ELEMENTARY and MIDDLE SCHOOL | GRADES 5–8
DE Docs: Money Mastery | Activity

Title
Scam Spotters

DE DOCS: MONEY MASTERY

Use this classroom activity before or after showing *DE Docs: Money Mastery*. This activity can be used beforehand to get students thinking about using online and mobile banking in a safe manner and increase student engagement with the video. If students watch the video first, the activity can be used to reinforce concepts discussed in the documentary, particularly the advice provided by banking expert, Juan, who provides advice for protecting your finances and avoiding scams. The activity offers specific suggestions of when to show or mention the video.

Overview

How do you stay safe while banking online? In this lesson, students explore the concept of phishing and how it can lead to identity theft. The lesson begins with an interactive introduction comparing traditional fishing to the malicious practice of phishing, helping students understand the dangers of sharing personal information online. Through a hands-on activity involving mystery messages, students learn to identify and respond appropriately to various digital communications. The lesson includes a discussion of safe banking practices, reinforced by recalling tips shared by an expert in the *DE Docs: Money Mastery* video. The session concludes with a role-play activity and reflective exit ticket, allowing students to apply what they've learned and articulate their understanding of safe digital banking.

Learning Objectives

Students will:

- Define phishing and explain how it relates to identity theft.
- Practice evaluating digital messages and determining the appropriate response.
- Demonstrate their understanding of safe digital banking by role-playing conversations with a relative or another adult.

National Standards for Personal Financial Literacy

VI. Managing Risk 4–1: People are exposed to risk when there is a chance of loss or harm. Risk is an unavoidable part of daily life.

VI. Managing Risk 8–1: Financial loss can occur from unexpected events that damage health, wealth, income, property, and/or future opportunities.

VI. Managing Risk 8–7: Identity theft is the use of someone else's personal identification information to commit a crime.

MATERIALS

- *DE Docs: Money Mastery*
- **Mystery Messages**—enough copies to make sure each student will receive one message (repeats are okay); fold and tape the messages or place them in sealed envelopes
- **Next Step Signs**—one copy of each, taped around the room in advance of the lesson
- **Tape**—enough to hang the three signs

Engage

- Ask students if they have ever gone fishing before. Follow up with students who say they have with questions, such as:
    - Did you catch any fish? What kind?
    - Who did you go with?
    - Did you have fun?
- If no students respond, share a story about someone you know (or make up) who went fishing, caught several fish, and enjoyed their time out on the water.
- Share with students that most people associate fishing with catching fish—often with a pole or a rod and reel. They might even catch them in a net.
- Explain to students that there is another type of phishing that is not good. It involves people fishing for personal information. While it sounds just like fishing, this version is spelled P-H-I-S-H-I-N-G, instead. Write the word PHISHING on the board or a flip chart to reinforce the spelling.
- Let students know that phishing often leads to identity theft; the use of another person's personal information for financial gain. Share examples such as people having credit cards and loans opened in their name and never knowing about it. If you or someone you know has been the victim of identity theft, share a brief version of the story. Knowing about phishing and being able to spot it can help people prevent becoming a victim of identity theft.

INTERACTIVE STORYTELLING

Want to make this more compelling? Consider bringing a fishing rod or related props to create a visual and tactile connection.

Teach

Inform students that you want them to see if they can "spot the scam." Tell them to imagine that they have just received an important message related to their bank account. Some are sent via text, some by email, and others through their bank's mobile app.

- Distribute a **Spot the Scam Message** to each student. Ask them to keep the message sealed until told to open them.
- Tell students that they may encounter a word or phrase that they do not know. If this happens, they can ask a neighbor for help or come to you. Below are terms students might encounter and need assistance understanding:
    - **Account:** A place where you keep your money at a bank so you can save it, spend it, or use it when you need it.
    - **Compromised:** When something, like your bank account, is not safe anymore because someone might have gotten in without permission.
    - **Deposit:** When you put money into your bank account to keep it safe or save it.

