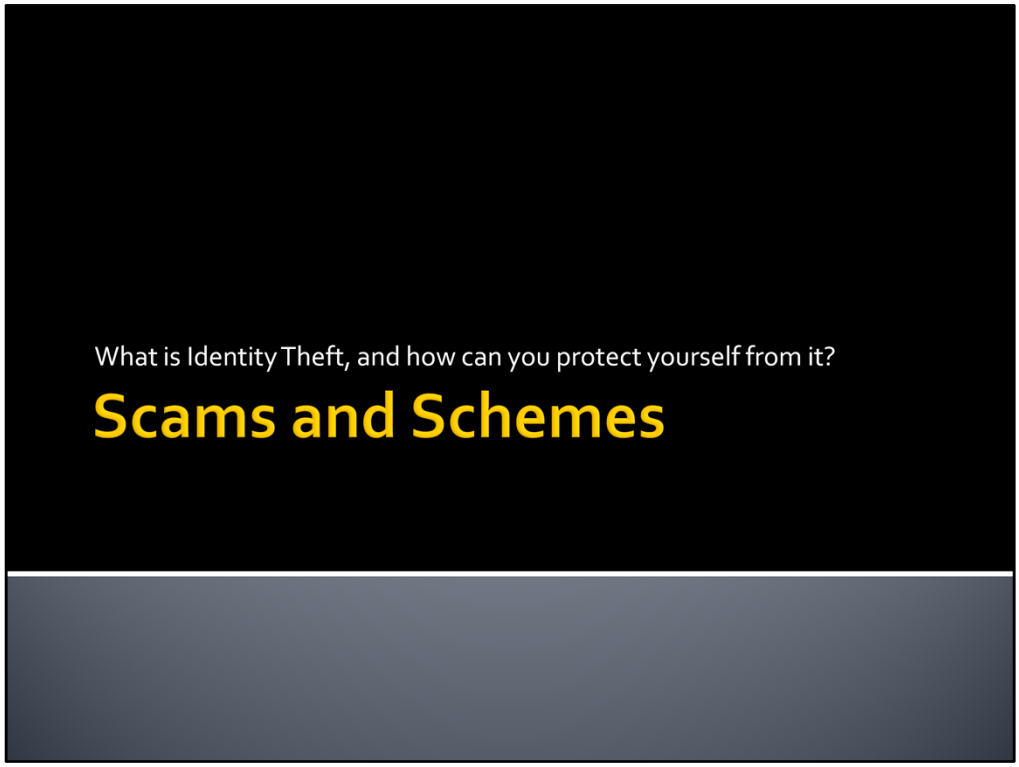
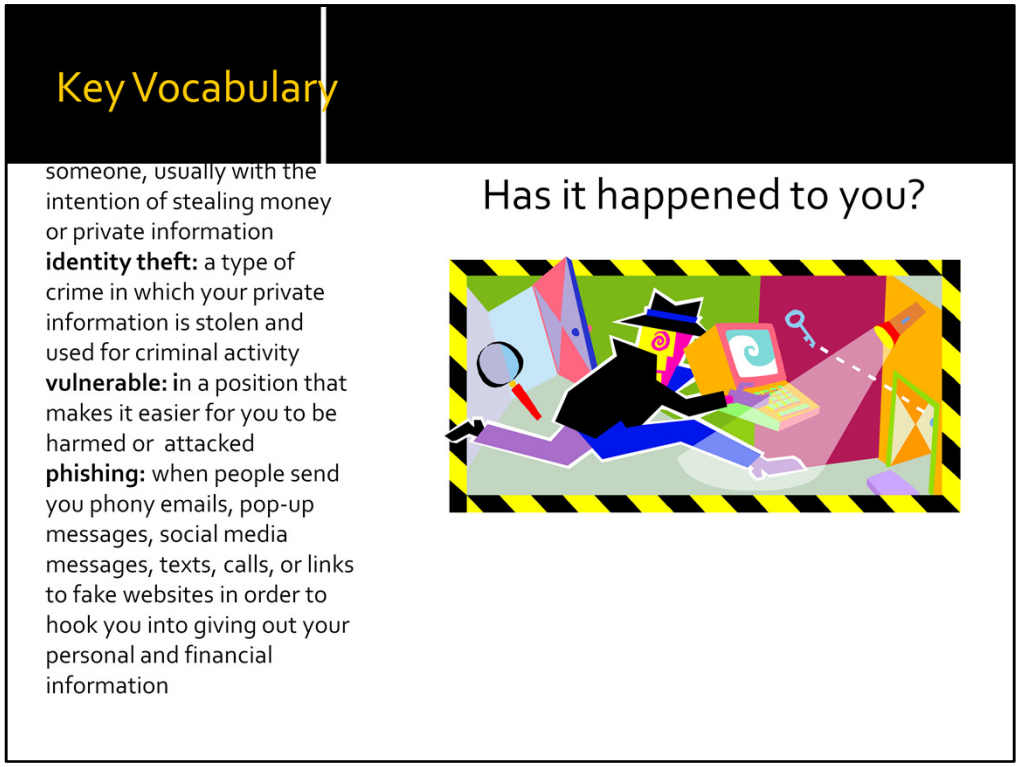


