containing every other triangle.

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

Block 2 – 200.1.3.1.1 is the invalid IP address.

4.1.d (CONTINUED)

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

   1. Line 1 – the word "are" is repeated.
   2. Lines 2-3 – the word "to" is repeated.
   3. Line 4 – "mitstakes" should be "mistakes".
   4. Line 4 – the period is missing.
   5. There are actually only 4 "wrongs" in the sentence. Once you figure this out, you have identified a 5th wrong. BUT, finding a 5th wrong with this sentence makes it a true sentence, so "wrong #5" is not really a wrong. There are in fact only 4 "wrongs." This puzzle has no final answer; that's what's "wrong" with it!

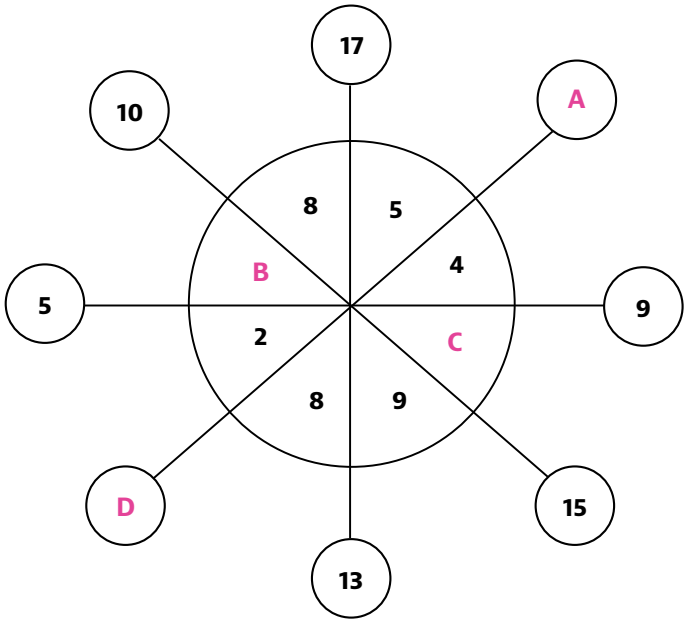
Programmer

7. Ramona is 12, and her father is 38. When Ramona is half her father's age, how old will he be? **52; the difference between their two ages is 38 – 12, or 26. So when she is 26, he will be 26 x 2, or 52.**

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

   The numbers in the "pie pieces" opposite each circle add up to the numbers in the circles.

   A = 10 (8 + 2)
   B = 7 (9 – 2); (15 – 8)
   C = 1 (10 – 1); (5 – 4)
   D = 9 (5 + 4)



SECTION 1 CONTINUED

EXTENSION

Review "Reflection on Activity 4.1.b" with the class as a whole. Start with a discussion of the "associated thought processes" shown in the table on page 90 and what students understand them to mean. Then take a poll among students of which types of cyber jobs felt most comfortable and uncomfortable to them. Follow-up discussions can draw on students' responses to the reflection exercise, laying out and expanding upon what they understand the "thought processes" to mean and their experiences putting them to use in the exercises.

Which exercises were easier or harder for them? Did they find any particularly fun or comfortable? Or the opposite? How would students expand upon or modify the descriptions of the associated thought processes required for each type of job, based on their experiences?

Next, ask students to reflect on how they organized themselves in Activities 4.1.c and 4.1.d. Who in the group seemed comfortable leading these efforts? How did it feel to be responsible for their own group construction? If they were asked to put themselves together as a team of cybersecurity professionals filing all five of the job types, who in the group would fill each of the jobs? As a result of this exercise, students should have some understanding of not only their own aptitudes for cybersecurity work but also a general sense of which kinds of job functions might suit them best.

SECTION 1 CONTINUED

RESOURCES

General discussion of the cybersecurity workforce gap with recommendations about how to attract new people to the field and develop the human capital needed to address global cybersecurity workforce needs.

https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

List of top cybersecurity skills in high demand, from Champlain College, one of the leading cybersecurity education programs among four-year colleges.

https://online.champlain.edu/blog/top-cybersecurity-skills-in-high-demand

Soft skills useful for cybersecurity professionals, from the Infosec Institute, a leading provider of continuing professional education in the field.

https://www.infosecinstitute.com/resources/professional-development/security-pro-5-soft-skills/

Academic article highlighting the importance of resilience, agility, and analytical thinking as workplace skills people can use to complement and extend the capabilities of AI systems.

