Think before you share

Overview

In this activity, you'll lead a discussion with the class supplemented by a handout for your students. The activity should take approximately 15-20 minutes, including discussion time.

Objectives



At the end of the activity students should be able to:

- · Recognize that information they share on the web can travel quickly and broadly.
- Understand that information they share on the web can influence their reputation in the real world.
- Think about the possible consequences of sharing their information online before they take that step.

DISCUSSION 📑 💨



Key points O

You can't control information once it's out in the world.

Information shared on the web (through social media posts, comments, and videos) can spread quickly and take on a life of its own. What you post or send can easily be forwarded, copied, or found by other Internet users, including strangers, or people you know who aren't necessarily your friends.

You are what you share.

What you share online can influence your real world reputation. Other people's impressions of you can change based on what you share, and posting inappropriate information can have negative consequences you may not have considered. That can mean impacting your place on the soccer team, summer job opportunities, or even one day, what college you go to.

Use your powers for good.

The Internet is an awesome tool for having fun and making new friends, but with great power comes great responsibility! You can just as easily lose friends as make them based on how you manage your reputation online.

QUESTIONS FOR THE CLASS



What types of information are your friends sharing online?

Have you seen things "go viral?" How? What have been some of the consequences of this?

How can you take more control and be more responsible for what you're sharing? Give a specific example.

Think before you share



ACTIVITY

Explore examples of online information sharing

1 After the discussion session, distribute the activity handout.

2 Students will be asked to review and describe three fictional yet typical online profiles of young adults around their age. Then, students will be asked to reflect on the three words they might choose to describe those people.

3 By completing this activity, students will reinforce their own understanding of how information online can shape someone's impression and how what they say online can be reflective of who they are.

WRAP-UP

Gauge students' understanding of the activity objectives

Wrap up the activity with a class discussion reviewing your students' handout answers.

KEY POINTS O_____

We draw conclusions about people by their posts.

What you share online says a lot about you to the outside world. What do the items shared or posted on each profile tell you about them?

People willingly share a lot of personal information online.

A lot of the information shared on these profiles could be viewed publicly or by people they didn't know. Also, some things shared could be personal and he/she might want to keep it private instead of sharing them with the world.

You are what you share.

What you post, share, and comment on online can give someone the right or wrong impression. Be sure that the way you would want someone to describe you matches the actions you take online.

(1)

Think before you share



Overview

What we share online can help someone express who they are and share what he or she is interested in with others. And of course it's fun to post, comment, and share photos with friends and family. But what someone posts online can say a lot about them and can be viewed and interpreted by a larger and unfamiliar audience.

ACTIVITY

Carefully review these three profiles. Once you have looked them over, jot down three words you might use to describe that person or profile. Get ready to discuss this exercise with the class in 5 minutes!



Relationship Status: It's complicated

Likes: Selena Gomez, Awesomeness TV, Switched at Birth, Beyonce, my friends!, Seventeen, dancing, Divergent, Snapchat, Kick, Hunger Games

Dislikes: one direction, family vacations, homework, football, chores

Comments: "Under the sea photos from the dance! looking good y'all!!! #YOLO #friend4lyfe #omg #slowdancingisboring"

"my little brother alex is SOOO annoying. 4 hour drive to the lake house on Friday is going to be a long one. UGH. #adopted? #mybrothersanalien"

"JUST SAW DIVERGENT. omg obsessed!! ps. I can't believe Jason tried to hold my hand. #parentchaperone #soembarrassing #justdontok

"BLAHHH pop quiz in Mr. Hastings class! Be prepared you guys. #shouldhavereadthat #teachersRmean"

"New purple socks today. Twizlers and a sprite at lunch. #trendy #spring #favs #mondays"

Games: Candy crush, FarmVille

Think before you share



15-20 min

ACTIVITY ^{□□} (continued)



Likes: Phillies, baseball, Flyers, fishing, kayaking, What does the fox say, R5, One Republic, painting, guitar, spending time with friends, Austin Mahone, museums

Dislikes: dancing, four square, justin bieber

Comments: "Won game! one more game to go before championship. Gotta practice more 1st base throws"

"i hate school dances. #notgoing"

"fishing this saturday with my dad at Penny Pack Park! gonna be awesome."
"anyone been to the science academy recently? parents dragging me
#sciencenerd"

"wish i could just be awesome at guitar. practicing is sooo boring.#pickupgameanyone?"

