



OBJECTIVE 47.3

INTERNET SAFETY

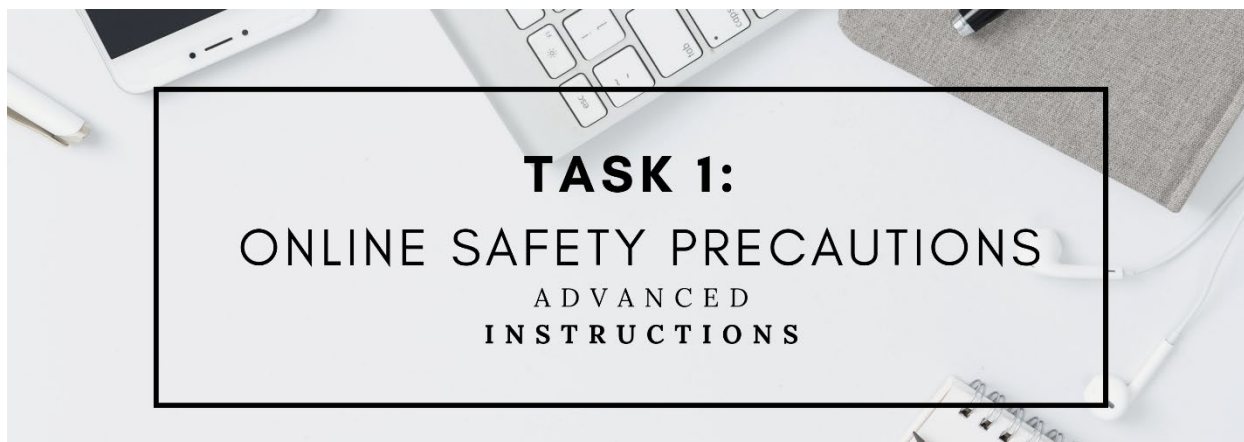
Teacher Resources

Task 1: Describe online safety precautions

Task 2: Write about Internet safety

Level: Advanced

Created for MSJC Adult Ed 2019-2020



Language and Literacy Objectives

Research, read and summarize literature pertaining to online ethics and the effects of the Internet on society and culture.

Read about and/or discuss issues, consequences & solutions related to using the Internet at home, school or work.

Identify common online safety issues and crimes (e.g. copyright infringement, plagiarism, fraud, identity theft, victimization of children,).

Identify vocabulary and/or describe actions and precautions that can be taken to reduce online risks such as identity theft, victimization of children (e.g. change password frequently).

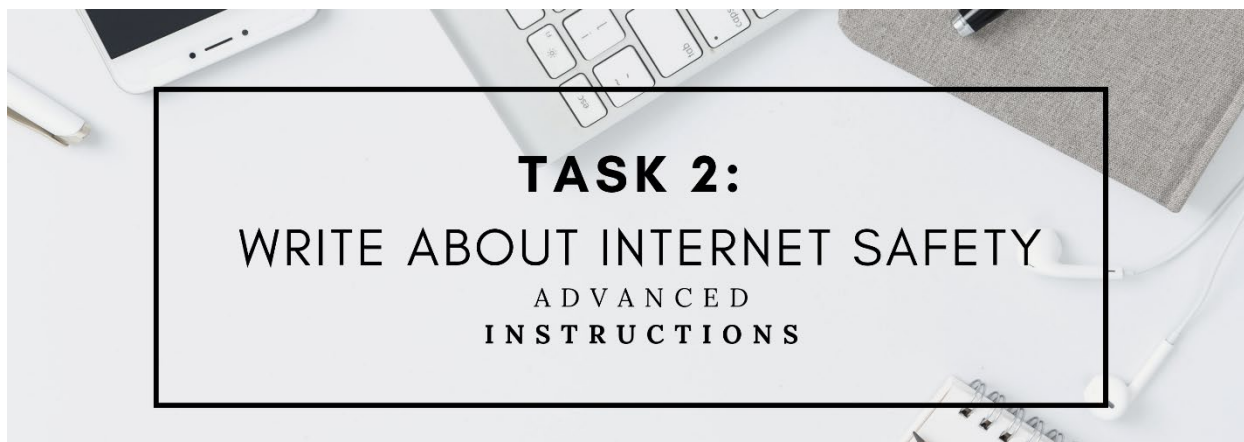
Introduction

Students will learn about precautions they can take online, cyber crimes, and privacy and security.

Task

Student talks about precautions they can take to avoid online risks and use the Internet safely.

Advanced: Describe 6 precautions to take online.



Language and Literacy Objectives

Research, read and summarize literature pertaining to online ethics and the effects of the Internet on society and culture.

Read about and/or discuss issues, consequences & solutions related to using the Internet at home, school or work.

Identify common online safety issues and crimes (e.g. copyright infringement, plagiarism, fraud, identity theft, victimization of children,).

Identify vocabulary and/or describe actions and precautions that can be taken to reduce online risks such as identity theft, victimization of children (e.g. change password frequently).

Introduction

Students will learn about internet crimes and how to prevent them.

