

Smart Alert Strong Kind Brave



**The
Cyber
Heroes▲**

**Digital Safety and
Citizenship Curriculum**

Welcome to the Cyber Heroes Curriculum, a joint programme between Google, Test Achats and Child Focus. This resource is part of the Cybersimple.be initiative and specifically designed to teach children the skills they need to move around safely in the online world.

This Curriculum gives teachers the tools and methods that they need to teach online safety in the classroom. The thematic plans, best suited from ages 8 to 12, provide essential thematics that can be used as background material for teachers to give pupils the right grounding so that they can grow up to be safe and responsible digital citizens.

Our five fundamental topics of digital citizenship and safety – the Cyber Code of Heroes – are:

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

These thematics are delivered in detail in Interland, a browser-based game that makes learning about digital safety interactive and fun – just like the Internet itself. Using Interland and the complementary curriculum, teachers can pick and choose the activities that best suit their students, or simply go through the entire series from start to finish.

We believe the Cyber Heroes programme will mark an important step in the right direction and ensure that our children learn about and explore the online world in the right way, while staying safe.

Table of Contents

Educator's Guide	4
Resource 1: Parent introduction email/letter template	
Resource 2: Frequently asked questions	
Thematic 01: Share with Care	7
Activity 1: When not to share	
Activity 2: Whose profile is this, anyway?	
Activity 3: How do others see us?	
Activity 4: Keeping it private	
Activity 5: Interland: Mindful Mountain	
Thematic 02: Don't Fall for Fake	19
Activity 1: Don't bite that phishing hook!	
Activity 2: Who are you, really?	
Activity 3: About those bots	
Activity 4: Interland: Reality River	
Thematic 03: Secure Your Secrets	36
Activity 1: How to build a great password	
Activity 2: Keep it to yourself	
Activity 3: Interland: Tower of Treasure	
Thematic 04: It's Cool to Be Kind	45
Activity 1: From bystanders to upstanders	
Activity 2: Upstander options	
Activity 3: ...but say it nicely!	
Activity 4: Mind your tone	
Activity 5: Walking the walk	
Activity 6: Interland: Kind Kingdom	
Thematic 05: When in Doubt, Talk It Out	61
Activity 1: When to get help	
Activity 2: Report it online, too	

Parent introduction email/letter template

Below is a template for a letter (or email) that you can customize to tell parents about this project and how they can use these tools to help their children learn to make good decisions about their own online safety.



Dear Parent,

When our children are young, we do our best to help them explore the online world while protecting them as best as we can against risks online. But as children mature into adolescents, our role as parents shifts, too. As youngsters gain more and more (online) independence, it is up to us to give them the grounding they need to be able to deal with their new world. From control to independence, where confidence and knowledge take centre stage.

At [school name], we believe it is vital to guide our students to:

- **Dare** to ask for help from a responsible adult in tricky situations.
- **Learn** to think critically and to evaluate online situations better.
- **Learn** to protect themselves from online risks.
- **Be smarter** about sharing information online: what, when and with whom.
- **Be kind** and respectful towards other people and their privacy.

This year our school will work through the Cyber Heroes programme, a multifaceted programme designed specifically to teach children the skills that they need to be safe (and smart) online. One of the tools for this is Interland, a browser-based game that makes learning about digital safety interactive and fun.

The Cyber Heroes programme was developed by Google, Test Achats and the educators from Child Focus. It provides fun learning experiences built around five fundamental thematics about 'online safety':

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

Smart, safe use of technology enhances the learning environment and can help our schools function better. We believe the Cyber Heroes programme will mark an important step in the right direction and ensure that our pupils at [school name] learn about and explore the online world in the right way, while staying safe.

If you're interested, we'd be happy to tell you more about this new programme, as well as about some of the new tools your children might start using at home. And given that communication is always the best prevention, we encourage you to ask them about what we're doing in class. Who knows – you might even pick up a few privacy and online security tricks yourselves!

Yours sincerely,
[You]

Frequently asked questions

Is it necessary to complete the thematics before Interland?

No – but we do recommend that the thematics be taught prior to playing Interland. The game is best when it reinforces the topics outlined in the curriculum – and it's more fun when students have had a chance to engage with you in dialogues, discussions, and brainstorming prior to the game play experience.

Do students need Google Accounts to take part to the Cyber Heroes activities and access the program online?

Nope! The Cybersimple.be platform, which hosts the Cyber Heroes program, is available to anyone who visits the site. No logins, no passwords, no emails.

What devices are compatible with the Interland game?

Interland works on any device that has an Internet connection and a web browser. That means most any desktop or laptop computer, tablet, or mobile phone is ready to help you the Cyber Heroes.

What are all the URLs?

- For the Cyber Heroes homepage, visit <https://www.cybersimple.be/en>.
- For the Interland game, visit https://beinternetawesome.withgoogle.com/en_be/.
- For the Cyber Heroes curriculum, visit <https://www.cybersimple.be/en/toolkit>.

Do I need special training to complete this, or be a special kind of teacher?

- First: Any K–12 teacher can teach this curriculum to their students. No extra training is required.
- Second: *Every* teacher is special. :)

What grade level is BIA best suited for?

The full program, including the curriculum, the game, and the resources on the website, was designed for users from ages 8 to 12. However, depending on how teachers tailor the curriculum, the topics can be helpful for any grade level.

How do kids learn from the game?

The game reinforces curriculum concepts by allowing them the freedom to explore healthy digital practices through play and understand digital interactions (and their consequences) in a safe, educational space.

Can each thematic be used in Google Classroom?

Yes, yes, and more yes. You can assign Interland to specific classes or sections, or make the resource available to all your students in the form of a class announcement.

Do I need to be a digital citizenship expert to use this program?

Not at all. The curriculum was designed so that any teacher can pick it up and teach it in their class. Furthermore, if you are interested in brushing up or learning more on digital safety and citizenship topics, you can take our online course for educators at edutrainingcenter.withgoogle.com/digital_citizenship/preview.

Can my students save their work on Interland?

Not in the current version, and that's not likely to. The Cyber Heroes program generates and stores no personally identifiable information whatsoever – including savefiles. The reason for this was purposeful – we wanted the experience to be accessible to everyone, so it's not necessary to have an account, a login, or a password.

That's good, but a lot of my students are proud they finished the game and of what they learned.

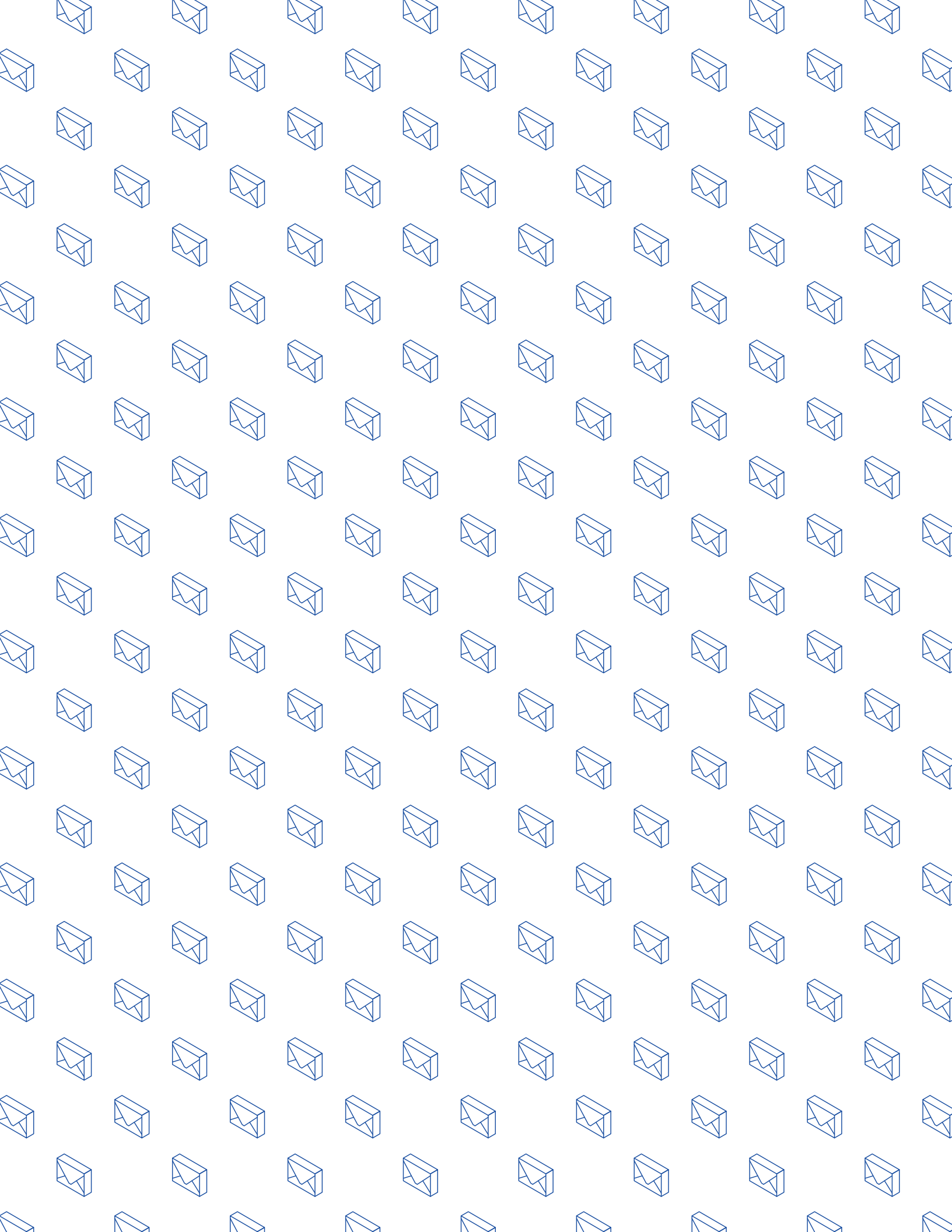
We hear you, and for that reason we have created a customizable certificate template so that you can enter a student's name and create a printable, personalized certificate of course completion for your students.