Makela, Elina, et al. (February 26, 2025). "Complement or substitute? How AI increased demand for human skills." arXiv; *https://arxiv.org/abs/2412.19754v3*

SECTION 2

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

LEARNING OBJECTIVES

- Understand the cyber threat environment in which K-12 schools operate.
- Experience with applying risk analysis and threat mitigation to real-world, familiar environment.

BRIEF BACKGROUND DISCUSSION OF ISSUE

K-12 school districts operate in an ever-more threatening cyber attack environment. Data breaches, online class invasions, ransomware attacks, and phishing campaigns are growing more common and more damaging every year. Even as officially reported incidents significantly understate the true scope of the problem, the frequency of known attacks has increased by a factor of more than 10 in the last five years. In reality, the problem is almost certainly worse.

School districts present an inviting target for cyber attacks for various reasons:

- In many cases, the IT infrastructure is out-of-date, with both hardware and software lacking protections that newer, state-of-the-art technologies can provide.
- Personnel and procedures can also be behind the times in relation to evolving threats, new kinds of attacks, and best practices in online security protocols.
- The extensive reliance on third-party vendors for testing, curriculum materials, business services, and other digital supports exposes school districts to external weaknesses in systems they do not control or even know to be operating.
- Increasing levels of online and technology-assisted learning, accelerated by Covid, expand the number and type of "attack surfaces" that make schools vulnerable to cyber attack.

For all these reasons, school districts are facing a range of rapidly changing, increasingly dangerous online threats, all the while operating under the same challenging circumstances as always, with money, time, and people all under stress.

Asking students to investigate and possibly get involved with a school's actual cybersecurity policies and procedures might present problems with access and involvement in topics beyond what is appropriate for students. Each individual school will have different constraints along these lines. The benefit, though, of putting students to work analyzing and even improving a school's security posture could be notable. As avid, active explorers of online environments, they bring unique experiences and knowledge. And any contributions they do end up making to their home school's online security systems could boost their interest and confidence in pursuing future work in the cybersecurity field.

TEXT LOCATION IN *OUTSMART CYBERTHREATS*: Pages 34-37

WARM-UP QUESTIONS:

1. How would students assess the level of online risk and threat faced by K-12 schools?
2. Have students heard of any cyberattacks carried out against K-12 schools? If so, what are they? If not, what kinds of attacks can they imagine?
3. What kinds of direct experiences have students had with digital learning activities? Which of these activities seem to pose more or less risks to potentially sensitive individual data?

ACTIVITY

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

This activity is based on data and reporting about cybersecurity incidents among K-12 school districts. The source documentation for the activity is found in "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report," published by the K-12 Security Information Exchange. The report itself – 20 pages of reading plus additional pages of end matter – is available at the following webpage: *https://www.k12six.org/the-report*

In the activity, students will first answer questions based on the report and then use the information to analyze cybersecurity issues related to their own school. These questions address the general nature of cybersecurity threats faced by school districts, requiring students to read the main body of the report. And they prompt students to reflect on and then gather information about circumstances peculiar to their own environment. This second part of the activity is presented as an "extension" because it might lead students into topics or information beyond what school leaders see as appropriate for them to investigate.

Students will now complete Activity 4.2.a, found on page 67 of their workbook. The activity is replicated with answers on the next two pages of this guide.

4.2.a

K-12 Schools Under Threat of Cyberattack

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 cyberattacks 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: Year in Review — 2022 Annual Report." The main part of the report is 20 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. If allowed and appropriate, your teacher will ask you then to apply lessons from the reading to the online computer environment in your own school.

The report can be found online at the bottom of this webpage:
https://www.k12six.org/the-report

Answers in purple.

1. The report states on page 4 that the number of publicly disclosed cybersecurity incidents in 2021 totaled 166, a decrease from the 408 incidents reported in 2020. Does this decrease suggest progress in K-12 cybersecurity operations? Or something else? Explain the reasons for your answer. Review pages 4-6 to find information related to this question.
   Hard to tell, but maybe not a clear sign of progress. With the widespread return to in-school learning after Covid, students and teachers spent more time in-person at school and less time online, thus reducing opportunities for cyberattacks. It is plausible that schools have improved their cybersecurity posture as a result of lessons learned during

4.2.a (CONTINUED)

Covid, as well. However, requirements for public disclosure of K-12 incidents are weak and widely flouted, in addition to the general tendency of organizations not to report data breaches and other cybersecurity incidents.

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?
   The report identifies large school districts in densely populated areas, especially in the suburbs, as the kind at greatest risk of suffering a cyberattack. This tendency could be the result of incidents in such school districts being more likely to get reported publicly and/or such school districts using more technologies and involving more people in online activities, thus increasing the volume and type of "attack surfaces."