  - **Exclusive:** Something special that only a few people can have or use.
  - **Fraud:** When someone tricks or lies to you to steal your money or get something they shouldn't.
  - **Inquiry:** A question you ask to find out more information about something.
  - **Social Security:** A government program that helps people by giving them money when they are older, sick, or can't work.
  - **Statement:** A paper or digital record from the bank that shows all the money that went in and out of your account over a period of time.
  - **Tax:** Money that people pay to the government to help pay for things like schools, roads, and other public services.
- Once everyone has a message, direct students to open and read them silently.
- Point out the three **Next Step Signs** posted around the room: Trust It (green light), Proceed with Caution (yellow light), and Stop! Don't Respond! (red light). Each represents an option students have once reading their message. Give students a moment to think about their decision.
- After students have read their messages and made their decisions, direct them to move to the sign that best matches how they would respond.
- Once in position, invite students to compare their messages in small groups and discuss the decisions they made.
  - What clues helped you decide whether to trust or be suspicious of the message?
  - Do you agree with the decision your classmate made? Why or why not?
  - Can you find someone else with the same message?
- To encourage even deeper conversations, direct students to pair up with someone who chose a different response and engage in a second discussion about their choice and that of their partner.
- With students still standing by the signs, invite each student to read their message. Using the reasons from the **Spot the Scam Messages**, clarify any positions and provide additional detail, as needed. Use this discussion to introduce the idea that not all messages related to banking are safe and that it's essential to be vigilant and cautious when dealing with digital communications related to finances.
- Challenge students to brainstorm questions a person could ask before deciding if a message is safe or not. Examples include, "Did the message ask for personal information?" or "Did the message create a sense of urgency?" Point these out as red flags that should cause someone to be very careful.
- If students have already watched ***DE Docs: Money Mastery***, ask them to recall the banking expert, Juan Garcia, who shared information about some of the dangers of online or mobile banking. See what tips students remember him sharing, including creating a strong PIN and password, using your phone's lock screen, and checking ATMs for skimming devices.
- If students have not watched ***DE Docs: Money Mastery***, play the video in its entirety. If pressed for time, show the Behind the Vault segment. Afterwards, ask students to recall the banking expert, Juan, who shared information about some of the dangers of online or mobile banking. See what tips students remember him sharing, including creating a strong PIN and password, using your phone's lock screen, and checking ATMs for skimming devices.

Conclude

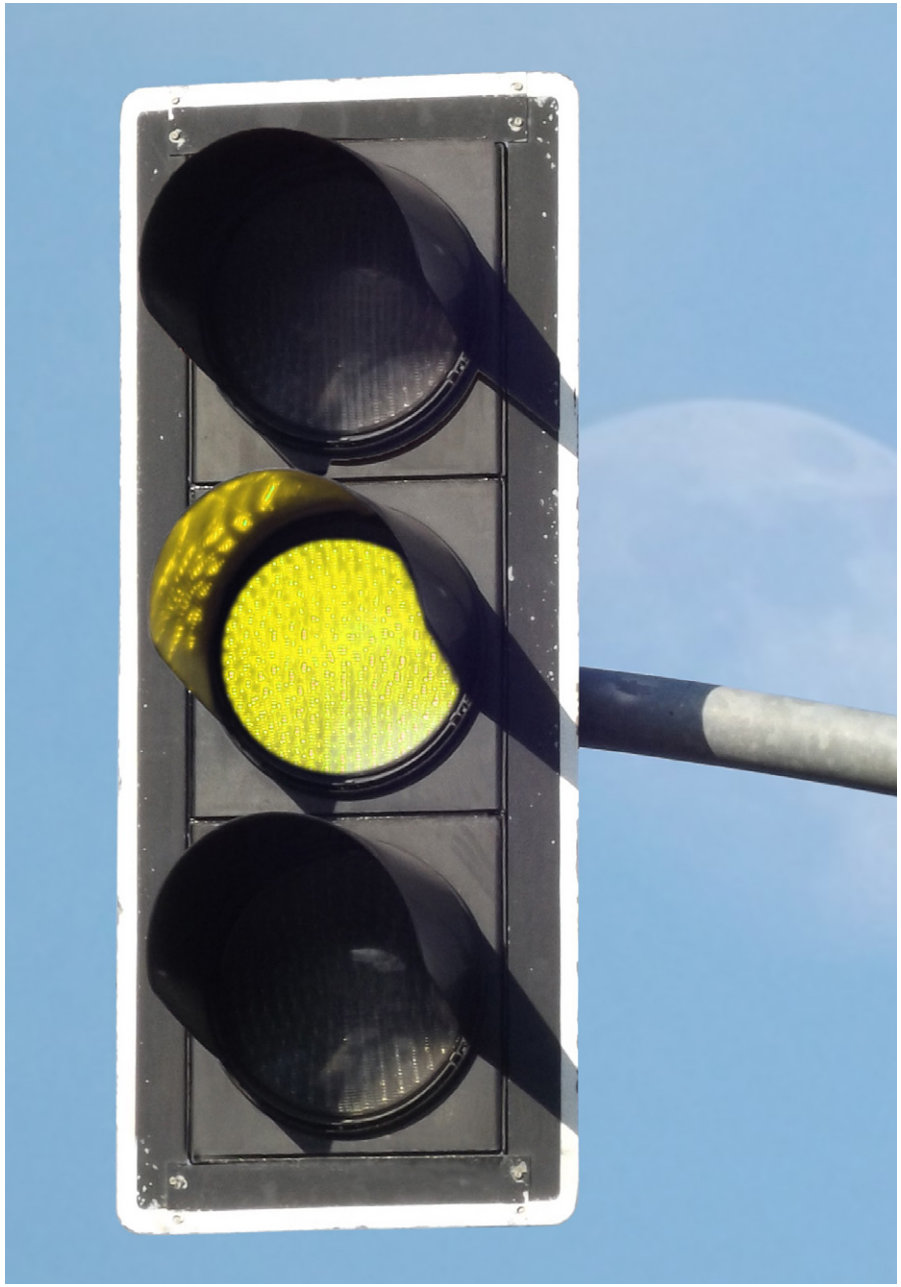
- Challenge students to think of a relative or other adult who asks for help or doesn't always understand technology. Ask students who comes to mind.
- With this person in mind, invite students to consider what they would tell this person about banking safely.
- Invite several students to role-play a conversation with the person they are thinking about. You or another student can play the part of the adult. Doing so can help students articulate what they've learned and practice explaining it in a way that is easy to understand.
- Direct students to submit an exit ticket completing one of the following sentences: "One thing I learned about digital banking safety is…" or "A tip I would give to someone about online banking is…"

