Scams and Schemes

Essential Question

What is identity theft, and how can you protect yourself from it?

Lesson Overview

Students learn strategies for guarding against identity theft and scams that try to access their private information online. They learn what identity theft is, what kinds of information identity thieves want, and what can be done with that information. Students then analyze phony emails and identify tricks that identity thieves use online. Finally, they create a phishing email that includes the features that they have learned about, and see if classmates can identify the scams.

Learning Objectives

Students will be able to ...

- understand what identity theft is and why it is important to guard against it.
- learn to recognize strategies that scam artists use to access private information.
- learn how to guard against phishing and identity theft.

Materials and Preparation

- Paper and markers or colored pencils (or computers with Microsoft Office if you are using the high-tech option in Teach 3).
- Copy the **Spotting Scams Student Handout**, one for each student.
- Review the **Spotting Scams Student Handout — Teacher Version**.

Family Resources

- Send home the **Online Security Family Tip Sheet (Middle & High School)**.

Estimated time: 45 minutes

Standards Alignment –

Common Core: RI.6-8.1, RI.6-8.4, RI.6-8.10, W.6-8.4, W.6-8.7, W.6-8.10, SL.6-8.1a-d, SL.6-8.4, SL.6-8.6, L.6-7.3a, L.6-8.6

NETS•S: 1a-c, 2a, 2d, 4a, 4d, 5a, 6a

Key Vocabulary –

scam: an attempt to trick someone, usually with the intention of stealing money or private information

identity theft: a type of crime in which your private information is stolen and used for criminal activity

vulnerable: in a position that makes it easier for you to be harmed or attacked

phishing: when people send you phony emails, pop-up messages, social media messages, texts, calls, or links to fake websites in order to hook you into giving out your personal and financial information

introduction

Warm-up *(5 minutes)*

ASK:

Do you know someone who has been scammed? What happened?	Students might tell stories of instances in which someone has been convinced to send someone else money or purchase a fake or bad product.
What is the purpose of a scam? What tricks do people use to carry out a scam?	Students should understand that the ultimate purpose of a scam is to get someone to give the scammer money, or information that can help the scammer steal money, such as a credit card number, ATM code, or password. To accomplish this, scammers tell lies and often pretend to be someone they are not.
Can people get scammed on the Internet? How?	Allow students to tell stories of friends or relatives who have been scammed online. Then encourage them to revisit what they know about scams, and how they might be used online. Sample responses: • Someone can be tricked into buying a bad or fake product online • Someone can be lured into sharing information that a scammer can use to steal from them

EXPLAIN to students that they will be learning about a variety of online scams, including which kinds of information scammers look for, and how that information can be used. They will also learn how to protect themselves against online scams.

teach 1

What Is Identity Theft? *(10 minutes)*

POINT OUT to students that people who scam others online don't always have to get money from them directly. Instead, they use a variety of strategies to trick people into giving out private information. They then use this information to access their bank and credit card accounts or other personal accounts. They can even "re-create" someone's identity and produce false documents, such as Social Security cards, credit cards, or drivers' licenses in someone else's name.

DEFINE the Key Vocabulary term **identity theft**.

ASK: *Can you guess what kinds of personal information identity thieves might look for?*

REVIEW the list below with students. Emphasize that identity thieves look for any information that might help them pretend to be their victims. Write the list on the board or have students take notes.

- Full name
- Date of birth and where you were born
- Current and previous addresses and phone numbers
- Driver's license or passport number
- Account numbers and the companies where you hold accounts (e.g., Amazon, PayPal, etc.)
- Passwords
- Social Security number

DEFINE the Key Vocabulary term **vulnerable**.

EXPLAIN that *anyone* is vulnerable to an online scam. Although teens might not think they're at risk, there are a few important reasons why they are vulnerable to identity theft – and why it matters. Cover the following points:

- Identity thieves look for "clean" Social Security numbers that haven't yet been used to get credit. They target teens and kids, who often have Social Security numbers that have no credit history yet. Identity thieves might sell or use these numbers, which would allow someone else to get a credit card or loan and build up debt under your name.
- Being a victim of identity theft can ruin your financial future and your ability to obtain loans and purchase things. For example, it could affect your ability to get a student loan for college or a loan to buy a car.
- In addition, if you use your parents' accounts and credit cards online, or fill out forms with your parents' information, you are sharing information that could potentially put your parents' identities at risk.
- It can take months, even years, to recover your identity if it's stolen. Cleaning up such a mess takes a lot of time and energy, and it can also be expensive.

teach 2

How to Catch a Phish *(15 minutes)*

ASK:

How do you think identity thieves might try to get your information?