Where can I find the other educator resources?

All Cyber Heroes educator materials can be found on our resources page at <https://www.cybersimple.be/en/toolkit>.

Is there an online community of Cyber Heroes users to share ideas or get help?

Yes! (And we love it.) We frequently share ideas and engage with teachers on Twitter. Please follow us to learn more about The Cyber Heroes and other topics at [@GoogleForEducation](https://twitter.com/GoogleForEducation).



Share with Care

Protecting yourself and your online reputation



Thematic overview

- Activity 1: **When not to share**
- Activity 2: **Whose profile is this, anyway?**
- Activity 3: **How do others see us?**
- Activity 4: **Keeping it private**
- Activity 5: **Interland: Mindful Mountain**

Themes

Teachers and parents understand how early digital mistakes can do lasting damage to someone's reputation. But it can be harder to convince pre-teens that a seemingly harmless post today could be misunderstood or viewed by people the post wasn't intended for. Now and in the future.

The activities below use practical examples to teach children how to maintain a positive online reputation by maintaining their privacy and managing their personal information themselves.

Goals for students

- ✓ **Create and maintain** a positive reputation online.
- ✓ **Respect** the privacy boundaries of others.
- ✓ **Understand and manage** your 'digital footprint'.
- ✓ **Dare to ask** a person you trust to help deal with sticky situations.

Share with Care

Vocabulary



Online privacy: A broad term that usually means the ability to control what information you share about yourself online and who can see and share it

Digital footprint (or digital presence): Your digital footprint is all the information about you that appears online. This can mean anything from photos, audio, videos, and texts to “likes” and comments you post on friends’ profiles. Just as your footsteps leave prints on the ground while you walk, what you post online leaves a trail as well.

Reputation: The ideas, opinions, impressions, or beliefs that other people have about you; something that you can’t be totally sure about but that you usually want to be positive or good

Personal information: Information that identifies a specific person – for example, your name, street address, phone number, Social Security number, email address, etc. – is called personal (or sensitive) info. Really think carefully before sharing this kind of information online.

Oversharing: Sharing too much online – usually this is about sharing too much personal information or just too much about yourself in a certain situation or conversation online.

Settings: This is the area in any digital product, app, website, etc., where you can define or adjust what you share and how your account is handled – including your privacy settings.

Share with Care: Activity 1

When not to share

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

Goals for students



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

Let's talk



Why does privacy matter?

Your digital footprint is what represents you online. This could mean photos, audio, videos, texts, “likes,” and comments you post on friends’ profiles. Just like it’s important to be a positive presence offline (like at school), it’s important to keep it positive online too.

The Internet makes it easy to communicate with family, friends, and people who love the same things that you do. We send messages, share photos, and join conversations on social networks – sometimes without thinking about who else can see them too. A picture or post you think is funny and harmless today could be seen and misunderstood by people you never thought would see it – now or way off in the future. Once something’s out there, it’s hard to take it back. Remember:

- Like everything else on the Internet, your digital footprint could be seen by people you’ve never met.
- Once something by or about you is online, it could be there forever. Think of this like you’d think about a permanent marker: The marks it makes can never be erased, even if you realize you meant to write something else.

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 you post and share online. Why else might privacy be important?

It’s also good to know when to post nothing at all – not to react to somebody’s post, photo, or comment or not to share something that isn’t true. Everybody’s heard “think before you post,” and that’s because it’s really good advice. The way to respect your own and other people’s privacy is to think about what’s okay to post, who might see your post, what effect it could have on you and others, and when not to post anything at all.

Continued on the next page →

Some questions for further discussion (these questions can also go home with students for follow-up family discussions):

- When is it okay to share a photo or video of someone else?
- Why are secrets so hard to keep?
- Is it ever okay to tell someone else's secret?
- What about if they're someone you care about and they're posting something that makes you feel they're in danger? If you think you should share that secret, should you tell them you're thinking about that before doing anything? Should they know you're worried?

Activity



1. Make up a secret

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

2. Tell your partner

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

- Would you share this secret with anyone?
- With whom would you share your secret and why?
- How would you feel if someone told everyone your secret without your permission?

3. Tell the class

Finally, each student will tell the class their pretend secret and how they felt about sharing it. The class can discuss their answers to the questions just above.

Takeaway

Secrets are just one type of personal information that we might want to keep private or share only with trusted family or friends. Once you've shared a secret, you're no longer fully in control of where it can go. What other kinds of information should we be careful to protect?

- Your home address and phone number
- Your email
- Your passwords
- Your usernames
- Your schoolwork and other documents you create

Share with Care: Activity 2

Whose profile is this, anyway?

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

Goals for students



- ✓ **Identify** ways information can be found online about people.
- ✓ **Consider** how judgments are made about a person when they post things online.
- ✓ **Determine** accuracy of information and identify the difference between assumption, opinion, and fact.

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 which can cause us to think things or make guesses about people that turn out not to be 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? How might we identify the source?

Activity



Materials needed:

- Collections of several fictitious or real people's online activities. You can hand out the worksheet "Whose profile is this, anyway?" or – as a class or for learners' individual homework activity to share the next day – collect examples using these ideas:
 - Social media accounts of family or celebrities, if age-appropriate
 - Printed-out browser history logs
 - Notebooks or devices for a short writing assignment

1. Study the person

If you decide to go with the collections on the worksheet, everyone gets a copy to read. If you go with collections gathered as a class, choose three people, put their info into lists like in the worksheet, and make sure everyone gets their own copy and reads it.

2. Write a description

Separate into groups, one character/person per group. Each group writes its own quick description of the person, answering the question: "Who do you think this person is?"

3. Reveal the truth

Okay, now here's the truth about our characters (remember to hold off reading these until each group's description is set):

- **Nina** is a high school senior. She's going to college next year, hopes to study chemical engineering, and eventually wants to start her own company. She cares most about: family, volunteering, pop culture, fashion.
- **Léa** is the starting pitcher on the high school baseball team. She's 15 and lives in Brussels. She has an 8-year-old sister. She cares most about: baseball, studying art, playing the guitar, hanging with her friends.

Continued on the next page →

- **Ahmed** is 14. He just joined the soccer team and has two cats. He's very good at sketching and likes to build robots on weekends. He cares most about: technology, his soccer team, animals and animal rights.

4. Discuss

Now, which of our guesses were correct, and which ones weren't? Why or why not? What did you learn from this activity?

Takeaway


When we see people's posts, comments, and photos, we make guesses about them that aren't always correct, especially if we don't know them. That's because what we're seeing online is only part of who they are and what they care about. It could also be someone they're just pretending to be, or it's something they're feeling only in the moment they're posting it. We can't really know who they are or how they really feel until we know them in person – and even then it takes time!


Worksheet: Activity 2


Whose profile is this, anyway?


Read each collection of the person’s online activity below. Based on what you see here, write a short description of what you think this person is like: What do they like, dislike, and care about most?


Nina


 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


 Speeding ticket


 Young Designers Conference at Antwerp University


 FINALLY SAW THE NEW SPY WARS MOVIE. Omg obsessed!


Léa


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

 I hate school dances. #notgoing


 Academy of Science, Brussels


 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


Ahmed


 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 a lot of the code for it.

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

Share with Care: Activity 3

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 for students



- ✓ **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 last a long time.
- ✓ **Develop** a goal to proactively create a positive online presence.

Let's talk



A new point of view

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

Let's take another look at the profile from our character's point of view.

- Do you think they want people to know all this personal info? Why or why not?
- What types of people might they (not) want to see it?
- How might this information be seen by other people?
- How might this information be used by other people?

Different situations call for different levels of privacy. Thinking about how other people would view what you post is the key to good online privacy habits.

Activity



Materials needed:

- A copy for each student of the fictitious profiles 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 | • Yourself in 10 years |
| • Friend | • Police | • Advertiser | |

What's important to you as the parent, principal, coach, friend, etc.? What conclusions would you reach about the character? How would you use that information? Cross out the information that you think our character wouldn't want you to see.

2. Present conclusions

Each group presents its results and explains its privacy choices. If appropriate for your class, this may be a good opportunity for role play.

Continued on the next page →

3. Class discussion

What are your top takeaways from this group activity? Why might the information we looked at tell an incomplete story? What do you think might be the consequences of someone forming a negative opinion about you based on what they found online?

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.

Share with Care: Activity 4

Keeping it private

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

Goals for students



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

Let's talk



Privacy scenarios: What should you do?

Scenario 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?

Scenario 2: Someone writes in their personal journal. Another person copies what they wrote and posts it online.

- Was the other person wrong to post the journal entry?
- How would you feel if someone did this with something you intended to keep private?

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

- Had the friend announced publicly that they were going away? Did they want everybody to know?
- Are there more private ways to communicate this message – such as sending a direct message or text?

Scenario 4: You know a student made a fake social media account impersonating another student in a negative way and includes their personal information.

- Does the student have a right to know?
- Should someone tell a teacher or other trusted adult? How? What could happen if nobody does?
- It's not obvious who made it, but you know who did it. Should you give this information to a trusted adult?

Activity



We're going to review four scenarios and talk about how each one might have a different privacy solution. We'll split up into four groups, discuss one scenario each, and then come back for a class discussion about our findings.

Takeaway

Different situations call for different responses online and offline. It's always important to respect other people's privacy choices, even if they aren't the choices you'd make yourself.

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.