3. What are the three most common types of cyberattack launched against K-12 school districts in 2021? See page 7 and thereafter to find related information.
   1. Ransomware
   2. Student data breach
   3. Class invasion

4. What group is responsible for the greatest number of data breaches at K-12 schools? Review pages 10 and thereafter for related information.
   K-12 vendors are responsible for the greatest number of data breaches, with 55 percent of all incidents attributed to them.

5. 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. **Answers will vary, depending on location.**

EXTENSIONS

1. How does your school district compare to the types of school districts described in the report, as described on pages 14-16? Based on this analysis, how would you assess the risk of your school district suffering a cyberattack?

2. Review the "K12 Six Essential Cybersecurity Protections" table on page 18. Pick out one of the four items on this list and investigate if and how your school works to fulfill the "recommended protective measure." You might start with researching online to find some examples of actions organizations can take to fulfill the goals. Then ask your teacher for help with finding people with responsibility for or knowledge of cybersecurity protections at your school. Compare what you learn about what is happening at your school with anything you have understood other schools or organizations do.

KEY TERM

Attack surface: The set of all possible points of entry into an online data system through which an unauthorized user can access the system and take possession of data.

RESOURCES

Website of an organization dedicated to tracking and sharing information about cyber attacks against K-12 school districts.
K-12 Cybersecurity Resource Center; *https://k12cybersecure.com/*

Network of K-12 information technology security officials and experts sharing best practices and information about keeping K-12 school districts safe from cyber threats. **K-12 Security Information Exchange;** *https://www.k12six.org/*

Federal government workforce framework for cybersecurity functions.
https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

Cyber Seek, an interactive map showing large volumes of data about s upply and demand in the cybersecurity job market.
https://www.cyberseek.org/

OUTSMART CYBERTHREATS APPENDIX A

PRE-ASSESSMENT TOOL

Before you read *Outsmart Cyberthreats*, answer the questions below to measure your opinions and understanding about online safety and cybersecurity.

AGREE OR DISAGREE

Pick a number from 1 to 4 to say if you agree or disagree with the statements below.

1. It's hard for other people to find personal information about me on the internet.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

2. On my own, there isn't much I can do to protect my personal information when I go online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

3. It's important to be careful with creating and using passwords for online accounts.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

4. As a student, my personal information is not of much value to cyber criminals.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

5. I understand how artificial intelligence makes my personal data online more vulnerable to theft and misuse.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

6. It's easy to figure out what you can trust and what you can't trust online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

7. I understand how to tell the difference between a real and a scam email.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

PRE-ASSESSMENT TOOL (CONTINUED)

8. I often think about the risk of bad things happening when I go online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

9. I understand something about the different kinds of jobs people do in cybersecurity.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

10. I could imagine myself having a career in cybersecurity.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

11. I could explain how to stay safer online to my parents.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

TRUE OR FALSE

Answer the questions below with a T for True or F for False.

1. The data that companies gather about us mostly involves just things we buy or links we click on.
2. Artificial intelligence tools help keep us safer online.
3. Since most kids don't have credit cards or bank accounts, their personal data isn't worth much to cyber criminals.
4. As long as you keep it secret, it's fine to use the same password for different online accounts.
5. As long as an email includes personal information about me, it's safe.
6. Most data breaches result from failures in machine security.
7. Risk is part of everything we do online.
8. You can't have a career in cybersecurity without advanced knowledge of computers and math.

PRE-ASSESSMENT TOOL (CONTINUED)

MULTIPLE CHOICE

All the questions below have one or more correct answers. Choose all the answers that you think might be right for each question.

1. How do companies gather information about us online?

a. Tracking what we do on their websites
b. Looking at our social media accounts
c. Using AI tools to search for us online
d. Looking at information in people's Contacts files
e. Analyzing words we use to search for things online

2. Which of these features of an email might indicate a phishing attempt?

a. Attachments you didn't expect
b. An unknown or strangely constructed return email address
c. Appeals to emotion or urgency
d. The promise of something for nothing, or for surprisingly little
e. An email that starts with Re: or Fwd:

3. Pick out the careers below that could be related to cybersecurity.

a. Computer programmer
b. Teacher
c. Building engineer
d. Mayor
e. FBI agent

4. What skills do you think are important to have in a cybersecurity career?

a. Imagination
b. Computers
c. Teamwork
d. Logic
e. Solving puzzles

OUTSMART CYBERTHREATS APPENDIX A

PRE-ASSESSMENT TOOL ANSWERS

TRUE OR FALSE

1. The data that companies gather about us mostly involves just things we buy or links we click on. **F**
2. Artificial intelligence tools help keep us safer online. **T**
3. Since most kids don't have credit cards or bank accounts, their personal data isn't worth much to cyber criminals. **F**
4. As long as you keep it secret, it's fine to use the same password for different online accounts. **F**
5. As long as an email includes personal information about me, it's safe. **F**
6. Most data breaches result from failures in machine security. **F**
7. Risk is part of everything we do online. **T**
8. You can't have a career in cybersecurity without advanced knowledge of computers and math. **F**

MULTIPLE CHOICE

1. How do companies gather information about us online?

   a. Tracking what we do on their websites
   b. Looking at our social media accounts
   c. Using AI tools to search for us online
   d. Looking at information in people's Contacts files
   e. Analyzing words we use to search for things online

2. Which of these features of an email might indicate a phishing attempt?

   a. Attachments you didn't expect
   b. An unknown or strangely constructed return email address
   c. Appeals to emotion or urgency
   d. The promise of something for nothing, or for surprisingly little
   e. An email that starts with Re: or Fwd:

3. Pick out the careers below that could be related to cybersecurity.

   a. Computer programmer
   b. Teacher
   c. Building engineer
   d. Mayor
   e. FBI agent

4. What skills do you think are important to have in a cybersecurity career?

   a. Imagination
   b. Computers
   c. Teamwork
   d. Logic
   e. Solving puzzles

OUTSMART CYBERTHREATS APPENDIX A

POST-ASSESSMENT TOOL

Now that you have read *Outsmart Cyberthreats* and learned more about online safety and cybersecurity careers, answer the questions below. Some of these questions are repeated from the pre-assessment exercise, and your answers are meant to show if and how the book has changed your understanding or opinions about cybersecurity.

AGREE OR DISAGREE

Pick a number from 1 to 4 to say if you agree or disagree with the statements below.

1. It's hard for other people to find personal information about me on the internet.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

2. On my own, there isn't much I can do to protect my personal information when I go online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

3. It's important to be careful with creating and using passwords for online accounts.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

4. As a student, my personal information is not of much value to cyber criminals.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

5. I understand how artificial intelligence makes my personal data online more vulnerable to theft and misuse.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

6. It's easy to figure out what you can trust and what you can't trust online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

POST-ASSESSMENT TOOL (CONTINUED)

7. I understand how to tell the difference between a real and a scam email.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

8. I often think about the risk of bad things happening when I go online.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

9. I understand something about the different kinds of jobs people do in cybersecurity.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

10. I could imagine myself having a career in cybersecurity.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

11. I could explain how to stay safer online to my parents.

___1 Strongly Agree ___2 Agree ___3 Disagree ___4 Strongly Disagree

TRUE OR FALSE

Answer the questions below with a T for True or F for False.

1. Companies gather, buy, and/or sell data about their customers all the time.
2. Artificial intelligence tools make it easier for cyber criminals to do bad things online.
3. Cyber criminals don't care about K-12 schools because their data isn't that valuable.
4. The longer the password, the better.
5. It's always safe to click on a link in a text or message from someone I know.
6. Keeping a vigilant "security mindset" can help you identify possible online threats, even when everything seems safe.
7. You can set up devices, browsers, and online accounts to share different amounts of personal information.
8. Cyberattacks can only do damage to people in their online lives.

POST-ASSESSMENT TOOL (CONTINUED)

MULTIPLE CHOICE

All the questions below have one or more correct answers. Choose all the answers that you think might be right for each question.

1. Which of the following elements would help you make a strong password?

    a. Lower- and upper-case letters
    b. Your birthdate, home address, or other easy-to-remember numbers in your life
    c. Lyrics from a favorite song
    d. Name of a pet or favorite sports team
    e. Special characters like $, %, or #

2. How do companies gather information about us online?

    a. Tracking what we do on their websites
    b. Looking at our social media accounts
    c. Using AI tools to search for us online
    d. Looking at information in people's Contacts files
    e. Analyzing words we use to search for things online

3. Which of these features of an email might indicate a phishing attempt?

    a. Attachments you didn't expect
    b. An unknown or strangely constructed return email address.
    c. Appeals to emotion or urgency
    d. The promise of something for nothing, or for surprisingly little
    e. An email that starts with Re: or Fwd:

4. Which of the following are parts of a trustworthy online data system?

    a. Timeliness
    b. Availability
    c. Confidentiality
    d. Reliability
    e. Integrity

POST-ASSESSMENT TOOL (CONTINUED)

