

**Smart**  
**Alert**  
**Strong**  
**Kind**  
**Brave**

**Be  
Internet  
Awesome.**

# Be Internet Awesome.

Welcome to the Internet Awesome Curriculum, a collaboration between Google and the Internet Keep Safe Coalition (iKeepSafe.org). This resource is part of Be Internet Awesome, a multifaceted program designed to teach kids the skills they need to be safe and smart online.

The Internet Awesome Curriculum gives educators the tools and methods they need to teach digital safety fundamentals in the classroom. The lesson plans, best suited for grades 3 to 5, bring the most critical teachings to the surface—acting as backup for educators priming students to be safe and responsible digital citizens.

Our five fundamental topics of digital citizenship and safety—the Internet Code of Awesome—are:

- **Share with Care (Be Internet Smart)**
- **Don't Fall for Fake (Be Internet Alert)**
- **Secure Your Secrets (Be Internet Strong)**
- **It's Cool to Be Kind (Be Internet Kind)**
- **When in Doubt, Talk It Out (Be Internet Brave)**

These lessons are delivered via Interland, a playful browser-based game that makes learning about digital safety interactive and fun—just like the Internet itself. Using Interland and the complementary curriculum, educators can pick and choose the activities that best suit their students, or progress through the entire series from start to finish.

The International Society of Technology in Education has recognized Be Internet Awesome as a resource that prepares students to meet the 2016 ISTE Standards for Students and has awarded it with the Seal of Alignment for Readiness.

The Internet Awesome Curriculum and Interland game are two of several resources for families and educators to encourage safe online habits. For additional resources from Google, visit [g.co/BeInternetAwesome](https://www.google.com/BeInternetAwesome).

# Be Internet Awesome

## Intro letter/email template

---

Here's a template for a letter (or email) that you can customize to tell parents how new education tools are helping their kids learn to make good decisions about their online safety and behavior.



### Dear Parents,

When our kids are young, we do our best to help them get the most out of the Internet while protecting them from the online world's risks and downsides. But as children mature into teenhood, our role shifts to helping them learn to make their own safe and ethical decisions as they navigate their digital lives.

At [school name], we believe this means preparing our [grade] students to:

- **Think critically** and evaluate online sources.
- **Protect themselves** from online threats, including bullies and scams.
- **Get smart about sharing:** what, when, and with whom.
- **Be kind and respectful** toward other people and their privacy.
- **Ask for help** from a parent or other adult with tricky situations.

This year these efforts will include Be Internet Awesome, a multifaceted program designed to teach kids the skills they need to be safe and smart online. One of the resources, Interland, is a playful browser-based game that makes learning about digital safety interactive and fun—just like the Internet itself. Developed by Google in partnership with the educators and online safety experts at iKeepSafe.org, Be Internet Awesome provides fun, age-appropriate learning experiences built around five foundational lessons:

- **Share with Care**
- **Don't Fall for Fake**
- **Secure Your Secrets**
- **It's Cool to Be Kind**
- **When in Doubt, Talk It Out**

Smart, safe technology usage can help students learn better, and help our schools function better. We believe the Be Internet Awesome program will mark an important step toward our goal of ensuring that all our students at [school name] are learning, exploring, and staying safe online.

If you're interested, we'll be happy to share more information about this new program, including introductions to some of the resources your kids might start using at home. We encourage you to ask them about what we're doing in class; you might pick up a few privacy and security tricks yourselves!

Sincerely,

[You]

# Table of Contents

## **Share with Care** ..... 6

- Activity 1: **Can you keep a secret?**
- Activity 2: **The profile guessing game**
- Activity 3: **How do others see us?**
- Activity 4: **Privacy in practice**
- Activity 5: **Interland: Mindful Mountain**

## **Don't Fall for Fake** ..... 16

- Activity 1: **Don't bite that phishing hook!**
- Activity 2: **Who are you, really?**
- Activity 3: **Interland: Reality River**

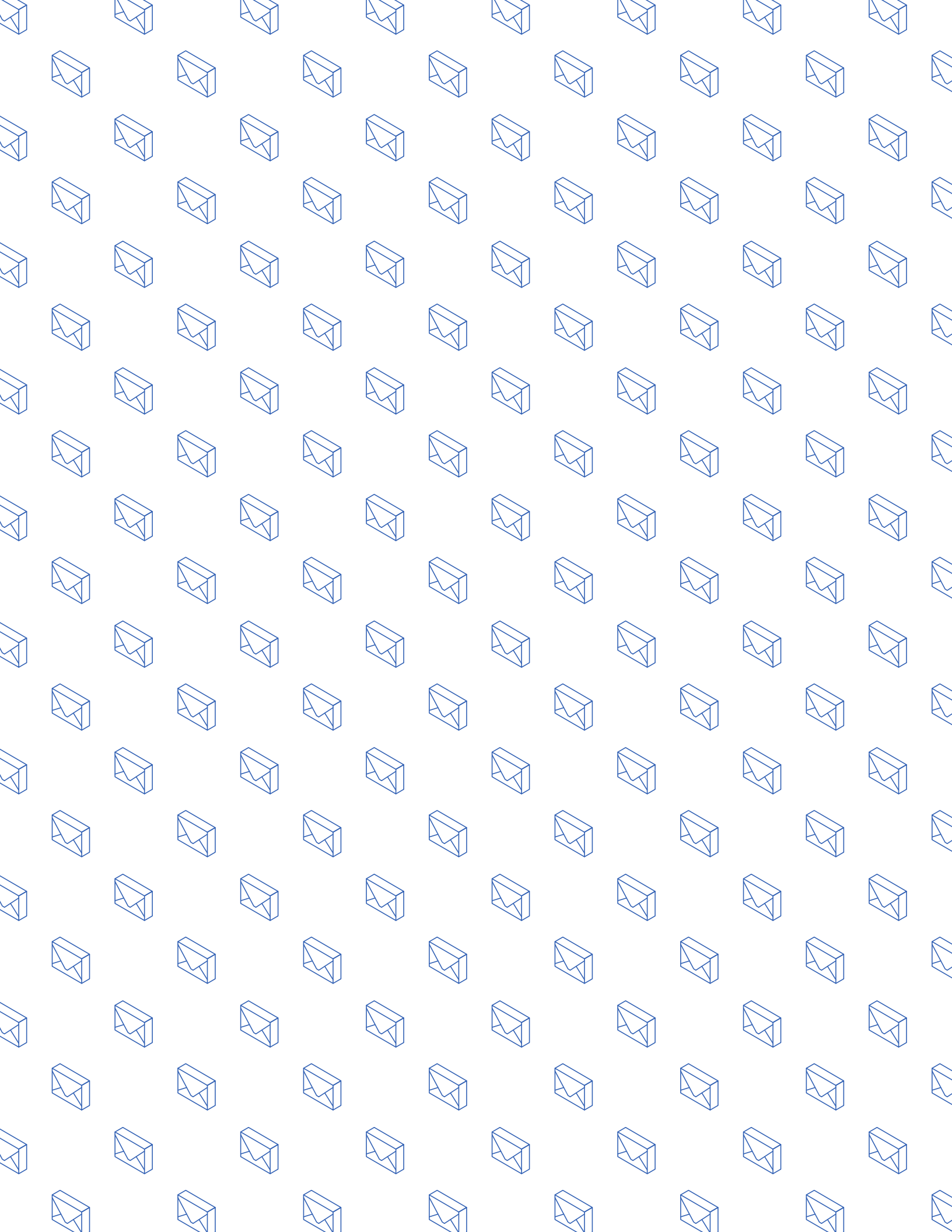
## **Secure Your Secrets** ..... 29

- Activity 1: **How to build a great password**
- Activity 2: **Keep it to yourself**
- Activity 3: **Interland: Tower of Treasure**

## **It's Cool to Be Kind** ..... 37

- Activity 1: **How can I be an upstander?**
- Activity 2: **...but say it nicely!**
- Activity 3: **Mind your tone**
- Activity 4: **Walking the walk**
- Activity 5: **Interland: Kind Kingdom**

## **When in Doubt, Talk It Out** ..... 47



# Share with Care

## Protecting your online reputation

---

### Lesson overview

- Activity 1: **Can you keep a secret?**
- Activity 2: **The profile guessing game**
- Activity 3: **How do others see us?**
- Activity 4: **Privacy in practice**
- Activity 5: **Interland: Mindful Mountain**

---

### Themes

Teachers and parents understand how early digital mistakes can do lasting damage to one's reputation. But it can be harder to convince preteens that a seemingly harmless post today could in the future be misunderstood by unintended audiences.

