Lesson 20: Protect Yourself

TOPIC: CONSUMER PROTECTION

Time: 70 min

Subject Connections:
- English Language Arts
- Social Studies
- Technology

Supplies:
- Projector (for teacher presentation slides)
- Access to the Internet (optional)

Preparation:
- Make copies of student handout
- Set up projector with presentation slides

OVERVIEW:
In this lesson, students explore **identity theft**, prevention strategies for protecting personal information, and the consequences of identity theft in different real-world scenarios. From **phishing**, **pharming**, and **text message scams** to detecting **employment fraud**, students learn how to differentiate between multiple unethical deceptions. After identifying identity compromises, students also research methods to protect themselves through consumer rights and discover ways to prevent identity theft. Students learn the essential steps to take if their information has been breached and what to do after those first action steps are taken.

OBJECTIVES:
1. Explain identity theft
2. Evaluate consumer rights and protection laws
3. Demonstrate how to protect personal information

INDIVIDUAL HANDOUTS:
- Spot Identity Theft
- This Job, Not That Job*
- Steps to Take*

TEACHER PRESENTATION SLIDES:
- Identity Theft
- What Do Thieves Do with Your Information?
- Types of Identity Theft (3)
- Job Scams

ESSENTIAL QUESTIONS:
- What is identity theft?
- How do I protect myself?

ASSESSMENT ACTIVITIES:

Pre-Assessment:
- **Slide:** Identity Theft
- **Slide:** What Do Thieves Do with Your Information?
- **Handout:** Steps to Take

Post-Assessment:
- **Handout:** Spot Identity Theft
- **Handout:** This Job, Not That Job

***Money Smart Portfolio Handouts**

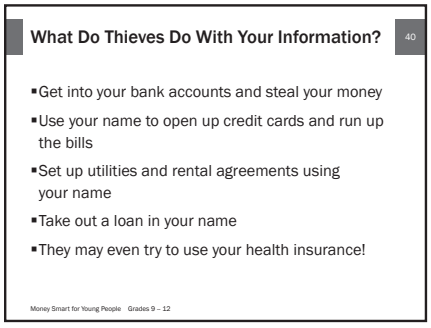
Instruction Steps

WARM UP
You Are The Only You, Right?

10 MINUTES

Open the lesson by showing the ***Identity Theft*** slide. Tell students there is only one of each of you. Or is there? DNA analysis can prove you are the only you scientifically, but there are many crafty criminals that may be able to steal personal information (for example: your Social Security number, birth date, or credit card numbers) and use your identity to commit fraud or other crimes.

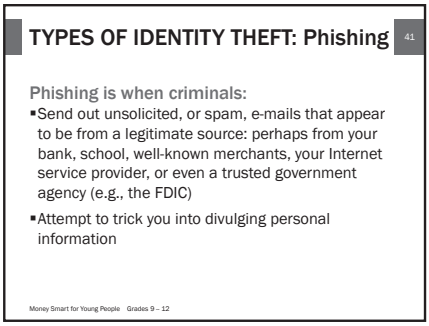
Tell students that identity theft is a serious problem because, despite the efforts of law enforcement, identity theft is becoming more sophisticated and the number of new victims is growing. If the crime is not detected early, you may face months or years of cleaning up the damage to your reputation and credit rating. You may even lose out on loans, jobs, and other opportunities.



Next, display the ***What Do Thieves Do with Your Information?*** slide and review the motives behind identity theft.

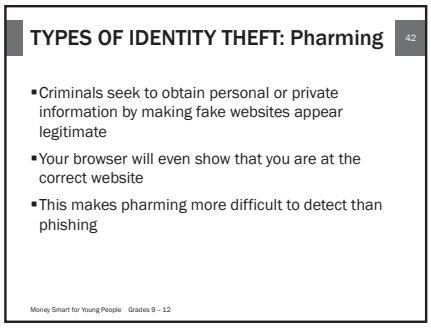
GUIDED EXPLORATION
Compromising Information

25 MINUTES

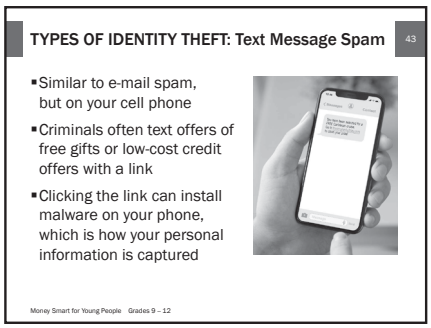


Share the (3) ***Types of Identity Theft*** slides and review each of the different tactics thieves use to steal information.