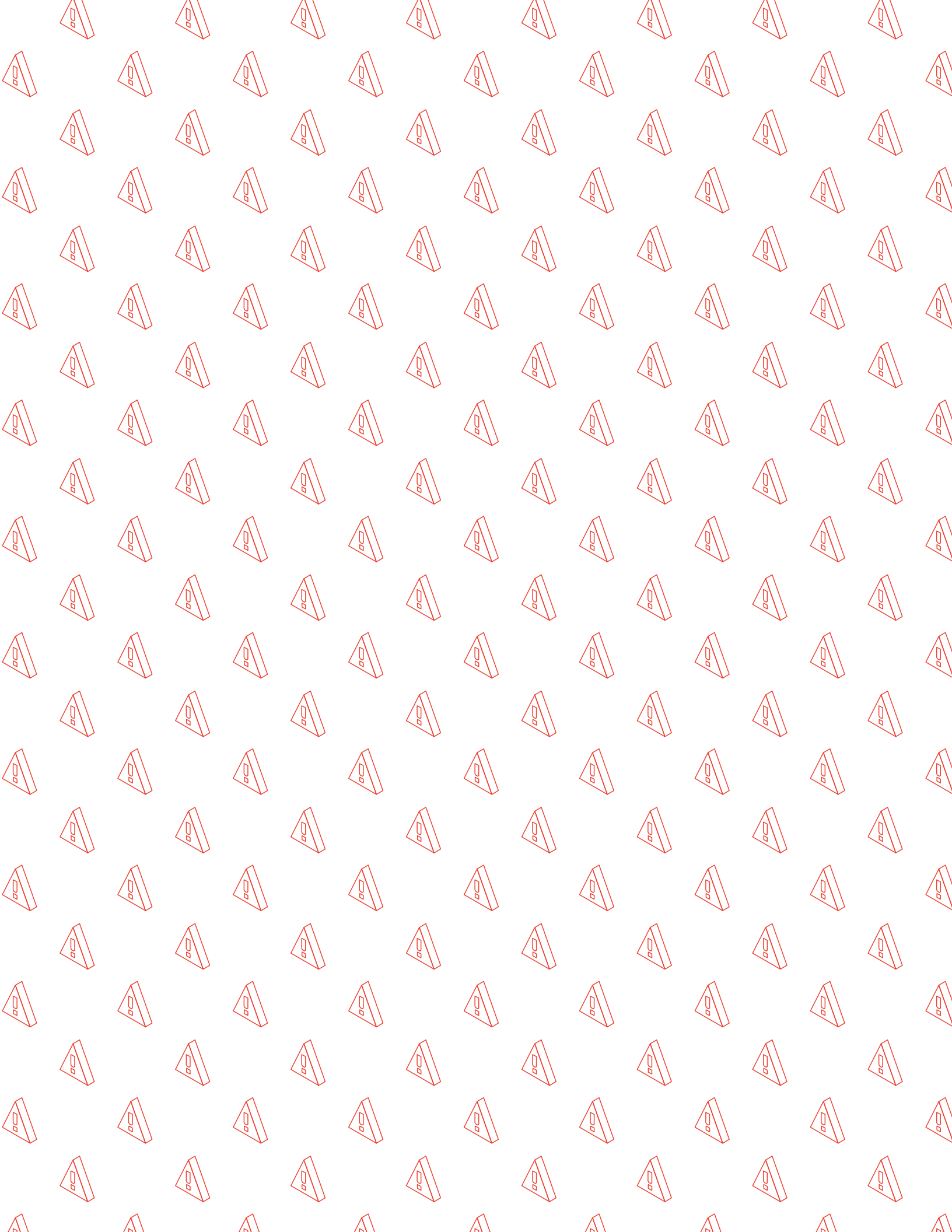
Open a web browser on your desktop or mobile device (e.g., tablet), and visit https://beinternetawesome.withgoogle.com/en_be/interland/mindful-mountain.

Discussion topics



Have your students play Mindful Mountain and use the questions below to prompt further discussion about the thematics learned in the game. Most students get the most out of the experience by playing solo, but you can also have students pair up. This may be especially valuable for younger learners.

- Of all the posts you shared in the game, which type do you think you would share most often in real life? 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 their 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 thematics 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? What about if someone accidentally shares something too personal with you?



Don't Fall for Fake

Staying away from phishing and scams



Thematic overview

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

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

Activity 3: **About those bots**

Activity 4: **Interland: Reality River**

Themes

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

Goals for students

- ✓ **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.

Don't Fall for Fake Vocabulary



Bot: Also called a “chatbot” or “virtual assistant,” this is a piece of software that operates online or on a network to automatically answer questions, follow commands (like giving directions to your new friend’s house), or do simple tasks (like play a song).

Phishing: An attempt to scam you or trick you into sharing login information or other personal information online. Phishing is usually done through email, ads, or sites that look similar to ones you’re already used to.

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: False; an action or message designed to fool, trick, or mislead someone

Manipulation: Someone controlling or influencing another person or situation unfairly, dishonestly, or under threat. Alternatively, things you find online may be manipulated, such as a photo that has been edited to make you believe something that isn’t true.

Fraudulent: Tricking someone in order to get something valuable from them

Firewall: A program that shields your computer from most scams and tricks

Malicious: Words or actions intended to be cruel or hurtful. Can also refer to harmful software intended to do damage to a person’s device, account, or personal information.

Catfishing: Creating a fake identity or account on a social networking service to trick people into sharing their personal information or into believing they’re talking to a real person behind a legitimate account, profile, or page

Clickbait: Manipulative online content, posts, or ads designed to capture people’s attention and get them to click on a link or webpage, often to grow views or site traffic in order to make money

Don't Fall for Fake: Activity 1

Don't bite that phishing hook!

Students play a game where they study various emails and texts and try to decide which messages are legit and which are phishing scams.

Goals for students



- ✓ **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 attachments they try to get you to open – can also put viruses on your computer. Some viruses use your contacts list to target your friends and family with the same, or a more personalized, phishing attack. Other types of 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. Others can be sneaky and really convincing – like when a scammer sends you a message that includes some of your personal information. That's called spearphishing, and it can be very difficult to spot because using your info can make it seem like they know you.

Before you click on a link or enter your password in a site you haven't been to before, it's a good idea to ask yourself some questions about that email or webpage. Here are some questions you could ask:

- Does it look professional like other websites you know and trust, with the product's or company's usual logo and with text that is free of spelling errors?
- Does the site's URL match the product's or company's name and information you're looking for? Are there misspellings?
- Are there any spammy pop-ups?
- Does the URL start with https://with a little green padlock to the left of it? (That means the connection is secure.)
- What's in the fine print? (That's often where they put sneaky stuff.)
- Is the email or site offering something that sounds too good to be true, like a chance to make a lot of money? (It's almost always too good to be true.)
- Does the message sound just a little bit weird? Like they might know you, but you're not completely sure?

Continued on the next page →

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 get tricked by a scam, let your friends and people in your contacts know right away, because they could be targeted next.
- Use settings to report the message as spam, if possible.

Activity



Materials needed:

- Handout: "Phishing examples" worksheet

Answers to "Phishing examples" worksheet:

1. **Real.** The email asks the user to go to the company's website and sign into their account on their own, rather than providing a link in the email or asking them to email their password (links can send users to malicious websites).
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 studies these examples of messages and websites.

2. Individuals indicate choices

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

3. Groups discuss choices

Which examples seemed trustworthy and which seemed suspicious? Did any answers surprise you? If so, why?

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? Does it offer to fix something you didn't know was a problem?

- **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, quizzes or "personality tests" could be gathering facts to make it easy to guess your password or other secret information. Most real businesses 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.

Continued on the next page →

- **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. No fine print at all can be just as bad, so pay attention to that too.

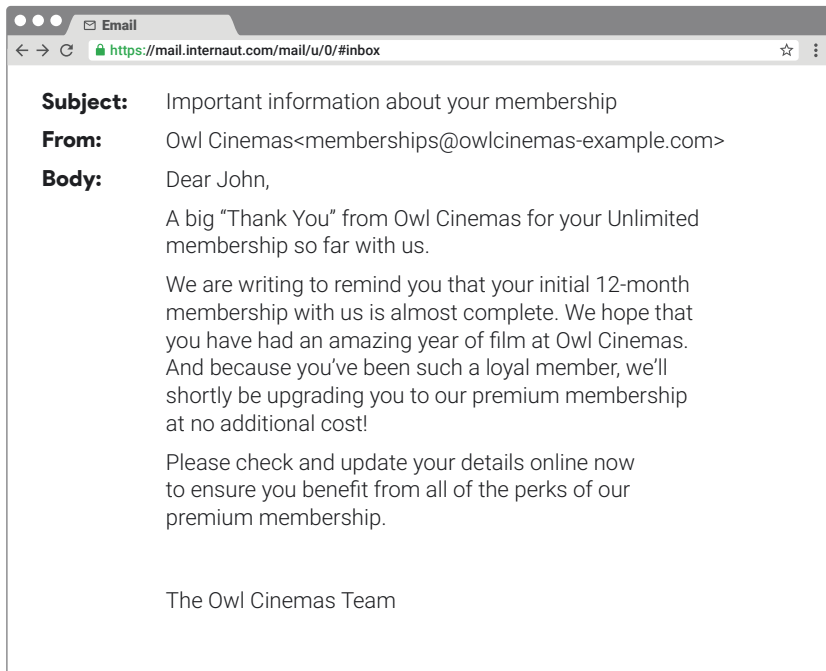
Note: For the purposes of this exercise, assume that Internaut mail is a real, trusted service.

