### **Unit 02: Be Internet Alert**

# Don't Fall for Fake

Steering clear of scammers, fakers, info that doesn't help and other Internet stuff that tries to trick your brain—and learning how to find the good stuff

Lesson overview	Lesson 1 Lesson 2	Popups, catfishing and other scams Who's this 'talking' to me?	Grades <b>2-6</b> Grades <b>2-6</b>		
	Lesson 3	Is that really true?	ML Grades 2-6		
	Lesson 4	Spotting untrustworthy information online	ML Grades 4-6		
	Lesson 5	If we were a search engine	ML Grades 2-6		
	Lesson 6	Practicing Internet search	ML Grades 2-6		
	Lesson 7	Interland: Reality River	Grades <b>2-6</b>		
 Themes	 It's import	ant for kids to understand that contacts or content t	they encounter online		
	respond to	n, identity or property. Online scams aim to get Inter o fraudulent posts and pitches—sometimes from per they know.			
Goals for students		stand that what people tell you online isn't necessar			
	Learn how scams work, why they're a threat, and how to avoid them.				
		<b>nine</b> the validity of information and messages onlinulation, unsubstantiated claims, fake offers or prize			
 Standards	ISTE Stan	<b>dards for Educators:</b> 1a, 2c, 3b, 3c, 4b, 5a, 6a, 6d, 7a			
addressed	ISTE Standards for Students 2016: 1c, 1d, 2b, 2d, 3b, 3d, 7b, 7c				
	AASL Learning Standards: I.b.1, I.c.1, I.c.2, Ic.3, I.d.3, I.d.4, II.a.1, II.a.2, II.b.1, II.b.2,				
	II.b.3, II.c.1, II.c.2, II.d.1, II.d.2., III.a.1, III.a.2, III.a.3, III.b.1, III.c.1, III.c.2, III.d.1, III.d.2,				
	IV.a.1, IV.a.2, IV.b.3, V.a.2, VI.a.1, VI.a.2, VI.a.3				

# Don't Fall for Fake Vocabulary

### Lessons 1 and 2

**Catfishing:** Creating a fake identity or account online to trick people into friending them or sharing their personal information

**Malicious:** Words or actions intended to be cruel or hurtful. This word can also refer to harmful software intended to do damage to a person's device, account, or personal information

**Phishing:** An attempt to scam you or trick you into sharing your login or other personal information online. Phishing is done through email, social media, texts, ads or web pages that look similar to ones you're already used to but are fake.

**Scam:** A dishonest attempt to make money by tricking people into sharing their login, personal info, contacts, etc. or tricking people out of their money or digital property

**Smishing (or SMiShing):** A scam that uses text messages to trick you into doing something, like share a login or other personal info, click on a link to a bad site or download bad software

**Spearphishing:** A phishing scam where an attacker targets you more specifically by using pieces of your own personal information

**Trustworthy:** Able to be relied on to do what is right or what is needed

### Lesson 3

**Credible:** Believable; someone who is credible uses evidence, and you can be confident they are telling the truth.

**Expertise:** Special skill or knowledge about a particular thing; experts have expertise

**Motive:** The reason that someone does something; intention

**Source:** Someone or something that provides information

**Vlogger:** A person who is known for regularly posting short videos on a blog or social media.

### Lesson 4

**Deceptive:** False; an action or message designed to fool, trick or lie to someone

**Deceptive news:** News that intentionally lies or distorts the truth—the popular name for it these days is "fake news"

**Disinformation:** False information intended to trick or mislead you

**Evidence:** Facts or examples that prove something is true or false

Misinformation: False Information

Skeptical: Willing to question claims of truth

### Lessons 5 and 6

**Clickbait:** Content that attracts attention and could push you to click on a link to a certain site by using interesting formatting or catchy phrases

**Keyword:** A word directly related to the topic of your Internet search—one of the words you really need to do your search because no other word describes your topic better

**Query:** A keyword, set of keywords or a question you type into a search window (or box) to find information online. Sometimes a search takes more than one query to find what you're looking for.

