Lesson | Internet Safety Basics

Use stories and scenarios to help students evaluate online safety decisions.

Objective

Students will determine what information is safe to share online, learn digital-related vocabulary, and identify factors that make passwords weak or strong.

Standards

CCSS.ELA

- RL.3.1 Answer questions to demonstrate understanding of a text
- RL.4.1 Refer to text details and examples
- RL.5.1 Quote from a text when explaining
- L.3.6 (also 4.6, 5.6) Use domain-specific words

SEL

- Social awareness

Time

45 minutes

Materials

- Share With Care activity sheet
- Password Power! activity sheet

Vocabulary Support

Visit **g.co/BeInternetAwesomeEducators** for definitions and more lessons in the Be Internet Awesome curriculum

- personal information (p. 10)
- online privacy (p. 10)
- digital footprint (p. 10)
- scam (p. 30)
- hacker (p. 60)

Part 1: Share With Care

1 Prompt students: Think of a time when a friend did something you didn't want them to do. Explain: This can also happen easily online, such as a friend posting or texting a silly photo of you to someone else without asking you first.

2 Display the terms *personal information, online privacy,* and *digital footprint* on the board. Ask students what they already know about these terms. As a class, create a graphic organizer for each term by splitting a paper into four sections for a definition, a visual, an example, and a non-example.

3 Discuss *digital footprint* and explain that once something is on the internet, it is there forever. Clarify that even texting, commenting, emailing, or sharing information via messages or games counts as putting something on the internet, and can be shared with people you might not want to receive it. You should always think twice before you post.

4 Have students work in groups to decide which of these can be shared, when, and with whom: **a)** pictures of yourself, **b)** personal information such as a home address, **c)** pictures of others, **d)** your favorite game. Distribute the Share With Care activity sheet, and discuss as a class.

Part 2: Protect With Passwords

1 Display the terms *scam* and *hacker* on the board. Ask students what they already know about these terms. As a class, create a Frayer model for each term. Add a definition, a visual, an example, and a non-example for each.

2 Ask students what they know about passwords. Explain the components of creating a strong password: using a minimum of 8 characters that include a mix of upper- and lowercase letters, symbols, and numbers. The stronger the password, the harder it is for hackers to take your information. Remind students never to use personal details like birthdays or names. Create a list as a class with some examples of strong and weak passwords.

3 Hand out the Password Power! activity sheet. Then review answers as a class.

ANSWERS

Share With Care: **1.** No. Picture includes the name of his school, which is personal information. **2.** No. Rashad can share only if his friend says it's OK. **3.** No. Never share your email and password; Rashad doesn't know who is asking for the info, and he should tell his mom, because it looks like a scam.

Password Power: **1.** Weak: Uses personal information, isn't eight characters. **2** and **3.** Strong: Hard for hackers to guess, but both Luis and Mei have a way to remember it. Mixes capitalization, special characters, and numbers. Fits the minimum of eight characters.