- **Phishing** is when criminals send out unsolicited, or "spam," e-mails that appear to be from a legitimate source: perhaps from your bank, school, well-known merchants, Internet service provider, or even a trusted government agency (for example: the FDIC). Criminals attempt to trick you into divulging personal information.



- **Pharming** is when criminals seek to obtain personal or private information by making fake websites that appear legitimate. Your browser will even show that you are at the correct website. This makes pharming more difficult to detect than phishing.



- **Text message spam** is similar to e-mail spam, but on your cell phone. Criminals often text offers of free gifts or low-cost credit offers with a link. Clicking the link can install malware on your phone, which is how your personal information is captured.

MONEY SMART TIP!
Visit the Federal Trade Commission's scam alert website at **www.consumer.ftc.gov/features/scam-alerts**. Review several trending scams, such as Bitcoin blackmail scams, and discuss how technology advancements are changing the way identity thieves initiate fraudulent activities.

Invite students to share experiences they have had with **phishing, pharming,** or **text message spam.**

Ask students if they have ever received any spam e-mails or texts and what they did when it happened. Explain that if an offer sounds too good to be true, then it probably is!

Next, ask students how they think they can protect themselves and what could be some ways to avoid identity theft. Invite students to share their answers, and emphasize that we can take the following actions to protect ourselves:

- Do not share Social Security number, credit/debit card numbers, PIN numbers, or passwords.
- Always review bank statements thoroughly.
- Lock financial documents and records in a safe place.
- Lock personal devices, such as phones, with passcodes.
- Utilize smartphone security features such as remote wipe, which will delete data on a device in the event of theft.
- Online, only "friend" people you know and don't overshare personal details on social networking sites.
- Shred old documents that include personal information such as account numbers and Social Security number.
- Before getting rid of an old computer or phone, dispose of all personal information stored on it.

- Choose combinations of upper- and lower-case letters, numbers and symbols that are hard for a hacker to guess. Don't, for example, use your birthdate or address. Also don't use the same password for different accounts because a criminal who obtains one password can log in to other accounts. Finally, make sure to change your passwords on a regular basis.
- Some people opt to use online tools to create and keep track of passwords or other information from multiple accounts. If you want to use their services, thoroughly research the company behind the website, including making sure that you're dealing with a legitimate entity and not a fraudulent site. Also ask what protections the website offers if it experiences a data breach or loss of data.
- If someone asks you to share personal information, such as at a place of employment or doctor's office, ask why they need it and how your information will be protected.
- Although website privacy policies can be long and complex, it is important to familiarize yourself with them to understand how your personal information is collected and used.
- Before paying for a purchase online, make sure the website you're on has "https" at the beginning of its URL with a lock symbol. This means the site has a protected network connection. Websites with "http" at the beginning of the URL with no "s" are more vulnerable to attacks by scammers who steal credit card information by monitoring network traffic.
- Avoid using public Wi-Fi to make purchases online, login to your financial accounts, or access other sites that have sensitive information about you.
- Monitor your credit report. You have a right to one free credit report every 12 months from each credit reporting agency.

Grade-Level Modifications:

Beginner: Share with students additional examples of the types of identity theft and make sure students can identify the differences among each before moving on to the Free Exploration section.

Advanced: Have students research current events and find a news article that addresses any of the types of identity theft. Have students present their article and analyze it together as a class. For recent examples, visit the Federal Trade Commission's Scam Alerts at **www.consumer.ftc.gov/scam-alerts.**

Help students understand that while they should work to minimize risks such as by not oversharing information, they are also protected by law. Explain that federal law requires financial institutions to keep your personal financial information private and ensures that the general public does not have access to your personal financial information.