**Search engine/Internet search:** A software program or "tool" people use to find information—including locations, photos and videos—on the Web

**Search results:** A collection of information you get in a search engine after you type your query and hit the "Search" or "Send" button

## Popups, catfishing and other scams

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

Goals for students	<ul> <li>Learn techniques people use to scam other people online or on devices.</li> </ul>				
	<ul> <li>Review ways to prevent online theft.</li> </ul>				
	Know to talk to a trusted adult if they think they're a victim of an online scam.				
	<ul> <li>Recognize the signs of scam attempts.</li> </ul>				
_	Be careful about how and with whom they share personal info.				
Let's talk	What's a scam, anyway?				
	A scam is when someone tries to trick you so they can steal something—like your				
	login, personal information, money or digital property. Scammers sometimes pretend				
	to be someone you trust, and they can show up in a popup, webpage, text or even a				
	fake app in ad ar app stores. Their messages and the unappendent how try to cond				

login, personal information, money or digital property. Scammers sometimes pretend to be someone you trust, and they can show up in a popup, webpage, text or even a fake app in ad or app stores. Their messages—and the unsafe pages they try to send you to—can also put viruses on your device. Some use your contact list to target your friends and family with the same kind of attack. Other types of scams might try to trick you into downloading a bad app by looking like the real one or bad software by telling you there's something wrong with your device.

Remember: A texter, website or ad can't tell if there's anything wrong with your device or computer! So if they say there is something wrong, they're trying to scam you. Also remember (you may have heard this before, but it's good): If you get a message from someone you don't know or even think you **might** know, and it sounds fantastic, exciting, or a little too good to be true, it very probably is exactly that (too good to be true).

**Note to teacher:** You could ask the class if they've ever heard that, get a show of hands, then ask them if they've ever seen a message like that themselves—or if a family member has. If not, GREAT, and if it happens in the future, they know how to protect themselves, their family and their stuff.

Some scams 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 hard to spot because using your info can make it seem like they know you. Another kind, which you've probably heard of, is catfishing—when someone creates a fake page or profile pretending to be someone you know or you're a fan of so they can trick you. Then there's smishing (scams in text messages) and phishing (in email).

So before you do what someone asks—like click on a link or share your login—it's a good idea to ask yourself some questions about that message. Here are some questions you could ask:

- If it's from a business, does it look professional, with the product's or company's usual logo and text that doesn't have spelling errors?
- It's never a good idea to click to a website from the message, but you can go to your web browser, search for the business and click to it from search, then ask yourself: Does the site's URL match the product's or company's name and information you're looking for? Are there misspellings?
- Is the message coming in the form of really annoying spammy popups?
- Does the URL start with https:// with a little green padlock to the left of it? (That's good, it means the connection is secure.)
- What's in the fine print? (That's sometimes where they put sneaky stuff, if they bother to. It's also not good if there's **no** fine print.)
- Is the message offering something that sounds too good to be true, like a chance to make money, get a better digital thing for your avatar or character, become famous, etc.? (It's almost **always** too good to be true.)
- Does the message sound just a little bit weird? Like they're saying they know you and you think it's possible, but you're not completely sure?

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

- Tell your parent, teacher or other adult you trust 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 get that tricky message next.
- Report the message as spam, if possible.

### Activity



#### Materials needed:

• Handout: "Phishing examples" (answers provided on page 39) **Possible modification for grades 2–3:** Divide the class into 5 groups and assign one example from the worksheet to each group. After each group has had a chance to analyze the example, discuss as a class.

### 1. Divide class into groups

### 2. Each group studies examples

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

### 3. Individuals indicate choices

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

### 4. Groups discuss choices

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

#### Answers to student handout: "Phishing examples"

- 1. Real. The message 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 message or asking you to email your password (links can send you 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
- 6. Fake. Not secure and suspicious URL
- Fake. Not secure and suspicious URL and suspicious offer in exchange for bank details

### 5. 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?

### Does this app look right?

Sometimes fake apps—apps that look a whole lot like real ones—get advertised in website popups or show up in app stores. There are all kinds of nasty things they do if they're downloaded to a phone—steal your information or contacts, install bad software, etc. Look out for spelling mistakes, a tiny number of user review or sloppy (not very professional) graphics.

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

Free offers usually aren't really free—the senders usually want to get something from you.

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

Some scammers 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 in a message or from anywhere except their own websites.

### Is it a chain message or social post?

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

### Does it have fine print?

At the bottom of most documents you'll find the "fine print." This text is tiny and often contains the stuff you're supposed to miss. For example, a headline at the top might say you've won a free phone, but in the fine print you'll read that you actually have to pay that company \$200 per month. No fine print at all can be just as bad, so definitely 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 scams in games, webpages, apps and messages—and know that if it sounds fabulous or a way to get something for free, it's probably fake. And if you do get fooled, make sure you tell an adult you trust right away.