Lesson Overview

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.

Lesson Objectives

- 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.



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

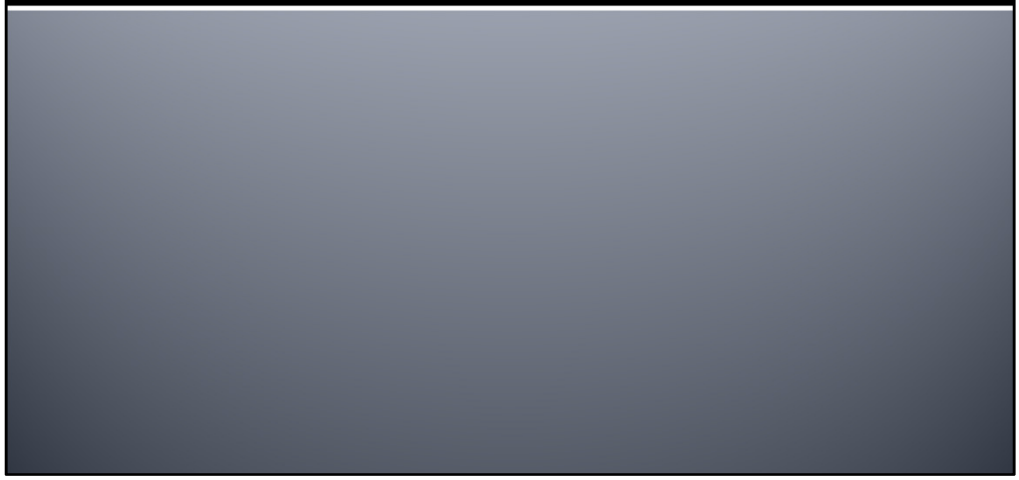
Someone can be lured into sharing information that a scammer can use to steal from them

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.

What is Identity Theft?

What is your identity, how can it be stolen?



Your Identity:

- Full Name
- Date and Location of Birth
- Current and Previous Street Address
- Home/Cell Number
- Driver's License/Passport/ Social Security Number
- Bank/Credit Account Numbers
- Username/Passwords

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. Emphasize that identity thieves look for any information that might help them pretend to be their victims.

Identity Scams:

- 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
- 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.