Tell students that federal privacy laws give them the right to stop or "opt out" of sharing some of their personal financial information, and that, if you opt out, you limit the extent to which the company can provide your personal financial information to nonaffiliated, or groups outside of the company.

MONEY SMART TIP!

Discuss with students the importance of contacting credit-reporting agencies in the event of identity theft and checking your credit score. Refer to Lesson 7, ***Capacity, Character, Collateral, Capital,*** for more information on the three major credit-reporting agencies: Equifax (**www.equifax.com**), Experian (**www.experian.com**), and TransUnion (**www.transunion.com**).

Next, distribute the ***Spot Identity Theft*** handout and review each scenario. Ask students to raise their hands for "Yes" or "No" for each story, and then engage students in a discussion about why or why not identity theft is possible.

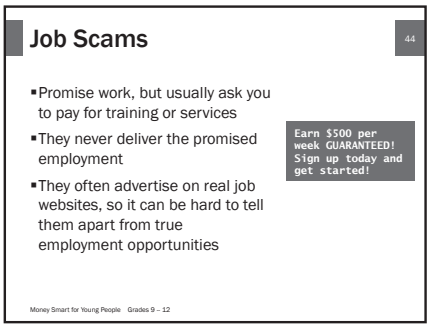
MONEY SMART TIP!

In today's online world, students often share personal information freely, without fully considering who exactly might have access to that information. Ask students whether they know what personal information is and is not OK to share about themselves online.

Tell students that, if they participate in online discussions or social media, personal information such as their full name, Social Security number, bank account numbers, or parents' credit card account numbers should always be kept private. While it may be OK for students to share some personal information on social media, such as what movies they like to watch or names of books they like to read, they must understand who will read their information. Identity thieves often find information about people's lives through social media and use it to answer "challenge" questions on their accounts to gain access to their money and personal information.

INDEPENDENT EXPLORATION
More Scams

30 MINUTES



Note: These activities are more independent than the Guided Exploration activities and may be used as homework assignments, collaborative group work, or independent study.

Tell students that it is not just spam we have to be on the lookout for and that there are other scams that can cause significant financial turmoil.

Display the ***Job Scams*** slide and review with students that employment scams are growing in popularity among criminals because they offer a "solution" to finding work, such as a paid certification or training with the promise of a job at the end—only the job never comes. The criminals take your cash and move on to the next victim.

Distribute the ***This Job, Not That Job*** handout and have students work together in small groups to analyze each of the job offerings. Challenge each group to identify which job is legitimate and which is not, documenting their supporting reasons.

Invite volunteers to share their conclusions with the class, and review why one job offer is more credible than the other. Reiterate that employment scams often make false promises, and if an opportunity sounds too good to be true, then it likely is.

MONEY SMART TIP!
Share and discuss with students the *Job Scams* video (3 minutes) from the Federal Trade Commission's website at **www.consumer.ftc.gov/articles/0243-job-scams.** Expand the discussion of scams by reviewing the many additional kinds of fraudulent behavior at **OnGuardOnline.gov** (**www.consumer.ftc.gov/features/scam-alerts**).

Next, tell students that being aware of the types of spams and scams to look out for is critical, but it is also important to know what to do if their personal data are compromised. Ask students what steps they think they should take if they suspect their identity has been stolen.

Distribute the ***Steps to Take*** handout and have students work in small groups to gather research and complete the worksheet.

Invite volunteers to share their answers with the class and help students understand that taking no action when you suspect identity theft is not a good approach. It is better to address the issue and seek assistance in resolving it so that minimum financial damage is done.

WRAP UP
Shield Of Protection

5 MINUTES

Close the lesson by asking students to write a brief reflection to the following prompt: Using what you have learned in this lesson, define what you will do to help create a shield of protection for your personal data.

Extended Exploration

Note: Use the following ideas to extend financial literacy concepts throughout the school year within core content areas through English Language Arts, Math, Social Studies and Economics, and Technology activities, projects, and discussions. Duration of activities will vary.

ENGLISH LANGUAGE ARTS

Writing Prompts:

Why is cybercrime so popular? What is it about the Internet that has made it possible for thieves to expand their network of crimes?