Task

Student will complete an authentic writing task. 1) Describe a common cyber crime, 2) give detailed examples to illustrate how to prevent it, and 3) give reasons why it is important to prevent that particular cyber crime.



TASKS 1 & 2:

47.3 INTERNET SAFETY

ADVANCED
RESOURCES

Resources Provided:
<ul style="list-style-type: none">- Vocabulary (Quizlet)- Conversation Questions- Internet Safety Tips- Presentation: Internet Crimes and Wrongdoings- Helpful Video Presentations- Activity: FlipGrid- Task Practice- Scams and Schemes Packet (Phishing information and practice)- Digital Citizenship Packet

Vocabulary

https://quizlet.com/_7rds8n?x=1jqt&i=23gz6j

Cyber crime: illegal activity that involves the use of computers or the Internet

Fraudulent: intended to deceive people in an illegal way, in order to gain money, power, etc.

Risk: possibility that something bad, unpleasant, or dangerous could happen

Precaution: something you do in order to prevent something dangerous or unpleasant from happening

“red flag”: something that shows or warns you that something might be wrong or illegal

Personal information: facts or details about you, such as birth date, phone number, address, account numbers, passwords, etc.

Bitcoin: digital or virtual currency that uses peer-to-peer technology to facilitate instant payments that is untraceable

Wifi: technology allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area

Instant message: allows you to quickly exchange written messages with people you know

Craigslist: centralized network of online communities, featuring free online classified ads, with sections devoted to jobs, housing, personal ads, for sale, services, etc.

Social media: websites and applications that enable users to create and share content or to participate in social networking, such as Instagram, Snapchat, Facebook, etc.

Computer updates: updating your operating system brings it up-to-date with the latest drivers, system utilities, and security software

Web browser: an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

Virus: A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself, a virus is deployed by attackers to damage or take control of a computer

Antivirus: a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Firewalls: a part of a computer system or network which is designed to block unauthorized access while permitting outward communication.

VOCABULARY

Internet Safety 47.3



1 **CYBER CRIME / INTERNET CRIME**

illegal activity that involves the use of computers of the Internet



2 **FRAUDULENT**

intended to deceive people in an illegal way, in order to gain money, power, etc.

3 **RISK**

possibility that something bad, unpleasant, or dangerous could happen



4 **PRECAUTION**

something you do in order to prevent something dangerous or unpleasant from happening



5 **"RED FLAG"**

something that shows or warns you that something might be wrong or illegal

6 **VIRUS**

A computer virus, much like a flu virus, is designed to spread from host to host. Deployed by attackers to damage or take control of a computer.



7 **PERSONAL INFORMATION**

facts or details about you, such as birth date, phone number, address, account numbers, passwords, etc.



8 **WI-FI**

technology allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area



VOCABULARY

Internet Safety 47.3



9

WEB BROWSER

an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

10

COMPUTER UPDATES

updating your operating system brings it up-to-date with the latest drivers, system utilities, and security software



11

INSTANT MESSAGE

allows you to quickly exchange written messages with people you know (faster than email!)

12

SOCIAL MEDIA

websites and applications that enable users to create and share content or to participate in social networking, such as Instagram, Snapchat, Facebook, etc.



13

CRAIGSLIST

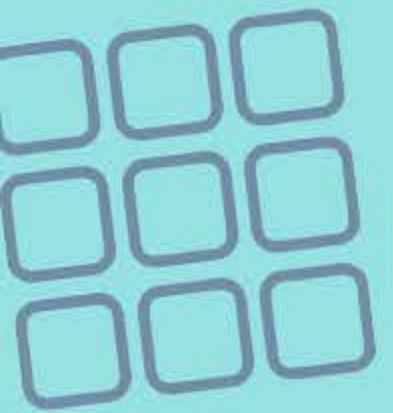
centralized network of online communities, featuring free online classified ads, with sections devoted to jobs, housing, personal ads, for sale, services, etc.



14

ANTIVIRUS SOFTWARE

a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.



15

FIREWALL

a part of a computer system or network which is designed to block unauthorized access while permitting outward communication



16

BITCOIN

digital or virtual currency that uses peer-to-peer technology to facilitate instant payments that is untraceable

Conversation Questions

(modified from <http://iteslj.org/questions/internet.html>)

What are some security issues you must think about when you access the Internet?

How can the internet help you learn English? Do you take advantage of this?

Have you or anyone you know been the victim of a cyber crime? What happened?

Do you think it's possible to prevent certain kinds of cyber crimes? Which ones and how?

What should the penalty be for cyber criminals?

How have science and technology changed what crimes are committed? How about the way we solve them?

Where is the best place to put the family computer?

What should you do if you or a family member is being stalked or bullied online?

Why should you be careful about giving out personal information to people that you meet online?

Are older people disadvantaged by today's usage of the Internet? How?

Do you think that the Internet will replace libraries or stores?

Would you consider meeting with someone that you met on the Internet?

Do you think the Internet is making people more impatient and that we are becoming a society where we all want instant satisfaction?

How has the Internet changed society?

Do you know how to protect your personal information online? What can you do?