5. How does AI make it harder to know what to trust online?

a. Chatbot agents sound just like real people
b. AI tools can make up personal data that seems real
c. Phishing campaigns made by AI don't have obvious mistakes in them
d. AI can make fake audio and video files that sound completely real
e. It makes computers run faster when you go online

6. Pick out the careers below that could be related to cybersecurity.

a. Computer programmer
b. Teacher
c. Building engineer
d. Mayor
e. FBI agent

7. Which of the following are categories of risk involved in online activities?

a. Damage
b. Threat
c. Opportunity
d. Vulnerability
e. Attack

9. What skills do you think are important to have in a cybersecurity career?

a. Imagination
b. Computers
c. Teamwork
d. Logic
e. Solving puzzles

10. Pick out the types of technical cyber jobs from the list below.

a. Analysts
b. Creators
c. Managers
d. Investigators
e. Counselors

OUTSMART CYBERTHREATS APPENDIX A

POST-ASSESSMENT TOOL ANSWERS

TRUE OR FALSE

1. Companies gather, buy, and/or sell data about their customers all the time. **T**
2. Artificial intelligence tools make it easier for cyber criminals to do bad things online. **T**
3. Cyber criminals don't care about K-12 schools because their data isn't that valuable. **F**
4. The longer the password, the better. **F**
5. It's always safe to click on a link in a text or message from someone I know. **F**
6. Keeping a vigilant "security mindset" can help you identify possible online threats, even when everything seems safe. **T**
7. You can set up devices, browsers, and online accounts to share different amounts of personal information. **T**
8. Cyberattacks can only do damage to people in their online lives. **F**

MULTIPLE CHOICE

1. Which of the following elements would help you make a strong password?

a. Lower- and upper-case letters
b. Your birthdate, home address, or other easy-to-remember numbers in your life
c. Lyrics from a favorite song
d. Name of a pet or favorite sports team
e. Special characters like $, %, or #

2. How do companies gather information about us online?

a. Tracking what we do on their websites
b. Looking at our social media accounts
c. Using AI tools to search for us online
d. Looking at information in people's Contacts files
e. Analyzing words we use to search for things online

3. Which of these features of an email might indicate a phishing attempt?

a. Attachments you didn't expect
b. An unknown or strangely constructed return email address
c. Appeals to emotion or urgency
d. The promise of something for nothing, or for surprisingly little
e. An email that starts with Re: or Fwd:

POST-ASSESSMENT TOOL ANSWERS

4. Which of the following are parts of a trustworthy online data system?

a. Timeliness
b. Availability
c. Confidentiality
d. Reliability
e. Integrity

5. How does AI make it harder to know what to trust online?

a. Chatbot agents sound just like real people
b. AI tools can make up personal data that seems real
c. Phishing campaigns made by AI don't have obvious mistakes in them
d. AI can make fake audio and video files that sound completely real
e. It makes computers run faster when you go online

6. Pick out the careers below that could be related to cybersecurity.

a. Computer programmer
b. Teacher
c. Building engineer
d. Mayor
e. FBI agent

7. Which of the following are categories of risk involved in online activities?

a. Damage
b. Threat
c. Opportunity
d. Vulnerability
e. Attack

9. What skills do you think are important to have in a cybersecurity career?

a. Imagination
b. Computers
c. Teamwork
d. Logic
e. Solving puzzles

10. Pick out the types of technical cyber jobs from the list below.

a. Analysts
b. Creators
c. Managers
d. Investigators
e. Counselors

NATIONAL CRYPTOLOGIC FOUNDATION
CYBER CENTER FOR EDUCATION & INNOVATION

THE NATIONAL CRYPTOLOGIC FOUNDATION

The National Cryptologic Foundation (NCF) was established in 1996 to support activities, displays, and artifact acquisition for the National Cryptologic Museum (NCM). Its mission has broadened to include a robust cyber education program and to deliver an innovation approach to solving cybersecurity challenges. Our support of the NCM remains a vital part of our mission, especially with our partnership with NSA.

National Cryptologic Foundation
808 Landmark Drive, Suite 223, Glen Burnie, MD 21601
Phone (443) 795-4498
booklet@cryptologicfoundation.org; CFC #31493

OUR CORE VALUES

Educate the public and inspire students to explore cryptology, STEM and cyber-related fields of study.

Stimulate and innovate by serving as a platform to bring big ideas to the table that support, educate and communicate with the public on the next generation of the cyber ecosystem.

Commemorate all "those who serve in silence" in the cryptologic mission with courage and distinction and whose contributions help enhance and preserve our way of life.