What rights do you feel you should have as a consumer in order to keep your identity safe and protected?

What role should the government play in protecting your privacy rights?

Suggested Readings:

When a Criminal's Cover Is Your Identity: Minimizing the Risk of Identity Theft by the FDIC: Read a checklist for identity theft prevention and what to do if your identity is stolen. **www.fdic.gov/consumers/consumer/news/cnsum18/idtheft.html**

How to Spot a Scammer by the Bureau of Consumer Financial Protection: Read about ways to avoid identity theft. **www.consumerfinance.gov/about-us/blog/how-spot-scammer/**

MATHEMATICS

Activity/Project Ideas:

Have students review identity theft statistics and calculate the probability of becoming a victim of identity theft based on national averages.

SOCIAL STUDIES AND ECONOMICS

Discussion Topics:

Explore and discuss what role the government should play in protecting citizens from identity theft.

Discuss identity theft on a global level and compare how identity thieves work around the world. Use examples from the FBI's list of common fraud schemes **www.fbi.gov/scams-and-safety/common-fraud-schemes**.

Classroom activities from the Consumer Financial Protection Bureau (CFPB)

The CFPB has developed a set of classroom activities to help teachers develop and support the building blocks of financial capability in their students. Each activity is designed to be completed within a single class period and includes a teacher guide and supporting student material. Some specific activities that are relevant to this lesson include:

Defining fraud and identity theft	Students define key terms related to fraud and identity theft and create a word wall in the classroom. **www.consumerfinance.gov/practitioner-resources/youth-financial-education/teach/activities/defining-fraud-identity-theft**
Acting out fraud and identity theft	Students develop and act out skits depicting possible fraud and identity theft and ask classmates to guess which type of crime is occurring. **www.consumerfinance.gov/practitioner-resources/youth-financial-education/teach/activities/acting-fraud-identity-theft**

	Students put their developing understanding of fraud and identity theft to use as they play the role of a consumer affairs advice columnist responding to letters from readers. **www.consumerfinance.gov/practitioner-resources/youth-financial-education/teach/activities/giving-advice-consumer-protection**
Giving advice about consumer financial protection	Students design a poster or pamphlet to teach consumers what to do if their ATM, debit, or credit card or card number is lost or stolen. **www.consumerfinance.gov/practitioner-resources/youth-financial-education/teach/activities/protecting-your-money-campaign**
"Protecting your money" campaign	

Answer Key

Student Handout 1: ***Spot Identity Theft***

1. No way! They could use the number to commit fraud.
2. No way! It could be anybody trying to do damage to your login account.
3. Provide it. If you researched the institution, you know it is legitimate and OK to give information to receive the service you need.
4. Ask him to borrow a pair of scissors to cut them up before you throw them away, so no one else can get his information from them.
5. Yes, you should make sure that the number you are instructed to call is really the credit card company's phone number, and then call the phone number to find out if it is true or not.

Student Handout 2: ***This Job, Not That Job***

Job 1 is a potential scam because it does not provide full, detailed information (for example: there is no company name and the e-mail looks suspicious). The offer also sounds too good to be true at $600/week and advertising very little work needed. In contrast, Job 2 offers details about the company, including a website where applicants can verify the company's credentials, as well as training/education requirements needed to perform the job and specific hours and pay. Job 2 is more forthright in information and is transparent in expectations and hours.

Student Handout 3: ***Steps to Take***

1. *How soon should you act if you suspect identity theft?*
   Immediately! If you take action quickly, you can stop an identity thief from doing more damage.

2. *What are immediate steps you should take if you suspect identity theft?*
   Place an initial fraud alert, order your credit reports, and create an identity theft report.

3. *What is involved in each step?* Describe how each step works.
   The first step is to place an initial fraud alert. Three national credit reporting companies keep records of your credit history. If someone has misused your personal or financial information, call one of the companies and ask for an initial fraud alert on your credit report. A fraud alert is free. You must provide proof of your identity.

   The second step is to order your credit report. The credit reporting company will explain your rights and how you can get a free copy of your credit report. Order the report and ask the company to show only the last four digits of your Social Security number on your report.