Do you think people spend too much time on their smartphones? What can we do about this?

INTERNET SAFETY TIPS



Make your safety a priority



1 SECURE YOUR SECRETS

- NEVER share your personal information online, including passwords, social security number, etc.
- Create strong, complex passwords and keep them in a safe place.

PRACTICE SAFE BROWSING

2

- Use a secure browser, and use websites with <https://> when possible
- Install and use antivirus software and firewalls.
- Don't click on unfamiliar links or websites.
- Be careful of using public wi-fi, is easily hackable!



3

KEEP SOFTWARE UP TO DATE



- Allow your computer to automatically scan and update your software
- Don't forget to update your smartphone apps as well

DON'T FALL FOR FAKE

4

- Be wary of pop-up ads and strange web links.
- Know how to spot fake emails and websites.
- Don't download or click any unfamiliar web links!



5

COMMUNICATE RESPONSIBLY

- Be thoughtful of the information you share online.
- Be careful who you meet online and what you post.

Internet Crimes and Wrongdoings Presentation

Website: <https://www.canva.com/design/DADvKDc6eN8/y2Vl-d2Aooy-wDDNuTyqnA/view>

PowerPoint Presentation:

https://drive.google.com/file/d/1Jt_ycbVrkTclWRNGxdbownauvVS5Dwt/view?usp=sharing

Internet Safety 47.3

WHAT ARE THEY AND HOW TO PREVENT THEM



Internet Crimes and Wrongdoings

Helpful Video Presentations

These are short video presentations created by my colleagues and me in our Master's program in Educational Technology about Internet safety and Internet crimes.

Digital Citizenship - <https://youtu.be/GV0tvdVyyNQ>

Password and Wi-Fi Safety - <https://www.youtube.com/watch?v=DilcUBTAiMM>

Phishing - <https://youtu.be/JnwSYIX1VBA>

BitCoin - <https://youtu.be/mrijbT5IEqc>

Ransomware - https://youtu.be/66E_PR6mS2I

Identity Theft - <https://my.visme.co/projects/vdjd1g3d-id-theft>

Do Your iPhone Apps Know Too Much? (App Permissions) - <https://prezi.com/v/femkmmen3h3w/>

Personal Online Privacy - <https://www.youtube.com/watch?v=4jQP1Z0OTTI>

FlipGrid

www.flipgrid.com/internetsafety473

“Flipgrid is video the way students use video ... social, engaging and fun! It’s easy and friendly to use.” Students can record short videos to share and collaborate with others. “Flipgrid empowers student voice and builds global empathy through shared learning processes, stories and perspectives.”

Students simply need to register for a FlipGrid account with a Google email or Microsoft email (Outlook, Hotmail, MSN, Live, etc.).

Activity:

Students can create short videos together and post them on FlipGrid for other classes to share and respond.

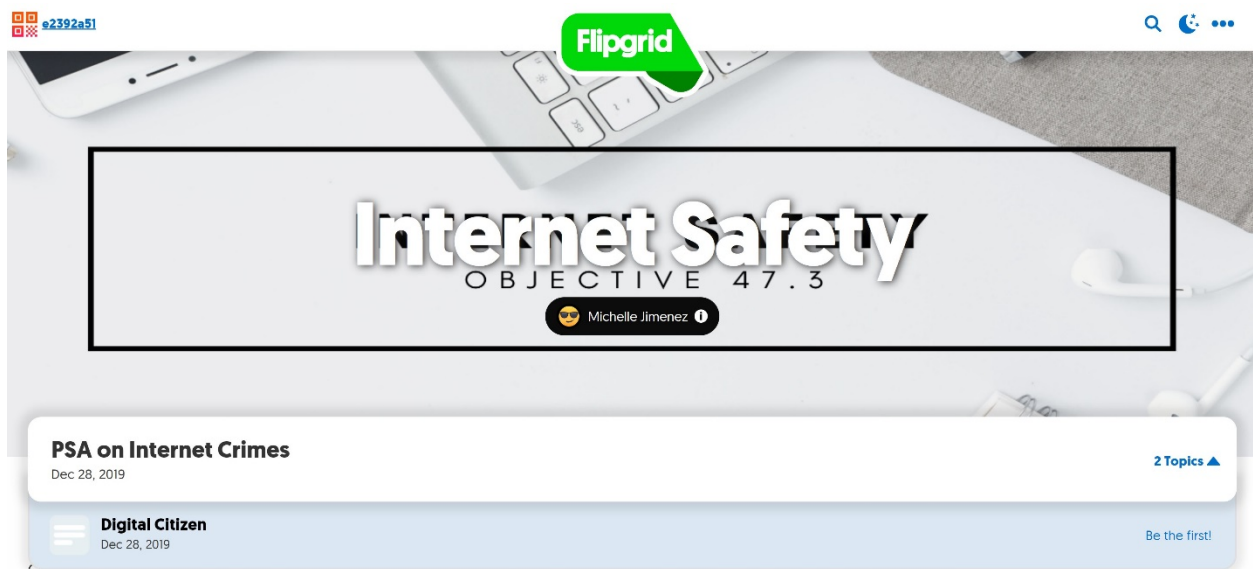
There are two topics to share and collaborate on:

1) PSA on Internet Crimes

Create a PSA for Internet Crimes. What is your cyber crime? Why is it a crime? Give some examples. How can it be prevented?