These activities use concrete examples to teach students how to maintain a positive online reputation by managing their privacy and protecting their personal information.

---

### Goals

- ✓ **Create and manage** a positive reputation online.
- ✓ **Respect** the privacy boundaries of others.
- ✓ **Understand** the potential impact of a mismanaged digital footprint.
- ✓ **Ask** for adult help dealing with sticky situations.

---

### Standards addressed

**ISTE Standards for Teachers:** 1a, 1b, 1d, 2a, 2c, 3b, 3d, 4a, 4b, 4c, 4d, 5b **ISTE Standards for Students 2016:** 1d, 2a, 2b, 2d **AASL Learning Standards:** 1.1.1, 1.1.2, 1.1.8, 1.3.3, 1.3.5, 2.1.3, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4

# Share with Care

## Vocabulary



### **Digital footprint**

Your digital footprint is everything on the Internet that makes you you! This could mean photos, audio, videos, texts, blog posts, and messages you write on friends' pages.

### **Personal information**

Information about a specific person. Your personal information can be varying degrees of public or private, depending on how sensitive it is.

### **Settings**

The area in any digital product, app, website, etc., where you can define or adjust what you share and how your account is handled

### **Boundary**

A point or limit that indicates where two things become different, or unofficial rules about what should not be done. Behavior is acceptable on one side of the boundary, but not on the other.

# Can you keep a secret?

Students pair up and compare pretend secrets to start thinking about zones of privacy.

## Goals



- ✓ **Understand** what kinds of personal information should be kept private.
- ✓ **Remember** that everyone deserves to have their secrets kept private.
- ✓ **Identify** other types of personal information that can be found online.

## Let's talk



### Why does privacy matter?

Your digital footprint is everything on the Internet that's about you. This could mean photos, audio, videos, texts, your posts on friends' pages, etc. As you get older, a strong online presence can bring with it all kinds of benefits. The Internet makes it easy to communicate with family, friends, and people who love the same things that you do. We send messages, share pictures, and join conversations on social networks, sometimes without giving it a second thought.

But all this online connection can also pose various risks. Once something's out there, there's no turning back. A picture or post that you think is funny and harmless today could be seen and misunderstood in the future by people you never wanted to show it to. Remember:

- Like everything else on the Internet, your digital footprint could be seen by anyone in the world.
- Once something about you is online, it could be online forever.

That's why your privacy matters. You can protect it by sharing only things that you're sure you want to share—in other words, by being careful about what persona you create online. Knowing when to stay silent is the key to respecting other people's privacy and protecting your own.

## Activity



### 1. Make up a secret

First, everyone think of a pretend secret (not something real).

### 2. Tell your partner

Okay, got your secrets? Now let's all pair up, share your secret with your partner, and discuss these two questions:

- Would you share this secret with anyone?
- With whom would you share your secret and why?

### 3. Tell the class

Finally, each student will tell the class their secret and what they decided about sharing it.

Continued on the next page →



## Share with Care: Activity 1 (continued)

---

### Takeaway

Secrets are just one type of personal information that we might want to keep private, or share only with trusted family or friends. What other kinds of information should we be careful to protect?

- Your home address and phone number
- Your email password and other online passwords
- Your usernames
- Your schoolwork and other documents you create
- Your photos, videos, music, and other content

# The profile guessing game

Students study a collection of personal information about a fictitious character in order to try to deduce things about this person.

## Goals



- ✓ **Identify** ways information can be found online about people.
- ✓ **Decide** what you know about someone based on their personal data.
- ✓ **Realize** not all these inferences accurately represent a person.

## Let's talk



### How we know what we (think we) know

There's a lot of personal information to be found on the Internet. Some of that information can cause us to make assumptions about people that aren't true. These are the questions we're going to explore:

- What can we learn about a person from their personal information?
- What can we guess from personal information, even if we aren't sure?
- Do we know how this information was collected in the first place?

## Activity



### Materials needed:

- Various fictitious personal data sources. You can use the handout on the next page, or create one using these ideas:
  - Social media accounts, if age appropriate
  - Printed-out browser history logs
  - Printed-out list of locations where they "checked in" (restaurants, coffee shops, Wi-Fi hotspots)
  - Notebooks or devices for a short writing assignment

### 1. Study the person

First, everyone gets their own copy of our character's digital footprint and gives it a read.

### 2. Write a description

Then we'll separate into groups, and each group will write their own quick description of this person. Who do you think they are?

### 3. Reveal the truth

Okay, now here's the truth about our characters:

- **Jenny** is a high school senior. She is going to college next year and hopes to study business, and eventually start her own fashion label. She cares most about: family, volunteering, pop culture, fashion.
- **Tyler** is the starting pitcher on the high school baseball team. He is 16 and lives in Philadelphia. He has an 8-year-old sister. He cares most about: baseball, art, playing the guitar, his friends.
- **Leah** is 17. She just joined the soccer team and has two cats. She is very good at engineering and likes to build robots on weekends. She cares most about: technology, her soccer team, animals and animal rights.

Now, which of our guesses were correct, and which ones weren't?

Continued on the next page →

## Share with Care: Activity 2 (continued)

### Takeaway

Our assumptions about people aren't always right, but too often we use these inaccurate conclusions to judge or make decisions about someone. Always try to make sure you really know the things about people that you think you know!


Read each description of a person's online activity below. After each example, write a short description of who you think this person is. What do they like, dislike, and care about?

## Jenny

Under-the-sea photos from the dance!  
Looking good, y'all!

 Best Ways to Battle Zits

My little brother alex is SOO annoying.  
Maybe he's an alien

 Laser Tag Arena, Maple St.

 Young Designers Conference  
at Thompson University

FINALLY SAW THE NEW SPY WARS  
MOVIE. Omg obsessed!

## Tyler

Won game! One more game to go  
before championship. Gotta practice  
more 1st base throws.

I hate school dances. #notgoing

 Academy of Science,  
Philadelphia

 10 Signs Your Parents are  
Trying to Ruin Your Life

Fishing this saturday with my dad at  
Penny Pack Park! Gonna be awesome

 La La Luna at  
City Center Area

## Leah

 Barney's Burger Emporium

Missed the winning goal. ugh.  
At least we tied.

 25 Photos of Puppies

 The Westfield High Junior Prom

Check out my friend's website!  
I wrote the code for it.

New high score!!  
Yessss. I luv gem jam!!

<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>	<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>	<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>
---	---	---

# How do others see us?

Students explore how different types of people – parents, employers, friends, the police – would see the character from the previous activity.

## Goals



- ✓ **Understand** the perspectives of people other than ourselves when we're deciding whether or not to share information online.
- ✓ **Consider** the consequences of exposing personal information: What you share becomes part of your reputation, which can be permanent.

## Let's talk



### A new point of view

The information in your digital footprint could tell people more about you than you meant to reveal – and the consequences can be significant.

Let's take another look at the profile from our character's POV.

- Do you think he or she wants people to know all this personal info?
- How might this information be used by other people?

Different situations call for different levels of privacy. Seeing the world from someone else's point of view is the key to getting privacy right.