Takeaway

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

Worksheet: Activity 1

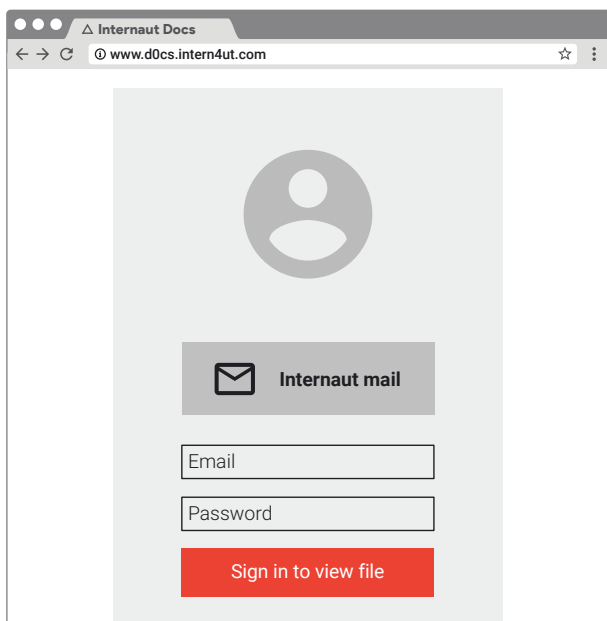
Phishing examples



1. Is this real or fake?

Real

Fake

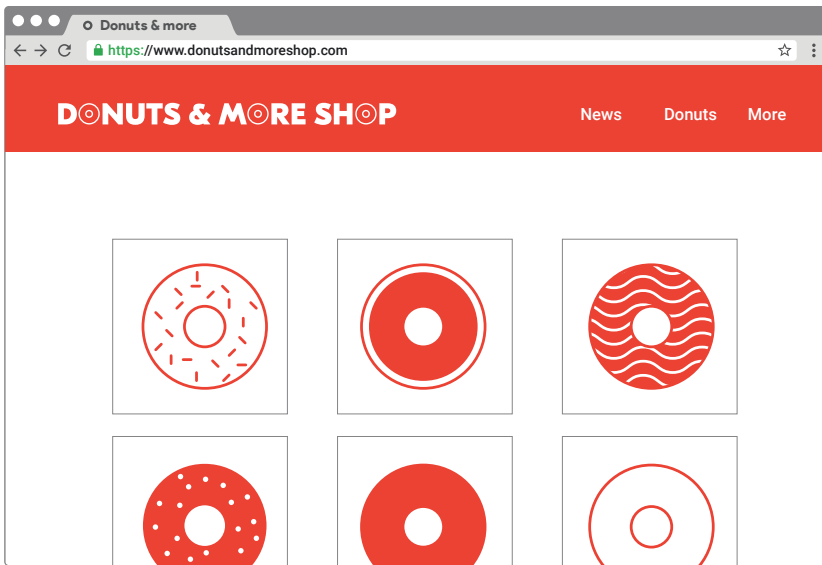


2. Is this real or fake?

Real

Fake

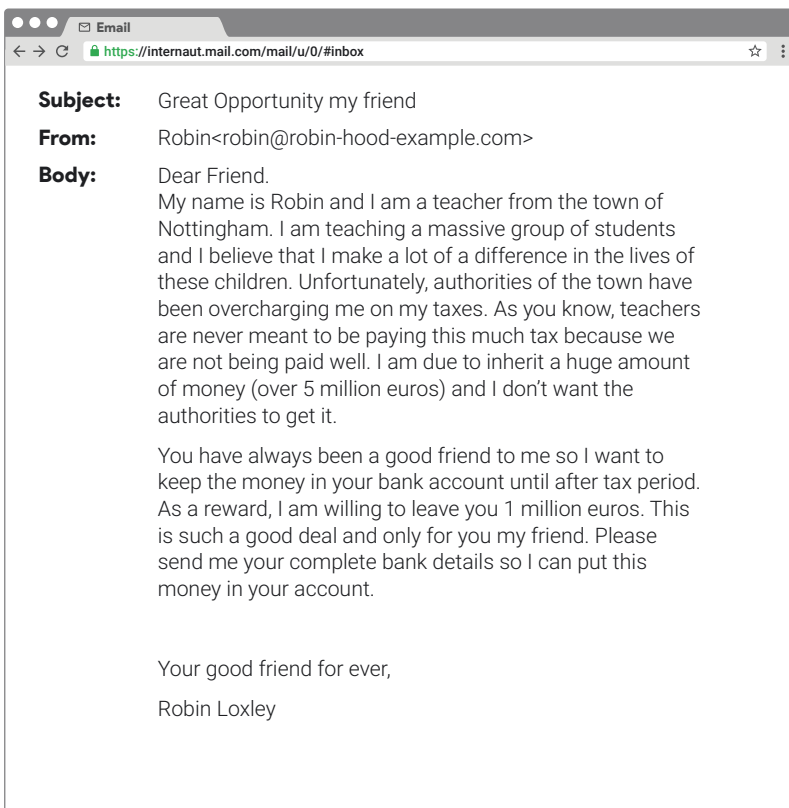
Continued on the next page →



3. Is this real or fake?

Real

Fake



4. Is this real or fake?

Real

Fake

Continued on the next page →

Internet Accounts
http://www.internautaccounts.com-genuine-login.com/

Internaut Accounts

Hey, is that really you?

It looks like you're signing into your account from a new location. Just so we know this is you – and not someone trying to hijack your account – please complete this quick verification. [Learn more](#) about this additional security measure.

Choose verification method

☒ Confirm my phone number:

Internaut mail will check if this is the same phone number we have on file – we don't send you any messages.

☐ Confirm my recovery email address:

Internaut mail will check if this is the same email address we have on file – we won't send you any messages.

[Continue](#)

5. Is this real or fake?

Real

Fake

Don't Fall for Fake: Activity 2

Who are you, really?

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

Goals for students



- ✓ **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 whom 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 your friend, you can tell it's them by the sound of their voice, even though you can't see them. The online world is a little different, though. Sometimes it's harder to be sure someone is who they say they are.

In apps and games, people sometimes pretend to be someone else as a joke, or to mess with them in a mean way. Other times, they impersonate people to steal personal information. When you're on the Internet, people you don't know could ask to connect with you. The safest thing to do is not to respond or to tell a parent or adult you trust that you don't know the person trying to connect with you. But if you decide it's okay to respond, it's a really good idea to see what you can find out about them first. Check their profile, see who their friends are, or search for other information that confirms they're who they say they are.

There are multiple ways to verify someone's identity online. Here are a few examples to get us started.

Educator note

You might consider leading a class brainstorm on the question “How do we verify a person's identity online?” first; then continue the conversation with these thought starters.

- **Is their profile photo suspicious?**

Is their profile photo blurry or hard to see? Or is there no photo at all, like a bitmoji or cartoon character's face? Bad photos, bitmojis, photos of pets, etc., make it easy for a person to hide their identity in social media. It's also common for scammers to steal photos from a real person in order to set up a fake profile and pretend to be them. Can you find more photos of the person with the same name associated?

- **Does their username contain their real name?**

On social media, for instance, does their screen name match a real name? (For example, Jane Doe's profile has a URL like SocialMedia.com/jane_doe.)

- **Do they have a profile bio?**

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 a bunch of information copied or pulled together randomly to create a fake profile. Is there anything in their bio that you can confirm by searching for it?

- **How long has the account been active? Does the activity you see line up with your expectations?**

Is the profile new or does it show a lot of activity? Does the person have mutual friends with you like you would expect? Fake accounts usually don't have much content or signs of people posting, commenting, and socializing in them.

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 to hold the strips (each group of students will pick one)
- Phishing cheat sheet

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. Feel free to write more messages that you think would be even trickier. If you do, each group should share the messages they create with the other groups.

Takeaway

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

Who are you, really?

Here are five scenarios of messages anyone could get online or on their phone. Each has a list of ways you could respond, some great and others not so much. See if they make sense to you – or if you think of other responses. If one of these scenarios really happens to you and you're not sure what to do, the easiest response is no response. You can always ignore or block them. It also never hurts to talk with a parent or teacher about it.

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? – Peter." What do you do?

- **Ignore Peter.** If you don't know him, you can just decide not to talk to him, period.
- **"Hi, Peter. Do I know you?"** If you aren't sure, ask first.
- **Block Peter.** If you've checked who he is and decide to block him, you won't get any more messages from him. On most social media platforms, he won't even know you blocked him.
- **Check Peter's profile.** Be careful – fake profiles are easy to make! Check this guy's friends list and see whom he's connected to. His circle of friends can be another way to tell whether or not he's real – especially if you don't know anyone he knows! If not much is going on on his page, that's another hint that he isn't for real.
- **Add Peter to your friends list.** IF he seems okay. This isn't recommended, unless you've verified who he is and checked with an adult you trust.
- **Give him personal info.** Never give personal information to people you don't know.

Scenario 2

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

- **Block Arthur.** This would feel rude if you actually know her. But if you're sure you didn't meet anyone named Arthur last summer or she's sending you too many texts and oversharing about herself, it would be fine to block her.
- **Ignore Arthur.** If you don't know this person, you can just not respond.
- **"Hi, Arthur. Do I know you?"** This is a safe option if you aren't sure whether you met her and want to figure out if you did by finding out a little more. But don't tell Arthur where you were last summer!
- **"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 →

Scenario 3

You get a direct message from @soccergirl12, someone you don't follow. "Hey! Love your posts, you are SO funny! Give me your phone number and we can talk more!" What do you do?

- **Ignore @soccergirl12.** You don't have to respond if you don't want to.
- **Block @soccergirl12.** If you find this person strange and block them, you'll never hear from them again – unless they start a new fake profile and contact you as a different fake person.
- **"Hi, do I know you?"** If you aren't sure, be sure to ask questions before giving out personal information like your phone number.
- **"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, whether it's through parents, teachers, or some other trusted person.