2) Digital Citizen

What does it mean to be a good Digital Citizen?



Task Practice

Read the story below and answer the questions.

Story #1:

George was checking his work email. He clicked on email that looked like it was from his IT representative. It read, "New security updates need to be performed on our servers. Please re-validate your mailbox now for maintenance and updates of your mailbox." George clicked on the link and typed in his username and password to authenticate. Nothing happened immediately, but soon he got reports that his email had been used to send out massive amounts of other questionable emails. His email became full of spam and tons of other memberships to websites that he did not sign up for.

What is the internet crime in the story?

How could this crime be prevented in the future?

Why is it important to prevent this crime?

Task Practice

Read the stories below and answer the questions.

Story #2: Jenna

Jenna received an email from Netflix. It said “Hi Dear, Your Netflix account is on hold because of a billing problem.” Then it included a link to update her billing information. She thought the email looked real, so she entered her credit card number. After about a week, she found out that her credit cards had been maxed out and her bank accounts had been emptied.

What is the internet crime in the story?

How could this crime be prevented in the future?

Why is it important to prevent this crime?

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.

REMINDE 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 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.

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 inconvenience.

[Click here to confirm your account](#)

Regards,
US Bank Online Customer Service

This email has been sent by US Bank.

Phishing Features

Email Message

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 urgently 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

Phishing Features

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 inconvenience.

[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 urgently 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],

Generic greeting

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.

Too good to be true

Link in email

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!

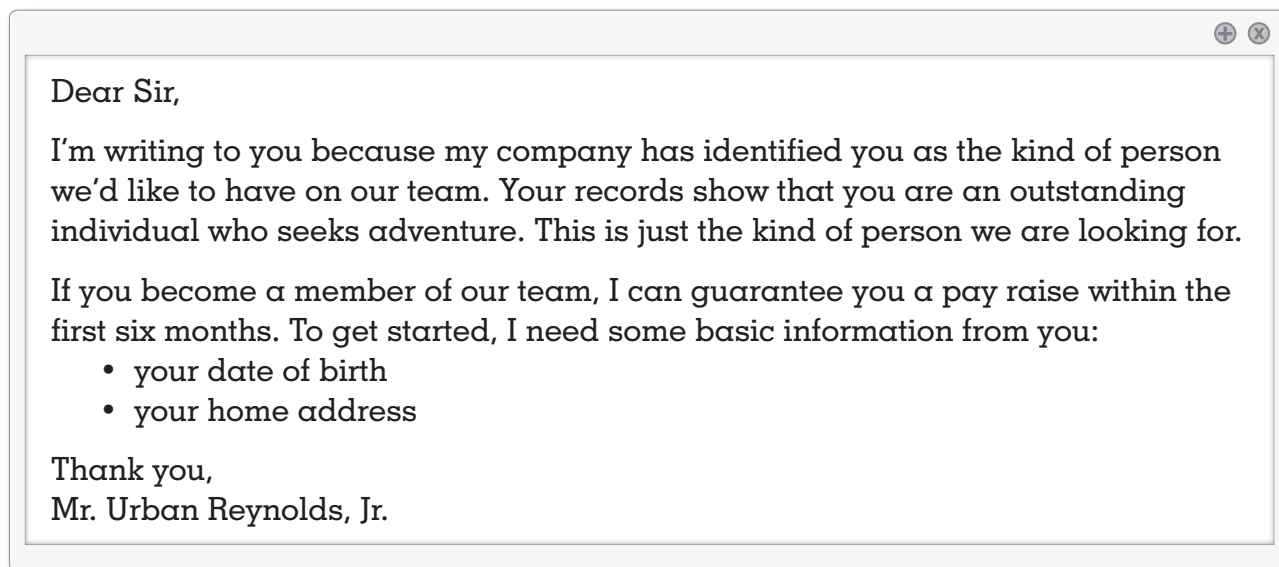
Marcus Gohl

Scams and Schemes

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:



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

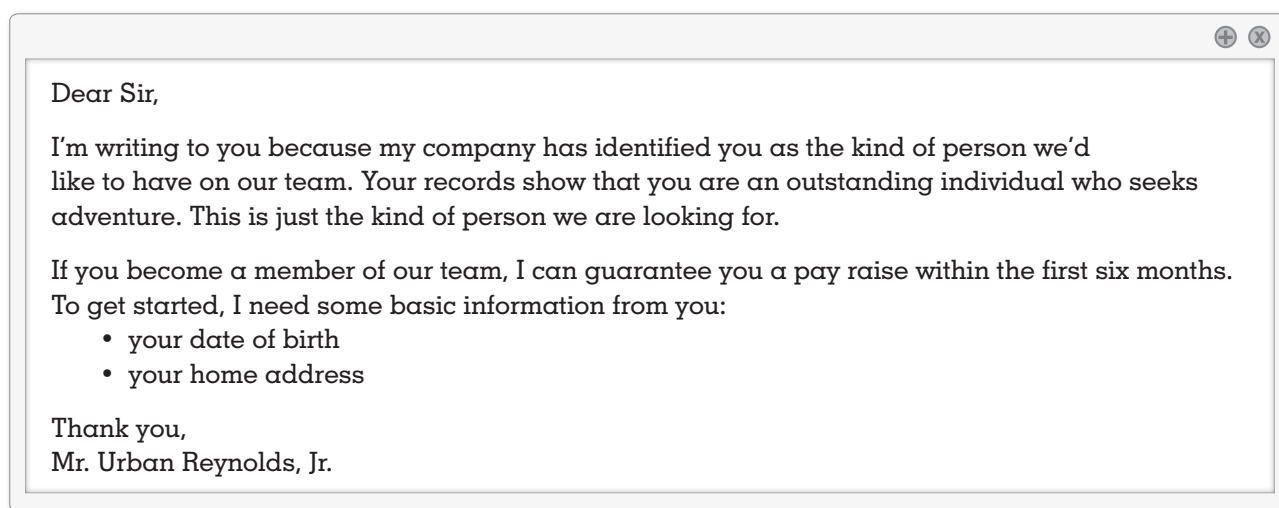
1. A type of crime in which your private information is stolen and used for criminal activity is called:

- 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:



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.



Digital Citizenship

Student Packet
Grades 9-12



Digital Life 102

1. Using the chart below, show whether the following sentences are an upside (positive) or downside (negative) of media life.

Upsides	Downsides

- a) Private information can be copied and sent to anyone
- b) You can stay in touch with friends easily
- c) Many fun things online are also free
- d) You may spend less time with others face to face
- e) Anything you do online leaves a permanent record
- f) You can look up information quickly

2. What does digital citizenship mean?

- a) Any information about you on the Internet
- b) Using digital media safely, responsibly, and respectfully
- c) An online membership
- d) Not giving credit to someone else's work

3. Which is an example of digital media?

- a) Computers
- b) Social network sites
- c) Video games
- d) All of the above

Oops! I Broadcast It on the Internet

.....

1. Using the example below, determine what the word *consequence* means.

Ivan emails his friend about something secret that happened at school. Later, Ivan notices that the email has been posted online. A consequence of Ivan sharing the information through email is that the information was shared publicly online.

A *consequence* is:

- a) Someone you met online
- b) The effect of something that happened earlier
- c) An Internet post

2. True or false: If you send a text message, you can control what happens to the message after you send it.

- a) True
- b) False

3. Which of the following is an example of oversharing online?

- a) Posting a message on your friend's wall that says you dislike your basketball coach
- b) Posting a photo of you playing basketball
- c) Inviting your friends and family to your next basketball game by email

Copyrights and Wrongs

ASSESSMENT

1. Decide which kind of license is best for each student's work. Write the letter of each answer in the chart below.

Copyright	Creative Commons	public domain

- a) An original song that Janelle doesn't want anyone to copy or distribute without her permission
- b) A digital illustration that Sasha wants credit for but doesn't mind if others use without her permission
- c) An original documentary that Dom wants complete ownership of in case the documentary makes money
- d) An article that Ryan finds in a government database
- e) A collection of photos that Artie wants credit for but doesn't care if others use
- f) A photo that Marcus wants others to share and use however they want for the purpose of creating new artwork

2. Read the following scenario. Then answer the question below.

Lola takes a photo of the mountains near her home. She uploads the photo to the Internet with "Copyright 2011 Lola Dominguez" next to the image. About a week later, she checks one of her favorite blogs and sees that the blogger has posted her photo on the blog and has posted a creative writing story to go with it.

True or false: If the blogger doesn't ask Lola's permission to use the photo but still gives her credit, the blogger can post Lola's photo with his story.

- a) True. Copyright is pretty relaxed, so even though Lola put "Copyright" on her photo the blogger can do what he wants.
- b) False. When you copyright something, the only way that others can use the work without your permission is if they change the original meaning of the work. Adding a story to the photo doesn't change the original photo, so the blogger can't use it.
- c) False. When you copyright something, others have to ask your permission before using it.
- d) True. Even though Lola put "Copyright" on her photo, the blogger doesn't have to ask permission because he posted his own original story to go with it.

.....

3. What is the safest way to use someone else's creative work, no matter what kind of license it has (copyright, Creative Commons, etc.)?