## Activity



### Materials needed:

- A copy for each student of the fictitious profile from Activity 2

### 1. Take a new point of view

Now we're going to break into groups, and each group will be thinking about our character from the POV of one of these types of people:

- Parent
- Coach
- Employer
- Friend
- Police
- Advertiser
- Yourself in 10 years

What's important to your type? What conclusions would they reach about this profile? Cross out the information that you think our character would not want your group to see or that it would be unwise for them to reveal.

### 2. Present conclusions

Finally, each group presents their results and explains their privacy choices.

## Takeaway

Different people can see the same information and draw different conclusions from it. Don't assume that people online will see you the way you think they'll see you.

# Privacy in practice

---

The class reviews three written scenarios and discusses what might be the best privacy solution for each one.

---

## Goals



- ✓ **Study** how to see privacy concerns from different people's points of view.
- ✓ **Understand** how different scenarios demand different levels of privacy.

---

## Let's talk



---

### Privacy scenarios: What should you do?

**Example #1:** A kid you know at school gets bitten by a weird insect that causes an ugly multicolored rash on her stomach. She doesn't want other people to know.

- Do other people have a right to know?
- Should you be the one to tell them?

**Example #2:** Someone writes in their diary. Another person copies what they wrote and posts it online.

- Was the other person wrong to post the diary entries?
- How would you feel if someone did this with your diary?

**Example #3:** Someone posts, "Have a good vacation," on a friend's social media page.

- Had the friend announced publicly that they were going away?
- Are there more private ways to communicate this message—i.e., sending a private message or text?

---

## Activity



---

We're going to review three scenarios and talk about how each one might have a different privacy solution.

---

## Takeaway

---

Different situations call for different responses. And it's always important to respect other people's privacy choices, even if they aren't the choices you yourself would make.

## Share with Care: Activity 5

# Interland: Mindful Mountain

---

The mountainous town center of Interland is a place where everyone mingles and crosses paths. But you must be very intentional about what you share and with whom...information travels at the speed of light and there's an oversharer among the Internauts you know.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/Interland](https://g.co/Interland), and navigate to the land called Mindful Mountain.

---

### Discussion Topics



Play the game with your classroom and use the questions below to prompt further discussion about the lessons learned in the game.

- Of all the posts you shared in the game, which type do you think you would share most often in real life? And why?
- Describe a time when you may have accidentally shared something that you shouldn't have.
- Why do you think the character in Mindful Mountain is called an oversharer?
- Describe the oversharer's character and how his actions affect the game.
- Did playing Mindful Mountain change the way you'll think about sharing with others online in the future?
- Name one thing you'll do differently after joining in these lessons and playing the game.
- What is one example of a possible negative consequence from sharing something with the public instead of just your friends?
- What steps can you take if you accidentally share something personal?



# Don't Fall for Fake

Staying away from phishing and scams

---

## Lesson overview

Activity 1: **Don't bite that phishing hook!**

Activity 2: **Who are you, really?**

Activity 3: **Interland: Reality River**

---

## Themes

It's important for kids to understand that the content they find online isn't necessarily true or reliable, and sometimes may involve malicious efforts to steal their information. Phishing and other online scams encourage Internet users of all ages to respond to mysterious pitches from people they don't know, or from people pretending to be someone they do know.

---

## Goals

- ✓ **Understand** that just because something is online doesn't mean it's true.
- ✓ **Learn** how phishing works, and why it's a threat.
- ✓ **Recognize** fake offers, prizes, and other online scams.

---

## Standards addressed

**ISTE Standards for Teachers:** 1a, 1b, 2a, 3d, 4a, 4b, 4c, 4d **ISTE Standards for Students 2016:** 1d, 2a, 2b, 2c, 2d, 3a, 3b **AASL Learning Standards:** 1.1.1, 1.1.5, 1.1.6, 1.1.8, 1.2.4, 1.2.6, 1.3.3, 1.3.5, 2.1.1, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 4.1.7, 4.3.2, 4.3.4, 4.4.4 **C3:** II:A, II:B, II:C, III:A, III:B, III:C, III:D



# Don't Fall for Fake

## Vocabulary



### **Phishing**

A phishing attack happens when someone tries to trick you into sharing personal information online. Phishing is usually done through email, ads, or sites that look similar to sites you already use.

### **Spearphishing**

A phishing scam where an attacker targets you more precisely by using pieces of your own personal information

### **Scam**

A dishonest attempt to make money or gain something else of value by tricking people

### **Trustworthy**

Able to be relied on to do what is right or what is needed

### **Authentic**

Real, genuine, true, or accurate; not fake or copied

### **Verifiable**

Something that can be proven or shown to be true or correct

### **Deceptive**

Intended to make someone believe something that isn't true

### **Fraudulent**

Done to trick someone for the purpose of getting something valuable

### **Firewall**

A program that shields your computer from most scams and tricks

## Don't Fall for Fake: Activity 1

# Don't bite that phishing hook!

A game where students study various emails and texts and try to decide which messages are legit and which are phishing scams

### Goals



- ✓ **Learn** techniques people use to steal identities.
- ✓ **Review** ways to prevent identity theft.
- ✓ **Know** to talk to a trusted adult if they think they're a victim of identity theft.
- ✓ **Recognize** the signs of phishing attempts.
- ✓ **Be careful** about how and with whom they share personal info.

### Let's talk



#### What is this phishing thing, anyway?

Phishing is when someone tries to steal information like your login or account details by pretending to be someone you trust in an email, text, or other online communication. Phishing emails – and the unsafe sites they try to send you to or the downloads and attachments they try to get you to open – can also put viruses on your computer that use your contact list to target your friends and family with more phishing emails. Other scams might try to trick you into downloading malware or unwanted software by telling you that there's something wrong with your device. Remember: A website or ad can't tell if there's anything wrong with your machine!

Some phishing attacks are obviously fake. But others can be sophisticated and convincing. For instance, when a scammer sends you a message that includes some of your personal information, it's called spearphishing, and it can be very effective.

It's important to know how to spot anything odd or unusual in emails and texts early, before you click on questionable links or enter your password on risky websites.

Here are some questions to ask when you're assessing a message or site:

- Does it include the indicators of a trustworthy site, such as badges?
- Does a site's URL match the name and title you're looking for?
- Are there any pop-ups? (They're often bad news.)
- Does the URL start with `https://` preceded by a green padlock? (That means the connection is encrypted and secure.)
- What's in the fine print? (That's where they put the sneaky stuff.)

And what if you do fall for a scam? Start with this: Don't panic!

- Tell your parent, teacher, or other trusted adult right away. The longer you wait, the worse things could get.
- Change your passwords for online accounts.
- If you do fall for a phishing attempt or scam, let any friends who might be targeted as a result know.
- Use settings to report the message as spam, if possible.

Continued on the next page →

## Don't Fall for Fake: Activity 1 (continued)

---

### Activity



#### Materials needed:

- Student handout:  
Phishing examples

#### Answers to student handout:

##### Phishing examples

1. **Real.** The email asks the user to sign in to their account on their own, rather than providing a link that could be malicious.
2. **Fake.** Suspicious and not secure URL
3. **Real.** Note the https:// in the URL
4. **Fake.** Suspicious offer in exchange for bank details
5. **Fake.** Not secure and suspicious URL

#### 1. Groups study examples

Let's divide into groups, and each group study these examples of messages and websites.

#### 2. Individuals indicate choices

Decide "real" or "fake" for each example, and list reasons why below.

#### 3. Groups discuss choices

Which examples seemed trustworthy and which seem suspicious? Did any answers surprise you?

#### 4. Further discussion

Here are some more questions to ask yourself when assessing messages and sites you find online:

##### • Does this message look right?

What's your first instinct? Do you notice any untrustworthy parts?

##### • Is the email offering you something for free?

Free offers usually aren't really free.

##### • Is it asking for your personal information?

Some websites ask for personal info so they can send you more scams. For example, "personality tests" could be gathering facts to make it easy to guess your password or other secret information. Most real businesses, on the other hand, won't ask for personal information over email.