Scenario 4

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

- **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 sketchy, it might be better not to answer – or just block them.
- **"Is that you Justine? U R CUTE too! I live in 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 any other personal information, check them out, even if you think you know them. Never meet someone in person that you know only from online interactions.

Scenario 5

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?" What do you do?

- **Ignore.** If you don't know this person but you do have a friend named Sam, the best thing to do is 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 best 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.

Don't Fall for Fake: Activity 3

About those bots

Students are interacting with more and more nonhuman “voices” coming out of devices, apps, and sites these days – mostly at home, but perhaps increasingly at school. Sometimes they’re called “chatbots,” sometimes “virtual assistants,” often just “bots.” This is a simple Q&A activity designed to get the class thinking out loud together about interacting with bots.

Note: Try to keep the discussion open-ended; this activity is designed to engage critical thinking, not deliver any conclusions.

Goals for students



- ✓ **Learn** about this interactive technology showing up in more and more places in students’ lives.
- ✓ **Identify** experiences with bots of various kinds.
- ✓ **Analyze** the impact these technologies can have on daily life – both positive and negative.

Let's talk



More and more people use bots these days. Have you heard that word used? Some people call them “chatbots” or “virtual assistants.” They’re used for a gazillion things: playing games, checking the weather, answering questions, getting directions, notifying you when time’s up, etc. Sometimes they have a human name, other times their names just describe what they do, such as Dog A Day, a bot that sends a photo of a dog every day. Bots can be on mobile devices, online, in cars, or they can be special devices people keep in different rooms of their home. Let’s chat about what experiences this class has had with bots and get our thinking about them rolling. Here are some questions for us to consider:

- Do you know what a bot is?
- How many of you have talked to a bot? On what kind of device?
- Who wants to tell us what that’s like?
- What do you think bots work best for (examples to get people thinking: ask for the weather report, get the news, play a game, ask for information)?
- Bots use what’s called AI, or artificial intelligence. In a way, AI learns from what you ask so it can get better at helping you. To do this, bots sometimes “remember,” or record, what you ask and say. Does that make you think about what you’d tell a bot? If so, what would you tell it and what kind of information would you keep to yourself?
- Do you think it’s like talking to a human being? How is it and how is it not like that?
- How do people you know treat or talk to their bots?
- How would you talk to it? Would you be kind, or would you sometimes yell at it?
- Is it okay for people to yell at bots? Why or why not? (Is it like practicing a certain kind of interaction?)

- Sometimes really little kids think bots are humans. What would you tell a little sister, brother, or cousin to help them understand what they're chatting with?
- If bots can learn from us humans, can you think of something we shouldn't say because you wouldn't want your bot to learn it? (Hint: Think back to the activities in "Share with Care" and talk about how they relate to this.)
- Is it possible to classify information as "good or bad" or "real or fake"? How can we try to answer these questions?

Activity



After the discussion, as a class or in groups around classroom devices, search for images of bots and information (including news coverage) about them. Search terms might include "bots," "chatbots," "digital assistants," or "virtual assistants." Decide as a class if the information is good and have students pick one article to take home, read with their parents, and write a one-paragraph summary about.

Takeaway

Critical thinking is one of the best, most long-lasting "tools" we have for keeping our tech use positive – and the great thing is that it's a tool that gets better every time we use it. Thinking out loud together is a powerful, fun way to use and improve that tool.

Don't Fall for Fake: Activity 4

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), and visit https://beinternetawesome.withgoogle.com/en_be/interland/landing/reality-river.

Discussion topics



Have your students play Reality River and use the questions below to prompt further discussion about the thematics learned in the game. Most students get the most out of the experience by playing solo, but you can also have students pair up. This may be especially valuable for younger students.

- 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? If so, how?
- What's one thing that you think you'll do differently after joining in these thematics and playing the game?
- What are some clues that could signal that something is "off" or creepy 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



Thematic 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 for students

- ✓ **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.

Secure Your Secrets

Vocabulary



Privacy: Protecting people’s data and personal information (also called sensitive information)

Security: Protecting people’s devices and the software on them

Two-step verification (also called two-factor verification and two-step authentication): A security process where logging in to a service requires two separate steps or two “factors,” such as a password and a one-time code. For example, you may have to enter your password and then enter a code that was texted to your phone or a code from an app.

Password or passcode: A secret combination used to access something. It may take different forms; for example, you may have a four-digit number-only code that you use for your phone lock and a much more complex password for your email account. In general, you should make your passwords as long and complex as you can while still being able to remember them.

Encryption: The process of converting information or data into a code that makes it unreadable and inaccessible

Complexity: The goal when creating a secure password. For example, a password is complex when it has a mix of numbers, special characters (like “\$” or “&”), and both lowercase and uppercase letters.

Hacker: A person who uses computers to gain unauthorized access to other people’s or organizations’ devices and data

Secure Your Secrets: Activity 1

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 for students



- ✓ **Recognize** the importance of never sharing passwords, except with parents or guardians.
- ✓ **Understand** the importance of screen locks that protect devices.
- ✓ **Know** how to create passwords that are hard to guess, yet 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 for us to communicate with friends, classmates, teachers, and relatives. We can connect with them 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 ourselves, our info, and our devices means doing simple, smart things like using screen locks on phones, being careful about putting personal info on unlocked devices that can be lost or stolen, and, above all, building strong 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 and what specifically makes them bad. (Examples: your full name, your phone number, the word "chocolate.")

Who thinks these passwords are good? ;)

Continued on the next page →

Activity



Materials needed:

- Internet-connected devices for students or groups of students
- A whiteboard or projection screen
- Handout "Guidelines for creating strong passwords"

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 couple letters from each word in the phrase.
- Change some letters to symbols or numbers.
- Make some letters uppercase and some lowercase.
- Let's practice our new skills by playing the password game.

1. Create passwords

We'll split into teams of two. Each team will have 60 seconds to create a password. (Challenge option: Students share clues with the class first to see how much contextual information the class needs to be able to make an accurate guess.)

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

It's important and fun to create strong passwords.

Guidelines for creating strong passwords

Here are some tips for creating passwords to keep your information safe.

Strong passwords are based on a descriptive phrase or sentence that's easy for you to remember and difficult for someone else to guess – like the first letters in words that make up a favorite title or song, the first letters of words in a sentence about something you did – and include a combination of letters, numbers, and symbols. For example, “I went to Western Elementary School for grade 3” could be used to build a password like: lw2We\$t4g3.

Moderate passwords are passwords that are strong and not easy for malicious software to guess but could be guessed by someone who knows you (for example, lwenttoWestern).

Weak passwords commonly use personal information like a pet's name, are easy to crack, and can be guessed by someone who knows you (for example, “IloveBuddy” or “Ilikechocolate”).

DOs

- Use a different password for each of your important accounts.
- Use at least eight characters. The longer the better (as long as you can remember it!).
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.
- Make your passwords memorable so you don't need to write them down, which would be risky.
- Immediately change your password if you know or believe it may be known by someone other than a trusted adult.
- Always use strong screen locks on your devices. Set your devices to automatically lock in case they end up in the wrong hands.
- Consider using a password manager, such as one built into your browser, to remember your passwords. This way you can use a unique password for each of your accounts and not have to remember them all.

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, just the name of your school, favorite baseball team, a string of numbers (like 123456), etc. And definitely don't use the word “password”!
- Don't share your password with anyone other than your parents or guardian.
- Never write passwords down where someone can find them.

Secure Your Secrets: Activity 2

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 for students



- ✓ **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 you manage your privacy, security, and safety. It's important to know that your parents or guardian should always be making these decisions with you.

Activity

**Materials needed:**

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

Review options

I have my school device hooked up to the projection screen. Let's navigate to the settings page of this app, where we can see what our options are. Talk me through (encourage your students to help you)...

- Changing your password
- Going through your sharing, location, and other settings and figuring out which ones are best for you
- 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 the family and friends you choose
- Enabling two-factor or two-step verification
- Setting up recovery information in case you get locked out of your account

Which privacy and security settings are right for you is 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.

Continued on the next page →

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 a page with your passwords in plain sight, such as on your computer or desk. Safeguard your list, and protect yourself by hiding it somewhere safe.

Secure Your Secrets: Activity 3

Interland: Tower of Treasure

Mayday! The Tower of Treasure is unlocked, leaving the Internaut's valuables like contact info and private messages at high risk. Outrun the hacker and build a fortress with strong passwords to secure your secrets once and for all.