Encourage students to share some responses, even if they have not previously encountered identity theft.

DEFINE the Key Vocabulary term **phishing**.

EXPLAIN to students that the best way to avoid phishing scams is to be skeptical about any online request for personal information. It's also good to be skeptical of online messages or posts from friends that seem out of character for them, which is a warning sign that their accounts have been hacked. There are clues that can help students spot phishing, and they will learn some of these in the next part of the lesson by studying one type of phishing scam: a phony email message.

DIVIDE students into pairs.

DISTRIBUTE the **Spotting Scams Student Handout**, one per student.

READ aloud the instructions found on the **Spotting Scams Student Handout – Teacher Version**, and share with students the extended explanation of each feature of a phishing email.

INSTRUCT student pairs to complete the handout together. When students are done, have two pairs get together to exchange their handouts and compare their answers.

INVITE volunteers to share their answers with the class. Use the **Spotting Scams Student Handout – Teacher Version** for guidance.

REMIND students that phishing emails can be very convincing, and some may not contain many of the clues they just learned about. So it's smart to distrust any email that asks them to provide private information.

teach 3

Protect Yourself from Online Scams *(10 minutes)*

TELL students that if they ever encounter something online that they believe might be a phishing scam, they should observe the following rules:

- Avoid opening the message or email in the first place
- Don't click on any links or download any attachments. They might contain viruses or spyware.
- Don't reply
- Mark as "junk mail" or "spam" for your email provider, or report it to your social network site.
- If you are concerned about an account you have with a company, contact its customer service by phone. Make sure you verify the company's contact information elsewhere online first.

TELL students that they can also protect themselves from Internet scams by learning how identity thieves think. They will create a phishing email, or some other form of online or mobile scam, using what they learned about phishing scams.

Optional: You may wish to show students examples of real phishing emails from Consumer Fraud Reporting before students create their own examples (http://www.consumerfraudreporting.org/phishing_examples.php). Some examples of popular scams on Facebook can be found in the online Huffington Post article, "Facebook Scams You Need to Know About" (www.huffingtonpost.com/2011/05/22/facebook-scams-hacks-attacks_n_864906.html#s281483&title=Fake_Page_Spam).

INSTRUCT students to choose at least four of the eight features of a phishing email listed in their **Spotting Scams Student Handout**. Have them create a phishing email that demonstrates the four features they choose to highlight.

INVITE students to present their examples to the class. Classmates can try to identify which features tipped them off to the fact that this is a phishing email. Alternatively, students can trade examples with a partner and try to spot each other's scam.

closing

Wrap-up *(5 minutes)*

You can use these questions to assess your students' understanding of the lesson objectives. You may want to ask students to reflect in writing on one of the questions, using a journal or an online blog/wiki.

ASK:

What kinds of information do identity thieves look for – and why?	Students should respond with examples of private information, such as full name, address, date of birth, account numbers, and passwords. Identity thieves try to use this information in order to "re-create" someone's identity for unlawful purposes, mainly to secure loans and buy things.
How do thieves try to get at your information?	Thieves use phishing to try to get at people's personal information. Have students discuss some of the features of phish ing they learned about.
What can you do to avoid falling for online scams?	Students should remember to be suspicious of any online communication that asks for private information, or that seems out of character for a friend to have sent or posted. Students should know not to reply to such messages, not to click on any links or attachments, and to report the message as spam or junk to their email provider or social network site. If they are concerned about one of their accounts, they should call the company's customer service department using a number they found elsewhere online – not within the message they received.

WRITE the following URL and email address below on the board. Tell students that they can go to www.ftc.gov/idtheft for help if they, or their parents, find their identities have been stolen. Students can also forward any spam emails they receive to spam@uce.gov.

Extension Activity

Have students visit OnGuardOnline (www.onguardonline.gov). Instruct them to click on "games" and play the "Spam Scam Slam" game. This game is a great way to extend learning about phishing schemes. Afterward, invite students to share one new thing they learned about email scams.