##### • Is it a chain email or social post?

Emails and posts that ask you to forward them to everyone you know can put you and others at risk. Don't do it unless you're sure of the source and sure the message is safe to pass on.

##### • Does it have fine print?

At the bottom of most documents you'll find the "fine print." This text is tiny, and often contains the stuff you're supposed to miss. For example, a headline at the top might say you've won a free phone, but in the fine print you'll read that you actually have to pay that company \$200 per month.

#### Note

For the purposes of this exercise, assume that Internaut Mail is a real, trusted service.

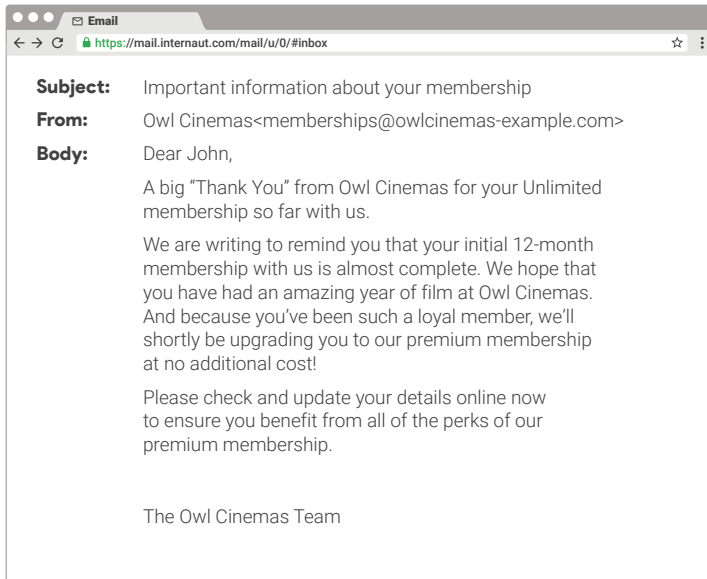
---

### Takeaway

When you're online, always be on the lookout for phishing attacks in your email, texts, and posted messages—and make sure you tell the right people about it if you do get fooled.

## Worksheet: Activity 1

# Phishing examples



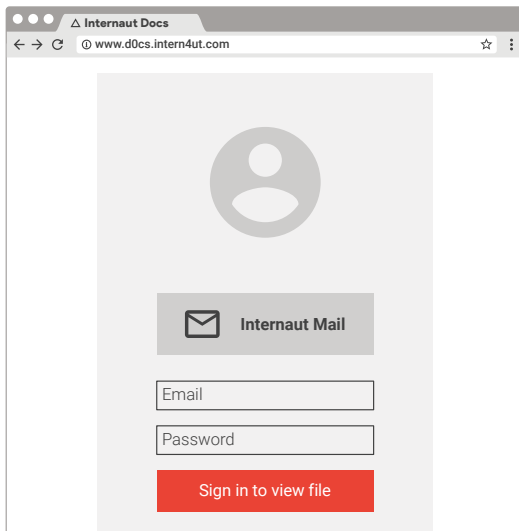
### 1. Is this real or fake?

\_\_\_\_\_

Real

\_\_\_\_\_

Fake



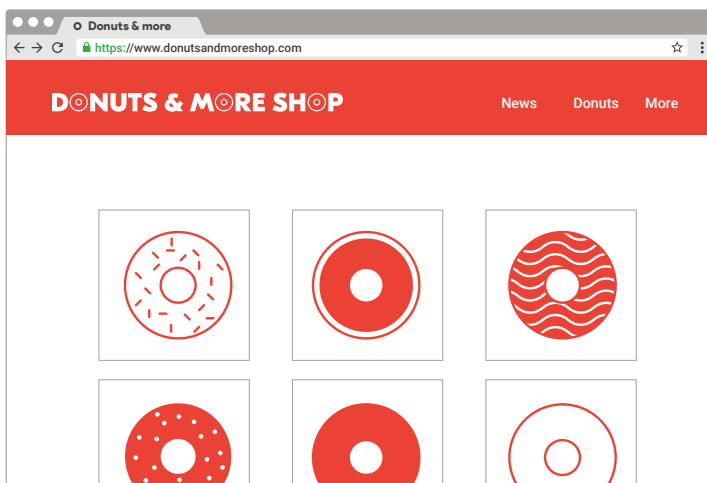
### 2. Is this real or fake?

\_\_\_\_\_

Real

\_\_\_\_\_

Fake



### 3. Is this real or fake?

\_\_\_\_\_

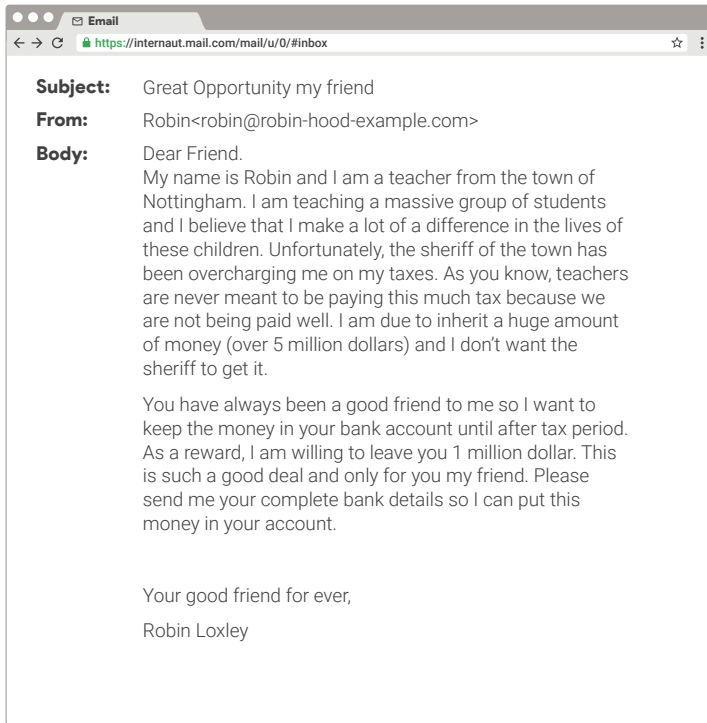
Real

\_\_\_\_\_

Fake

Continued on the next page →

## Worksheet: Activity 1 (continued)



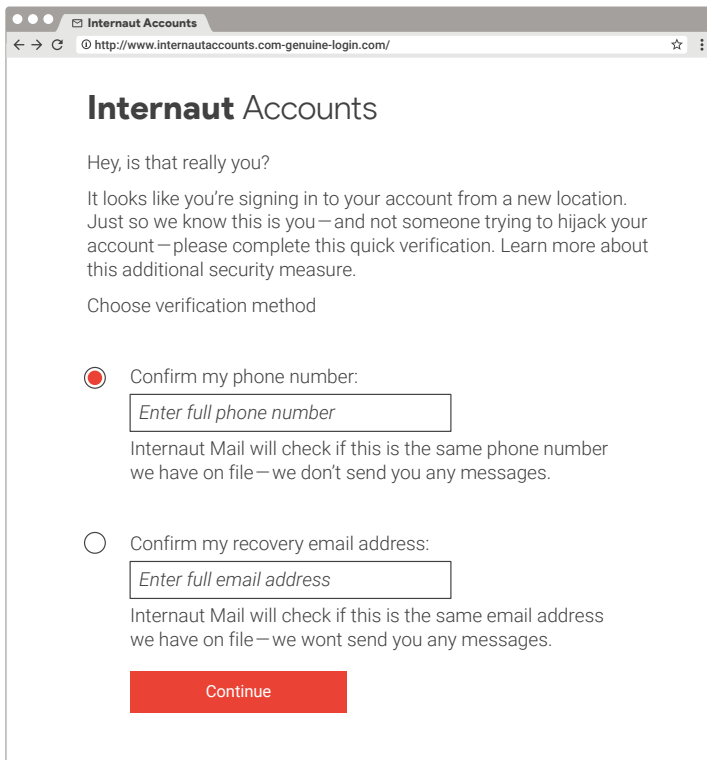
### 4. Is this real or fake?