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

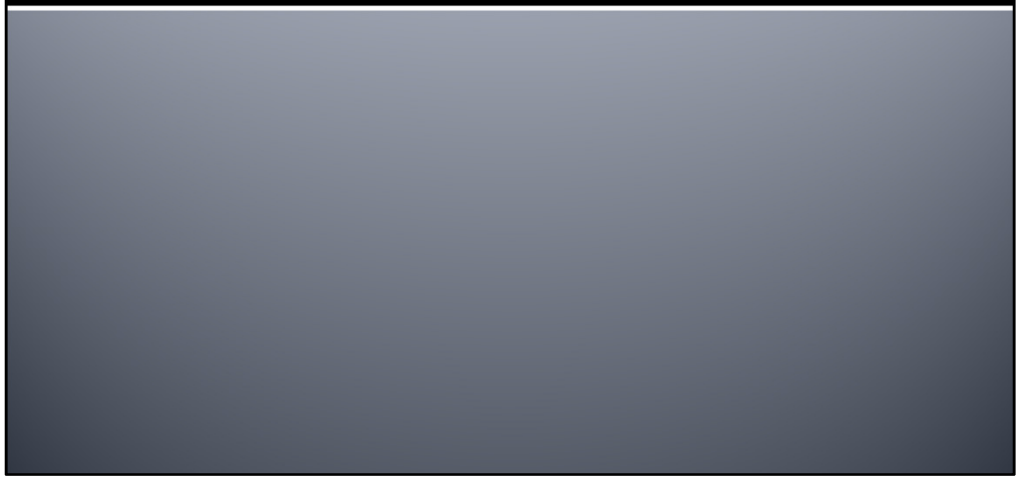
Identity Scams:

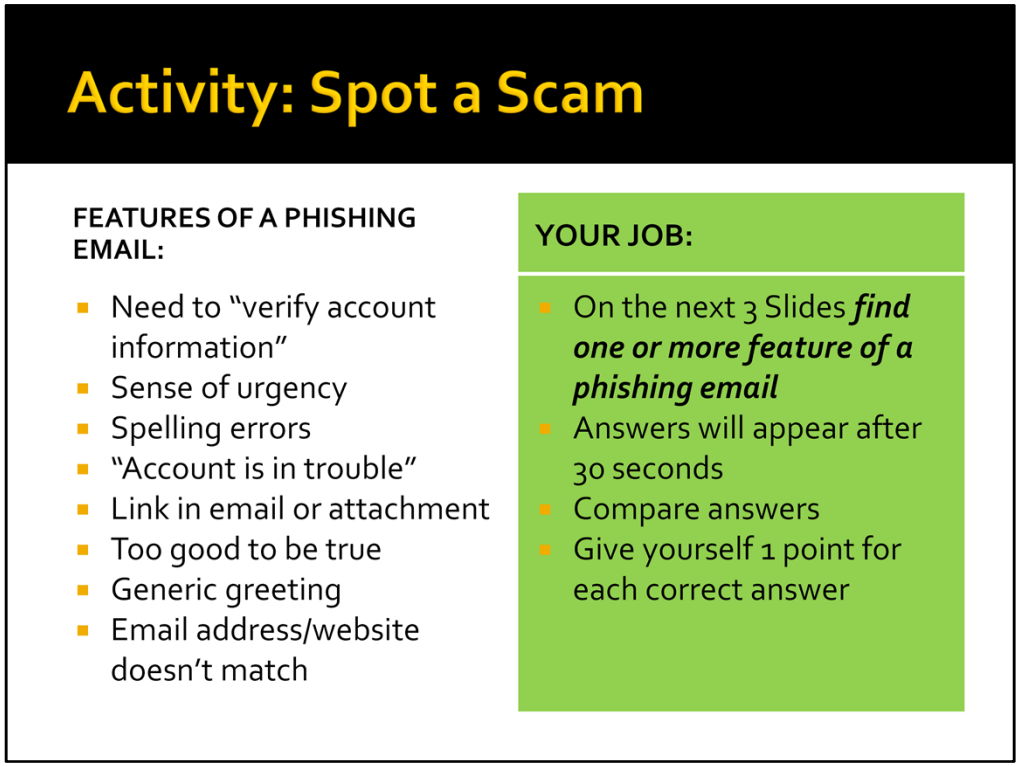
- If children use parents' accounts and credit cards online, or fill out forms with parents' information, they are sharing information that could potentially put parents' identities at risk.
- It can take months, even years, to recover your identity if it's stolen. Cleaning up such a mess takes a lot of time and energy, and it can also be expensive.