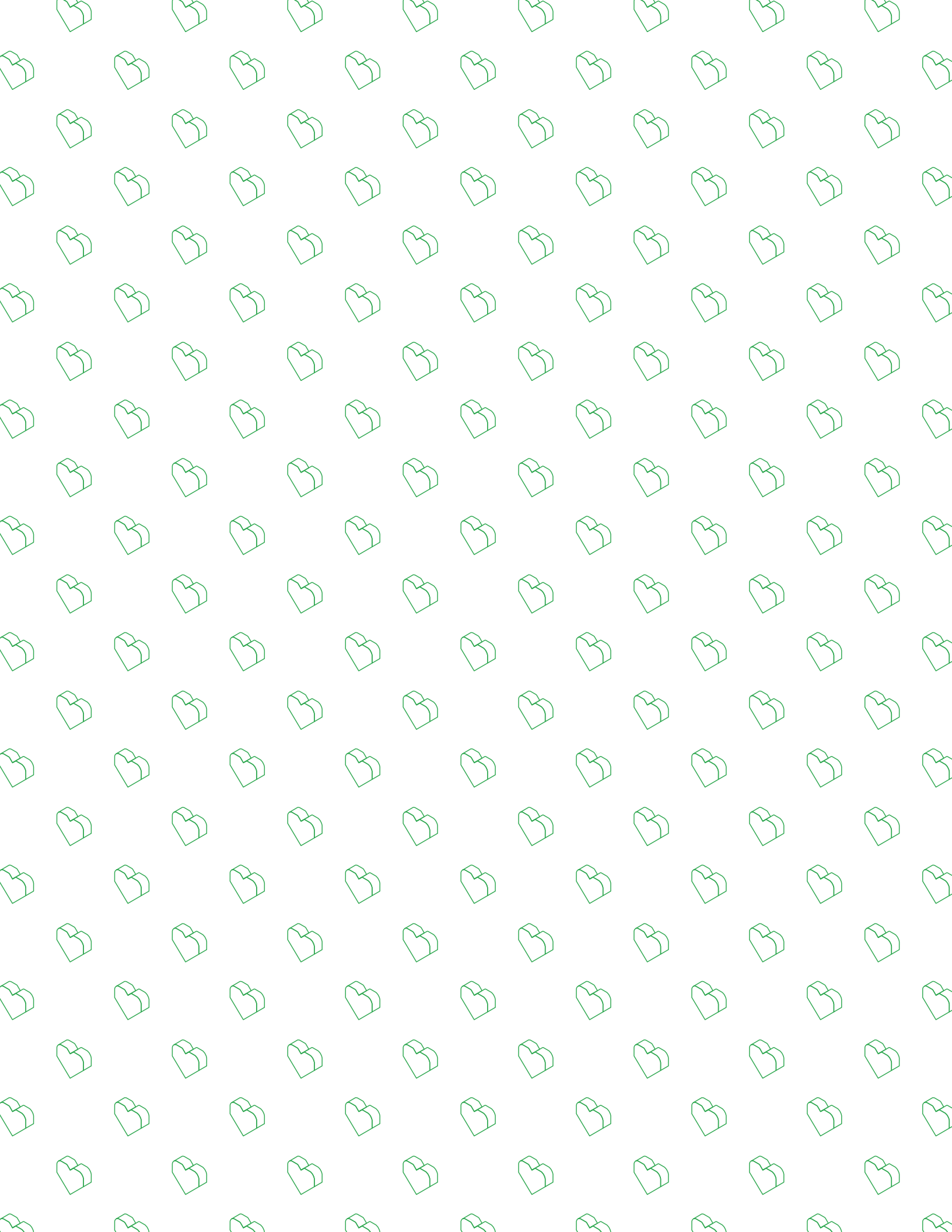
Open a web browser on your desktop or mobile device (e.g., tablet), and visit https://beinternetawesome.withgoogle.com/en_be/interland/tower-of-treasure.

Discussion topics



Have your students play Tower of Treasure and use the questions below to prompt further discussion about the thematics learned in the game. Most students get the most out of the experience by playing solo, but you can also have students pair up. This may be especially valuable for younger students.

- 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 playing 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 thematics 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



Thematic overview

Activity 1: **From bystanders to upstanders**

Activity 2: **Upstander options**

Activity 3: **...but say it nicely!**

Activity 4: **Mind your tone**

Activity 5: **Walking the walk**

Activity 6: **Interland: Kind Kingdom**

Themes

The digital world creates new challenges and opportunities for social interaction, for kids and all the rest of us. Social cues can be harder to read online, constant connecting can bring both comfort and anxiety, and anonymity can fuel crushes and compliments as well as harm to self and others.

It's complicated, but we know that the Internet can amplify kindness as well as negativity. Learning to express kindness and empathy – and how to respond to negativity and harassment – is essential for building healthy relationships and reducing feelings of isolation that sometimes lead to bullying, depression, academic struggles, and other problems.

Research shows that rather than simply telling kids not to be negative online, effective bullying prevention 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 when it arises.

Goals for students

- ✓ **Define** what being positive means and looks like online and offline.
- ✓ **Lead** with positivity in online communications.
- ✓ **Identify** situations in which a trusted adult should be consulted.

It's Cool to Be Kind

Vocabulary



Bullying: Purposefully mean behavior that is usually repeated. The person being targeted often has a hard time defending themselves.

Cyberbullying: Bullying that happens online or through using digital devices

Harassment: A more general term than bullying that can take many forms – pestering, annoying, intimidating, humiliating, etc. – and can happen online too

Conflict: An argument or disagreement that isn't necessarily repeated

Aggressor: The person doing the harassing or bullying; though sometimes called the “bully,” bullying prevention experts advise never to label people as such.

Target: The person being bullied or victimized

Bystander: A witness to harassment or bullying who recognizes the situation but chooses not to intervene

Upstander: A witness to harassment or bullying who supports the target privately or publicly, sometimes including trying to stop and/or report the incident they witnessed

Amplify: To increase or widen participation or impact

Exclusion: A form of harassment or bullying used online and offline; often referred to as “social exclusion”

Block: A way to end all interaction with another person online, preventing them from accessing your profile, sending you messages, seeing your posts, etc., without notifying them (not always ideal in bullying situations where the target wants to know what the aggressor is saying or when the bullying has stopped)

Mute: Less final than blocking, muting is a way to stop seeing another person's posts, comments, etc., in your social media feed when that communication gets annoying – without notifying that person or being muted from their feed (not helpful in bullying)

Anonymous: An unnamed or unknown person – someone online whose name or identity you don't know

Trolling: Posting or commenting online in a way that is deliberately cruel, offensive, or provocative

Report abuse: Using a social media service's online tools or system to report harassment, bullying, threats, and other harmful content that typically violates the service's terms of service or community standards

It's Cool to Be Kind: Activity 1

From bystanders to upstanders

Students practice identifying the four roles of a bullying encounter (the person who bullies, the target of the bullying, the bystander, and the upstander) and what to do if they're a bystander or a target of bullying.

Goals for students



- ✓ **Identify** situations of harassment or bullying online.
- ✓ **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?

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 as we would want to be treated. When bullying or other mean behavior happens, most of the time there are four types of people involved.

- There's the aggressor, or person(s) doing the bullying.
- There's also someone being bullied – the target.
- There are witnesses to what's going on, usually called bystanders.
- There are witnesses to what's going on who try to positively intervene, often called upstanders.

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 the person
- Report them – tell my parent, teacher, sibling, or someone else I trust, and use the reporting tools in the app or service to report the harassing post, comment, or photo

If you find yourself a bystander when harassment or bullying happens, you have the power to intervene and report cruel behavior. Sometimes bystanders don't try to stop the bullying or help the target, but when they do, they're being an upstander. You can choose to be an upstander by deciding not to support mean behavior and standing up for kindness and positivity. A little positivity can go a long way online. It can keep negativity from spreading and turning into cruelty and harm.

Continued on the next page →

If I'm the bystander, I can be an upstander by...

- Finding a way to be kind to or support the person being targeted
- Calling out the mean behavior in a comment or reply (remember to call out the behavior, not the person), if you feel comfortable with that and think it's safe to do so
- Deciding not to help the aggressor by spreading the bullying or making it worse by sharing the mean post or comment online
- Getting a bunch of friends to create a "pile-on of kindness" – post lots of kind comments about the person being targeted (but nothing mean about the aggressor, because you're setting an example, not retaliating)
- Reporting the harassment. Tell someone who can help, like a parent, teacher, or school counselor.

Activity



Materials needed:

- Handout: "From bystanders to upstanders" worksheet

Answers to "From bystanders to upstanders" worksheet:

Scenario 1: B, U, B (because not helping the situation), U, U

Scenario 2: U, B, U, U

Scenario 3: U, U, B, B, U

Scenario 4: The answers are all yours!

1. Read scenarios and categorize responses

After discussing the roles, pass out the worksheet and give students 15 minutes to read the three scenarios and categorize each response. If there's time, have them create that fourth scenario together as a class.

2. Discuss the answers

Before or at the end of the discussion, ask them if they can tell you why it can be nice to have upstanders around at school and online.

3. Discuss those that were hard to categorize

If there's time, ask your students if any of the responses were hard to categorize and why. Have a discussion about that.

Takeaway

Whether standing up for others, reporting something hurtful, or ignoring something to keep it from being amplified even more, you have a variety of strategies to choose from depending on the situation. With a little kindness, anyone can make a huge difference in turning bad situations around.

Worksheet: Activity 1

From bystanders to upstanders

So now you know that a bystander can use their powers for good and be an upstander by helping someone out who's being bullied. Below are three scenarios that are examples of online bullying or harassment. If you want, create a fourth scenario that happened with people you know, and come up with responses that include both upstanding and basic bystanding. Each of the three scenarios already created has a list of responses. Read each response and decide whether it's what a bystander would do or what an upstander would do, then put a "B" for "bystander" or a "U" for "upstander" in the blank next to the response. If there's time, have a class discussion about the ones that seemed to make it harder to decide and why.

Scenario 1

A friend of yours dropped her phone by the drinking fountain near the school soccer field. Someone found it and sent a really mean message about another student to a bunch of people on her soccer team, then put the phone back by the drinking fountain. The student who was targeted told your friend she was a terrible person for sending that message, even though she wasn't the one who sent it. No one knows who sent the mean message. You...

- ☐ Feel sad for your friend but do nothing because no one knows who did that mean thing to her.
- ☐ Go find the person targeted and ask them how they feel and whether you can help.
- ☐ Spread the drama by sharing the mean message with other friends.
- ☐ And your friend get everybody on the soccer team to post compliments about the person who was targeted.
- ☐ And your friend anonymously report the incident to your principal, letting them know that everybody needs to talk about good phone security and locking their phones.

Continued on the next page →

Scenario 2

Your teacher created a class blog for language arts, giving the class the ability to write, edit, and post comments. The next day she's out sick and the substitute doesn't notice that things are going south in the class blog – someone is posting seriously mean comments about one of the students in the class. You...