\_\_\_\_\_

Real

\_\_\_\_\_

Fake



### 5. Is this real or fake?

\_\_\_\_\_

Real

\_\_\_\_\_

Fake

# Who are you, really?

Students practice their anti-phishing skills by acting out, and discussing possible responses to, suspicious online texts, posts, pictures, and email.

## Goals



- ✓ **Recognize** that their online audience might be bigger than they think.
- ✓ **Confirm** that they really know the identity of the people they talk with online.
- ✓ **Stop and think** before they “friend” or connect with someone online.
- ✓ **Be careful** about who they give personal information to, and what kinds of things they share.
- ✓ **Ask** questions and/or seek help from an adult if they aren't sure.
- ✓ **Tell an adult** if someone tries to discuss something online that makes them uncomfortable.
- ✓ **Act with honesty** in all their online interactions.

## Let's talk



### How do you know it's really them?

When you're on the phone with a friend, how can you tell it's them, even though you can't see them? Sometimes people pretend to be other people online in order to tease them. Other times, they impersonate others in order to steal personal information. When you're on the Internet, strangers could ask to connect with you. It's up to you to decide whether you want to connect with that person, and what or how to reply.

Fortunately, you can verify people's identity and spot scammers. Here are a few ideas to start thinking about.

#### • Is their profile picture suspicious?

Is their profile picture blurry or hard to see? If so, be cautious; a blurry photo is easier to hide behind. It's also common for scammers to steal photos from a real person in order to set up a fake profile.

#### • Does their displayed name match their username?

On social media, for instance, does their profile URL match their given name? (For example, Jane Doe, with an address that's something like SocialMedia.com/jane.doe.)

#### • Do they have a personal biography?

If so, does it sound like it was written by a real person? Fake accounts might not have much “About Me” information, or might have grouped together some information to create a fake profile.

#### • How long has the account been active?

Is the profile new or does it show a lot of abnormal activity? Fake accounts often lack a history of posts or social interactions.

Continued on the next page →

## Don't Fall for Fake: Activity 2 (continued)

---

### Activity



#### Materials needed:

- A copy of the "Who are you, really?" worksheet cut into strips, with one scenario on each strip
- A bowl or container for students to pick strips from
- Cheat sheet on pages 25 and 26

#### 1. Groups review scenarios

Okay, now we're going to separate into groups. Each group will pick a scenario from this container and talk about how you should respond to this situation.

#### 2. Groups act out scenarios

Now each group acts out its scenario: one student narrating, a second performing the "message," a third responding, maybe a fourth explaining the reasoning.

#### 3. Class discusses groups' choices

Finally, let's use this cheat sheet to discuss each group's choices.

---

### Takeaway

You control who you talk to online. Make sure the people you connect with are who they say they are!

# Who are you, really?

---

**Scenario 1**

You get a message request online from a stranger. "Hey! You seem like a fun person to hang out with. Let's have some fun together! Can you add me to your friends list? –Jason"

..... ✂

**Scenario 2**

You get a text message on your cell phone from someone you don't recognize. "Hey, this is Jen! Remember me from the summer?"

..... ✂

**Scenario 3**

After math class with Mrs. Beckstrom you get this message on your cell phone. "I'm Mark from your Math class with Mrs. Beckstrom. Did u understand the homework?"

..... ✂

**Scenario 4**

You get a message from someone you don't follow. "Hey! Love your posts, you're SO funny! Give me your phone number and we can talk more!"

..... ✂

**Scenario 5**

You get a chat from someone with whom you aren't familiar. "I saw you in Math class today. U R CUTE! What is your address? I can come over 2 hang out."

..... ✂

**Scenario 6**

You receive a message online. "Hey, I just met your friend Sam! She told me about you, would love to meet you. What's your address?"

..... ✂



# Who are you, really?

---

## Scenario 1

You get this message from someone you don't recognize: "Hey! You seem like a fun person to hang out with. Let's have some fun together! Can you add me to your friends list? — Jason"

- **Ignore Jason.** If you don't know him, you can just decide not to talk to him, period.
- **"Hi, Jason. Do I know you?"** If you aren't sure, ask first.
- **Block Jason.** If you've checked who he is and decide to block him, you won't get any more messages from him.
- **Add Jason to your friends list.** Not recommended, unless you've verified who he is.
- **Check Jason's profile.** If he seems okay, you can add him to your friends list. But be careful—profiles are easy to fabricate! Check this guy's friends list to see who he's connected to; his circle of friends can be another way to tell whether or not he's real.
- **Give him personal info.** Should you respond something like, "Great to know new people in the neighborhood! I'm new in this town. We can meet after school sometime (I go to Emerson Middle school)"? No way! It's never good to give away personal information to people whom you don't know, especially online.

---

## Scenario 2

You get a text message on your cell phone from someone you don't recognize. "Hey, this is Jen! Remember me from the summer?"

- **Block Jen.** This could be a rude thing to do if you actually know her. Use this option only if you know her but you don't want to get her messages anymore, or you're sure you didn't meet anyone named Jen last summer.
- **Ignore Jen.** Like we said above, if you don't know this person, you can just not talk to her, period.
- **"Hi, Jen. Do I know you?"** This is a safe option if you aren't sure what to do.
- **"Hey! What's up? Nice to reconnect."** This is fine, as long as you do actually remember her from the summer!
- **"Are you the girl with the red hair?"** If you aren't sure whether you know her, you can try to get more information to help you remember.
- **"I don't remember you but we can still meet sometime."** Really not a good idea; you should never offer to meet with anyone you don't know.

Continued on the next page →

## Phishing cheat sheet: Activity 2 (continued)

---

### Scenario 3

After math class with Mrs. Beckstrom, you get this message on your cell phone. "I'm Mark from your Math class with Mrs. Beckstrom. Did u understand the homework?"

- **Ignore Mark.** As always, if you don't know this person, you don't have to respond at all.
- **Block Mark.** A good choice if you're sure there's no Mark in Mrs. Beckstrom's math class.
- **"Hi, Mark. Are you the one sitting behind me?"** If you aren't sure, you can ask.
- **"Sure. Can explain after school."** This is a good choice only if you're sure who this person is.
- **"I don't take Math with Mrs. Beckstrom – I have Mr. Snyder."** If you don't trust this person based on what they said, your best choice is to ignore the message. Certainly you shouldn't be giving them personal information, like the name of your math teacher.
- **"Call me at (650) 555-3444."** Probably not; unless you're certain that you know this person, it's not a good idea to send your personal information.

---

### Scenario 4

You get a message from someone you don't follow. "Hey! Love your posts, you are SO funny! Give me your phone number and we can talk more!"

- **Ignore @soccergirl12.** You don't have to respond if you don't want to.
- **Block @soccergirl12.** If you find this person suspicious and block them, you'll never hear from them again.
- **"Hi, do I know you?"** If you aren't sure, ask questions before giving out personal information.
- **"Okay, my number is..."** Nope! Even if you've verified who this person is, it isn't a good idea to give out personal information over social media. Find another way to get in touch, through parents, teachers, or some other trusted person.

---

### Scenario 5

You get a chat from someone you don't know. "I saw you in Math class today. U R CUTE! What is your address? I can come over 2 hang out."

- **Ignore.** Probably a good choice.
- **Block this person.** Don't hesitate if you get a bad feeling about someone.
- **"Who are you?"** Probably not. If the message sounds suspicious, it might be better not to answer or block them.
- **"Is that you Lizi? U R CUTE too! I live at 240 Circle Ct."** This isn't a good idea, even if you think you know who it is. Before you give someone new your address or other personal information, check them out, even if you assume you know them.

