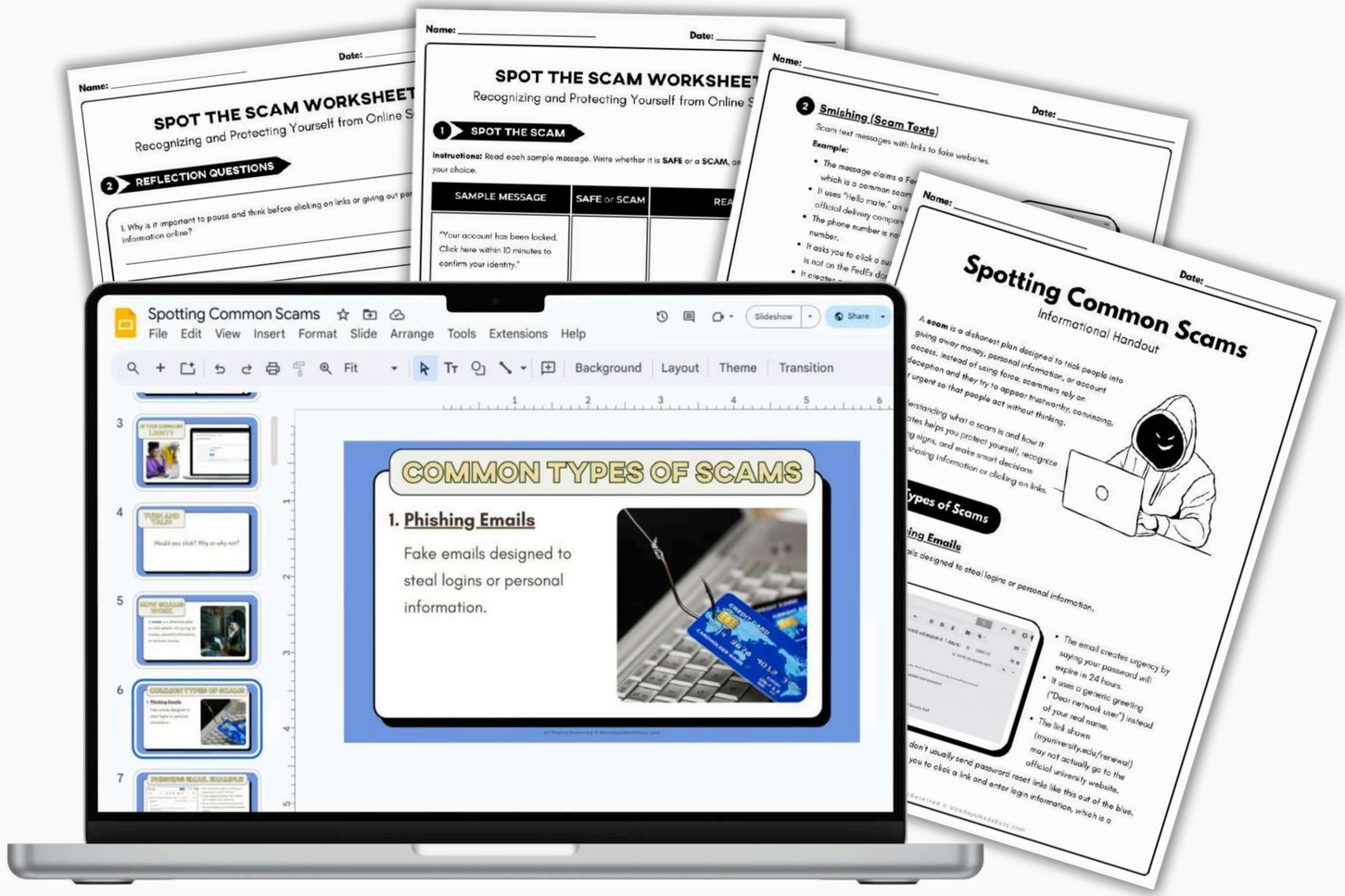
Internet Safety and Scam Spotting Lesson

Show students how to identify online scams and protect their personal information