At-Home Activity

Have students work with a parent or adult family member to come up with a set of security rules for their home computers and/or computers that family members use at school, work, or the library. In addition to the strategies they learned in class, students should research additional security rules at OnGuardOnline (www.onguardonline.gov/articles/0009-computer-security). After they have compiled their set of rules, students should take one concrete step toward improving their online security – for example, changing passwords or backing up files. You may wish to have students share their rules with the class, and then invite volunteers to combine them to create an online security poster to display in the classroom.

Scams and Schemes

Directions

Each of the following email messages is an example of a phishing scam. Read the features of a phishing email below. Then circle or highlight any examples of those features in each of the three messages. List the features in the blank spaces provided, and draw a line connecting each feature to the part of the email it relates to.

Features of a Phishing Email

- Need to verify account information
- Link in email or attachment
- Sense of urgency
- Too good to be true
- Spelling errors
- Generic greeting
- Account is in trouble

Email Message

From: no_reply@emailinternet.chase.com
Subject: Account Status

Attention US Bank Customer,

Due to a recent security check on your account, we require you to confirm your details. Failure to do so within 24 hours will lead to account suspension. Sorry for the inconveenince.

Click here to confirm your account

Regards,
US Bank Online Customer Service

This email has been sent by US Bank.

Phishing Features

Email Message

Phishing Features

From: custservice@paypalonline.com
Subject: We've Limited Your Account

Dear PayPal User,

We recently noticed one or more attempts to log into your account from a foreign IP address. For security reasons, we have limited access to your account.

If you did not initiate the log ins, please visit PayPal Online urjently perform the steps necessary to verify you are the account holder. Performing this action will lift the limited access and restore your account.

https://www.paypal.com/us/cvi-limit/webscr?-run

Sincerely,
PayPal Security and Theft

From: Swiss International Lottery
Subject: Award Notification

Dear [Firstname Lastname],

Congratulations! You may receive a certified check for up to $500,000,000 U.S. Cash! One lump sum! Tax free! Your odds of winning are 1-6. Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want!

If you choose to receive your winnings please contact IMB INSURANCE & BROKERS. They will use their diplomatic courier service to deliver your check. Please contact them with the following details below:

Company name: IMB INSURANCE & BROKERS

Address: Geneva, Switzerland
Contact Person: Mr. Alexander Caspari
(Director Foreign Remittance Department)
Direct Tell: +44-802 655 4889
Fax: +44-802 655 4890
Direct Email: ACaspari@IMBInsurancebrokers.com
Congratulations again!
Marcus Gohl

Scams and Schemes

Directions

Each of the following email messages is an example of a phishing scam. Read the features of a phishing email below. Then circle or highlight any examples of those features in each of the three messages. List the features in the blank spaces provided, and draw a line connecting the feature to the part of the email it relates to.

Features of a Phishing Email

Need to verify account information: Phony emails will try to trick you into giving up account information, passwords, or clicking on a phishing link, where you fill out information that identity thieves can collect and use. Usually what they're asking for doesn't make sense if you think about it, because they should already have that information!

Sense of urgency: When the message says you only have a limited time to respond, it is often the sign of a scam.

Spelling errors: Scam emails often include spelling and grammatical errors. A real company would not send out messages containing such errors.

Account is in trouble: Identity thieves try to make you worry that something is wrong with your account, so you will feel you must immediately respond to the email to fix it.

Link in email or attachment: Phishing emails often have a link within the email or an attachment that you are urged to click on. This link can lead you to a site or form where you (unknowingly) give your information to criminals. You should never respond to or click on links in such emails. Instead, go directly to the main website, and from there check your account.

Too good to be true: Scam emails often offer things that are too good to be true, like the easy chance to win free money or prizes.

Generic greeting: You might see a generic greeting that does not personally address you. Reputable companies send emails where they address their customers by name.

Email Message

Phishing Features

From: no_reply@emailinternet.chase.com
Subject: Account Status

Attention US Bank Customer,

Due to a recent security check on your account, we require you to confirm your details. Failure to do so within 24 hours will lead to account suspension. Sorry for the inconveenince.

Click here to confirm your account

Regards,
US Bank Online Customer Service

This email has been sent by US Bank.

