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 children

- ✓ **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!

Children 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 children

- ✓ **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.)

Continued on the next page →

- Does the message sound just a little bit weird? Like they might know you, but you're not completely sure?

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

You'll need:

- 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. Study examples

Let's make your children study these examples of messages and websites.

2. Indicate choices

Select "Real' or "Fake" for each example, and say why below.

3. Discuss choices

Which examples appeared trustworthy and which seemed suspicious?
Did any of the answers surprise you?

4. Further discussion

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

- **Does this message look right?**
  What's your first impression? Do any aspects strike you as being untrustworthy?

- **Is the email offering you something for free?**
  Free offers usually aren't really free (even if there are).

- **Is the message asking for your personal information?**
  Some websites ask for personal info so they can send you more scams.
  For example, a "personality test" in which you disclose personal information that can be used to make it easy to guess your password or other secret information.
  Most genuine businesses will never ask for personal information by email.

- **Is it a chain email or post on social media?**
  Emails and posts that ask you to forward it 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 →

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

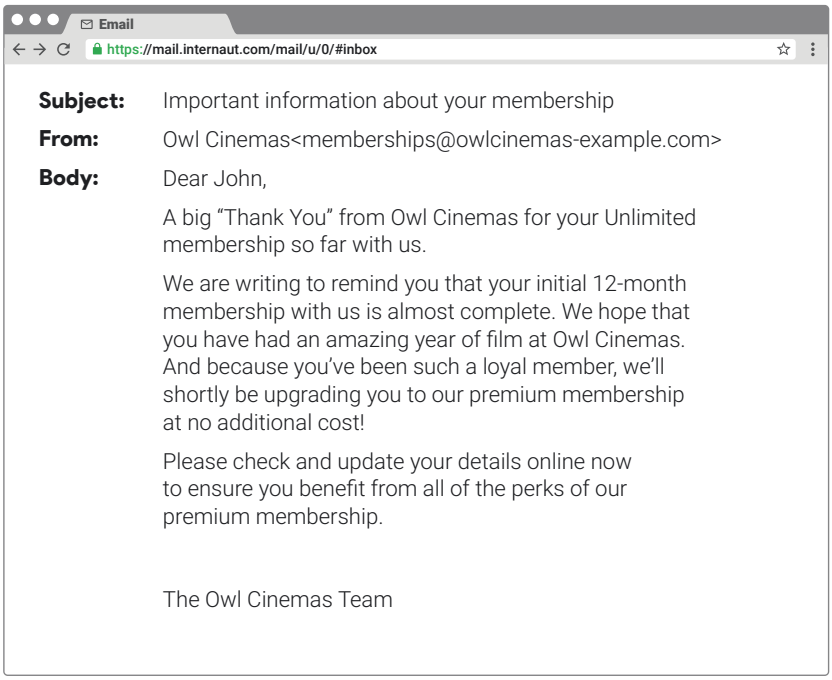
Note: For the purposes of this exercise, assume that 'Internaut Mail' is a real, trusted service."