"Tyler just checked in - Academy of Science Philadelphia"

"Tyler shared '10 signs your parents are hippies"



Likes: Lolcatz, PUPPIES!!, video games, soccer, world cup, katy perry, twitter, puzzles, reading, summer

Dislikes: popular cliques, makeup, football, skiing

Comments: "New high score!! yessss. #candycrush #finally" "check out my new website! made all the jewelry myself #proud #hobbie #codeiscool

"jennifer lawrence is so cool. wish i could meet her!"
"PUPPIES!! '25 puppies that love to cuddle"
"missed the winning goal. ugh. at least we tied. #nexttime #cupcakesmakeitbetter"

HOW ABOUT YOU?

Now that you've had a chance to review the above profiles, what three words would you want someone to describe you with?

Lock up and

LOG OUT



Overview

This activity has two parts that should last approximately 5-7 minutes each (15 min in total):

Part 1: Protecting your personal information with strong passwords. In this portion, you'll lead a discussion with the class supplemented by a handout for your students.

Part 2: Protecting your personal information by logging out of shared public computers and devices. You'll lead a second discussion paired with an optional exercise.

Objectives

At the end of the activity students should be able to:

- Create strong passwords.
- Say why it's important to keep passwords safe and private.
- Identify situations where they may need to logout of online accounts
- Understand the consequences of not logging out of personal accounts when using a shared device.

DISCUSSION 1

Key points O

Passwords are an important security measure in order to keep safe online.

By knowing how to create strong passwords you can further safeguard your personal information.

Don't share your password unless it's with a parent or trusted adult.

Like the key to your house or the combination to your locker, pass-

words protect things that are of value to you and shouldn't be shared.

QUESTIONS FOR THE CLASS



What components contribute to a strong password?

Why is it important to only share passwords with a parent or trusted adult?

ACTIVITY 1

Review example passwords

• After the discussion session, distribute the activity handout. The handout shows several examples of strong and weak passwords.

2 Students should identify the stronger password and explain why it's the better choice. They should also write down as many tips for creating a strong password as they can remember.

3 Let students know that you'll come back to the handout, and transition to Discussion 2.

Lock up and

LOG OUT



DISCUSSION 2 REP

Key points O

Protect your info by logging out of shared public computers and devices.

Protecting your information online also means logging out of websites, programs, and applications that are used on public or shared computers when you're done with them.

If you don't log out of public computers, someone could log in as you and access your accounts and information. More sensitive online activities should be done on your own devices. For example, logging into any account that is tied to a credit card, any account with personal or private information, etc.

QUESTIONS FOR THE CLASS



Why is it important to log out of public or shared computers?

What happens if you don't log out (of public or shared computers)?

ACTIVITY 2 🖘

Explore where and how students sign in online

• Question for students: Think of all the places you regularly sign in to use a computer that isn't yours. What about school spaces, libraries, or shared home computers? Have students jot down their notes in a notebook.

Optional: Teacher can copy this list onto the board, or students can post their sticky notes somewhere in the classroom.

Question for students: Have you, or someone you know, ever forgotten to log out of a site or a computer that was accessed by other people? What happened, and why does this matter? Have students jot down their thoughts in their notebooks or on sticky notes.

WRAP UP

Gauge student understanding of the activity objectives

Wrap up Activity 2 with a class discussion reviewing your students' handout answers in Part 1 and their notes in Part 2. Potential additional questions to review with your class:

Do you know a friend that has forgotten to log out of a shared computer? What happened?

Have you ever heard someone share a password with a friend? Do you think he/she might make a different choice in the future?

Do you know a friend who has opened a web browser and noticed someone else had forgotten to log out? What did he/she do?

Thinking about your friends, which tip do you think might be most memorable to them? What tip do you think might be most useful to him/her?

Lock up and

LOG OUT



TEACHER DISCUSSION PREP 🛹 💨

Part 1: Protecting your info with strong passwords

People often use passwords that aren't very secure. They're often too short, easy to guess (a home address, pet's name, birthday, etc.), or commonly used (password, welcome 123). Some people even use the same password for multiple websites. This is risky and can make it easier for scammers and hackers to access personal information.