- ☐ Comment on the comments by saying things like, "This is so not cool" and "I am _____'s friend, and this is not true."
- ☐ Ignore it until your teacher gets back.
- ☐ Get other students to post nice comments and compliments about the student being targeted.
- ☐ Tell the substitute that mean behavior is happening in the class blog, and they might want to let the teacher know.

Scenario 3

There's an online game that a bunch of your friends play a lot. Usually game chat is mostly about what's actually happening in the game. Sometimes it gets a little nasty, though that's usually more like friendly rivalry than anything really bad. But this one time, one player starts saying really nasty stuff about one of your friends who's playing, and they just won't stop. They even keep it up the next day. You...

- ☐ Call up your friend and tell them you don't like this any more than they do and ask them what they think you two should do.
- ☐ Call everybody you know who plays with you guys (making sure your friend knows you're doing this) to see if you can get everybody's agreement that it's time to call out the nastiness.
- ☐ Decide to wait and see if the kid stops, then maybe do something.
- ☐ Walk away from the game for a while.
- ☐ Look for the game's community rules and if bullying isn't allowed, report the nasty behavior using the game's reporting system.

Scenario 4

Create a real-life scenario as a class, based on a situation one of you has heard about, then come up with both bystander and upstander responses to show you definitely know what we're talking about now!

It's Cool to Be Kind: Activity 2

Upstander options

Often students want to help out a target of bullying but don't know what to do. This activity shows them they have choices, offers examples, and gives them an opportunity to create positive responses of their own.

Goals for students



- ✓ **Make** the right decisions when choosing how and what to communicate.
- ✓ **Identify** situations in which waiting until you are face-to-face with someone is a better way to communicate than sending a text or message that may be taken the wrong way.

Let's talk



When you see someone being mean to another person online – making them feel embarrassed or left out, making fun of them, disrespecting them, hurting their feelings, etc. – you always have choices. First, you can choose to be an upstander instead of a bystander by helping the target. Second, if you choose to be an upstander, you have options for what kind of action you take.

The most important thing to know is that it can really help someone being targeted just to be heard if they're sad – and to know that someone cares.

Now, not everybody feels comfortable standing up for others **publicly**, whether online or in the school lunchroom. If you do, go for it! You can...

- Call out the mean behavior (not the person), saying it's not cool.
- Say something nice about the target in a post or comment.
- Get friends to compliment the target online, too.
- Offline, you can invite the person to hang out with you on the playground or sit with you at lunch.

If you don't feel comfortable helping out publicly, that's fine. You can also support the target **privately**. You can...

- Ask how they're doing in a text or direct message.
- Say something kind or complimentary in an anonymous post, comment, or direct message (if you're using media that lets you stay anonymous).
- Tell them you're there for them if they want to talk after school.
- In a quiet conversation in person or on the phone, tell them you thought the mean behavior was wrong and ask if they feel like talking about what happened.

No matter how you choose to be an upstander, you have both public and private options for **reporting**. This could mean reporting bullying behavior via a website or application interface, or reporting what's going on to an adult you trust.

Continued on the next page →

Activity



Materials needed:

- A whiteboard or easel with large white pad on which students can stick sticky notes
- Handout: “Upstander options” worksheet
- Sticky notes for each group of students

In this activity, we’re going to try out what it’s like to be an upstander, so let’s assume our whole class has made the choice to help out the target.

1. Divide into groups of five students per group

Each group should designate a reader and a writer.

2. Groups read and discuss the hurtful situations together

The three situations are provided in the worksheet on the next page.

While groups are discussing, the teacher divides the whiteboard or easel into two large spaces with the headlines “Public Support” and “Private Support.”

3. Groups choose or create their two kinds of responses for each

Students can work with the sample responses in “Let’s talk” or create their own.

4. Students post their choices to the board and read out loud to the whole class

The teacher can then facilitate a class discussion based on the choices the students made.

Takeaway

Lots of times when you see somebody being hurt or harassed, you want to help but you don’t always know what to do. You now know many ways to help the target – and that you have options for supporting them in ways that you’re comfortable with. You have the power to help people in a way that works for you!

Upstander options

Now that you're in your groups, each group gets to decide how you want to be an upstander. Ask for one volunteer in your group to be a writer (on the sticky notes) and one to be a reader. The reader reads the first situation out loud and then the groups take five minutes for each situation to discuss and decide how you'd support the target publicly and how you'd support them privately. The writer writes your decisions on two sticky notes and sticks one note in the Public column and one note in the Private column on the whiteboard. To make your decision, use the ideas the class just discussed together OR make up your own way to help the target. Repeat that process for situation 2 and situation 3.

Note: There's not just one right way to support a target because each person (both target and bystander) is different and each situation is different. We're just trying out different upstander options.

Situation 1

A student posts a video of themselves singing a cover to a famous pop artist's song. Other students start posting mean comments under the video. What do you do to support the student who posted the video? Work with some of the ideas previously discussed or agree on your group's own response.

Situation 2

A student sends another student a screenshot of a comment your friend posted and makes a nasty joke about it. The screenshot gets reposted and goes viral at school. What will you do to support the student whose comment was screenshotted and shared? Choose one of the ideas we just discussed as a class – or decide on your own response.

Situation 3

You find out that a student at your school created a fake social media account using another student's name and posts photos and memes that say mean things about other students, teachers, and the school. What do you decide to do to support the student who's being impersonated in this mean way? Consider some of the ideas previously discussed or come up with your own response.

It's Cool to Be Kind: Activity 3

...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 for students

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

Let's talk**Turning negative to positive**

Kids your age are exposed to all kinds of online content, some of it with negative messages that promote bad behavior.

- Have you (or anyone you know) seen someone be negative on the web? How did that make you feel?
- Have you (or anyone you know) ever experienced a random act of kindness on the web? How did it 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 whiteboard or projection screen
- Handout: "...but say it nicely!" worksheet
- 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?

Educator note

Younger students may need some modeling on how to revise comments. Completing one example as a class together could be a good way to ensure students' success when thinking independently.

3. Present responses

Now each team will perform their responses for both situations.

Continued on the next page →

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 3

...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 Yasmine is the only one in class not going on the camping trip this weekend.

Everybody wear purple tomorrow but don't tell Ingrid.

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 Nina looks kinda like a Smurf?



It's Cool to Be Kind: Activity 4

Mind your tone

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

Goals for students



- ✓ **Make good decisions** when choosing how and what to communicate – and whether to communicate at all.
- ✓ **Identify** situations when it's better to wait to communicate face-to-face with a peer than to text them right away.

Let's talk

**It's easy to misunderstand**

Young people use different types of communication for different kinds of interaction, 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 – or even mean?

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. The class probably has great examples too, so let's write some on the board for us to discuss.

- "That's so cool"
- "Whatever"
- "I'm so mad at you"
- "CALL ME NOW"
- "Kk fine"

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., 😞 😐 😊).

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 a text. Be sure you choose the right tool for your next communication – and that you don't read too much into things that people say to you online. If you are unsure what the other person meant, find out by talking with them in person or on the phone.

It's Cool to Be Kind: Activity 5

Walking the walk

Students discuss how kids can model behavior for adults, too.

Goals for students



- ✓ **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 – and what kids can teach adults!**

It's important to teach kindness. But it's just as important to model the thematics of kindness that we teach. There are plenty of examples of how bullying and harassment aren't just issues for kids. Just look at how adults sometimes treat each other online, in the news media, 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 meanly toward each other, in your everyday life or in the media? 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 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.)

Do you think some kids start bullying or making unkind comments because they see adults around them or in the news doing these things? Yes to all the above? Please give examples. What would YOU do instead – how would you be a better role model for adults?

Educator note

Consider taking this discussion to the next level by creating a "kindness campaign" at your school! At the beginning of a class period, each student writes and delivers one note of affirmation for another student, which both sets the tone for a positive class period and serves as a reminder that we can be forces for positivity both online and off. You could even start a class like this each week!

Takeaway

How you and your friends treat each other online will have a big impact on the digital world your generation builds – not to mention the offline world too.