---

### Scenario 6

You receive this message: "Hey, I just met your friend Sam! She told me about you, would love to meet you. What's your address?"

- **Ignore.** If you don't know this person but you do have a friend named Sam, your safest choice is to check with Sam first before responding to this message.
- **Block.** If you don't know this person and you don't have a friend named Sam, it's probably a good idea to use your settings to block this person from contacting you further.
- **"Who are you?"** Probably not a great idea; if you don't know the person, it's better not to answer, at least until you've heard back from Sam.

# Interland: Reality River

---

The river that runs through Interland flows with fact and fiction. But things are not always as they seem. To cross the rapids, use your best judgment and don't fall for the antics of the phisher lurking in these waters.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/Interland](https://g.co/Interland), and navigate to the land called Reality River.

---

## Discussion Topics



Reality River should foster students' thinking. After they play, these questions should facilitate discussion of the game's themes.

- Describe a time when you had to decide if something was real or fake online.  
What signs did you notice?
- What is a phisher? Describe its behaviors and how it affects the game.
- Did playing Reality River change the way you'll evaluate things and people online in the future?
- What's one thing that you think you'll do differently after joining in these lessons and playing the game?
- What are some clues that could signal that something is "off" about a certain situation online?
- How does it feel when you come across something questionable online?
- If you really aren't sure whether something is real, what should you do?



# Secure Your Secrets

Getting real about privacy and security

---

## Lesson overview

Activity 1: **How to build a great password**

Activity 2: **Keep it to yourself**

Activity 3: **Interland: Tower of Treasure**

---

## Themes

Online privacy and security issues don't always have clear right and wrong solutions. Protecting your personal and private information – all the stuff that makes you you – means asking the right questions and finding your own educated answers.

---

## Goals

- ✓ **Learn** why privacy matters, and how it relates to online security.
- ✓ **Practice** how to create strong passwords.
- ✓ **Review** the tools and settings that protect against hackers and other threats.

---

## Standards addressed

**ISTE Standards for Teachers:** 1a, 1b, 2a, 3b, 4a, 4b, 4c, 4d, 5a **ISTE Standards for Students 2016:** 1d, 2a, 2d **AASL Learning Standards:** 1.1.8, 1.3.5, 2.1.3, 2.3.1, 2.3.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4 **C3:** II:A, II:B, II:C, III:A, III:B

# Secure Your Secrets

## Vocabulary



### **Privacy**

Protecting your personal information and that of others

### **Security**

Using good habits for securing hardware and software

### **Two-step verification**

A security process where logging in to a service requires two steps. You may have to enter in your password and enter in a code that was texted to your phone number, for example

### **Security token**

A key fob or other small hardware device that you carry in order to authorize access

### **Password**

A secret combination used to access something

# How to build a great password

Students learn how to create a strong password – and make sure it stays private after they create it.

## Goals



- ✓ **Recognize** the importance of sharing their passwords only with their parents or guardian.
- ✓ **Learn** about the passwords that protect their devices.
- ✓ **Understand** how to create passwords that are hard to guess and easy to remember.
- ✓ **Choose** the right security for their login settings, including two-factor verification.

## Let's talk



### Better safe than sorry

Digital technology makes it easy to communicate with friends, classmates, teachers, and more. We can connect with the world in so many ways: via email, text, and instant messages; in words, pics, and videos; using phones, tablets, and laptops. (How do you connect with your friends?)

But the same tools that make it easy for us to share information also make it easier for hackers and scammers to steal that information and use it to damage our devices, our relationships, and our reputations.

Protecting all the stuff that goes into creating our online reputations means doing simple, smart things like using screen locks on our devices, being careful about putting personal info on devices that can be lost or stolen, and above all, choosing good passwords.

- Who can guess what the two most commonly used passwords are?  
(Answer: "1 2 3 4 5 6" and "password")
- Let's brainstorm some other bad passwords.  
(Examples: your full name, your phone number, the word "chocolate")

Who thinks these passwords are good?

Continued on the next page →

## Secure Your Secrets: Activity 1 (continued)

---

### Activity



#### Materials needed:

- Internet-connected devices for students or groups of students.
- A chalk/whiteboard or projection screen
- Student handout: Guidelines for creating strong passwords

Let's practice our new skills by playing the password game.

#### 1. Create passwords

We'll all split into teams of two. Each team will have 60 seconds to create a password.

#### 2. Compare passwords

Two teams at a time will write their password on the board.

#### 3. Vote!

For each pair of passwords, we'll all vote and discuss whose is stronger.

---

### Takeaway

Here's an idea for creating an extra-secure password.

Think of a fun phrase that you can remember. It could be your favorite song lyric, book title, movie catchphrase, etc.

- Choose the first letter or first two letters from each word in the phrase.
- Change some letters to symbols.
- Make some letters uppercase and some lowercase.

---

### Guidelines for creating strong passwords

Here are some tips for creating passwords to safeguard your secrets.

**Strong passwords** are based on a descriptive sentence that's easy for you to remember and difficult for someone else to guess.

**Moderate passwords** are passwords that are strong and not easy to guess by bad software, but could be guessed by someone who knows you.

**Weak passwords** commonly use personal information, are easy to crack, and can be guessed by someone who knows you.

---

### DOs

- Use a unique password for each of your important accounts.
- Use at least eight characters.
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.

---

### DON'Ts

- Don't use personal information (name, address, email, phone number, Social Security number, mother's maiden name, birth dates, etc.), or common words in your password.
- Don't use a password that's easy to guess, like your nickname, name of your school, favorite baseball team, etc.
- Don't share your password with anyone other than your parents or guardian.



# Keep it to yourself

Teacher uses a school device to demonstrate where to look, and what to look for, when you're customizing your privacy settings.

## Goals



- ✓ **Customize** privacy settings for the online services they use.
- ✓ **Make decisions** about information sharing on the sites and services they use.
- ✓ **Understand** what two-factor and two-step verifications mean, and when to use them.

## Let's talk



### Privacy equals security

Online privacy and online security go hand in hand. Most apps and software offer ways to control what information we're sharing and how.

When you're using an app or website, look for an option like "My Account" or "Settings."

That's where you'll find the privacy and security settings that let you decide:

- What information is visible in your profile
- Who can view your posts, photos, videos, or other content that you share

Learning to use these settings to protect your privacy, and remembering to keep them updated, will help keep you as safe as possible.

## Activity



### Materials needed:

- One school device hooked up to a projector and able to display an example account deemed appropriate for class demonstration (e.g., a temporary email or website account)

### 1. Review options

I have my school device hooked up to the projection screen. Let's navigate to the settings page of this app. We can see that our options include:

- Changing your password
- Getting alerts if someone tries to log in to your account from an unknown device
- Making your online profile—including photos and videos—visible only to circles of family and friends that you choose
- Enabling two-factor or two-step verification

### 2. Additional verification options

Let's talk about two-step and two-factor verifications.

- Two-step verification: When you log in to your account, it will require two steps. For example, it may ask you to enter your password AND text you a code that expires in 10 minutes to enter.
- Two-factor verification: The system will require two types of information to log you in. For example, it may ask for your normal password AND your fingerprint.

Continued on the next page →

## Secure Your Secrets: Activity 2 (continued)

---

Which privacy and security settings are right for you? That's something to discuss with your parent or guardian. But remember, the most important security setting is in your brain—you make the key decisions about how much of your personal info to share, when and with whom.

---

### Takeaway

Choosing a strong unique password for each of your important accounts is a good first step. Now you need to remember them and also keep them safe.

Writing down your passwords isn't necessarily a bad idea. But if you do this, don't leave the page with your passwords in plain sight, such as on your computer or desk. Safeguard your list, and protect yourself, by keeping it somewhere that isn't easily visible.