### Worksheet: Lesson 1

# **Phishing examples**

••• Email				
$\leftrightarrow$ $\rightarrow$ $C$ $\triangleq$ https://	//mail.internaut.com/mail/u/0/#inbox	☆	:	
Subject:	Important information about your membership			
From:	Owl Cinemas <memberships@owlcinemas-example.com></memberships@owlcinemas-example.com>			
Body:	Dear John,			
	A big "Thank You" from Owl Cinemas for your Unlimited membership so far with us.			
	We are writing to remind you that your initial 12-month membership with us is almost complete. We hope that you have had an amazing year of film at Owl Cinemas. And because you've been such a loyal member, we'll shortly be upgrading you to our premium membership at no additional cost!			
	Please check and update your details online now to ensure you benefit from all of the perks of our premium membership.			
	The Owl Cinemas Team			

### 1. Is this real or fake?

Real

Fake



3. Is this real or fake?

Fake

	://internaut.mail.com/mail/u/0/#inbox	☆ :	4. Is thi	S I Cal UI	lanc.
ect:	Great Opportunity my friend				
:	Robin <robin@robin-hood-example.com></robin@robin-hood-example.com>				
/:	Dear Friend. My name is Robin and I am a teacher from the town of Nottingham. I am teaching a massive group of students and I believe that I make a lot of a difference in the lives of these children. Unfortunately, the sheriff of the town has been overcharging me on my taxes. As you know, teachers are never meant to be paying this much tax because we are not being paid well. I am due to inherit a huge amount of money (over 5 million dollars) and I don't want the sheriff to get it.		Real		Fak
	You have always been a good friend to me so I want to keep the money in your bank account until after tax period. As a reward, I am willing to leave you 1 million dollar. This is such a good deal and only for you my friend. Please send me your complete bank details so I can put this money in your account.				
	Your good friend for ever,				
	Robin Loxley				
	aut Accounts //www.internautaccounts.com-genuine-login.com/	☆ ::	5. Is thi	s real or t	fake?
① http://		☆ :	5. Is thi	s real or t	fake?
© http://	//www.internautaccounts.com-genuine-login.com/	☆ :	5. Is thi	s real or t	f <b>ake?</b>  Fak
<ul> <li>http://</li> <li>http://</li></ul>	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. a so we know this is you – and not someone trying to hijack account – please complete this quick verification. Learn more ut this additional security measure.	<b>☆</b> ::		s real or t	
<ul> <li>http://</li> <li>http://</li></ul>	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. : so we know this is you—and not someone trying to hijack : account—please complete this quick verification. Learn more	☆ ::		s real or a	
<ul> <li>http://</li> <li>http://</li></ul>	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. a so we know this is you – and not someone trying to hijack account – please complete this quick verification. Learn more ut this additional security measure.	<b>☆</b> ::		s real or	
© http:// Int Hey, It loc Just your abou Choo	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. a so we know this is you – and not someone trying to hijack a account – please complete this quick verification. Learn more ut this additional security measure. ose verification method	☆ ::		s real or	
© http:// Int Hey, It loc Just your abou Choo	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. : so we know this is you — and not someone trying to hijack : account — please complete this quick verification. Learn more ut this additional security measure. ose verification method Confirm my phone number:	☆ ::		s real or	
© http:// Int Hey, It loc Just your abou Choo	//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. : so we know this is you – and not someone trying to hijack : account – please complete this quick verification. Learn more ut this additional security measure. ose verification method Confirm my phone number: <i>Enter full phone number</i> Internaut mail will check if this is the same phone number	☆ ::		s real or	
© http:// Int Hey, It loc Just your abou Choo	<pre>//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? oks like you're signing into your account from a new location. is so we know this is you – and not someone trying to hijack account – please complete this quick verification. Learn more ut this additional security measure. ose verification method Confirm my phone number: Enter full phone number Internaut mail will check if this is the same phone number we have on file – we don't send you any messages.</pre>	☆ ::		s real or	
© http:// Int Hey, It loc Just your abou Choo	<pre>//www.internautaccounts.com-genuine-login.com/ ternaut Accounts is that really you? bks like you're signing into your account from a new location. t so we know this is you – and not someone trying to hijack account – please complete this quick verification. Learn more ut this additional security measure. ose verification method Confirm my phone number: Enter full 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:</pre>	<b>☆ :</b>		s real or	



### 6. Is this real or fake?

Real		

Fake



### 7. Is this real or fake?

Real

Fake

### Don't Fall for Fake: Lesson 2 Who's this 'talking' to me?

Students practice their anti-scam skills by acting out—and discussing possible responses to—suspicious online messages, posts, friend requests, apps, pictures and email.

