NEXT GEN PERSONAL FINANCE

# Middle School Course

## 7.3 Scams

## Student Activity Packet

Spanish version

| Name: | Date: |
|---|---|

# INTRO

### TALK TO A PARTNER

1. You want to enter an online contest. You could win $1,000! To enter the contest the website asks you to provide your full name, email address, social security number, and birthdate. Do you still enter the contest?

   Write your explanation in the box below. Then, discuss your reasoning with a partner.

# LEARN IT

### ARTICLE: Common Scams Targeting Children and Teens

There are many different types of scams today that target young people. Read this article to learn about some of the most common scams. Then, answer the questions.

## Common Scams Targeting Children and Teens

Many young people today spend a significant amount of time online, which makes them the perfect target for online scammers. The whole goal of a scam is to steal your personal information, your money, or both. Here are some of the most common scams young people should look out for.

1. **Online Shopping Scams**: These scams promise products or services for unbelievably low

prices - like $25 for an iPad. You provide your payment information, but the product never arrives.

2. **Fake Contests**: You pay a fee to enter the contest and provide your personal information after being told you've won…but the contest ends up being a fake.

3. **Online Quizzes**: You answer questions that are really about your personal information, which can then be used to hack into your personal accounts.

4. **Talent Scouting Scams**: You pay an entry fee and provide your personal information and even photos to join a talent contest or casting call.

5. **Pop-Up Scams**: While browsing a website, a pop up window comes up with a link. You click the link and it downloads malware or spyware onto your device, which captures personal information.

6. **Money Transfer Scams**: You receive a text from someone saying they accidentally sent you money digitally (through an app like Venmo or Cash App) and they're asking for the money back. You send the money back but later realize that you never received their original payment.

7. **Online Gaming Scams**: You share personal information to get free in-game currency, "skins", or other gaming features. You may also click on links that download malware or spyware.

8. **Financial Aid Scams**: While applying for scholarships, grants, or financial aid you provide your banking information to pay an application and processing fee. Sometimes, you might even receive a fake check but then be asked to send a part of the money back to pay taxes or fees. By the time you've cashed the check and discovered it's fake, you've already made a payment.

9. **Phishing Texts**: You receive text messages urgently asking you to fix an issue in your social media or banking accounts. You click the link in the text which downloads malware onto your mobile device.

10. **"Free" Service Scams**: You sign up for a service that claims to be free, but it really charges you a regular fee.

11. **Explicit Image Scams**: Scammers pose as friends or people who want to start a relationship and ask young people to share explicit images. They then threaten to share the explicit images unless the victim provides payment.

**Protect Yourself:**

- Be aware of the types of scams and their warning signs
- Shop only on trusted sites
- Do not click on links in emails, texts, or pop-ups
- Do not share your (or a family member's) personal information (address, birthday, phone numbers, etc.)
- Do not share passwords, even with friends

Source

1. Why do you think it's so important to educate yourself on the different types of scams?

2. What is one thing you can do better to protect your personal information?

**VIDEO: What is Phishing?**

1. Pretend you are teaching your younger sibling about phishing. What would be your kid-friendly definition?

2. What are some signs that an email is a phishing email?

# DO IT

## ANALYZE: Phishing Clues

As you just learned, phishing is when scam artists send fake text, email, or pop-up messages to get people to share their personal and financial information. Criminals use the information to commit identity theft. Let's learn more about how to identify a phishing message.

### PART ONE: REVIEW - Phishing Clues

Review the phishing clues below. These clues help you identify phishing scams.

- ***Unexpected cash/prize***
- ***Claims there is problem with your account***
- ***Sense of urgency***
- ***Misspellings/Grammatical errors***
- ***Incorrect web address***
- ***Message not addressed to you personally***
- ***Unusual download extension***

### PART TWO: ANALYZE - Phishing Scams

As you've learned, it is important you know how to identify phishing scams. Follow your teacher's directions to complete the activity using the list of phishing clues you reviewed in Part One and the examples provided by your teacher.

1. Which phishing clues can you identify in Example #1 that confirm it is a scam? Explain.

2. Which phishing clues can you identify in Example #2 that confirm it is a scam? Explain.

3. Which phishing clues can you identify in Example #3 that confirm it is a scam? Explain.

4. Which phishing clues can you identify in Example #4 that confirm it is a scam? Explain.

5. Which phishing clues can you identify in Example #5 that confirm it is a scam? Explain.

## EXIT TICKET

1. In your own words, explain what a scam is.

2. Describe a type of scam that often targets young people.

3. What is one thing someone can do to protect their personal information?