Extend

- **Password Creation:** Invite students to create strong passwords on slips of paper. Remind them not to share their passwords with anyone and discuss what makes a password strong (e.g., a mix of letters, numbers, and symbols). Collect the passwords and redistribute them. Direct students to compare passwords with other members of the class and form a line from strongest to weakest password. Students can share "spots" along that line.
- **Poster Challenge:** Challenge students to create posters highlighting ways to stay safe while using digital banking.
- **Safe Online Shopping:** Direct students to research tips for safe online shopping and create a digital safety guide for their peers or others.
- **Family Discussion:** Encourage students to talk with their families about what they learned and share the banking safety tips at home.

Trust It

Proceed with Caution



Stop! Don't Respond!

Spot the Scam Messages

Directions: Make two copies. Keep one as your answer key. With the other, cut out the messages and discard the answers. Fold and tape each one or place them in separate, sealed envelopes. Make sure to mix them up before distributing them to students.

Email **We are offering a new savings account option. Click here to learn more about it on their official website.**	Email **Your bank has successfully updated your contact information as requested. If you did not make this change, contact customer service immediately.**	Email **We are confirming that your recent transaction using the bank's mobile app has been processed.**	Text **You requested a password reset via our website. Please use this link to reset your password within the next 30 minutes.**
Trust It: Promotional emails from banks are common and can be trusted when linked to the official site.	**Trust It:** Confirmation of an account change that you requested is a safe email.	**Trust It:** Transaction confirmation emails are expected after legitimate purchases.	**Trust It:** If initiated by the user, password reset emails are safe.

Notification **We have successfully processed a direct deposit to your account. You can view the details by logging into your account.**	Notification **Your monthly statement is ready for review. You can log into your account directly through the bank's official website or app to view it.**	Text **Your automatic savings transfer will occur tomorrow as scheduled. No action is needed unless you want to make changes in your online account.**	Text **This is a bill payment reminder. Please make sure you have enough money in your account by the due date.**
Trust It: Direct deposit notifications are standard and can be trusted.	**Trust It:** This is a common and legitimate notification from a bank.	**Trust It:** Automated savings reminders are typical and safe.	**Trust It:** Bill payment reminders from your bank are trustworthy.

Spot the Scam Messages

Notification **You have received an official tax document from your bank for the upcoming tax season. Please download it from your online account.**	Text **Our customer service team has responded to your inquiry about recent account activity. View their response by logging into your account.**	Email **Our fraud protection department detected no unusual activity this month. No further action is needed unless you notice unexpected activity on your statement.**	Notification **Your credit card statement is now available. Please log into your account to view the details.**
Trust It: Banks regularly send tax documents at the appropriate time.	**Trust It:** Replies to inquiries made by the customer are expected.	**Trust It:** Routine fraud monitoring updates are normal.	**Proceed with Caution:** Not all notifications are valid. Log into the account from an app rather than the notification.