About this lesson: Because it's about social interaction, this lesson would seem to be for students in upper elementary grades (5–6), but because more and more kids aged 7–9 are playing online games, many of them with other players rather than solo, this lesson is good preparation even for grades 2–3. We hope teachers in those grade levels will find out if their students are gaming and, if so, what they love about it and whether they've experienced anything sketchy. To maximize learning, just keep it light, open and judgment-free.

### **Goals for students**



- Understand that people contacting us may not be who they say they are.
- **Be sure** the person is who they say they are before replying.
- Ask questions or get help from an adult if it's hard to tell who the person is.

### 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. 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, to get something from you or to be mean. Other times, they impersonate people to steal personal information or digital property like skins or game money. The safest thing to do is not to respond or to tell a parent or other 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 page or profile, see who their friends are or search for other information that tells you they're who they say they are.

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

**Note to teacher:** 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.

### • If there's a photo of the message sender, is it a little suspicious?

Is their 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. If there's a photo, can you find more photos of the person with that name online?

### Does their screen name 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.)

### Does their page have info about them?

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 info that you can confirm by searching for it with the name on the profile?

• How long has the account been active? Does the activity make sense to you? Is the page or profile new, or does it show a lot of activity going back a ways? Does the person have mutual friends with you, like you would expect? Fake accounts usually don't have much content or signs of other people posting, commenting, and socializing in them.

### 1. Groups review scenarios

Okay, now we're going to separate into 5 groups. Each group will pick a scenario from this container.

**2. Groups choose one or more responses** from the cheat sheet and talk about why you picked that response to the situation. Feel free to write more messages that you think would be even trickier.

### 3. Class discusses groups' choices

Finally, let's use this cheat sheet for class discussion about all the scenarios. Each group reads its scenario and tells the class about their response and why they chose it (or them). The class discusses.

Takeaway

along)

Activity

Materials needed:

on each strip

Worksheet: "Who's this

'talking' to me?" cut into strips, with one scenario

• A bowl or container to hold

the strips (each group of students will pick one)

Student outline on page 46

(one per student to follow

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

Worksheet: Lesson 2

# Who's this 'talking' to me?

Scenario 1	You get a friend request from a random player in a game: "Hey you're good! We should play together! Add me?"
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?"
Scenario 3	You get a message from someone you don't follow. "Hey! Love your posts, you're SO funny! Give me your phone number and we can talk more!"
Scenario 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."
Scenario 5	You receive a message online. "Hey, I just met your friend Sam! She told me about you, I want 2 meet u. Where do u live?"

### Student outline: Lesson 2 Who's this 'talking' to me?

Here are five scenarios of messages anyone could get online or on their phone. Each one has a list of ways you could respond, some great and others not so much. See which one (or two) makes the most sense to you—or if you think of other responses. Now talk about it, then we'll discuss it as a class.

**Everybody please note:** 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 them or block them. It also never hurts to talk with a parent or teacher about it, especially if it bothers you.

Scenario 1	You get a friend request from a random player in a game: "Hey you're good! We should play together! Add me?" What do you do?				
	• Ignore it. If you don't know them, you can just decide not to add them.				
	<ul> <li>Block them. You won't get any more messages from them—and, In most games and apps, they won't even know you blocked them.</li> </ul>				
	<ul> <li>Change your settings. Go into the game's settings, see if you can turn off all friend requests and check that box. That way, you won't even have to decide whether or not to accept requests from random players.</li> </ul>				
	• Check them out online. See if they have a page or profile so you can see if they're really a player—do they have experience, followers, have they streamed content? Do your friends know if they're for real? Only if they look like they're a gamer really into this game should you even consider friending them. But it's really best for kids just to play with their offline friends.				
	• Add them to your friends list. IF they seem ok. This isn't recommended, unless you've verified who they are and checked with an adult you trust or at least your friends, to see if they know who the person is. If you play with them, with a mic or headset, be sure to keep the chat only about the game—never share your full name or any other personal info.				
	<ul> <li>Give them personal info. Definitely not. You know: Never ever give away personal information to people you don't know.</li> </ul>				
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?				
	• <b>Block Corey.</b> 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.				