   The third step is to create an identity theft report, which will help you deal with credit reporting companies, debt collectors, and businesses that gave the identity thief credit or opened new accounts in your name.

4. *What's next? After immediate action, what else can you do to ensure your identity is safe?*
   Monitor your progress and pay attention to all of your accounts.

Lesson 20: Protect Yourself

SPOT IDENTITY THEFT

Name: _____

Read each scenario and answer the questions. Check the box of the correct answer.

1. You answer the phone one evening at home. The voice on the other end is offering a free weekend trip to a ski resort, but to get your coupon you must give a credit card number. It sounds like a great idea. Do you give the number?

   ☐ Yes! I need a vacation!

   ☐ No way! They could use the number to commit fraud.

2. You receive a text message from someone who says he is in your math class, but you do not know him. He says that he needs to get on the school network to check homework, but he lost his password. He wants to "borrow" yours. Should you give it to him?

   ☐ We had homework tonight, so it must be someone from class.

   ☐ No way! It could be anybody trying to do damage to your login account.

3. You want to open a savings account at an online-only bank. But when you start filling in the information to open the account, it asks you for your Social Security Number to verify your identity. Do you provide it or consider another bank?

   ☐ Provide it. If you researched the institution, you know it is legitimate and OK to give information to receive the service you need.

   ☐ Consider another bank. You should never give out your Social Security Number.

4. Your dad just paid all the family bills for the month. He hands you a stack of bill stubs and asks you to throw them away. You should:

   ☐ Trash them. You do not want to disobey your dad.

   ☐ Ask him to borrow a pair of scissors to cut them up before you throw them away, so no one else can get his information from them.

5. You receive a letter in the mail from a well-known credit card company. It says they are "concerned about recent activity on your account" and they want to protect their customers. But you have never had a credit card with that particular company. There is a 1-800 number to call to speak with a fraud service representative. Should you call it?

   ☐ Yes, you should make sure that the number you are instructed to call is really the credit card company's phone number, and then call the phone number to find out whether it is true or not.

   ☐ No, they will ask for private information from you and you know not to give it out.

Lesson 20: Protect Yourself

THIS JOB, NOT THAT JOB

Read the job advertisements below and decide which job may be a scam and which one is the real deal. Be prepared to support your reasons.

JOB 1

Title: Customer Service Rep. (looking for HIGH-ENERGY, SMILING FACES!)

Description: Do you want to get paid now and work from home? Do you want the freedom and flexibility to spend your day the way YOU want to and earn up to $600/week? If that sounds like you, then this is the opportunity of a LIFETIME. We are hiring work-from-home customer service reps…and ALL you have to do is call our customers with a friendly and helpful style.

We PAY well — up to $600/week — and if you are the right person, you may even be able to grow into a full-time position!

What are you waiting for? E-mail us at trainingseminarpros49@tsp.com to enroll in our low-cost $49 training today! All trainings lead to BIG work…all while staying in the comfort of your own home.

JOB 2

Title: Care for Customers, Inc. hiring Customer Service Representative

Description: Care For Customers, Inc., is a full-service customer sales organization with over 50 years in business. Visit our website at www.CareForCustomersInc.com and learn about our many satisfied customers.

We are currently hiring one Customer Service Representative that has at least five years of experience in the customer service industry. A high school diploma is required, and an associate's or bachelor's degree in business, communications, or related field is a plus.

The position is part-time (20–28 hours each week) for $14.00/hour. Please send your resume and three references to jobs@CareforCustomersInc.com.

Lesson 20: Protect Yourself

STEPS TO TAKE

Name: _____

What do you do if you think your identity may have been compromised? Find out now by putting your research skills to the test. Visit the Federal Trade Commission's website at **www.consumer.ftc.gov** and locate information to complete the chart below. Be prepared to present your answers to the class.

QUESTIONS	YOUR ANSWERS
How soon should you act if you suspect identity theft?	
What are immediate steps you should take if you suspect identity theft?	
What is involved in each step? Describe how each step works.	
What's next? After immediate action, what else can you do to ensure your identity is safe?	