YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.

Teacher's Guide to

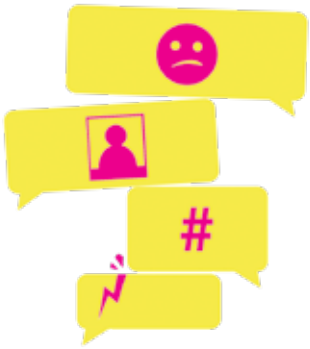
OUTSMART CYBERTHREATS

Learn how to take good care of your data.
BONUS: Discover a cool new career in cybersecurity!

WHAT'S INSIDE

WHAT'S INSIDE CONTINUED

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 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. This kind of data can also be bought and sold and then aggregated into extremely detailed, valuable individual profiles associated with our real-world identities.

For example, Microsoft bought LinkedIn and its 400 million users for just over $26 billion. That price suggests a value of about $65 for each individual user of the platform. For Google, an individual user is worth about $180, for Facebook almost $160. These kinds of values can vary across different kinds of internet services, but the takeaway 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 Twitter?
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. 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.

SECTION 1 CONTINUED

KEY TERM

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

Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. (See next page for further source information.)

EXTENSIONS

Introduce students to the website, *www.spokeo.com*. Suggest that they search the names of their parents 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.

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.

SECTIONS

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.

   Answers could include: misspellings, grammatical errors, sense of urgency, and the fact that the email was sent from a gmail account.

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

   _____

   _____

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

   _____

   _____

2.2.b

You and Your Data Shadow

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

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

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
10. immunization records, medical records, etc

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

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 or other authorities taking away phone for misuse

EXPLORE A FUTURE IN CYBERSECURITY

GOAL

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

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 CONTINUED

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.

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

ACTIVITY

4.1.a: Riddles and Puzzles to Tickle Your Brain

Students try to solve riddles and puzzles that expose them to the different ways of thinking and reasoning that cybersecurity professionals must apply in their cybersecurity work. At the end of the activity, students should reflect on their experience with each type of exercise. Which ones were easier or harder, more fun or not so much? In all cases, seeing a problem from a perspective other than the obvious angle that first presents itself will be required. This ability is widely valued in the cybersecurity field.

Students will now complete Activity 4.1.a on page 43 of their workbook. The activity is replicated with answers on the next four pages of this guide.