	• <b>Ignore Corey.</b> Like we said above, if you don't know this person, you can just not respond.				
	• <b>"Hi, Corey. Do I know you?"</b> 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!				
	<ul> <li>"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.</li> </ul>				
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.				
	• <b>Block</b> @ <b>soccergirl12.</b> 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				
	<ul> <li>"Hi, do I know you?" If you aren't sure, be sure to ask questions before giving out personal information like your phone number.</li> </ul>				
	• <b>"Okay, my number is"</b> 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.				
	<ul> <li>"Who are you?" Probably not. If the message sounds sketchy, it might be better not to answer—or just block them.</li> </ul>				
	• <b>"Is that you Lizi? U R CUTE too! I live in 240 Circle Ct."</b> This isn't a good idea, even if you think you know who it is. Before you give someone your address or any other personal information, check them out, even if you think you know them. Never meet someone in person that you only know from online interactions.				

### Scenario 5

You receive this message: "Hey, I just met your friend Sam! She told me about you, I want 2 meet u. Where do u live?" 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: Lesson 3 Is that really true?

**Media literacy background for teachers:** In addition to helping students use analytical questions to evaluate source credibility, we also want them to understand that information comes from lots of places (not just textbooks). So they need to apply their skills to analyze all types of media. When they get to that point, they're ready to move on to analyzing special categories of media, like news or scientific data.

Note: This is a media literacy lesson good for everybody to learn but may be a little over the heads of students in grades 2-3, so see a suggested modification below under "Activity."

### **Goals for students**

- Identify the tools you already use to know that information is credible.
- Consider how certain things like expertise and motive affect credibility.
- Learn 4 questions for evaluating source credibility.
- Understand that a source that's credible on one topic is not necessarily credible on other topics.
- Know that checking multiple sources often helps you see whether information is credible.

### Let's talk



### What makes something or someone credible or trustworthy?

Every day you make decisions about what to believe and what not to believe. Was that video you saw credible? Was it trying to persuade you of something? Is your older brother telling you the truth or teasing? Is that rumor you heard about a friend true?

What do you do when you're trying to decide if someone is telling the truth? Do you already use these clues?:

### What you know about a person

For example, you know if a classmate is really good at something or has a history of being truthful or playing practical jokes or being mean, so you can usually tell when they are serious or joking or lying.

### What a person knows about you

For example, your parents know what kinds of foods give you a stomachache; the ads on TV do not, so you follow your parents' advice about what to eat. The school librarian knows your interests and what kinds of books you like, so you trust her book recommendations.

### Tone of voice and facial expression

For example, you know that your friend means the opposite of the words they say if they roll their eyes and act snarky while they tell you they had a **terrible** time at the new skate park.

### The situation

For example, when friends are playing around and one teases you about your new haircut, you know it's just a joke. But if someone at school says the exact same words to embarrass you in front of the whole class, it's an insult.

When we hear things from a media source like a video, a person on TV, or website, we don't personally know the source and they don't know us. We may not be sure about whether to believe them.

Even when someone we know sends us a text there are no clues from facial expressions or tone of voice, so we might not be sure what they mean. That's when we need to ask questions...

### Activity

**Recommended modification for grades 2–3:** If you feel your students are ready to discuss whether a source is credible, complete steps 1 and 2 only.

### 1. Evaluating sources

If you wanted a recommendation for a great new video game, would you ask your grandmother? Or, to ask it another way, is your grandmother a **credible** source for information on video games? A **credible** source is one that we can trust to give us accurate **and** relevant information.

Make a pro/con list to explain the benefits and drawbacks of asking your grandmother for video game advice.

Did your list look something like this?

PRO	CON
Grandma loves me and wants me	Grandma doesn't play video games
to be happy	and doesn't know much about them
Grandma is pretty good at finding	Grandma doesn't know which games
information when she doesn't know	I already have or what types of games
the answer herself	I like

If your list looked like that, you've just used two of the most common tools we have to decide if a source is credible: **motive** and **expertise**. "Expertise" is a special skill or knowledge about a particular thing; experts have expertise. "Motive" is someone's intention, the reason they say or do something.

Which item in the list gives you information about grandma's motives? Which items say something about her expertise? So is the grandma on this pro/con chart a credible source for information about which new video game to get? She wouldn't lie, but it would probably be better to ask someone who cares about us **and** who also knows something about gaming and the types of games we like.

### Materials needed:

• Handout: "Deciding what's credible" (one per student)

We may also know that Dad is a great cook but is clueless about fashion, our coach knows basketball but not gymnastics, or that Grandma can fix almost any toy but doesn't know anything about video games. **Just because a person is an expert on one thing doesn't make them an expert on everything.** 

### 2. Make your own pros and cons list

If this is the first time you have thought about how you use **motive** and **expertise** as clues to decide which information sources are credible, you might want to practice some more.

