YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.

Student Workbook

OUTSMART CYBERTHREATS

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

TABLE OF CONTENTS

PART 1

A DAY IN THE LIFE OF YOUR PHONE

WHAT YOU'LL LEARN

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

WHAT YOU'LL DO

Section 1: Companies Do Love to Gather Data

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

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

1.2.a: The Cost of Cybercrime, p 9

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

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

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

1.2.a

The Cost of Cyber Crime

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

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

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

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

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

Cyber crime incidents

1. _____

_____

2. _____

_____

3. _____

_____

PART 2

HOW THINGS GO WRONG ONLINE AND WHAT TO DO ABOUT IT

WHAT YOU'LL LEARN

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

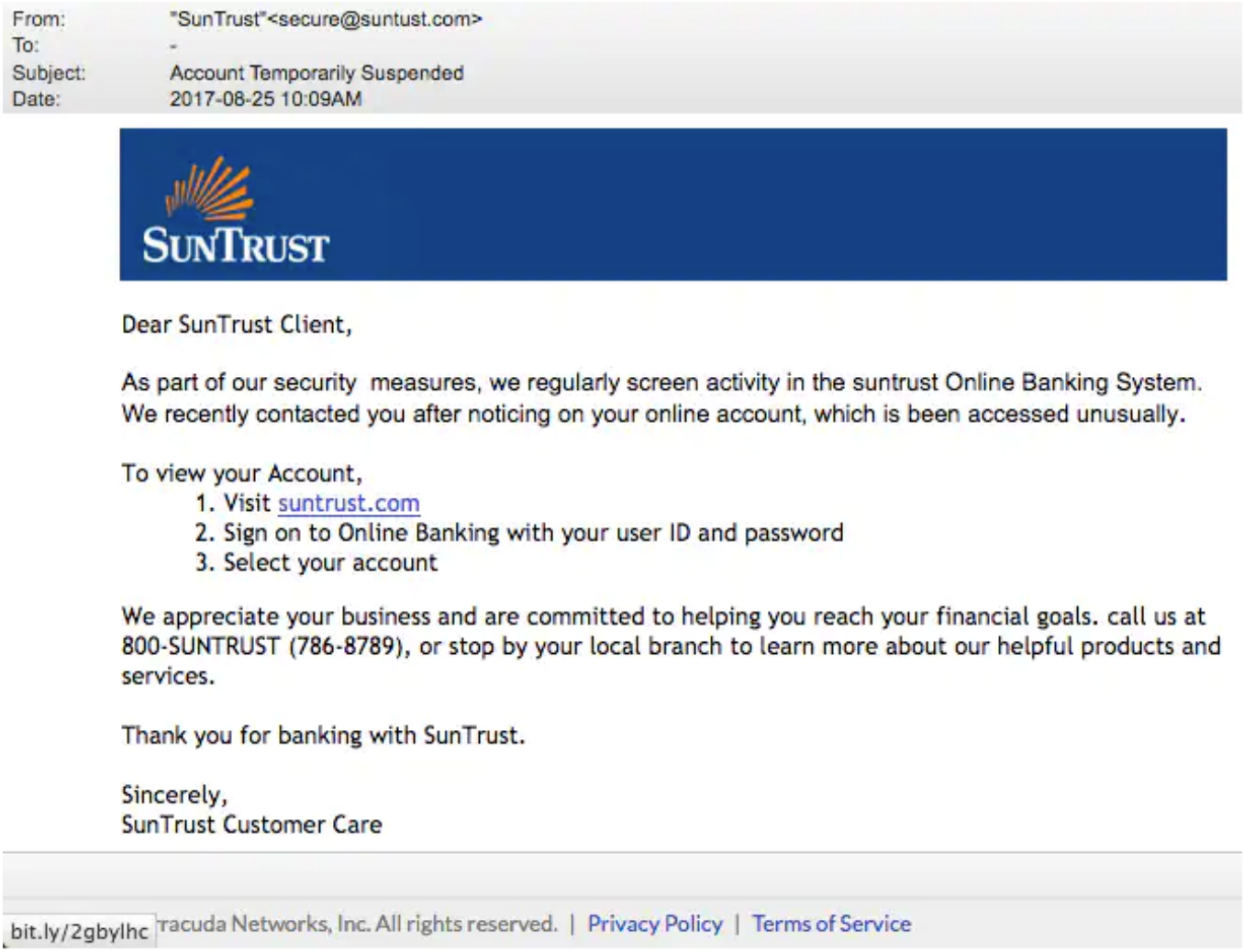
WHAT YOU'LL DO

2.1.a

What Are the Signs of a Bogus Email?

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

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



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

SUNTRUST

Dear SunTrust Client,

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

To view your Account,

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

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

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

2.1.b

How Good Are You at Spotting Phishing?

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

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

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

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

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

2.3.a

Make an Impossible-to-Crack Password

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

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

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

1. _____ _____ _____ _____ _____ _____

2. _____ _____ _____ _____ _____ _____ _____ _____ _____

3. _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

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

PASSWORDS	CRACKING TIME
1.	
2.	
3.	

PART 3

CONTROL YOUR RISK ONLINE

WHAT YOU'LL LEARN

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

WHAT YOU'LL DO

PART 4

EXPLORE A FUTURE IN CYBERSECURITY

WHAT YOU'LL LEARN

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

WHAT YOU'LL DO

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

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

Reflection on 4.1.a, p 48

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

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

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

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

4.1.a

Riddles and Puzzles to Tickle Your Brain

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

Investigator

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

---

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

---

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

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