Email **Your account will be locked unless you verify your identity. Please upload a copy of your ID via this link.**	Email **Please confirm your recent transaction by logging in through this link. If you did not make this transaction, contact us immediately.**	Email **You've won a prize from your bank! Click here to claim your reward.**	Text **There was an issue processing your recent payment. Please log in using this link to resolve the issue.**
Proceed with Caution: Requests for ID verification should prompt caution and verification through direct bank contact.	**Proceed with Caution:** Transaction confirmations that seem unfamiliar should prompt verification through direct contact.	**Proceed with Caution:** Be cautious with unexpected rewards. Confirm with the bank directly to avoid being scammed.	**Proceed with Caution:** Payment issues might be real but always proceed cautiously and verify through the official site.

Spot the Scam Messages

Email **You've been selected for an exclusive customer survey from our bank. Participate to receive a bonus.**	Email **You've received a cash back bonus from your bank. Log in through this link to see the details.**	Text **Your bank is updating its terms of service. Please review the changes by clicking this link.**	Text **Your account requires verification to ensure it remains active. Click here to start the process.**
Proceed with Caution: Surveys linked to rewards may be legitimate but should be approached with caution.	**Proceed with Caution:** Cash back offers can be legitimate, but verify by logging in directly to the bank's website.	**Proceed with Caution:** Be cautious with links in texts about policy updates. Instead, check the official website.	**Proceed with Caution:** Requests for account verification should always be handled cautiously.

Text **Security alert! There have been unusual login attempts from a different country. Log in through this link to secure your account.**	Email **Your bank has detected multiple failed login attempts. Click here to confirm if this was you.**	Email **You've been pre-approved for a loan! Click here to learn more and apply.**	Email **We are offering a special promotion if you sign up for a new credit card TODAY ONLY. Act quickly to receive extra reward points.**
Proceed with Caution: While concerning, this could be a phishing attempt. Verify directly through the bank's official contact channels.	**Proceed with Caution:** Failed login attempt notifications require careful action. Always verify through official channels.	**Proceed with Caution:** Pre-approval emails might be genuine but require careful examination before acting.	**Proceed with Caution:** Be careful with promotions that require you to act fast. Ensure the offer is real using the bank's website.

Spot the Scam Messages

Email	Text	Text	Email
We've detected unusual activity on your account. Click here to secure your account immediately.	**Urgent: You need to verify your account information within 24 hours to avoid having your account locked.**	**Please confirm your bank account number by clicking this link and entering your details.**	**Congratulations! You've won a cruise courtesy of your bank. Click here to claim your prize.**
Stop! Don't Respond! Phishing attempts often create a sense of urgency. Delete and contact the bank directly.	**Stop! Don't Respond!** Urgent messages asking for verification are likely scams. Delete immediately.	**Stop! Don't Respond!** Legitimate banks will never ask you to confirm your account details by clicking on a link. Delete this immediately.	**Stop! Don't Respond!** Unexpected prizes—especially big ones like a cruise—are a classic phishing tactic. Delete immediately.

Email	Email	Text	Email
You've been selected to receive a cash reward. Enter your bank details here to claim it.	**Your payment failed. Click here to re-enter your payment details.**	**Your bank account has been locked. Click this link to reactivate it now.**	**You've received a money transfer. Click here to accept the funds.**
Stop! Don't Respond! This is a phishing scam. Never enter your bank details into such forms. Delete immediately.	**Stop! Don't Respond!** Phishing emails often mimic payment failures. Delete and handle payments directly through the official site.	**Stop! Don't Respond!** This is a common scam. Never click the link; instead, contact your bank directly.	**Stop! Don't Respond!** Unsolicited money transfer notifications are a phishing attempt. Delete immediately.

Spot the Scam Messages

Email **You've received a cash back bonus from your bank. Log in through this link to see the details.**	Text **Dear customer, please confirm your Social Security number to verify your account.**	Email **You have an outstanding balance. Click here to pay now and avoid late fees.**	Email **Your bank account has been compromised. Enter your information here to secure it.**
Stop! Don't Respond! Cash back offers can be legitimate, but verify by logging in directly to the bank's website.	**Stop! Don't Respond!** No legitimate bank will ask for your Social Security number via text or email. Delete this immediately.	**Stop! Don't Respond!** Never click on links to pay balances from unsolicited emails. Handle payments through your bank's official site.	**Stop! Don't Respond!** This is a common phishing scam. Delete the email and contact your bank directly.