Imagine that you want to know how to be a better soccer player. Make pro/con lists for these choices so you can decide if they're credible sources:

- your grandma
- a blog by a winning high school basketball coach
- the best player on your team
- a website that sells soccer shoes and gives advice
- Videos that teach soccer practice techniques

What do you notice about the strengths and weaknesses of each source?

- Is there one that knows how to teach, but may not be familiar with soccer skills?
- Is there one that is a soccer expert but may not know how to teach?
- Is there one whose advice always seems to include buying something from them?
- Is there one that knows soccer but doesn't know you or which skills you need to work on?

Discuss: Who would be a good source to go to and why do you think so?

**Credibility** is rarely an all-or-nothing call. Most sources have strengths and weaknesses. That's why **the very best answers often come from asking many sources** and comparing their answers.

### 3. Steps to consider

Credibility isn't just about **who** we believe. It's also about **what** we believe. We get ideas about the world from all sorts of places, not just directly from people. A movie about a tsunami shows a giant wave—taller than a skyscraper—heading towards people on shore. Is that what tsunamis **really** look like? An ad implies that most scientists are men with crazy hair who wear thick glasses and white lab coats all the time. Is that true?

We can check out any source using the 3 Steps on the **Deciding what's credible** handout. They're about what we already know about motive and expertise.

### Step 1: Use common sense

Ask: Is it logical-does it make sense?

If a) what you're seeing doesn't make sense, b) you know it isn't true from your own experience, or c) it just doesn't work with facts you already know, you don't have to take any additional steps. You are looking at a source that is not credible.

### Step 2: Ask questions

Not just any questions, but these four:

### **Expertise**

### a) Does this source know me or care about me?

The answer to this question depends on the information you're looking for. If you're checking some information about plastic water bottles polluting the ocean, it really doesn't matter if the source knows you or not. But if a site promises that you will love their new toy, it would need to know what kinds of toys, games, or activities you like for their promise to be credible.

### b) Does this source know a lot about this topic? How did they learn what they know?

Some people think that the easiest way to find credible information is to ask a digital voice assistant. Digital assistants seem to know everything! Did you ever wonder how they can know all those answers? They use mathematical calculations (called "algorithms") to find answers.

For simple questions that only have one possible answer (like the temperature outside or the name of a celebrity famous for singing a particular pop song) they are usually a credible source. But if the question is complicated, it would be better to start with people or groups who have lots of experience or have earned awards or PhDs related to your topic. **Then** you can use a voice assistant to confirm that information (see Step 3).

### Motive

### c) What does this source want me to do or believe and why would they want me to do or believe that?

Does the source make money if you follow their advice? For example, do you think an influencer earns a fee if you buy the product they're wearing or talking about? Does a professional athlete wear a certain brand of shoe or shirt just because they like that brand or because they're paid to talk about it?

Money can often be one reason why you're seeing a logo or brand name in a video or ad—it can affect what the influencer or athlete is telling you (and what they're **not** telling you). They probably don't intend to hurt you, but it's possible that making money is more important to them than giving you all the facts or saying what is good for you.

d) Who benefits and who might be hurt if people believe this source?

This isn't always easy to tell. Here's an example:

Imagine an ad for an app that promises to make you a better student.

- What are the possible benefits? The app maker would benefit if you buy the app because they would make money. And you might benefit if the app really helped you.
- Who might be hurt if you believed the ad? You might be wasting your money if you bought the app. You might also be spending time practicing the wrong things, and then actually do worse in school. Or you might rely on the app, which can only make guesses about what you need, instead of seeking help from your teacher, who actually knows what you need.

### Step 3: Confirm

**Ask:** Do other **credible** sources back up what this source says?

The job isn't just to check **more** sources. It's to look for a variety of sources. If you can't find a variety of credible sources that agree with the source you are checking, you shouldn't believe that source.

### 4. Check your sources

Now that you understand, it's time to practice. Pick a question related to something you are covering in class or something you have seen online. Find a source that provides an answer to that question and, in small groups, use the questions on the handout to decide if the source is credible.

If you need some ideas, here you go:

- You need ideas for a birthday present for your friend. An ad for a local store claims their search tool, which has every item offered by the store, can help you find a gift for anyone on your list. Does that work for you?
- You are reading online reviews of a new pizza place and notice that three of the six 5-star reviews are from people with the same last name as the restaurant. Two others say it is the best pizza on the planet and one says it was not bad for a cheap slice. There are also fourteen negative comments. Would the positive reviews convince you to try their pizza?
- A pop up ad says that you are part of a very small group that has been selected to try a special "mermaid pill" that will give you the power to breathe underwater without scuba gear. All you have to do is send \$9.99 to cover shipping. Would you do it?
- You like a lot of the videos by a popular vlogger because they're funny, but they also say nasty things that you don't like about minority groups. Do you buy what they say because they're funny and really popular? Do you think that influences people?