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

How to Catch a Phish…

How identity thieves try to get your information?





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.

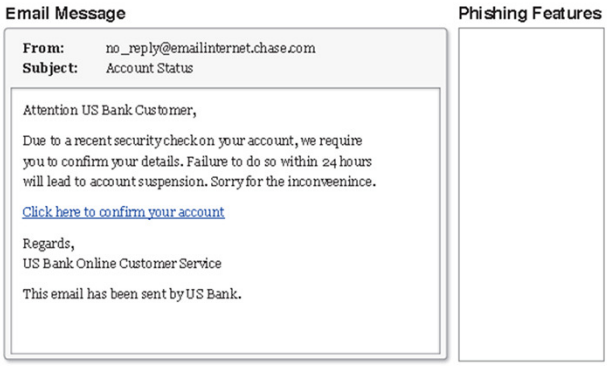
Account is in trouble: Identity thieves try to make you worry that something is wrong with your account, so you will feel you must immediately respond to the email to fix it.

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.

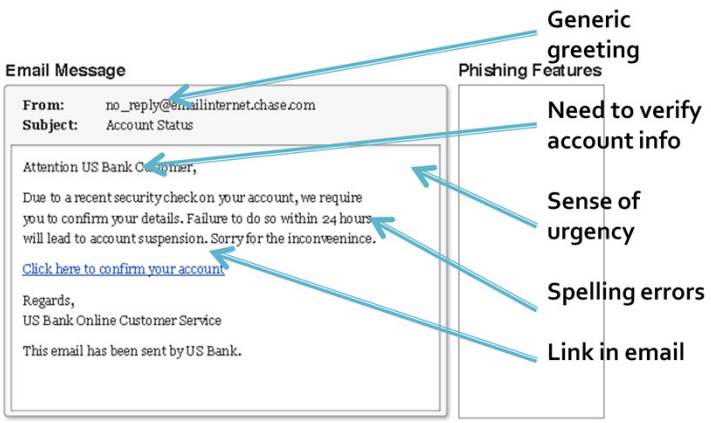
Email Address/Website Address does not match the company name the email is supposedly from: www.yahoo.com is www.link.mail.com or yahoomailnow.com

Activity: Email # 1



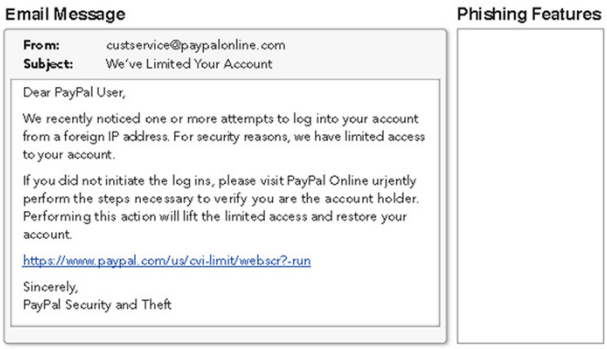
Student(s) should read emails carefully and identify features that would help them determine that this is a phishing/scam email. If session is in-person, a handout with the emails and instructions can be printed for each participant. Handouts and lesson plan will be available on http://ccis.ccsdtitle1.org website and from http://commonsensemedia.org

Activity: Email # 1



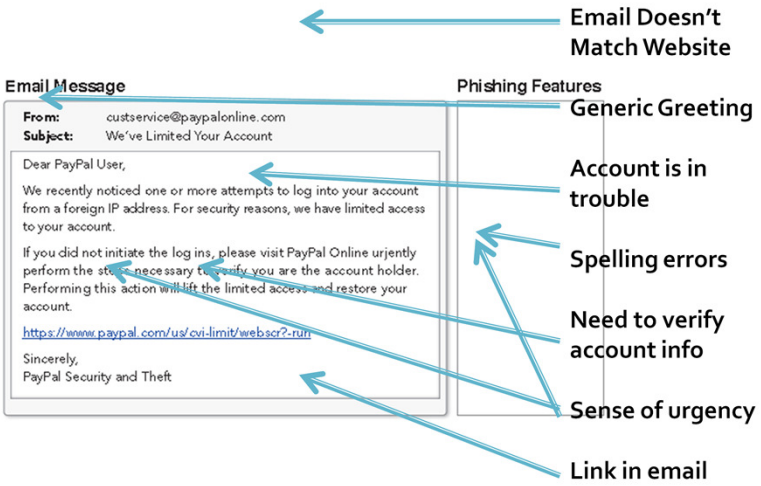
Students may find additional features or have alternative reasoning.