Some quick statistics

- 34% of teens say they have shared one of their usernames and passwords with someone other than their parent or guardian, including 23% who have shared it with a friend or significant other.
- Over three-quarters of teens (76%) are very or somewhat concerned about the privacy of their personal information being harmed by their online activity, including 43% who are very concerned. This is up from the two in three teens who were very (35%) or somewhat (30%) concerned a year ago.
- According to the CyLab at Carnegie Mellon University, children's social security numbers are 51 times more likely than adults to be used for fraudulent purposes.
- Nearly three-quarters of teens (73%) agree that because teens are more likely to have clean credit histories and are less likely to monitor their credit, it is reasonable to think they could be victims of identity theft.

Avoid sharing passwords

Passwords should NOT be shared with friends. They should only be shared with a parent or guardian. 1 in 3 teens has shared a password. Sharing passwords with people other than a parent can have serious consequences and make friends and family vulnerable.

TIPS FOR CREATING A STRONG PASSWORD

Longer is better. Use 8 or more characters.

Using a phrase makes it easy for you to meet the minimum number of characters.

Goodt0kn0w Combining characters, numbers, and letters also make a password stronger.

> Use something that is memorable and then swap letters with numbers to make it stronger.

Goodt0kn0w1 Goodt0kn0w#2 goodt0n0w3

Passwords should be different for each site. Changing the beginning or ending letters or numbers of a password can be enough to make them unique, secure, and memorable.

Example 1: Think about photos,

messages, and contact information you may have on just your phone that relate to other people. Anyone who has your password has access to that information, especially if your phone is linked to online accounts.

Example 2: Olivia and Emma were best friends who shared everything. To prove that they were best friends, Olivia shared her password with Emma. A few weeks later, Olivia and Emma got in a fight. Emma remembered she had Olivia's password so she signed into her account and posted some mean things and changed her photo. Then she changed Olivia's password, too, so Olivia couldn't log in to fix the problem.

Lock up and Log out



TEACHER DISCUSSION PREP 💦 💨

(continued)

Part 2: Protecting your info by logging out of shared computers

While logging into a computer or website can make your online experience better, logging out of a website and computer when you're done is very important when using a computer that isn't yours. Students in particular often use computers, tablets, and phones that aren't their personal devices. They often sign in from places like the library, a shared home computer, a borrowed friend or parent's device, at computer stores, while travelling on vacation, at the school computer lab, and more.

Closing a tab on a web browser does **not** automatically log someone out of a website. The user needs to actually select "Log out" to make sure the next person to use the device can't re-open the browser and access their information through the browser's history. If someone re-opens a page you've visited and you are still logged in, they have full access to your account information and can steal your identity by contacting people or posting things in your name.

Example 1: Mia went to a computer store and checked a personal account on a display computer connected to the web. She closed the browser window and left. Then, a stranger opened the browser to sign into their own account, but instead found they could access Mia's page with her personal information and the ability to pretend to be her online.

Example 2: While Ben was at his friend Lucas' house, Ben logged into his social media account on the shared family computer. He closed the browser and went to go hang out with Lucas. Later, Lucas' younger brother Alex opened the browser to hop online and found that he had access to Ben's account. Alex took a photo and posted an embarrassing comment about Ben and his brother and logged out. This example turned out to be fairly harmless but imagine if someone less friendly had accessed Ben's information — the outcome could have been much more serious!

Lock up and

LOG OUT



LOCK YOUR STUFF UP!

Most of us have personal stuff on the web that we want to keep safe. One of the best ways to keep those things safe is to make sure that you've got strong passwords on **everything**: your online accounts, computers, phones, tablets, and even apps.

ACTIVITY 1 =>	
Below are some example passwords. Check the box for the one you think is stronger and explain why.	
O Welcome or O HelloHello3 Why?	
O CallMeMaybe2012 or O 2012: CM.Maybe Why?	
O D0N'tBe3vil! or O Dontbeevil Why?	
O nasswords or O VOucan't GuessThis Why?	

ACTIVITY 2

Overview

Now that you're a password pro, think about whether there's a password (or two!) you want to change. And remember, even if you set the strongest password, it won't be effective if you share it with others. Only share your password with a parent or trusted adult. When you share your password with people other than your parents, you can put the people you care about at risk.

Think about all the photos and messages you have just on your phone – anyone who has your password has access to those.

Did you know

1 in 3 teens
has shared
a password?