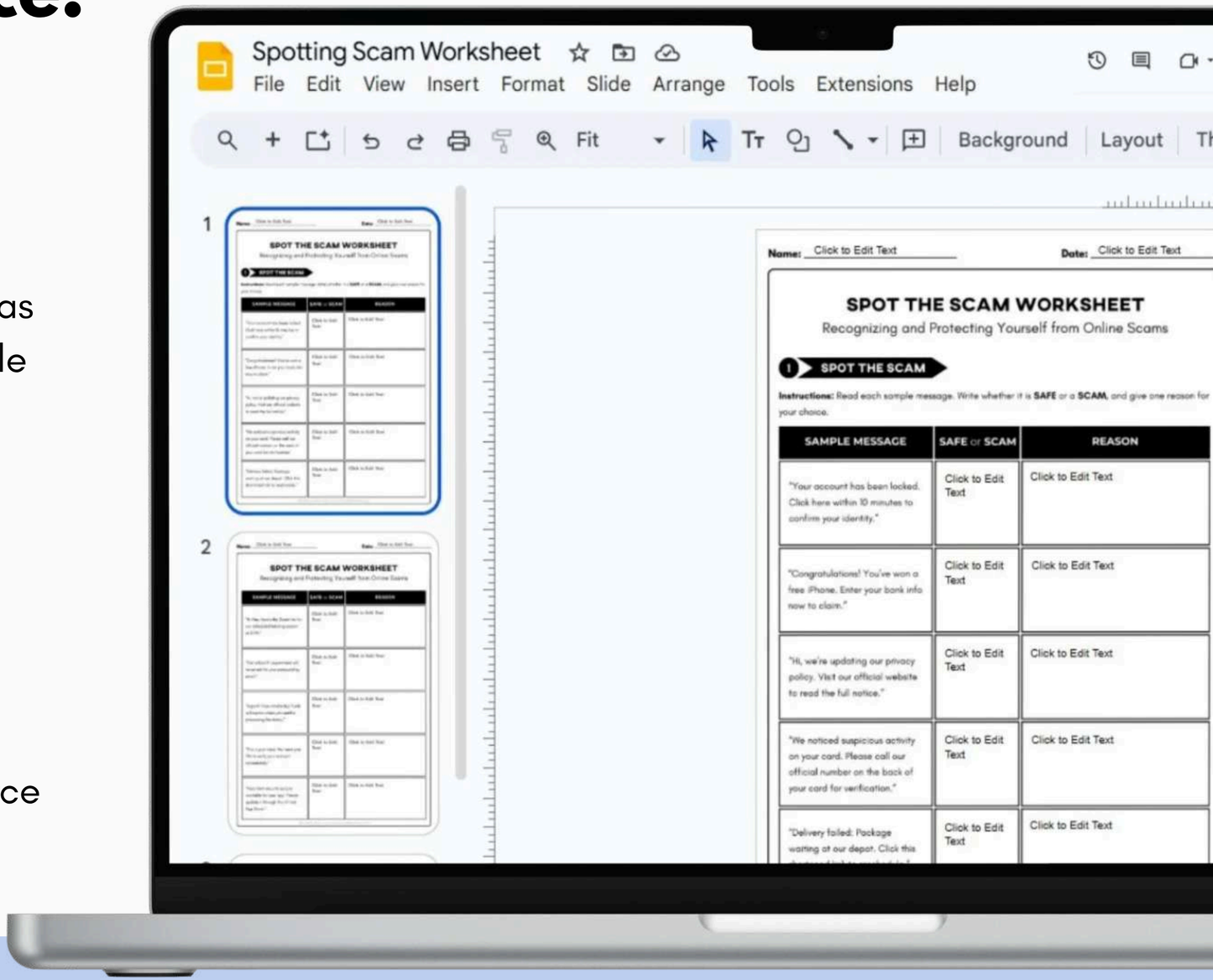
- **Guide students through identifying common online scam tactics** using real-world examples and clear explanations of safe digital habits.
- **Reinforce critical media literacy skills** with analysis activities that require students to evaluate messages, justify reasoning, and recognize warning signs independently.
- **Provide thoughtful discussion prompts** to reinforce empathy, accountability, and thoughtful online communication.