### Takeaway

Questions are our friends. When you ask good questions about sources **and** the information they provide, you'll get much better information. The more sources you use, the better. And remember that a great source for one subject doesn't mean it's great for everything.

# Handout: Lesson 3 Deciding what's credible

Helpful steps to identify credible from non-credible sources.

Step 1	Use common sense Is it logical?				
Step 2	Ask questions				
	Not just any questions, but these four:				
	Expertise				
	<ul> <li>Does this source know me or care about me (and does that matter)?</li> </ul>				
	• Does this source know a lot about this topic? How did they learn what they know?				
	Motive				
	<ul> <li>What does this source want me to do or believe and why would they want me to do or believe that?</li> </ul>				
	<ul> <li>Who benefits and who might be hurt if people believe this source?</li> </ul>				
Step 3	Confirm				
	Do other <b>credible</b> sources back up what this source says? Use online search—or work with your school media specialist in the library—to find other sources of information				
	about your subject (the sources could be book or news or magazine articles, online or offline). Go through Steps 1 and 2 with them too—ask the same questions about these sources too. If they're giving you the same information about your subject, it's pretty				

likely they're confirming that your source is credible.

### Don't Fall for Fake: Lesson 4

## Spotting untrustworthy information online

**Media literacy background for teachers:** Media literacy questions and observation techniques give students tools to navigate their way through disinformation without getting stuck in arguments or hurting relationships with friends and family. But they need to ask questions and get used to applying critical inquiry to information that comes their way.

### Goals for students

- Identify clues which indicate that a news or information source is deceptive.
- Use analytical questions and careful observation to evaluate source credibility.
- Understand the importance of checking a source's credibility before sharing their message.
- Develop the habit of analyzing all news and information, not just the stories we think are suspicious.

### Let's talk



Did you ever play one of those games where you hunt for mistakes hidden in a picture? Sometimes dealing with news is like that. There are a lot of people and groups who are so passionate about what they believe that they twist the truth to get us to agree with them. When their twisting is disguised as a news story, that's disinformation.

Some people don't learn how to spot fake information, but they share it anyway. That's how it spreads. And when people make choices about the things they do or believe based on that disinformation, it can get really hard for people to listen to each other calmly, argue respectfully, understand each other better, and solve problems.

So, if something looks or sounds like news, how can we tell the difference between what's real or credible and what's fake or misleading? There are clues we can learn to spot it—tricks used by people who are trying to mislead you. And there are questions we can ask that help us spot stories that aren't based on facts.

### Activity

### Materials needed:

- Image: "What's Wrong with this picture"
- Handout: "Deciding what's credible" from Lesson 3 (page 54)
- Worksheet: "Spotting phony URLs"

### Answers for worksheet: "Spotting phony URLs" Real:

abcnews.go.com bbc.com/news nbcnews.com nytimes.com washingtonpost.com usatoday.com

### Fake:

abcnews.com.co abcnews-us.com nbc.com.co nytimesofficial.com bbc1.site/business-news washingtonpost.com washingtonpost.com.co usatosday.com

### 1. What's wrong with this picture?

Take a look at the image below. Look carefully. Can you spot the differences between the two pictures?



What if someone told you where to look? Would that make it easier?

### There are 9 differences, did you spot them all?



Trying to tell if a news story is real or fake is sort of like this picture game. By looking really carefully, you can find important information. And it's a lot easier if you know what to look for.

So here are some clues to finding disinformation. If you spot these things, you are probably looking at a fake, or deceptive, story.

### Spotting phony URL's Handout

The first thing to look at is the URL (web address) for the site that published the story. Some fake sites try to fool you by choosing names that mimic a real site but with small differences. Most companies use short URLs because they are easier to remember and type, so URLs with added, unnecessary letters are often sites with false information.

Look at the handout:

- Circle all of the URLs that you think are real.
- When everyone is done, look at the answer key. Did you get them all right?

How could you check to see if a URL was a real news site? One way is to do a web search for the news organization or the URL. If the organization is credible a box can appear to the right of the search results on many platforms with a description of the organization, including their website address. If the URL isn't credible, you will often be able to scroll down and see headlines about the site being reported as a fake—or you'll find out the site isn't available anymore.