Activity: Email # 2



Student(s) should read emails carefully and identify features that would help them determine that this is a phishing/scam email. If session is in-person, a handout with the emails and instructions can be printed for each participant. Handouts and lesson plan will be available on http://ccis.ccsdtitle1.org website and from http://commonsensemedia.org

Activity: Email # 2



Students may find additional features or have alternative reasoning.

Activity: Email #3

Email Message

From: Swiss International Lottery
Subject: Award Notification

Dear [Firstname Lastname],

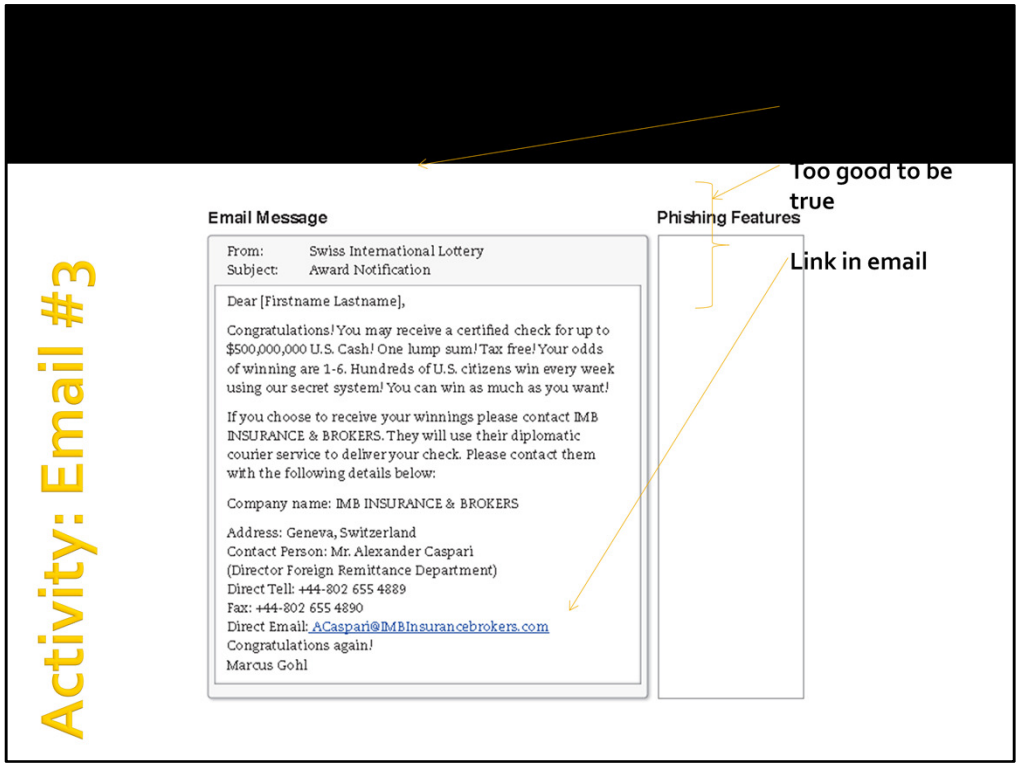
Congratulations! You may receive a certified check for up to $500,000,000 U.S. Cash! One lump sum! Tax free! Your odds of winning are 1-6. Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want!

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

Phishing Features



Also point out lack of clarity in this email, at first it says you MAY receive a check but in the next paragraph it tells you to contact a third party to receive your winnings and does not provide contact information for the primary company – the people who are awarding the prize.

