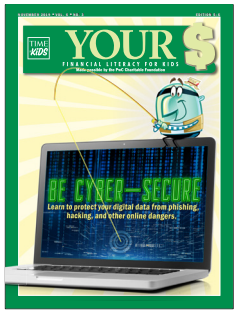
TIME for KIDS YOUR $ FINANCIAL LITERACY FOR KIDS
EDITION 5–6 TEACHER'S GUIDE
VOL. 6, NO. 3 NOVEMBER 2019



TEACHING THE COVER STORY

10 WAYS TO STAY SAFE ONLINE

Learn how to stay safe online from threats such as phishing and identity theft.

FINANCIAL-LITERACY STANDARDS
IV. Protecting and Insuring

COMMON CORE STANDARDS
RI.1, RI.3, RI.5, SL.1

From the Editor: Thanks to the PwC Charitable Foundation, *TIME for Kids* is pleased to offer teachers, students, and their families a monthly financial-literacy magazine.
***—Andrea Delbanco, Editor in Chief,* TIME for Kids**

FINANCIAL-LITERACY ESSENTIAL QUESTIONS FOR STANDARD I
Benchmark 1: What risks do you face online?
Benchmark 6: How can you protect yourself and your identity online?

READING FOR DETAIL

Engage the Reader

- Begin the lesson by asking students to define the word *theft*. Ask them to name some things that a person might want to steal. Then have partners talk about the effects that theft might have on a person.
- Read the title and intro text of this month's article, "10 Ways to Stay Safe Online," aloud. Present the idea of *identity theft*. Ask: Why would someone want to steal another another person's identity? How is this different from stealing an item? How does it affect the person whose identity was stolen?

Read the Text

- Provide students with an annotation guide to use while they read the rest of the text. Choose one color to identify online risks, another color to identify tips for avoiding these risks, and a symbol to identify tips that are new to students. Post this guide on the board, and then have students read the story independently.
- Bring the class back together and ask students to share which tips they feel they need to put into practice. Have them choose one of these tips as a goal.
- Draw students' attention to the structure of the text. The sentences in green should all have been highlighted as ways to avoid risks. The paragraph below each of these contains more tips and explains some of the risks involved. Ask students why they think the writer chose to organize the information in this way.
- Then point out that some tips don't clearly explain the risks involved with a behavior, such as the tip about creating a strong password. Have groups add an explanation to these tips.

Respond to the Text

- Ask each set of partners to think about why it's important to know about online safety. Have them consider whose responsibility it should be to teach online safety. Should it be taught by schools? Should it be taught by parents? Should online users be responsible for keeping themselves informed? Ask students to explain their feelings.
- Technology and the apps that students use are constantly changing. Ask each set of partners to work together to create a tip that does not appear in the article. This can be specific to an app or a popular website.

Extend Learning

- Have students complete the resource "Problematic Posts," on page 3 of this guide, to practice identifying risky online behavior. If time permits, have students create their own sample post and, with a partner, identify what is risky about it.

WITHIN THIS GUIDE

A NOTE FROM JEAN

Dear Teachers,

According to Common Sense Media, students age 8 to 12 spend an average of six hours a day online. Six hours. Perhaps in another issue we'll take up the topic of whether (and how) we should bring those numbers down. For now, we're focused on habits and practices that can keep kids and their personal data safe. Identity theft is a huge problem in this country, with about 15 million cases each year reported to the authorities, a million of them involving kids. No, we don't want to scare children, but it's important for them to understand that their personal information isn't valuable only to them and that it's up to them to protect it. While you're passing this information on to your students, you may want to put some of the tips into practice in your own life as well.

Have a great month!

Jean

ADDITIONAL RESOURCES

councilforeconed.org/standards

Visit for free teaching resources and to download the K–12 national standards for financial literacy.

ftc.gov/youarehere

Visit this website of the Federal Trade Commission for teaching resources on identity theft. Games featured on the site teach students how to and why they should protect their identity and how to spot scams.

ANSWER KEY FOR WORKSHEET

"Problematic Posts," p. 3:
1. John posted his location. 2. Kayla's password is her last name and a simple number sequence. 3. Jennifer provides her high school and date of birth.

PERSUASIVE WRITING

ARTICLE: "10 WAYS TO STAY SAFE ONLINE," PP. 2–4

Post the term *digital footprint* on the board. Ask students to raise a hand if they've heard this term. If only a few students have heard it, open a group discussion about the meaning of this term. Explain that a person's digital footprint is what represents that person online, and includes photos, likes and comments, and the sites he or she has visited.

Divide the classroom into two sections: "strongly agree" and "strongly disagree." Then read the following statements aloud so students can weigh in on them. 1) It is dangerous to make your account profile public. 2) It's okay to share the login credentials to your bank account with your best friend. 3) A strong password includes a combination of letters, numbers, and special characters. 4) To keep track of passwords, you should make them all the same. 5) When you delete a post that you've made online, it is gone forever.

After engaging in the activity, have students write a persuasive paragraph about one of the five statements. They should write to educate other kids on the topic.

PAIRED TEXT

DISCUSS A SIMILAR TOPIC WITH *TFK*

- Once students have read "10 Ways to Stay Safe Online," have them go to *timeforkids.com* to read "What's the Password?" (11/1/19). This story goes into detail about how passwords protect our online information.
- Engage the class in a discussion about online practices. Ask: What did we learn about password protection from this article? Do your account passwords make the cut?