- a) Assume that it's in the public domain and use it however you want
- b) Give credit to the creator
- c) Ask permission to use the work
- d) Check who owns the work

Feeling on Display

-
- 1. In the video “Feeling on Display” that your class watched, Claudia says, “There’s absolutely a double standard ... for girls, especially.” What did she mean by this statement?**
- a) In the same situation, people would treat girls and boys equally.
 - b) Girls post double the amount of photos that boys do.
 - c) In the same situation, people would treat a girl differently than a boy.
- 2. Which of the following is NOT an example of how someone might feel “on display” because of digital and social media?**
- a) Valeria receives comments on an Instagram photograph she took of a tree at a park.
 - b) Fiona asks her friend to take a photo again because she didn’t look good in the first one.
 - c) Ben gets 35 “Likes” on a photo that he posted of himself shirtless.
 - d) Michael uses a computer program to erase pimples he has in a photo before making it his profile picture.
- 3. True or False: It’s more common for girls to worry about other people posting ugly photos of themselves online than for boys to.**
- a) True
 - b) False

Turn Down the Dial on Cyberbullying

1. Reflect on each of these statements about the Internet. Circle three statements that support the idea that the Internet makes bullying easier and a bigger problem.

- | | |
|---|--|
| a) Information can spread very quickly on the Internet. | d) Anything someone says could stay on the Internet for a long time. |
| b) If you say something mean online, you don't have to worry about getting in a physical fight. | e) You can get support from groups on the Internet. |
| c) You can find lots of information on the Internet. | f) Parents, teachers, and students all use the Internet. |

2. Mei keeps getting mean comments on her Twitter posts. Cara, Mei's good friend, has seen the comments and wants to help. What can both girls do to make the situation better?

- a) Mei could delete her Twitter account. Cara could let Mei use her Twitter account so that Mei can still post, but no one knows it's her.
- b) Mei could ignore and block the bully. Cara could comfort Mei.
- c) Mei could tell the bully to back off, and Cara could post mean things about the bully on Twitter.
- d) Mei could tell the bully to back off, and Cara could get a group of friends to post embarrassing photos of the bully.

3. A(n) _____ helps to de-escalate, or lessen the impact of online cruelty by supporting and standing up for the person who is bullied.

- a) bystander
- b) Upstander
- c) target
- d) offender

Digital Life 102

Directions

First, take the quiz on your own. When you are done, trade with your partner. Together, use the answer key to calculate each other's score. Discuss what surprised you the most and which answers were the closest to or farthest from your own experiences.

YOUR SCORE

___ / 10

1. 82% of teens say that they own which of the following?

- a) cell phone
- b) smartphone
- c) iPod Touch or similar device
- d) iPad or similar device

2. What percent of teens describe themselves as “addicted” to their cell phones?

- a) 11%
- b) 27%
- c) 41%
- d) 63%

3. 68% of teens say they do which of the following at least once a day?

- a) text
- b) visit a social network
- c) instant message (IM)
- d) use email

4. What percent of teens agreed they wish they could “unplug” for a while?

- a) 13%
- b) 27%
- c) 29%
- d) 43%

5. 51% of teens visit social networking sites _____.

- a) at least once a day
- b) several times a day
- c) once a week or less
- d) never

6. What percent of teens say that they don't understand their social networking site's privacy policies?

a) 24%

b) 35%

c) 46%

d) 61%

7. True or false? More teens say they prefer texting with their friends than talking in person.

TRUE

FALSE

8. What percent of teens say they have said something bad about someone online that they wouldn't have said in person?

a) 25%

b) 35%

c) 49%

d) 67%

9. What percent of teens say that social networking helps them connect with people who share a common interest?

a) 35%

b) 42%

c) 57%

d) 66%

10. True or false? More teens say that social media makes them feel better about themselves than worse.

TRUE

FALSE

Note: All statistics and answer feedback (except for question #4) come from Social Media, Social Life: How Teens View Their Digital Lives, the 2012 research report from Common Sense Media's Program for the Study of Children and Media. We surveyed more than 1,000 13- to 17-year-olds nationally to understand how they perceive social media (like Facebook and Twitter) affects their relationships and feelings about themselves.

Oops! I Broadcast It on the Internet

Brittney's Story

1. *Why do you think Brittney and her friends wanted to broadcast themselves in the first place?*
2. *Brittney regrets posting the photos, but are there situations when you think it would be okay, even helpful, to get comments from others online? What are those situations?*
3. *In what ways did Brittney's actions impact her later? Can you imagine how the posts may impact Brittney in the future, even beyond college?*
4. *Is there anything that you learned from Brittney's story that made you think about incidents in your own life or your friends' lives? If so, can you share those stories (leaving out personal details)?*

Case Studies

case study 1

Emma's Secret Crush Goes Viral

Over the past few weeks, Emma has developed a huge crush on José. She thinks he might like her, too. She knows gossip travels like lightning at school, so she tells only her best friend, Chantal, by texting her after school: "Do you think José likes me? I kinda have a little crush on him." Emma also swears Chantal to secrecy over the phone later that night. Though Chantal vows to keep her secret, she forwards Emma's text to Zeke, who forwards it to a friend, who ... you know the rest! The next day at school, one of the soccer players, Ted, texts Emma: "Emma+José=so adorable." Emma is shocked and embarrassed because she told only her best friend, and then swore her to secrecy.