# Interland: Tower of Treasure

---

Mayday! The Tower is unlocked, leaving the Internaut's valuables like personal info and passwords at high risk. Outrun the hacker and build an untouchable password every step of the way to secure your secrets once and for all.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/Interland](https://g.co/Interland), and navigate to the land called Tower of Treasure.

---

## Discussion Topics



Tower of Treasure will get students thinking. After they play, use these questions to start a discussion of the game's themes.

- What are the elements of a super strong password?
- When is it important to create strong passwords in real life? What tips have you learned on how to do so?
- What's a hacker? Describe this character's behaviors and how they affect the game.
- Did Tower of Treasure change the way you plan to protect your information in the future?
- Name one thing you'll do differently after learning these lessons and playing the game.
- Craft three practice passwords that pass the "super strong" test.
- What are some examples of sensitive information that should be protected?



# It's Cool to Be Kind

## The power of online positivity

---

### Lesson overview

Activity 1: **How can I be an upstander?**

Activity 2: **...but say it nicely!**

Activity 3: **Mind your tone**

Activity 4: **Walking the walk**

Activity 5: **Interland: Kind Kingdom**

---

### Themes

The digital world creates particular challenges for kids. Social cues can be harder to read online, anonymity can encourage negative behavior, and online bullying is easily repeated and leaves a digital footprint.

But the Internet can amplify kindness as well as negativity. Learning to convey kindness and empathy—and how to respond to negativity and harassment—is essential for building healthy relationships and reducing feelings of isolation that can sometimes lead to bullying, depression, academic struggles, and other problems.

Research shows that rather than simply telling kids not to be negative online, effective safety education addresses the underlying causes of negative behaviors. These activities encourage students to interact positively from the start and teach them how to deal with negativity if it happens.

---

### Goals

- ✓ **Define** what being positive online looks like.
- ✓ **Define** what being positive means, online and off.
- ✓ **Lead** with positivity in online communications.

---

### Standards addressed

**ISTE Standards for Teachers:** 1b, 1d, 2a, 3b, 4a, 4b, 4c, 5a **ISTE Standards for Students 2016:** 2a, 2b **AASL Learning Standards:** 1.1.5, 1.3.3, 1.3.5, 2.1.3, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 2.4.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.2, 3.3.3, 3.3.6, 4.1.7, 4.2.3, 4.3.4, 4.4.4 **C3:** I:B, I:D, I:E, I:F, I:H, II:C

# It's Cool to Be Kind

## Vocabulary



### **Bullying**

Unwanted, aggressive behavior that is repeated (or has the potential to be repeated) over time

### **Bystander**

Someone who has the power to intervene or report bad behavior but doesn't do anything to stop it

### **Upstander**

Someone who intervenes to stop and/or report inappropriate behavior

### **Harassment**

To create an unpleasant or hostile situation by uninvited and unwelcome verbal or physical conduct

### **Amplify**

To make something louder or stronger

### **Block**

To help prevent an individual from accessing your profile, sending you messages, etc.

# How can I be an upstander?

Students practice identifying the three roles of a bullying encounter (bully, target, and bystander) and what to do if they're a bystander or a target.

## Goals



- ✓ **Evaluate** what it means to be a bystander or upstander online.
- ✓ **Learn** specific ways to respond to bullying when you see it.
- ✓ **Know** how to behave if you experience harassment.

## Let's talk



### Why does kindness matter?

Sometimes it's important to remind ourselves that behind every username and avatar there's a real person with real feelings, and we should treat them that way. When bullying or other inappropriate behavior happens, most of the time there are three types of people involved.

- There's a **bully**, or maybe more than one.
- There's also someone being bullied—the **target** or **victim**.
- And often there are one or more people whom we call **bystanders**.

A bystander has the power to intervene and report inappropriate behavior but doesn't do anything to stop it. Your goal is to be an upstander by fighting bad behavior and standing up for kindness and positivity. A little positivity can go a long way online. But the opposite is also true: A little negativity can spread into something big and ugly online.

Here are some ways that upstanders can help stop bullying and negative messages online:

- **Set a good example.**

Being a positive voice among your friends helps spread positive feelings all around.

- **Be a friend.**

Being consistently friendly—both online and offline—shows your classmates that they're not alone, which can be especially helpful if they're being bullied or just feeling sad.

- **Don't encourage bad behavior by giving it an audience.**

Don't "like" or respond to hurtful comments or posts. Sometimes bullies act aggressively in order to get attention, and if you and your friends don't encourage them, they're more likely to stop.

- **Don't pass on hurtful messages.**

Instead tell the person who sent the message that you don't think it was funny or acceptable, and consider contacting the person who was targeted to provide support and help them get help if needed.

- **Report mean, bullying behavior.**

Use online reporting tools or tell your parent, teacher, friend, or sibling.

Continued on the next page →

## It's Cool to Be Kind: Activity 1 (continued)

---

### Activity



#### Practice as a group

If you find yourself the target of bullying or other bad behavior online, here are some things you can do.

#### If I'm the target, I can...

- Not respond
- Block
- Report – tell my parent, teacher, sibling, or friend.

And what can you do if something bad is happening and you're a bystander?

#### If I'm the bystander, I can...

- Find a way to be kind
- Block
- Report – tell someone who can help, like my parent or teacher.

Taking action as a bystander is what makes you an upstander.

---

### Takeaway

Whether standing up for others, reporting something hurtful, or ignoring something to stop it from being amplified even more, you have a variety of strategies to choose from depending on the situation. Everyone is responsible for creating a great online experience.



## It's Cool to Be Kind: Activity 2

# ...but say it nicely!

In this activity, students work together to reframe negative comments in order to learn how to redirect negative interactions into positive ones.

### Goals



- ✓ **Express** feelings and opinions in positive ways.
- ✓ **Respond** to negativity in constructive and civil ways.

### Let's talk



#### Turning negative to positive

Kids your age are exposed to—and produce—a wide range of content, which can include lots of negative messages that promote bad behavior.

- Have you (or anyone you know) ever experienced a random act of kindness on the web? How did it make you feel?
- Have you (or anyone you know) seen someone be negative on the web? How did that make you feel?
- What simple actions can we take to turn negative interactions into positive ones?

We can respond to negative emotions in constructive ways by rephrasing or reframing unfriendly comments and becoming more aware of tone in our online communication.

### Activity



#### Materials needed:

- A chalk/whiteboard or projection screen
- Student handout: ...but say it nicely!
- Sticky notes or devices for students

#### 1. Read the comments

We're all looking at the negative comments.

#### 2. Write revisions

Now let's separate into teams of three and work on two kinds of responses to these comments:

- How could you have made the same or similar points in more positive and constructive ways?
- If one of your classmates made comments like these, how could you respond in a way that would make the conversation more positive?

#### 3. Present responses

Now each team will perform their responses for both situations.

### Takeaway

Reacting to something negative with something positive can lead to a more fun and interesting conversation—which is a lot better than working to clean up a mess created by an unkind comment.

## Worksheet: Activity 2

# ...but say it nicely!

---

Read the comments below. After each comment, discuss:

**1. How could you have made the same or similar points in more positive and constructive ways?**

**2. If one of your classmates made comments like these, how could you respond in a way that would make the conversation more positive?**

Use the spaces below each comment to write down ideas.

"Lol Connor is the only one in class not going on the camping trip this weekend."

"Everybody wear purple tomorrow but don't tell Lilly."

"Sorry I don't think you can come to my party. It'll cost too much money."

"No offense but your handwriting is embarrassing so you should probably switch groups for this project."

"This makes me cringe— who told her she can sing??"

"You can only join our group if you give me the login to your account."

"Am I the only one who thinks Shanna looks kinda like a Smurf?"

"👎👎👎"

# Mind your tone

Students interpret the emotions behind text messages to practice thinking critically and avoiding misinterpretation and conflict in online exchanges.

## Goals



- ✓ **Make good decisions** when choosing how and what to communicate.
- ✓ **Identify situations** when waiting to communicate until you are face-to-face with a peer is preferable to texting or messaging.