Have you ever shared a password and regretted it later? Have you ever shared a password with someone who you got into an argument with or who you're just not really friends with anymore? Keep your information safe – there are lots of great things you can share with your friends, but your password isn't one of them.

Think of a good password.

Take a minute to think about a few phrases that are memorable to you and write them down in the space below. These are phrases that you can then use to help you create (and remember!) strong passwords.

Lock up and

LOG OUT



LOG OUT WHEN YOU'RE DONE!

Overview

Similar to sharing your password, leaving a computer signed in to a website or not signing off a public or shared device could leave your information vulnerable to others. While doing this can make return visits to websites faster and easier, logging out when you're done keeps your information for your eyes only. A little extra time spent signing in and out is a small price to pay for protecting your information.

ACTIVITY 3

Think about which public computers you've used

1 Use the space below to list all of the places you've used a computer that isn't yours. Consider school spaces, libraries, shared home computers, etc.

Control what you share



15-20 min

Overview

In this activity, you'll lead a discussion with the class supplemented by a handout for your students. The activity should take approximately 15-20 minutes, including discussion time.

Objectives

At the end of the activity students should be able to:

- · Recognize which posts online should be shared with different groups of people.
- Use security settings to limit where and how their posts appear online.
- Understand the consequences of incorrect settings.

DISCUSSION R



Key points O

Not all information people post online is meant to be seen by everyone else online. Some information should be kept private or shared with a smaller audience.

Security settings can help you control who can see your posts so it's easier for you to keep your information safe.

The wrong settings can expose your personal details to more people than you intended.

OUESTIONS FOR THE CLASS



What kind of information do you share online?

Are there certain posts or things you share that you only want specific people to see? Share some examples.

Have you ever been surprised when someone has seen something you didn't mean for them to?

Have you ever checked or changed your settings on social media sites? What about apps, or devices?

ACTIVITY

Reviewing online privacy settings

1 After the discussion session, distribute the activity handout. The handout lists common types of personal information it's possible for students to share.

2 Students should mark which types of information they are willing to share with particular groups of people, like family, soccer friends, grade school friends, etc.

3 This activity will reinforce students' understanding of the objective by helping them pick which groups they should share information with so they can plan how to change their settings to match their choices.

WRAP-UP



Gauge student understanding of the activity objectives

Wrap up Activity 3 with a class discussion reviewing your students' handout answers.

Potential additional questions to review with your class:

- Have you learned anything about what types of information you wish to keep private?
- Do your settings reflect these preferences? If not, what will you do next to fix this?

Control what you share



TEACHER DISCUSSION PREP 🛹 💨



Not everything people post on the web is meant to be viewed by everyone else on the web. Some information should be private or shared with a limited audience.

Using the right settings can prevent the wrong people from seeing your personal or sensitive information.



Settings are often identified by an icon that looks like a gear or a wrench in the menu of an app or website.

Examples of using these sharing settings to share with specific people can be: sharing only with yourself, specific friends, friends of friends, or people looking for a specific hashtag (i.e #pets, #yolo, #bestday). The broadest setting shares everything you post with the entire web.

 There are often different privacy options for different types of information. For example, someone could share all their comments publicly but only share photos with family.

When people aren't careful with their settings, information can be shared more broadly than initially intended.

• Example: In 2012 it was reported globally that a 16-year old girl posted an invitation to her birthday online that was not limited to a smaller group of her friends. Since the invitation was public, 3,000 people showed up for the party at her house.

Control what you share



SET YOURSELF UP FOR SUCCESS!

Overview

Why should you use settings? The web allows you to share and connect like never before. However, just like in the real world, you share different things with different people. Settings let you share exactly what you want — photos, posts, comments, links — with exactly who you want.

ACTIVITY

Pick who should be able to see your information

1 What types of things do you typically share online? What apps or social media sites do you use most often?

2 Have you ever shared something that someone saw--but you didn't know they had access to your posts? What happened and how did that make you feel?

3 When was the last time you checked your settings? Do you know where your settings are for each social media network or app?

4 Based on what you've written, what will be your next steps to better control your security settings?



Protect yourself from phishing



Overview

In this activity, you'll lead a discussion with the class supplemented by a handout for your students. The activity should take approximately 15-20 minutes, including discussion time.