Takeaway

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

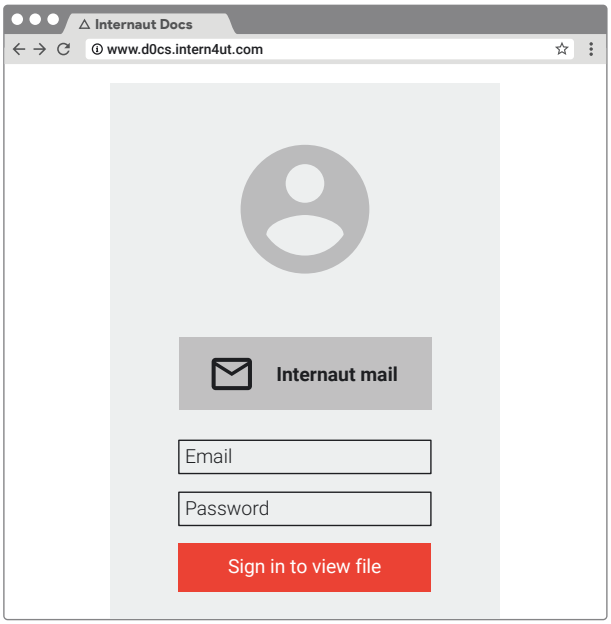
Worksheet: Activity 1

Phishing examples



1. Is this real or fake?

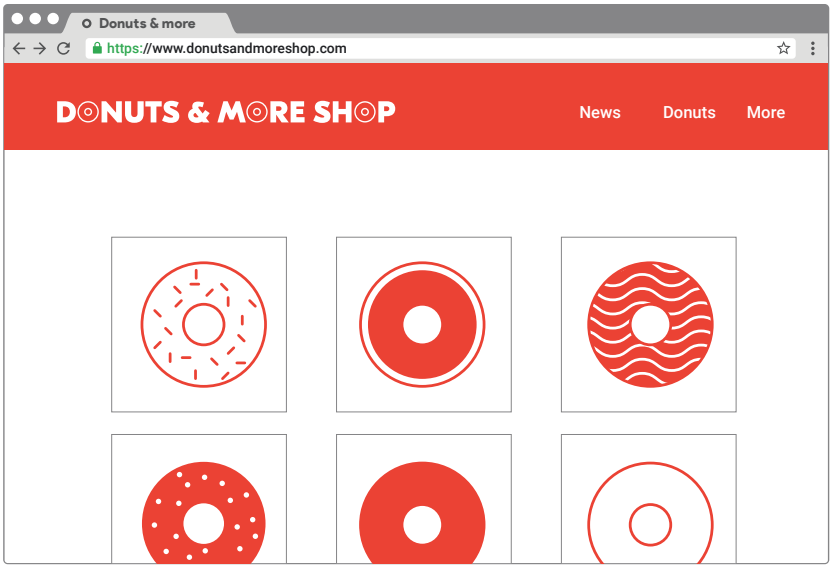
Real _____ Fake _____



2. Is this real or fake?

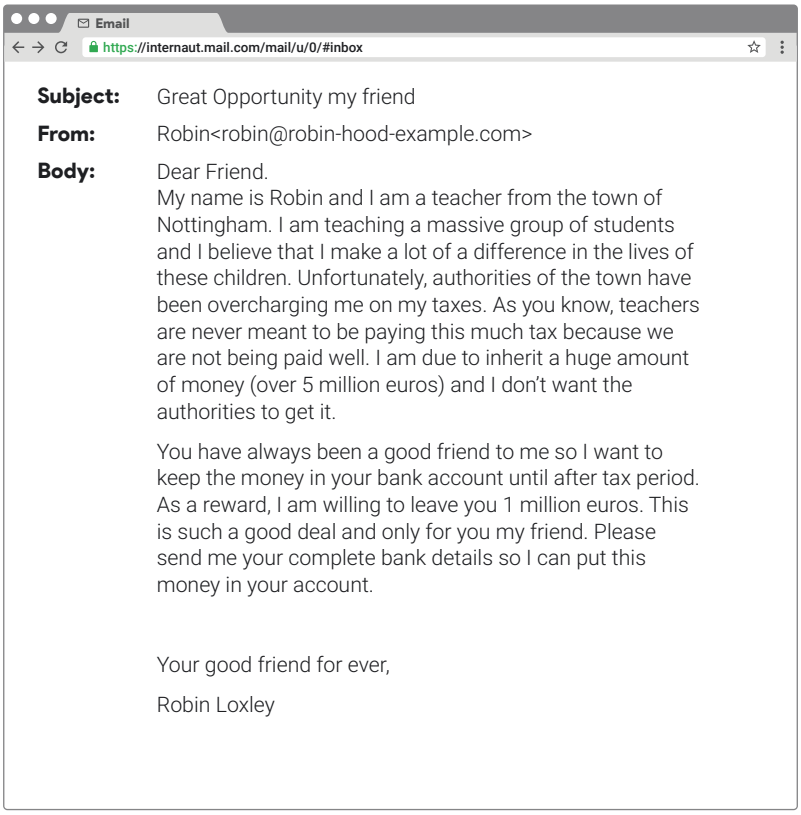
Real _____ Fake _____

Continued on the next page →



3. Is this real or fake?

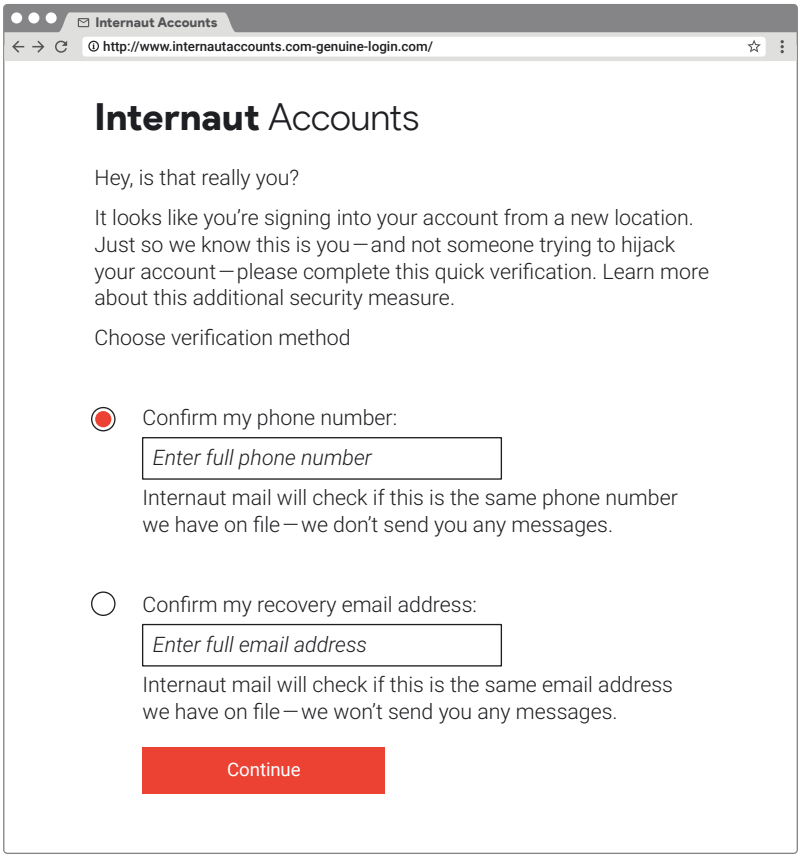
Real _____ Fake _____



4. Is this real or fake?

Real _____ Fake _____

Continued on the next page →



5. Is this real or fake?

Real

Fake

Don't Fall for Fake: Activity 2

Who are you, really?

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

Goals for children

- ✓ **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 family brainstorm on the question "How do we verify a person's identity online?" first; then continue the conversation with these thought starters.

Continued on the next page →

- **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?**
  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. Phishing cheat sheet

Pick one or several scenario from this container and talk about how you should respond to this situation. If there's 3 or more of you, you can start by acting out a scenario (one person narrating, a second performing the "message", a third responding, a fourth explaining the reasoning...), then discuss while checking the cheat sheet. Feel free to imagine more messages that you think would be even trickier.

Takeaway

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

Phishing cheat sheet: Activity 2

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? —Stan." What do you do?

- **Ignore Stan.** If you don't know him, you can just decide not to talk to him, period.
- **"Hi, Stan. Do I know you?"** If you aren't sure, ask first.
- **Block Stan.** 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 Stan'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 Stan 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 Corey! Remember me from last summer?" What do you do?

- **Block Corey.** This would feel rude if you actually know her. But if you're sure you didn't meet anyone named Corey last summer or she's sending you too many texts and oversharing about herself, it would be fine to block her.
- **Ignore Corey.** If you don't know this person, you can just not respond.
- **"Hi, Corey. 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 Corey 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 Lizi? 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

Children 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 children to think out loud together (or simply with you) 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 children

- ✓ **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 your children have 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, on your home 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 in family if the information is good 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 children play Reality River and use the questions below to prompt further discussion about the thematics learned in the game.

- 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?