Teach students how to navigate the internet safely

PURCHASE HERE

Included with this resource:

- Spotting Common Scams **Slideshow Lesson**
- How to Spot a Scam **Informational Handbook**
  - Encourage students to highlight terms such as “urgent language” and “unverified links” while reading through the content
- Spot the Scam **Analysis Activity**
  - Presents sample online messages
- **Detailed Answer Key**
- **Teacher Instructions** for how to use this resource



Includes Digital Version for Google Drive®

Spotting Scams Slideshow Lesson

Define internet safety and break down the anatomy of a scam message using accessible language and real-world examples

Introduce students to common scam tactics like **urgency, fake links,** and **requests for personal information**

Spotting Scams Informational Handbook

This reference handout summarizes warning signs of scams and reinforces key digital citizenship practices

Name: _____ Date: _____

6 Impersonation Scams

Fraudsters pretend to be banks, delivery companies, or government agencies to get money or data.

Example:

- The sender address looks like Citibank but uses a suspicious extra domain "securemygateway.com."
- The email claims "suspicious activity" to scare you into acting quickly.
- It asks you to click a link to "confirm your identity," which real banks rarely do by email.
- The link shown ("citibank-verification.com") is not the real C
- The message does not include any personal details, which n have.

7 Tech Support Scams

Fake virus alerts or tech support calls asking you to pay or give

Example:

- The pop-u Detected" program ru
- It gives a t to call for " antivirus co
- It uses urge like "hard-c to scare yo
- The web address (alert.scan001.com) is not an official site c company.
- Real security alerts don't appear as random browser pop-u number.

Name: _____ Date: _____

Spotting Common Scam

Informational Handout

A **scam** is a dishonest plan designed to trick people into giving away money, personal information, or account access. Instead of using force, scammers rely on deception and they try to appear trustworthy, convincing, or urgent so that people act without thinking.

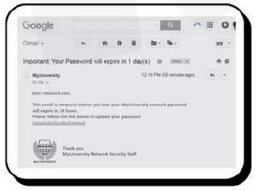
Understanding what a scam is and how it operates helps you protect yourself, recognize warning signs, and make smart decisions before sharing information or clicking on links.

Common Types of Scams

1 Phishing Emails

Fake emails designed to steal logins or personal information.

Example:



- The email creates urg saying your password expire in 24 hours.
- It uses a generic gree ("Dear network user") of your real name.
- The link shown (myuniversity.edu/renewal) may not actually go to the official university website.
- Real IT departments don't usually send password reset links like this out of the blue.
- The email tries to get you to click a link and enter login information, which is a phishing tactic.

Name: _____ Date: _____

2 Smishing (Scam Texts)

Scam text messages with links to fake websites.

Example:

- The message claims a FedEx package is waiting, which is a common scam tactic.
- It uses "Hello mate," an unusual greeting for an official delivery company.
- The phone number is not an official FedEx number.
- It asks you to click a suspicious shortened link that is not on the FedEx domain.
- It creates a sense of urgency by saying your package is "waiting" for you to act.

3 Fake Job Offers

Scammers pose as employers or recruiters to steal your informatio

Example:

- It pretends t invitation bu offer, which do.
- The email ca about "bette without any
- The sender n but scamme easily so you actual email
- It uses generic wording ("we have a similar position near you") job title or company name.
- The "View profile" and "Accept" buttons could lead to fake log to steal your credentials.
- It combines a social networking invite with a job offer, which is legitimate LinkedIn notifications.

Name: _____ Date: _____

Red Flags to Watch For

1. **Urgent or threatening language**
   - Scammers try to scare you with messages like "Act now or your account will
2. **Too good to be true offers**
   - Promises of huge prizes, free money, or easy jobs are usually scams.
3. **Requests for personal info or money**
   - Real companies will not ask for your passwords, PINs, or payment details by e text.
4. **Suspicious links or email addresses**
   - Look for weird spellings, extra numbers, or addresses that don't match the re
5. **Poor grammar or spelling**
   - Many scams have typos, awkward wording, or strange greetings ("Dear Cust

Protecting Yourself Online

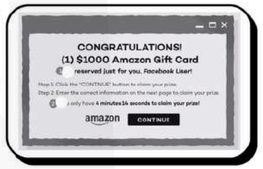
1. **Don't click suspicious links**
   - If unsure, don't tap or click.
2. **Verify with official sources**
   - Contact the company or person using their real phone number or website.
3. **Use strong passwords & 2FA**
   - Create unique passwords and turn on two-factor authentication to keep acc
4. **Report scams to a trusted adult**
   - Tell a teacher, parent, or school IT if you get a suspicious message.
5. **Trust your instincts—if unsure, don't respond**
   - If something feels off, it probably is.