Objectives

At the end of the activity students should be able to:

- · Define phishing.
- Identify and recognize emails, posts and websites that are fraudulent.
- Take the appropriate action where phishing scams are concerned: Never share any personal information like names, passwords or account information in phishing scams.

DISCUSSION R



Key points O

"Phishing" is the act of attempting to acquire information such as usernames, passwords and personal details by pretending to be a trustworthy source.

By knowing how to identify a phishing scam, you can protect yourself and your things. When in doubt, ask a parent, teacher, or trusted adult.

QUESTIONS FOR THE CLASS



What is phishing?

What are the main ways to identify and avoid phishing scams?

What should you do if you're not sure if something is real or a scam?

ACTIVITY

Explore examples of online phishing scams

- **1** After the discussion session, distribute the activity handout. The handout shows several images of legitimate and fraudulent websites and email examples.
- 2 Students should mark which types of information they are willing to share with particular groups of people, like family, friends, strangers and acquaintances.
- 3 This activity will reinforce students' understanding of the objective by helping them identify the difference between safe and potentially unsafe websites or emails.

WRAP-UP

Gauge student understanding of the activity objectives

Wrap up Activity 4 with a class discussion reviewing your students' handout answers. The Answer Key is included on the following page.

Potential additional questions to review with your class:

- Have you ever noticed a phishing scam before we learned about it today? What happened? What did you do?
- Which phishing technique do you think is the easiest to spot? What about the most difficult? What will you do if you see something online, and you're not sure if it's real or fake?



Protect yourself from phishing



TEACHER DISCUSSION PREP 🛹 💨



Tips for spotting online scams

Check the "From" email address field.

Always be sure to check the "From" address if you get an email. For example, typically scammers can re-create the look of a bank or shopping email, but they need to send it from a fake account. A more secure email address ending can be .org., .gov, or .edu but even these can be faked so it is important to double check the source.

Look for the "S" at the end of "http" in a URL.

If a URL has an "s" at the end of http (i.e https://), this means there is an extra layer of security added to website hosting the URL. You can trust these links more than those for URLs without the "s."

Remind students to NEVER give out their password or other sensitive information, like a social security number or bank account, over email.

Also, if a company does ask you to log into their site (like a gaming site or shopping site), don't do it through the link provided if you don't recognize the sender's address. Type the URL into a new browser window instead, and log in from there. If you're not sure what to do, ask a parent or guardian before you enter any private information.

If it sounds too good to be true, it probably is.

If it looks like you were sent a post or email from a friend, be sure to ask yourself if it sounds like something that person would write. Often scammers hack into an account and send fake emails/posts on behalf of the person whose account they have hacked. Chain mail is a good example of this: If you are asked to send the email on to 10 friends in order to win a really cool prize, it's probably fake.

Be careful when opening attachments.

Attachments in emails from people who don't normally send you attachments shouldn't be opened. Also, attachments from companies or organizations you don't know shouldn't be opened.

Protect yourself from phishing



Overview

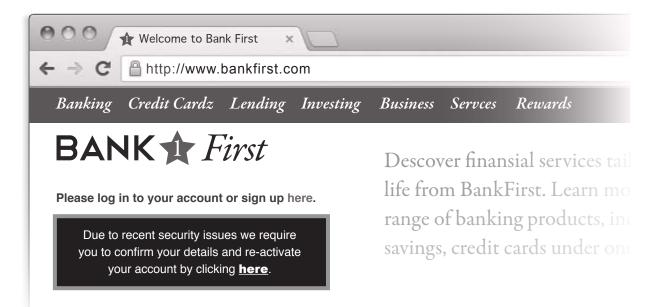
Accepting gifts from strangers can be dangerous, right? The same idea applies online. Scam artists offer you a deal that looks amazing to lure you in. This is called **phishing** — scam artists try to "fish" for more information about you by pretending to be someone you know.

ACTIVITY

Find something phishy

Here are examples of websites that seem like they could be real, but there's something wrong with the picture. Circle what looks strange or "off" to you and describe what the problem is in the space beneath the image.





Be positive



Overview

In this activity, you'll lead a discussion with the class supplemented by a handout for your students. The activity should take approximately 15-20 minutes, including discussion time.

Objectives

At the end of the activity students should be able to:

- Appreciate the importance of being kind online and helping to make the web a positive place.
- Understand how they can be leaders and set a positive example for others.
- Suggest actions they can take to make the web a better place.

