

Protecting your identity online

Students answer true-or-false questions about safe online behaviors and consider ways to protect themselves online.

Learning goals

Big idea

Fraud and identity theft harm millions of Americans every year.

Essential questions

- Why is it important to protect my identity when I'm online?
- What are some things I can do to protect myself from fraud and identity theft when I'm online?

Objectives

- Understand why fraud and identity theft are a risk
- Review practices that can help protect people from fraud and identity theft

What students will do



- Answer true-or-false questions about safe online behaviors.
- Explore ways to protect themselves online.

NOTE

Please remember to consider your students' accommodations and special needs to ensure that all students are able to participate in a meaningful way.

KEY INFORMATION

Building block:

-  Executive function
-  Financial habits and norms

Grade level: Middle school (6-8)

Age range: 11-14

Topic: Protect (Managing risk, Preventing fraud and identity theft)

School subject: CTE (Career and technical education), English or language arts, Fine arts and performing arts

Teaching strategy: Gamification

Bloom's Taxonomy level: Understand, Create

Activity duration: 45-60 minutes

National Standards for Personal Financial Education, 2021

Managing risk: 12-2, 12-4, 12-5, 12-7

These standards are cumulative, and topics are not repeated in each grade level. This activity may include information students need to understand before exploring this topic in more detail.

Preparing for this activity

- While it's not necessary, completing the "Acting out fraud" activity first may make this one more meaningful.
- Print copies of all student materials, or prepare for students to access them electronically.
- Print a copy of the "Knowing how to be safe online" statements in this guide to read aloud.
- Students will need blank paper to make "true" and "false" signs.
- To support Spanish-speaking students, there is a Spanish version of this activity.
 - You can use the worksheet available at https://files.consumerfinance.gov/f/documents/cfpb_building_block_activities_como-proteger-su-identidad-en-linea_tabla.pdf
 - A Spanish version of the guide is available at https://files.consumerfinance.gov/f/documents/cfpb_building_block_activities_como-proteger-su-identidad-en-linea_guia.pdf.

What you'll need

THIS TEACHER GUIDE

- **Protecting your identity online** (guide)
[cfpb_building_block_activities_protecting-your-identity-online_guide.pdf](https://files.consumerfinance.gov/f/documents/cfpb_building_block_activities_protecting-your-identity-online_guide.pdf)
- "Knowing how to be safe online" statements (in this guide)

STUDENT MATERIALS

- **Protecting your identity online** (worksheet)
[cfpb_building_block_activities_protecting-your-identity-online_worksheet.pdf](https://files.consumerfinance.gov/f/documents/cfpb_building_block_activities_protecting-your-identity-online_worksheet.pdf)
- Blank paper for "true" and "false" signs

Exploring key financial concepts

Millions of Americans are victims of fraud or identity theft each year. No matter where you live or how old you are, you may someday be affected by these crimes. Identity theft can happen over the phone by answering personal questions or online by clicking suspicious links or opening emails from unknown sources on your computer or phone. Knowing how to identify fraud and identity theft helps you better protect yourself and your money.

TIP

Because the types of fraud and the laws about fraud and identity theft change, students should be encouraged to always look for the most up-to-date information.

Teaching this activity

Whole-class introduction

- Tell students that they'll explore safe online behaviors.
- Be sure students understand key vocabulary:
 - **Fraud:** An illegal act that occurs when people try to trick you out of your personal information and your money.
 - **Identity theft:** Using your personal information – such as your name, Social Security number, or credit card number – without your permission.
- Distribute the “Protecting your identity online” worksheet and make sure students have blank paper for the “true” and “false” signs.
- Explain that they'll answer questions about protecting their identity online.

TIP

Visit CFPB's financial education glossary at consumerfinance.gov/financial-education-glossary/.

Individual work

- Students will work individually to complete their worksheets.
- Ask them to create two signs on the blank paper after they complete their worksheet, one that says “True” and one that says “False.”
- Once all the students are finished, read each statement aloud.
- Ask students to indicate whether they think the statement is true or false by holding up the appropriate sign.
- As students share their answers, keep a running tally on the board or on poster paper.

Wrap-up

- Once all the answers are tallied, review each question again and use the answer guide to share the correct answer.
 - You can use the answer guide's "Expanding understanding" section to add to the discussion.
- Encourage students to share their thoughts about why they answered each question the way they did.
- Ask students to share their responses to the reflection questions.

Suggested next steps

Consider searching for other [CFPB activities](#) that address the topic of protection, including managing risk and preventing fraud and identity theft. Suggested activities include ["Composing songs and verse about fraud"](#) and ["Protecting yourself from identity theft."](#)

Measuring student learning

Students' answers on their worksheets and during discussion can give you a sense of their understanding. This answer guide provides possible answers for the "Protecting your identity online" worksheet. **Keep in mind that students' answers to reflection questions may vary, as there may not be only one right answer.** The important thing is for students to have reasonable justification for their answers.

Knowing how to be safe online statements and answer guide

Statement	Answer	Expanding understanding
1. It's okay to give out personal information if someone sends you an email saying that you have an account with them and they seem to know some things about you.	False	Make sure you know who's getting your personal information and don't give it out through email or the Internet unless you know who you're dealing with. If a company emails you saying you have an account with them, don't click any links in the email. Instead, contact customer service through their website and ask if they sent a request.
2. It's safe to open any attachments or download any files as long as you do it from within the safety of your email account.	False	You should always be careful about opening any attachment or downloading any files from emails you receive, regardless of who sent them. Unexpected files may contain software that can hurt your computer.
3. Clicking on links in messages is only dangerous if you give your personal information out.	False	Don't open files, click links, or download programs from strangers. This could expose your computer to a virus or spyware that steals your passwords or other information you type.
4. The federal government requires sites and services meant for anyone 13 years old or younger to notify parents directly and get their approval before they collect, use, or disclose a child's personal information.	True	Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The goal of COPPA is to place parents in control over what information is collected from their young children online.
5. It's safest to stay permanently signed in to accounts.	False	If you stay logged in to accounts that have your personal information or use the automatic login feature (that saves your user name and password), your personal information is at risk if your computer is lost or stolen.
6. The "s" in https in a web address stands for secure.	True	If you see https as part of a website's URL, it means you can communicate securely with the web server. These sites use software that scrambles your information so other people can't access it over the Internet.

Statement	Answer	Expanding understanding
7. Avoid connecting to wi-fi networks that don't require a password to login.	True	Public wireless networks (wi-fi) are not secure. You should always use public networks with care. If you do connect your laptop or smartphone to the wi-fi in a coffee shop, library, or other public place, make sure you're using an encrypted website.
8. It's important to have virus protection on your computer and update it frequently.	True	It's important to be sure your computers are protected by reputable security software. Keep your software - including your operating system, the web browsers you use to connect to the Internet, and your apps - up to date to protect against the latest threats. Outdated software is easier for criminals to break into.
9. It's best to use the same password for many of your accounts because it's too difficult to remember multiple passwords.	False	It's good practice to use strong passwords for email and other online accounts. A strong password has a mix of upper- and lower-case letters, numbers and symbols. You should also protect your passwords. The longer the password, the harder it is to crack. Personal information, your login name, common words, or adjacent keys on the keyboard are not safe passwords.
10. Sharing your passwords with someone who is not a family member provides an extra layer of protection for your account.	False	People can protect their passwords by not sharing them with anyone, including their friends.