- Generic greeting
- Need to verify account info
- Sense of urgency
- Spelling errors
- Link in email

From: custservice@paypalonline.com
Subject: We've Limited Your Account

Dear PayPal User,

We recently noticed one or more attempts to log into your account from a foreign IP address. For security reasons, we have limited access to your account.

If you did not initiate the log ins, please visit PayPal Online urjently perform the steps necessary to verify you are the account holder. Performing this action will lift the limited access and restore your account.

https://www.paypal.com/us/cvi-limit/webscr?-run

Sincerely,
PayPal Security and Theft

- Account is in trouble
- Spelling errors
- Need to verify account info
- Sense of urgency
- Link in email

From: Swiss International Lottery
Subject: Award Notification

Dear [Firstname Lastname],

Congratulations! You may receive a certified check for up to $500,000,000 U.S. Cash! One lump sum! Tax free! Your odds of winning are 1-6. Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want.

If you choose to receive your winnings please contact IMB INSURANCE & BROKERS. They will use their diplomatic courier service to deliver your check. Please contact them with the following details below:

Company name: IMB INSURANCE & BROKERS

Address: Geneva, Switzerland
Contact Person: Mr. Alexander Caspari
(Director Foreign Remittance Department)
Direct Tell: +44-802 655 4889
Fax: +44-802 655 4890
Direct Email: ACaspari@IMBInsurancebrokers.com
Congratulations again!
Marcus Gohl

Generic greeting

Too good to be true

Link in email

Scams and Schemes

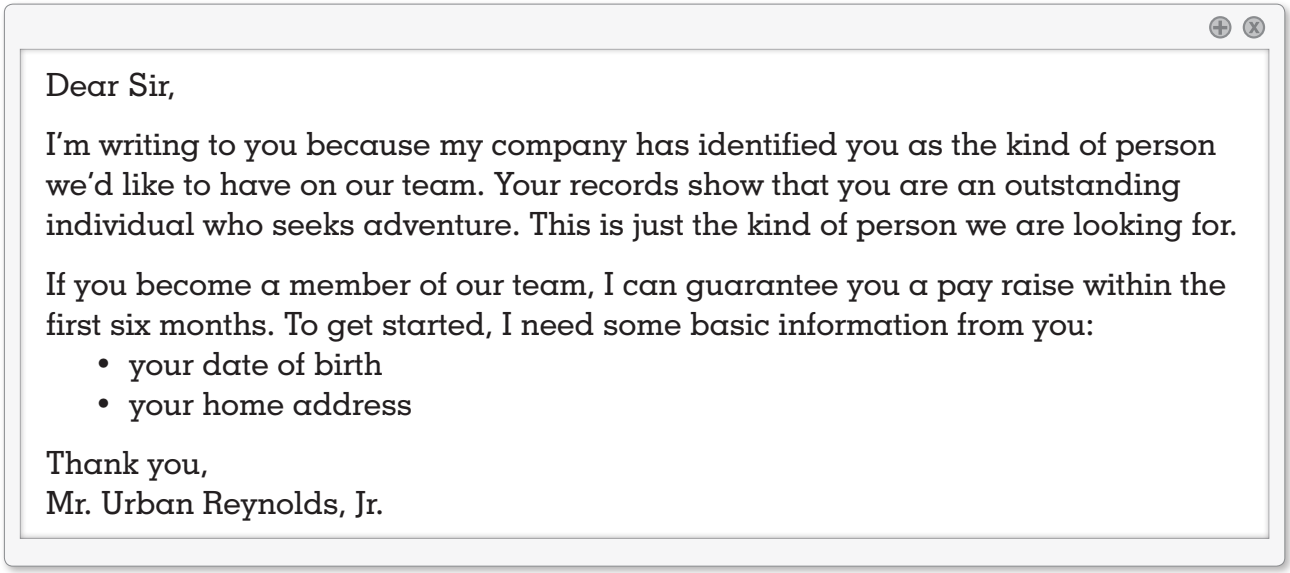
1. A type of crime in which your private information is stolen and used for criminal activity is called:

a) Identification

b) Identity theft

c) Burglary

2. Evan sees the following message in his inbox:



Dear Sir,

I'm writing to you because my company has identified you as the kind of person we'd like to have on our team. Your records show that you are an outstanding individual who seeks adventure. This is just the kind of person we are looking for.