1. *If you were Emma, what would you do when you got Ted's text? Who, if anyone, is most at fault for spreading Emma's secret?*
2. *How would this situation be different if Emma had told her friends about the crush in person instead of by sending a text message?*
3. *How could Emma resolve or fix the situation herself? Is there a way she could make the situation better?*
4. *Has anyone ever shared information about you or someone you know over IM, text, the Internet, etc. that you wanted to keep private? If so, what did you do?*

Tommy has been writing a blog about his life that he thought was pretty private because he used a username that wasn't his real name. But when his parents ask him why he decided not to try out for the basketball team, Tommy figures out that they have been reading his blog, because it's the only place he describes being picked on for being so short. Tommy is annoyed and surprised because he never told his parents about the blog and certainly didn't give them his username to access it. His blog is technically public, but he didn't think anyone could connect his blog with the "real" him. Tommy later finds out that his best friend's parents told his parents about the blog.

- 1. What would you say, if anything, to your parents if you were Tommy?*
- 2. How is Tommy's parents' reading his blog similar to or different from reading a diary that he's written in a notebook or paper journal?*
- 3. Do you think it's fair for Tommy's parents to read the things he posts on the Internet, given that his blog is technically public? Why or why not?*
- 4. Why might Tommy's parents want to read his blog? Given these reasons, how would you react if your parents asked to read your email or text messages?*
- 5. Have you ever been in a situation where your parents or someone else has asked to read something that you felt was private? If so, how did you feel? What did you do?*

Oops! I Broadcast It on the Internet

Eva's Story

1. What kinds of things do you think Eva and her friend were IMing to one another?
2. Do you think it was fair of Eva's friend's dad to look at the chat transcript?
3. What might be the consequences for Eva of her mom knowing about the IM chat?
4. Why might Eva have said things on chat that she wouldn't say in person?

Case Studies

case study 1

Emma's Secret Crush Goes Viral

Over the past few weeks, Emma has developed a huge crush on José. She thinks he might like her, too. She knows gossip travels like lightning at school, so she tells only her best friend, Chantal, by texting her after school: "Do you think José likes me? I kinda have a little crush on him." Emma also swears Chantal to secrecy over the phone later that night. Though Chantal vows to keep her secret, she forwards Emma's text to Zeke, who forwards it to a friend, who ... you know the rest! The next day at school, one of the soccer players, Ted, texts Emma: "Emma+José=so adorable." Emma is shocked and embarrassed because she told only her best friend, and then swore her to secrecy.

1. If you were Emma, what would you do when you got Ted's text? Who, if anyone, is most at fault for spreading Emma's secret?
2. How would this situation be different if Emma had told her friends about the crush in person instead of by sending a text message?
3. How could Emma resolve or fix the situation herself? Is there a way she could make the situation better?
4. Has anyone ever shared information about you or someone you know over IM, text, the Internet, etc. that you wanted to keep private? If so, what did you do?

Tommy has been writing a blog about his life that he thought was pretty private because he used a username that wasn't his real name. But when his parents ask him why he decided not to try out for the basketball team, Tommy figures out that they have been reading his blog, because it's the only place he describes being picked on for being so short. Tommy is annoyed and surprised because he never told his parents about the blog and certainly didn't give them his username to access it. His blog is technically public, but he didn't think anyone could connect his blog with the "real" him. Tommy later finds out that his best friend's parents told his parents about the blog.

- 1. What would you say, if anything, to your parents if you were Tommy?*
- 2. How is Tommy's parents' reading his blog similar to or different from reading a diary that he's written in a notebook or paper journal?*
- 3. Do you think it's fair for Tommy's parents to read the things he posts on the Internet, given that his blog is technically public? Why or why not?*
- 4. Why might Tommy's parents want to read his blog? Given these reasons, how would you react if your parents asked to read your email or text messages?*
- 5. Have you ever been in a situation where your parents or someone else has asked to read something that you felt was private? If so, how did you feel? What did you do?*

Copyrights and Wrongs

Directions

Read the instructions on this page. Complete the rest of the handout in groups, and be prepared to share your findings with the class.

Big, Little, and Small Advertising Agency
10 Madison Avenue
New York, New York

Hi there, B.L.S. creative teams

It's Frida from the photo department.

The Vegetable Farmers of America (VFA) have hired us to create print and billboard ads that encourage people to become vegetarians. These ads will be used in magazines and billboards nationwide.

We have gone through hundreds of images for them and have decided on five. It is your job to make the final decision on which of the five images to use. The photos, along with their source information, are in this packet.

Choose a photo that you believe will encourage someone to become a vegetarian, but be sure to also consider how the photo was originally used and how it is copyrighted.

For each photo, we need you to answer the following questions:

- 1. Who owns the photo? Who holds the copyright for the photo (if anyone), and who gets paid for its use?** Is it protected by copyright, available for free public use via Creative Commons, in the public domain, or some other way? In other words, what do we need to do to use the photo legally?
- 2. Who created the photo? What was it originally used for, and what does it show?** How do you think the creator might feel about having us use the photo in our ad campaign?
- 3. Is the photo right for our ad campaign?** To answer this question, you need to think about how the VFA might feel about having us use the photo in their ad campaign, and how the public might respond to an ad that uses this photo.