DISCUSSION



Key points

Everyone, including students, is responsible for creating a great online experience. There are lots of ways, big and small, to help make this happen today.

A little positivity can go a long way and have a huge ripple effect online. (The opposite is also true: a little negativity can spread into something big and ugly online.)

Everyone can be a leader and set a good example on the Internet for others.

If you see someone being mean, talk to an adult or take charge and report it yourself.

Only by acting can you make change happen for you and the people around you online (and in the real world).

QUESTIONS FOR THE CLASS



Have you ever experienced a random act of kindness on the web? How did it make you feel?

Have you seen someone be negative on the web? How did that make you feel?

What simple actions can you take to make the web a better place?

ACTIVITY 🖘

Have a positive impact online

1 After the discussion session, distribute the activity handout and group students into pairs. (Let students know that there will be an additional activity later in the session.)

2 The handout asks several questions of each group to help them reflect on how to be positive online.

3 This activity will reinforce students' understanding of the objective by having students discuss and record examples of online behaviors they've seen first-hand.

Be positive



WRAP-UP

Gauge students' understanding of the activity objectives

Wrap up Activity 5 with a class discussion reviewing your students' handout answers. Then, move on to explain the next activity.

Potential additional questions to review with your class:

- How can you help to make the Internet a better, more positive place?
- Have you ever seen someone be kind online (or has someone been kind to you) and inspired you to do the same? Do you think kindness can be contagious?
- Have you ever seen someone be unkind or offensive online? What happened? Did you act upon it? How did it make you feel?
- What are some ways to encourage people to be kind, not cruel, online?

WRAP-UP ACTIVITY

Be awesome online

Wrap up Activity 5 with a class discussion reviewing your students' handout answers.

The class can work together to suggest ideas about amazing things that they can do online. The teacher should capture these ideas on the blackboard or poster as the students call them out. This will help remind them that they can make the web a better place by doing cool and positive things online.

Optional Activity: Encourage students to commit to doing one of the positive things they wrote down online to brighten someone's day or be kind online. Hand out one card

per student or use sticky notes. The cards read,

"I promise to help make the web a better place. This week, I promise that my random act of Internet kindness will be to

Students should fill these out, share with the teacher or class, and keep them as a reminder of their pledge.

TEACHER DISCUSSION PREP 🗩 💨

Many students have heard the phrase, "treat others the way you want to be treated." This also applies online.

Since even the smallest online action can have a lasting impact, this means that a person should only post, comment, or forward something about someone else, if she wouldn't mind someone doing the same to her.

Encourage students to try to do

something positive on the web each day, like leaving an encouraging comment, or sending someone a "thank you" text message.

Provide students with tips for discussing online acts of kindness (and not-so-kind acts) with their parents.
This can be a difficult discussion and students may not know how to talk about it with adults.

You may want to partner with a guidance counselor or offer private

one-on-one time so that if students don't feel comfortable speaking publicly about unkind online acts like bullying or similar behaviors, they have a way of discussing it with an adult other than their parents.

Remind students that there are reporting settings on most social networks and communities. Let them know that they should feel empowered to take action if they see people, especially peers, behaving unkindly toward others online.

Be positive



PERFORM RANDOM ACTS OF (INTERNET) KINDNESS

Overview

You've probably heard the phrase, "treat others the way you want to be treated." The same rule applies online. Even the smallest action from you can have a lasting impact on someone else — whether you know it or not. What seems like a minor funny thing you might choose to post about someone else can actually be embarrassing or hurtful for that person. This means that you should only post, comment, or forward something about someone else if you wouldn't mind if someone made the same type of post about you.

ACTIVITY

Explore positive and negative online behavior

Ask and answer the following questions with your partner:

- **1** What are some cool, kind things you've seen happen on the Internet and how did they make you feel? What acts of Internet kindness have you seen and how did they make you feel?
- 2 How can you help to make the Internet a better, more positive place?
- **3** Have you ever seen someone be kind online (or has someone been kind to you) and inspired you to do the same? Do you think kindness can be contagious?
- 4 Have you ever seen someone be unkind or offensive online? What happened? How did it make you feel? How do you think it made the person feel?
- **6** What are some ways to encourage others to be kind, not cruel, online? How can you be a leader?