Name _____ Date _____

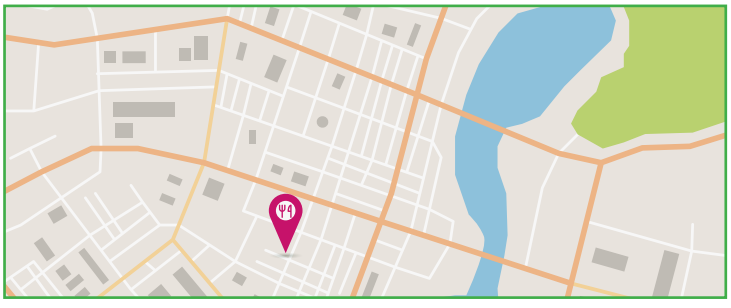
TIME for KIDS YOUR $ FINANCIAL LITERACY FOR KIDS

PROBLEMATIC POSTS

Read "10 Ways to Stay Safe Online" (November 2019). Then use the tips you've read about to explain the risks in each example below.

John Michael checked in to Pizza Place.
November 16 at 6:03pm · Jacksonville

Getting some dinner with friends before a 7:30 movie!



What is risky about this post? Explain.

LOG IN

kaylabrown@tfk.com

brown1234

Log In ☑ Remember me

What is risky about this? Explain.

jenmatthewsx0

Jennifer Matthews

Westfield High School '23
Born 04/15/05
Add me @jenmatx0

Follow

This account is private.
Follow this account to see their photos and videos.

What is risky about this post? Explain.

Common Core State Standards: RI.5.3, RI.6.3

Made possible by the pwc Charitable Foundation

TIME for KIDS

YOUR $

FINANCIAL LITERACY FOR KIDS
NOVEMBER 2019

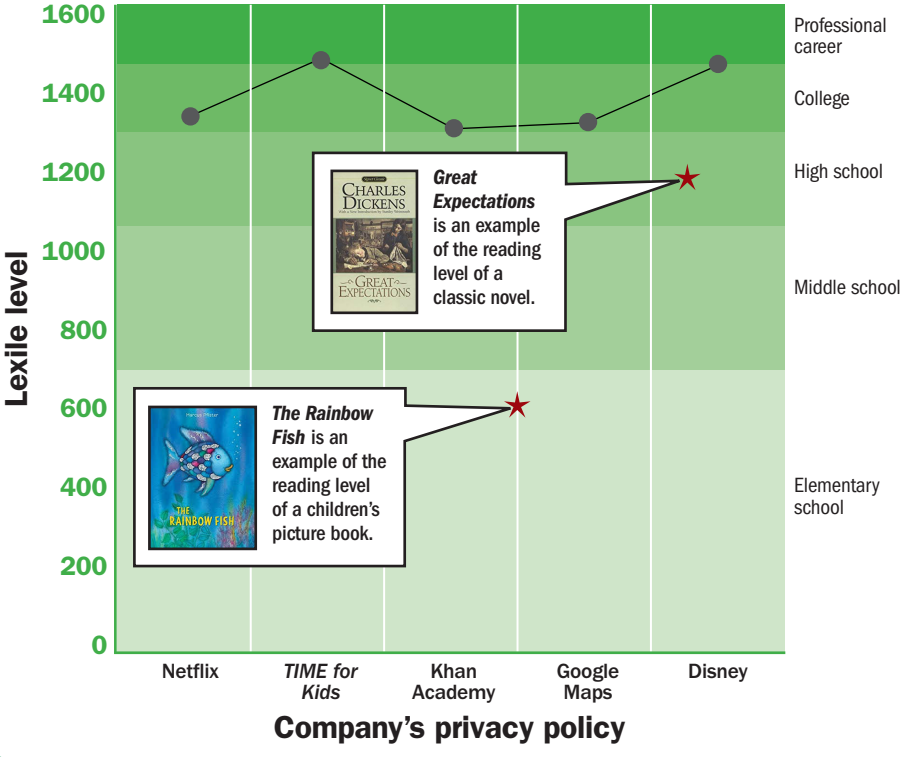
To connect families with the financial topics being discussed in the classroom, we are including this monthly newsletter featuring family resources. Teachers, please take a moment to photocopy this page and send it home with your students.

DEAR FAMILY,

Our children are growing up at a time when it's hard for them to imagine what the world was like before the technology that's now available to us. In this issue of *Your $*, we present them with 10 things they should be doing to stay safe online. As parents and caregivers, we are responsible for ensuring our kids are equipped for the 21st century by helping them make smart digital decisions.

One way adults can keep kids safe online is to know what will be done with the information they provide there. Many of us are guilty of skipping right over an app or website's privacy policy. This is understandable, given the length and complexity of some of these policies. Below is a breakdown of the reading levels of some common privacy policies and three quick tips for reading them.

Privacy Policy Reading Levels



QUICK TIPS

1. Scan the policy to locate the section about what kind of data is being collected about the user.
2. Scan the policy to locate the section about whether data is shared with third parties.
3. Search the policy for the word control to find what privacy controls are available to a user.

Made possible by the pwc Charitable Foundation