See you in the cafeteria,
Frida Miko
Director, B.L.S. Photo Department

PHOTO BOOK

For Creative Team's Eyes Only

Photo 1: Cattle Show, Flickr

Owner and copyright status: _____

Creator and original context: _____

Right for the ad campaign? Why or why not? _____



Okay, Frida. Photo 1 comes to us from Flickr, the photo-sharing site on the web. This photo is in a public album, created by a member of the Future Farmers of America, and is copyrighted through Creative Commons, a license that allows free use of materials by others. Some are allowed to be used for commercial purposes and some aren't. But don't worry, this one is okay to use for commercial purposes. However, we don't really know if this young farmer is aware that her photo from the local cattle show is available for commercial use.

Photo 2: Hindu Temple, Stock

Owner and copyright status: _____

Creator and original context: _____

Right for the ad campaign? Why or why not? _____



We can buy some images called stock photos. Well, technically, we buy permission to use it for a fee. But we can't forget to credit them! That's part of the deal. This photo comes from Pronto Pictures. It would cost \$1,500 to use in our advertising campaign. The image shows a Sri Mariamman Hindu Temple in Singapore. The cows are statues. Keep in mind that for Hindus, cows hold special significance as religious icons.

Photo 3: Dairy Cow, B.L.S. Ad Agency

Owner and copyright status: _____

Creator and original context: _____

Right for the ad campaign? Why or why not? _____



This photo takes me back to my days on the dairy farm. It's by one of our in-house photographers, Duncan. This means that we own the copyright. If someone else wanted to use this photo of Bessie, we would license the photo to them for a fee, depending on the use. But we can use it for free. Look at those big cow eyes.

Photo 4: Flank Steak, Flickr

Owner and copyright status: _____

Creator and original context: _____

Right for the ad campaign? Why or why not? _____



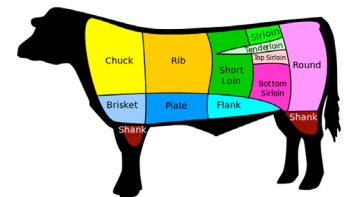
Photo 4 looks yummy! It's also from a public album on Flickr, one on how to prepare flank steak. The photo was taken and posted by a local chef, and it is listed for commercial use under Creative Commons. One thing this particular Creative Commons license allows us to do is alter or change the image.

Photo 5: Cuts of Beef, public domain

Owner and copyright status: _____

Creator and original context: _____

Right for the ad campaign? Why or why not? _____



So, do you know your cuts of beef? This photo is in the public domain, meaning that it's available for public use or alteration for any purpose. There's no author we need to get permission from to use it, and no one will come knocking to claim their "cut."

Feeling on Display

Directions

Watch the video “**Feeling on Display**.” Then answer the following questions as a group. Be prepared to share your answers with the rest of the class.

Part I: Pressure

- Marco says that people try to “prove something” with the photos they post online. What do you think he means by this? Do you agree?
- Zara says that girls worry about their image all the time – whether online or offline – and that they face more pressure than guys. Do you agree? Why or why not?

Part II: Judgment

- Carla says that regardless of gender, all teens judge one another. Do people judge how others look and act online? Does it differ for boys and girls? If so, how does it differ?
- What do you think of Claudia’s statement that it’s easy to judge other people online because “You have the safety net of being in front of a screen – you’re not face to face”?

Part III: Comments

- Both Linh and Leah talked about receiving compliments online. What do you think of what they said? Do people fish for compliments online? How might photos and photo comments boost people’s self-esteem?
- Do you think that people react differently to a “selfie” taken by a girl versus a “selfie” taken by a boy? Why or why not? (*Note: The term “selfie” is used to describe when someone takes a picture of themselves, either by holding a camera towards them or by using a mirror.*)

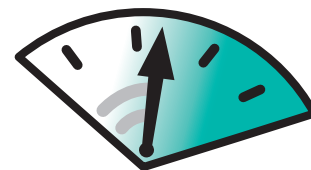
Part IV: Double Standards

- Do you think that a double standard exists between boys and girls when it comes to online appearance? If so, what?
- Randy says, “Some guys try to play the macho role without necessarily posting pictures of themselves flexing. ... It’s much more subtle but it’s still there.” What do you think he means by this? Do you agree?

Turn Down the Dial on Cyberbullying

Directions

Fill out the chart after watching the video, “**Stacey’s Story**.” One partner should complete the boxes on the left to show how the situation escalated. The other partner should complete the boxes on the right, which shows the initial incident, an escalating incident, and then two de-escalating incidents. Keep in mind that the incidents might not happen one after the other, even though they are shown this way.



After completing the chart, turn what you’ve written above into a diagram or map. Show how situations can escalate or de-escalate, using colors, shapes, and arrows.

Stacey’s Story	Turn Down the Dial on Cyberbullying
Initial incident (what happened first?):	Initial incident (what happened first?):
Escalating incident #1:	Escalating incident:
Escalating incident #2:	De-escalating incident #1:
Escalating incident #3:	De-escalating incident #2:



Common Sense is committed to
helping kids and families thrive in a
world of media and technology.