## Let's talk



### It's easy to misunderstand

Young people use different types of communication interchangeably, but messages sent via chat and text can be interpreted differently than they would in person or over the phone.

- Have you ever been misunderstood in text? For example, have you ever texted a joke and your friend thought you were being serious?
- Have you ever misunderstood someone else in a text or chat? What did you do to help clarify the communication? What could you do differently?

## Activity



### Materials needed:

- Sample text messages written on the board or projected

### 1. Review messages

Let's take a look at these sample text messages on the board:

- "That's so cool"
- "Whatever"
- "I'm so mad at you"

### 2. Read messages out loud

Now, for each message, we're going to ask one person to read it aloud in a specific tone of voice (e.g., angry, sarcastic, friendly).

What do you notice? How might these come across to other people? How might each "message sender" better communicate what they really mean?

## Takeaway

It can be hard to understand how someone is really feeling when you're reading what they wrote or texted. Be sure you choose the right mode for your next communication — and that you don't read too much into things that people say to you online.

# Walking the walk

---

Simple class discussion of how kids can model behavior for adults too

---

## Goals



- ✓ **Reflect** on the online behavior of adults.
- ✓ **Consider** how the way adults act can model behavior for younger generations.

---

## Let's talk



### What adults can teach kids

It's important to teach kindness. But it's just as important to model the lessons of kindness that we teach. There are plenty of examples of how bullying and harassment aren't just issues for kids—look at how adults can treat each other online, or in traffic jams.

We've been talking about how important it is to be kind to your classmates and friends online and off. Have you ever seen adults act negatively toward each other? Have you seen adults bullying each other? (Remember, we don't need to name names—let's just talk about the behaviors.)

Do you think some kids start bullying or making unkind comments because they see adults around them doing these things?

---

## Takeaway

How you and your friends treat each other online will have a big impact on the digital world that your generation builds. Do you think your generation can build an Internet that's kinder and more positive than the environments some adults have created for themselves?

A lot of adults think you'll probably be better at this too...

## It's Cool to Be Kind: Activity 5

# Interland: Kind Kingdom

---

Vibes of all kinds are contagious—for better or for worse. In the sunniest corner of town, cyberbullies are running amok, spreading negativity everywhere. Block and report bullies to stop their takeover and be kind to other Internauts to restore the peaceful nature of this land.

Open a web browser on your desktop or mobile device (e.g., tablet), visit [g.co/Interland](https://g.co/Interland), and navigate to the land called Kind Kingdom.

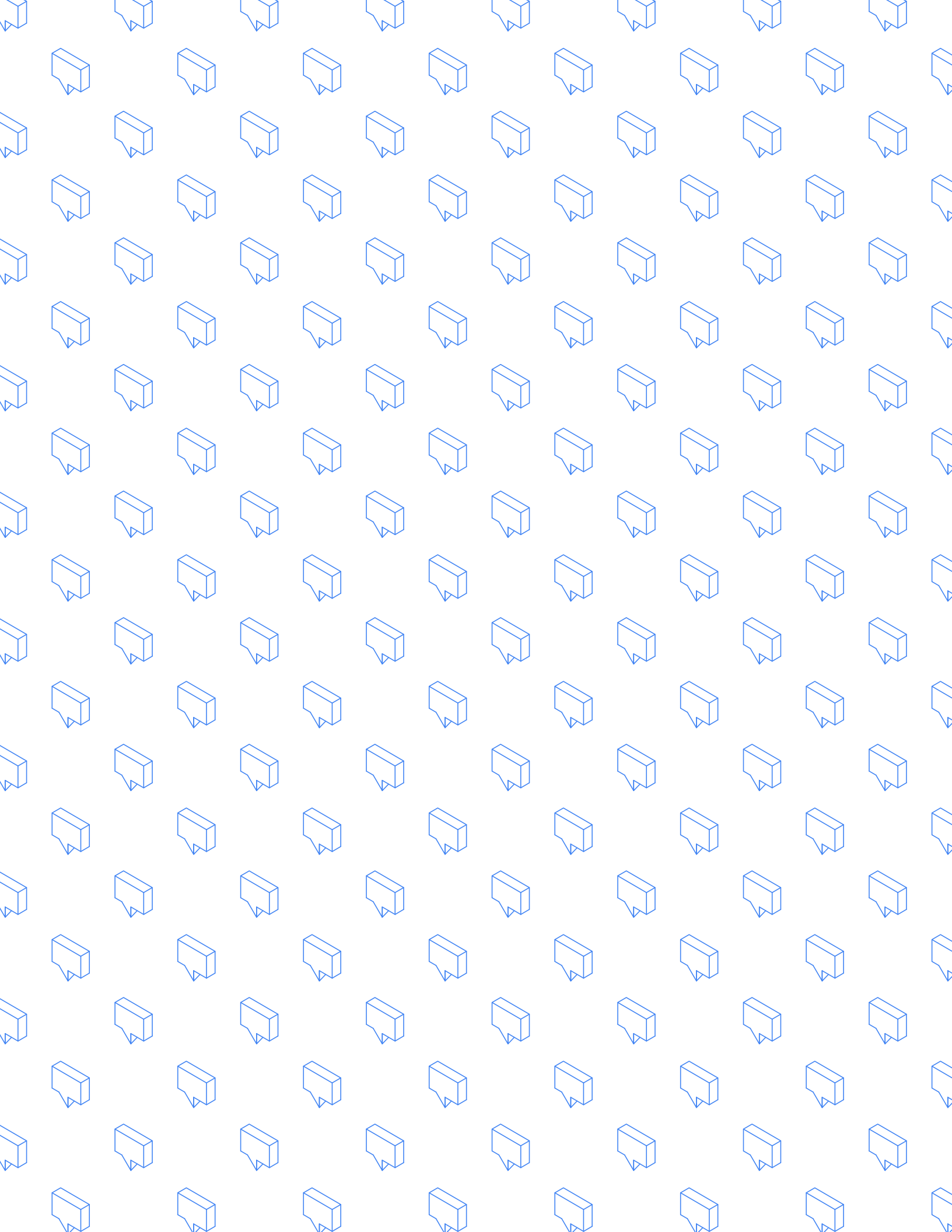
---

### Discussion Topics



Playing Kind Kingdom will foster students' thinking. Afterward, use these questions to start a discussion of the game's themes.

- What scenario in Kind Kingdom do you relate to most and why?
- Describe a time when you've taken action to spread kindness to others online.
- In what situation would it be appropriate to block someone online?
- In what situation would it be appropriate to report someone's behavior?
- Why do you think the character in Kind Kingdom is called a cyberbully? Describe this character's qualities and how his actions affect the game.
- Does this game change the way you plan to behave toward others?



# When in Doubt, Talk It Out

A brief guide to encouraging Internet Brave behavior

---

## Overview

One piece of advice that appears consistently throughout these lessons applies to any online activity: If you come across something questionable, talk to a trusted adult about it. Students should glean this from any one of the lessons, but for quick reference, below is a list of situations in which the “when in doubt, talk it out” principle might be most useful to your students.

Students should “talk it out” with a trusted adult whenever they feel the need. Some common situations include but are not limited to:

- They suspect that their account may have been compromised. (Discussion opportunity: What can you do to make your account security even stronger? See page 31.)
- They need help from a trusted adult remembering a password.
- They are unsure whether something is a scam, or suspect they might have fallen for one. (Discussion opportunity: What are the warning signs? See page 18.)
- Someone tries to discuss something online with them that makes them uncomfortable.
- They receive suspicious contact from a stranger.
- They want to discuss online acts of kindness and *unkindness*.
- They are concerned that they may have shared something online that they should not have.

Foster open communication in your classroom and remind students that you’re always there for backup. Having a student panel or work group, especially with slightly older students, is one effective way to build student agency around this topic.