Protect Yourself from Scams

The next step…

How to be Scam-Free

- Avoid opening emails/messages from strangers
- Read all emails looking for signs of phishing
- Do not click links or open attachments from spam or phishing emails
- Don't reply to spam/phishing emails
- Report phishing or "mark as spam"
- Find accurate phone numbers for your accounts and verify over the phone if you have questions (do not use the phone number from the email)

Think like a Phish…

A final activity to help you avoid scams and schemes.

Ask yourself:

- What kind of information do identity thieves look for? Why?
- How do thieves try to get that information?
- What can I do to avoid scams?

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 phishing they learned about.

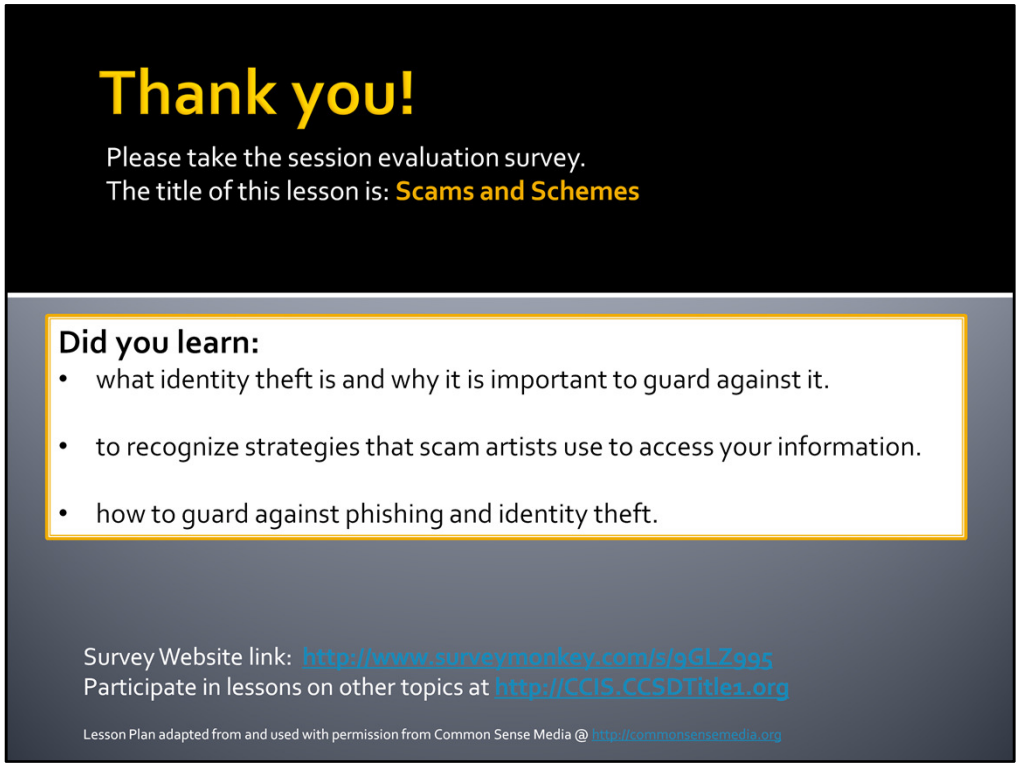
What can you do to avoid falling for online scams?
Students should remember to be suspicious of any online communication that asks for private information, or that seems out of character for a friend to have sent or posted. Students should know not to reply to such messages, not to click on any links 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.

Now try it yourself:

- Use 4 or more of the following features of phishing emails/scams and CREATE YOUR OWN phishing email
- Now, share that email and see if someone else can spot the scam! (Do not send via email or prank anyone, use this email to teach someone what you have learned.)

Other Sites to Visit:

- www.ftc.gov/idtheft - Federal Trade Commission ID Theft website
- www.OnGuardOnline.gov – additional security measures recommended by the government
- www.ccis.ccsdtitle1.org – view the other lessons we have for you!



Survey Monkey Evaluation Survey: http://www.surveymonkey.com/s/9GLZ995