If you become a member of our team, I can guarantee you a pay raise within the first six months. To get started, I need some basic information from you:

- your date of birth
- your home address

Thank you,
Mr. Urban Reynolds, Jr.

Which of the following is NOT a warning sign that this message is a scam:

a) The offer sounds too good to be true

b) It asks Evan for his private information

c) Evan is addressed as "Sir"

3. Sara finds a message on her phone that she thinks might be a scam. She should:

a) Forward the message to her friends to see if they think it's a scam too

b) Reply and ask the sender not to send more mail

c) Delete the message

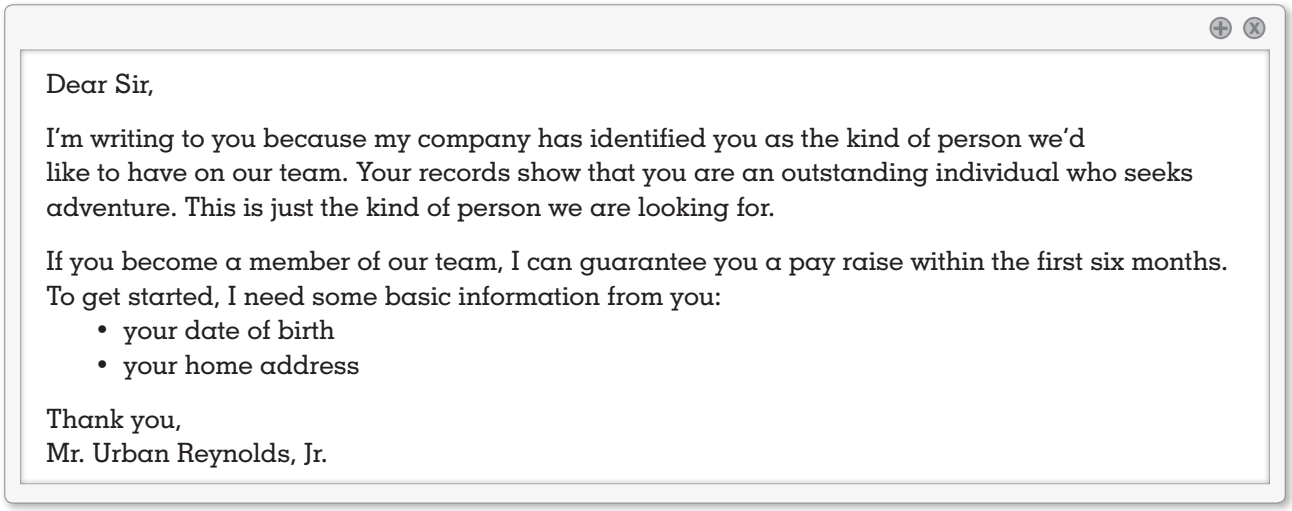
Scams and Schemes

1. A type of crime in which your private information is stolen and used for criminal activity is called:

a) Identification
b) Identity theft
c) Burglary

Answer feedback
The correct answer is **b**. You can help protect yourself from identity theft by watching out for online offers designed to trick you, and by guarding your private information.

2. Evan sees the following message in his inbox:



Dear Sir,

I'm writing to you because my company has identified you as the kind of person we'd like to have on our team. Your records show that you are an outstanding individual who seeks adventure. This is just the kind of person we are looking for.

If you become a member of our team, I can guarantee you a pay raise within the first six months. To get started, I need some basic information from you:

- your date of birth
- your home address

Thank you,
Mr. Urban Reynolds, Jr.

Which of the following is NOT a warning sign that this message is a scam:

a) The offer sounds too good to be true
b) It asks Evan for his private information
c) Evan is addressed as "Sir"

Answer feedback
The correct answer is **c**. Offers that seem too good to be true or that ask for private information may be scams. These kinds of messages should be marked as spam and deleted.

3. Sara finds a message on her phone that she thinks might be a scam. She should:

a) Forward the message to her friends to see if they think it's a scam too
b) Reply and ask the sender not to send more mail
c) Delete the message

Answer feedback
The correct answer is **c**. If Sara thinks the message might be a scam, she should delete it.