It's Cool to Be Kind: Activity 6

Interland: Kind Kingdom

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

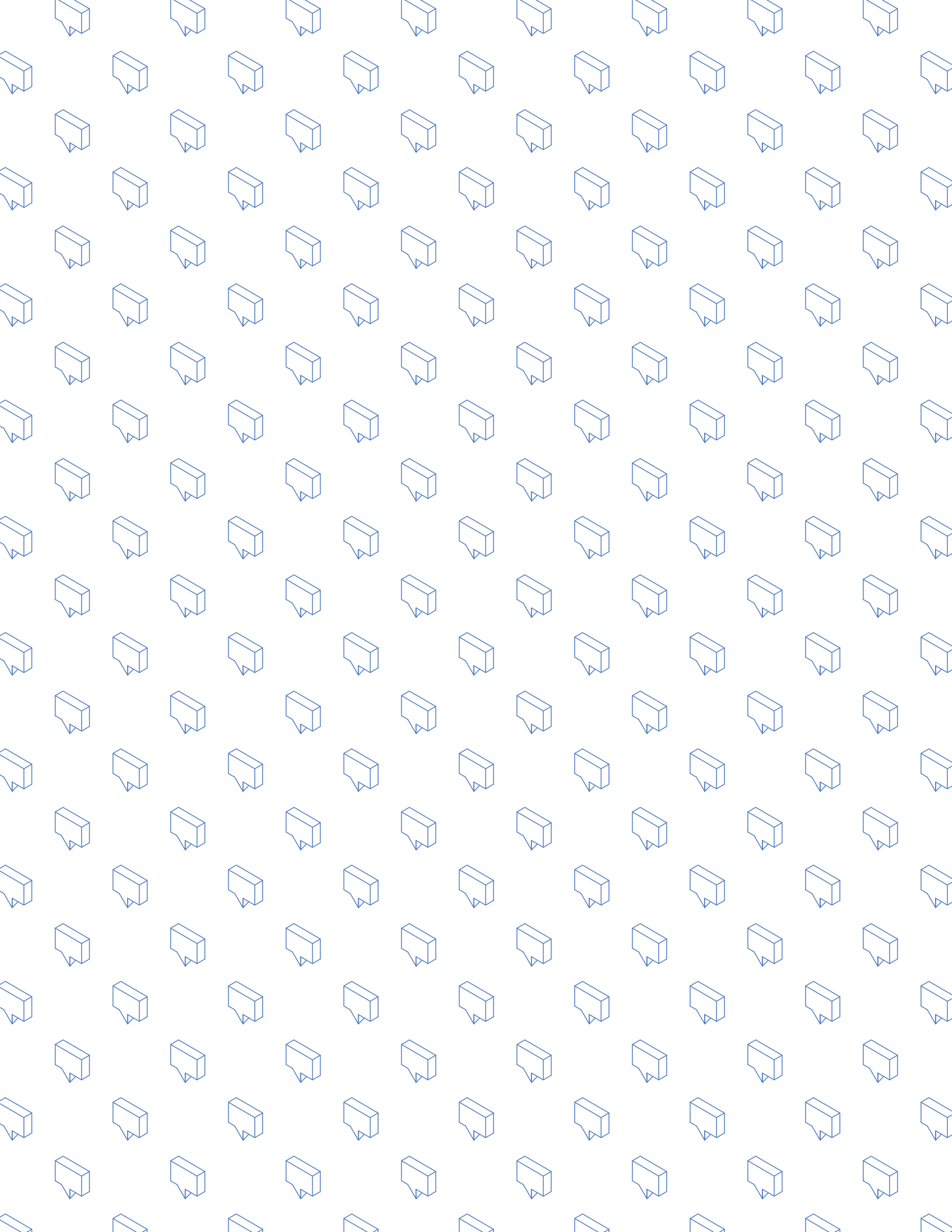
Open a web browser on your desktop or mobile device (e.g., tablet), and visit https://beinternetawesome.withgoogle.com/en_be/interland/kind-kingdom.

Discussion topics



Have your students play Kind Kingdom and use the questions below to prompt further discussion about the thematics learned in the game. Most students get the most out of the experience by playing solo, but you can also have students pair up. This may be especially valuable for younger students.

- 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 an aggressor? Describe this character's qualities and how their actions affect the game.
- Did playing Kind Kingdom change the way you plan to behave toward others? If so, how?



When in Doubt, Talk It Out

Defining and encouraging Internet Brave behavior



Thematic overview

Activity 1: **When to get help**
Activity 2: **Report it online, too**

Themes

It's important that kids understand they're not on their own when they see content online that makes them feel uncomfortable – especially if it looks like they or someone else could get hurt. They should never hesitate to get help from someone they trust. It's also good for them to know there are different ways to be brave and take action, from talking things out offline to using reporting tools online.

Goals for students

- ✓ **Understand** what types of situations call for getting help or talking things out with a trusted adult.
- ✓ **Consider** what options there are for being brave and why bringing adults into the conversation is important.

When in Doubt, Talk It Out

Vocabulary



Courageous: Brave; not necessarily fearless, though, because people are especially brave when they're scared or nervous but take positive action anyway

Compromised account: An online account that has been taken over by someone else so that you no longer have complete control of it

Student agency: A step beyond a student using their voice to speak up, student agency is the capacity to act or make change; including protecting or standing up for oneself and others; often seen as a necessary part of citizenship

Trust: Strong belief that something or someone is reliable, truthful, or able

When to get help

One piece of advice that appears consistently throughout these thematics is: If students come across something that makes them feel uncomfortable or worse, encourage them to report it – be brave and talk to someone they trust who can help, including you, the principal, or a parent. Students should pick this up from any one of the thematics, but just to be sure, here’s a class discussion focused specifically on the “when in doubt, talk it out” principle. Below, you’ll find a list of situations in which talking it out can really help.

Important educator notes

- 1. Children have been taught or conditioned not to “tattle” for so many generations that it has become a social norm, and bullying prevention experts have been working hard to help children understand the difference between “telling” and getting help. Help your students see that seeking support when hurtful things happen online is not “tattling”; it’s about getting help for themselves or peers when people are getting hurt.*
- 2. Fostering open communication in your classroom and reminding students you’re always there for backup support students’ agency and appropriate reporting.*
- 3. In the discussion below, any time students share about times they sought adult help, be sure the tone of the conversation is one that makes them feel proud and brave to have taken action, especially since they’re speaking up in front of peers.*

Goals for students



- ✓ **Recognize** that seeking help for oneself or others is a sign of strength.
- ✓ **Think out loud together** about situations where talking it out can really help.

Let’s talk



Here’s a whole list of situations you might run into online. We may not get through them all because I hope you’ll raise your hands when something on the list reminds you of a situation you’ve been in and what you did about it, so we can talk those situations out together.

Takeaway

It may not always seem like it, but being able to ask for help when you’re not sure what to do is a brave thing to do. If it’s to help you or someone heal something hurtful or stop harm from happening, it’s both smart and courageous.

Discussion topics



1. Silently read the list to yourselves. While you do, think about whether any of these situations happened to you, whether you wanted to ask an adult for help in any of them and if you did or not.

- You had this feeling that your account may have been compromised. (Discussion opportunity: What can you do to make your account security even stronger?)
- You needed help remembering a password.
- You were unsure whether something was a scam or thought you might have fallen for one. (Discussion opportunity: What are the warning signs?)
- Someone tried to discuss something online with you that made you uncomfortable.
- You received a creepy message or comment from a stranger. (Discussion opportunity: What makes something creepy?)
- You wanted to discuss something someone said online that was really nice OR really mean.
- You were concerned you may have shared something online you shouldn't have. Only tell us what it was if you feel comfortable sharing that, but even if you don't, tell us what you did about it.
- You saw a peer being hurtful to another student online.
- You saw someone threatening to start a fight or harm someone.
- Someone posted a fake profile about another student.
- You were concerned about another student because of something they posted or texted. (Discussion opportunity: Sometimes it's difficult to risk upsetting your friend, but isn't their safety and well-being more important?)

2. Raise your hand if you want to tell us what you did (or didn't do) and why. If someone already picked one, see if you have a different one we can talk about.

3. Let's discuss those situations.

Note for administrators

Having a student panel or working group in your school (or a middle/high school in your district) can be a very effective way to build student agency around this topic. If there already is a panel or peer mentoring group at your school, have the mentors walk through the above scenarios with younger students and share their own experiences of navigating them.

When in Doubt, Talk It Out: Activity 2

Report it online, too

Using a school device to demonstrate where to go to report inappropriate content and behavior in apps, the class considers various types of content, decides whether to report it, and talks about why or why not.

Goals for students



- ✓ **Be aware** of online tools for reporting abuse.
- ✓ **Consider** when to use them.
- ✓ **Talk about** why and when to report the abuse.

Let's talk



When meanness and other inappropriate content turn up online, people have options for taking action. In the last activity we talked about the most important one: talking it out with someone you trust. Another option is to report it to the app or service where you found it, which can help get the content deleted. It's important to get used to using online reporting tools.

Students should get in the habit of taking a screenshot of conversations or activity that's harmful or suspicious before using blocking and reporting tools (which could make a record of the activity inaccessible). This ensures that trusted adults can see what happened and help resolve this situation.

Activity



Materials needed:

- Handout: "Report it online, too!" worksheet

1. Figure out how to report a problem

Grab as many devices as your class has access to. If there are several, divide the class into groups. Together, find the tools in at least three school-related accounts for reporting inappropriate content or behavior. (If there's only one device or computer in the room, have groups of students take turns at that screen.)

2. Go through the scenarios

As a class, go through the seven situations on the worksheet.

3. Would you report it?

Ask students to raise their hands if they would report the content; then ask them to raise their hands if they wouldn't report it.

4. If so, why?

Ask someone who would report it to tell the class why, and ask someone who wouldn't report it to do the same.

Note: there is not just one right answer or approach. Make sure the class knows this before class discussion begins.

Continued on the next page →

Takeaway

Most apps and services have tools for reporting and/or blocking inappropriate content, and it can help the people involved, their community, and the platforms themselves if we use those tools. Before blocking or reporting inappropriate content, it's always wise to take a screenshot so that you have a record of the situation.

Report it online, too

Read each scenario below and raise your hand if you'd report it in the app or service where you found it. Prepare to explain why you would or wouldn't report it and explain why you chose that option, then discuss those choices as a class.

Note: Everybody should know that there is not one right choice to make, which is why discussion is helpful. No one should feel bad about what they chose to do. Even adults don't always know when or how to report.

Situation 1

A student posts a group photo in a public account, and you hate the way you look in it. Would you report that photo or not? How can you respond?

Situation 2

Someone creates an account of a student you know using their name and photo. They turned the photo into a meme and drew a moustache and other weird facial features on it, turning the photo into a joke. Would you report the account or not?

Situation 3

Someone posts lots of mean comments about a student in your school without using their name, but you have a feeling you know who it is. Would you report those comments or not?

Situation 4

A student creates an account with your school's name in the screen name and posts students' photos with comments that everybody hears about. Some of the comments are mean to students; some are compliments. Do you report the mean comments, the whole account, or both?

Situation 5

One night, you notice that a student has made a comment online saying they're going to fight with another student in the lunchroom the next day. Do you report that comment online or not? Do you report it to a teacher or principal the next morning or not? Or both?

Situation 6

You're watching a cartoon video and all of a sudden there's some weird content in it that's definitely not appropriate for kids and makes you feel uncomfortable. Do you report it or not?

Situation 7

You're playing an online game with friends and someone none of the players know starts chatting with you. They're not being mean or anything, but you don't know them. Do you ignore them or report them?