Name: _____ Date: _____

4 Lottery & Prize Scams

Messages claiming you've won money or a prize but asking for fees first.

Example:

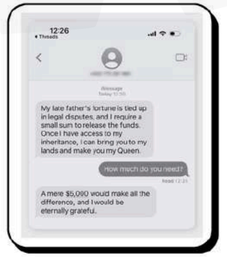


- It promises a $1,000 Amazon gift card for free, which is too good to be true.
- It uses a generic greeting ("Facebook User") instead of your real name.
- It creates pressure with a countdown timer to make you act fast.
- It asks you to enter personal information on the next page.
- The design and layout don't match official Amazon promotions.
- There is no official Amazon link or contact information shown.
- It appears as a pop-up, a common method used by scammers.

5 Romance Scams

Fake online relationships built to ask for money or gifts.

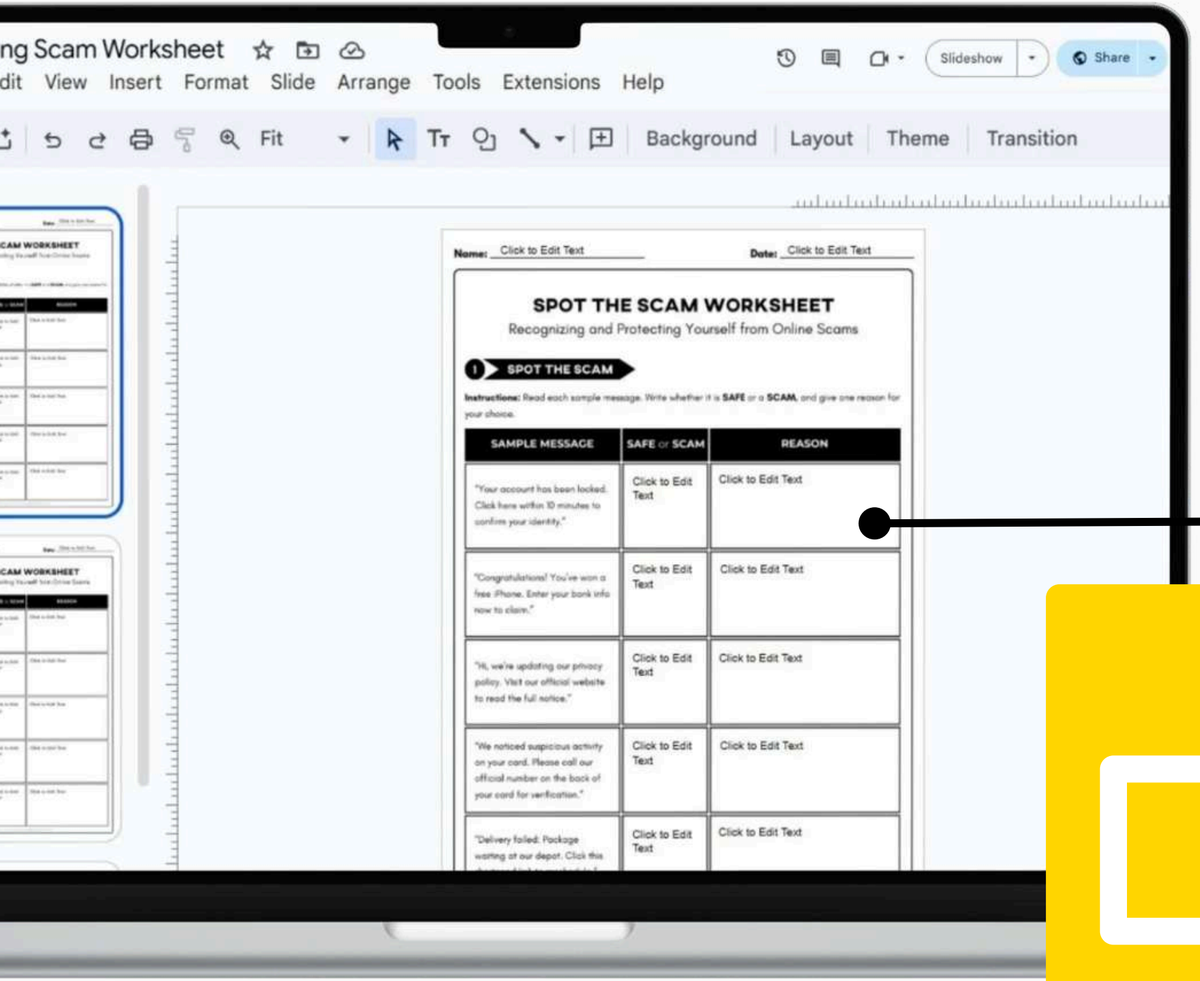
Example:

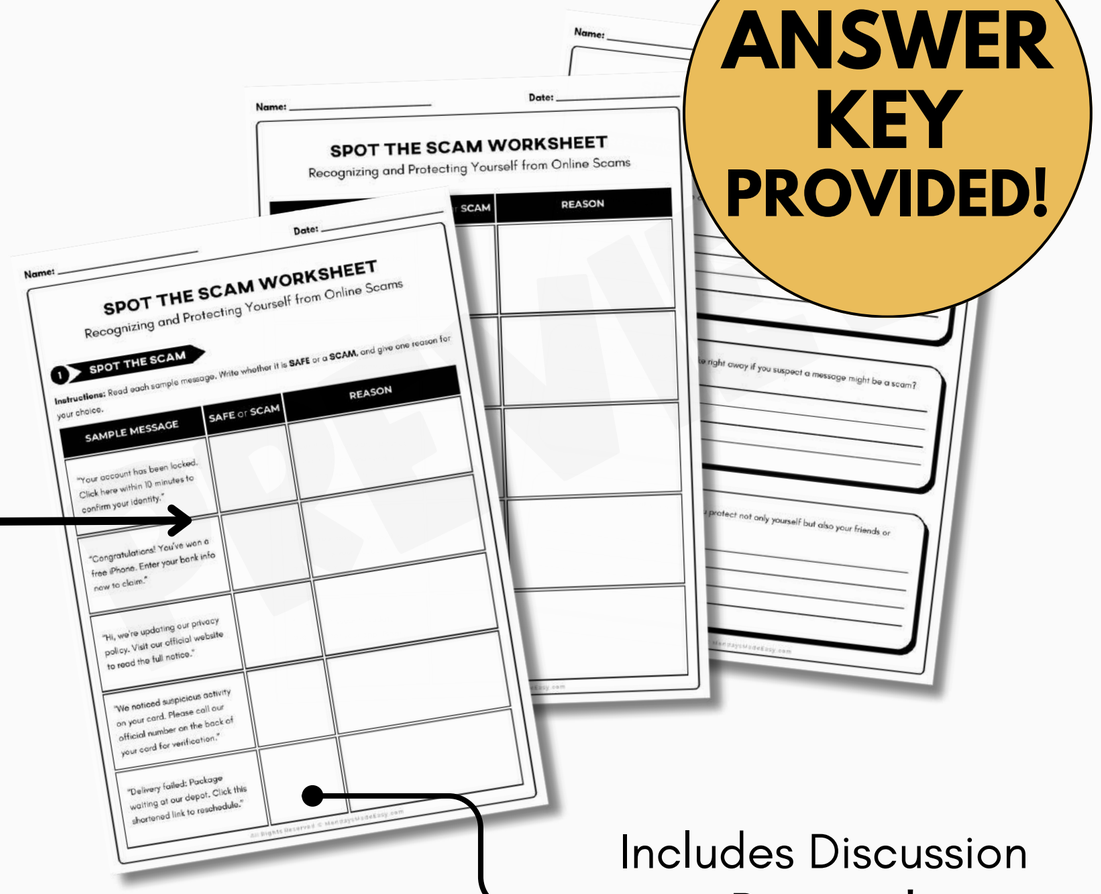


- The sender uses a dramatic story about a late father's fortune to gain sympathy.
- They promise wealth and love in return, which sounds too good to be true.
- They ask for $5,000 upfront to release the inheritance funds, a common scam tactic.
- They create urgency by implying the money is needed immediately.

Spot the Scam Activity

Students must decide whether each message is safe or a scam and explain their reasoning using evidence





ANSWER KEY PROVIDED!

Includes Discussion Prompts!