### 2. Inspecting headlines

Sometimes someone shares a news story without a URL. In those cases, here are some clues to use:

- a) A story starts with a picture of something that would interest us, like a cute dog, a celebrity, or an unusual stunt. But when we click, the story has little or nothing to do with the picture.
- b) Instead of letting you decide for yourself, people who are trying to convince you to agree with them sometimes use things like **boldface**, ALL CAPS, <u>underlining</u>, or exclamation points to get you to think what you're seeing is important and click on them, called clickbait. Real journalists don't use those techniques.
- c) To get you to read a story, some people include words in the headline like "shocking" or "outrageous" or "surprising." They know words like that make us curious. But **real** journalists let the news speak for itself. They tell the story and let us decide if it is shocking or surprising.

For example, look at this picture and headline:



# The shocking truth about what teachers do after school

Without reading ahead, what do you imagine the story is going to say? Why do you think that? What's your evidence?

### Here's the story:

"A recent State University survey of teachers found that 86% of teachers do what everyone does after work. They run errands, fix dinner, spend time with family, do household chores, and get ready for the next day. But lately, many teachers have been doing something unexpected.

A decade ago, economic troubles led many states to slash education budgets. That meant years without a pay raise for teachers. Unable to meet basic expenses on low salaries, many teachers now work second jobs. In some states teachers have even gone on strike for pay increases so they can quit second jobs and devote more time to their students."

Was the story what you thought it would be? Do you think that the picture and headline were accurate or misleading? What's your evidence?

### 3. Inspecting sources

When we analyze news, clues can be helpful, but they aren't always enough. Sometimes trustworthy news stories use techniques to attract our attention, and that can make them seem fake. And sometimes fake sources are so good at copying the real thing that it's hard to tell they're not. It's hard to tell them apart. For example...

#### Do these sound like trustworthy news organizations to you?:

American News National Review News Examiner World News Daily Report Weekly World News NewsWatch33

Actually, only *National Review* is real. How could you find that out? You could start by doing a Web search of the organization's name. See where the name appears besides the organization's own website. If it appears in Wikipedia or an article at a newspaper or news magazine's site, it's probably a credible organization. But see what those articles say about it! It's possible that they're all saying it's fake.

Find a story about your school, community, the latest diet fad, or anything in the news that interests you. Use the 3 Steps on the **Deciding what's credible** handout, along with the new clues you know, to decide if the story is real or deceptive.

### Step 1: Use common sense

Ask: Is it logical-does it make sense?

Sometimes it's obvious. If you see a headline like: **CELEBRITY HAS SECRET BABY WITH SPACE ALIEN**, logic probably tells you it isn't real.

Sometimes it isn't so obvious. If: a) what you're seeing doesn't make sense b) you know it isn't true from your own experience, or

c) it just doesn't work with facts your already know

...you are looking at a source that is probably fake news.

### Step 2: Ask the expertise and motive questions

(see pages 52 and 53)

### Step 3: Confirm

Ask: Do other credible sources back up what this source says?

Who else is reporting this story? (You can use Internet search to see if this story is covered by other news sources...) What other stories does the site include? Are they all from the same perspective or are there many views included? If you can't find a variety of reliable sources that are covering the story, you should be skeptical of that source.

### Takeaway

Now that you know how to use clues and questions to spot disinformation, you can ask smart questions and make careful observation part of your daily routine and with time, you'll be an expert in spotting fake stuff online. You now know how to analyze the information you get online. It's called critical thinking, and it's a media user's superpower.

# Worksheet: Lesson 4 Spotting phony URLs

### **Real or fake?**

Circle the correct answer.

usatoday.com	Real	Fake
abcnews.com.co	Real	Fake
washinqtonpost.com	Real	Fake
abcnews-us.com	Real	Fake
bbc.com/news	Real	Fake
abcnews.go.com	Real	Fake
nytimesofficial.com	Real	Fake
nbc.com.co	Real	Fake
washingtonpost.com	Real	Fake
nytimes.com	Real	Fake
washingtonpost.com.co	Real	Fake
bbc1.site/business-news	Real	Fake
nbcnews.com	Real	Fake
usatosday.com	Real	Fake

### Don't Fall for Fake: Lesson 5



Without using any technology (we'll do that in the next activity), students create "search results" together to start learning how Internet search works from the "inside out."

Goals	for	stud	ents
-------	-----	------	------

Learn fundamentals of online search.
 Search for information about a topic.

- Search for information about a topi
- Understand that search results are collections of information, not usually answers to a question.

Let's talk



### What is search?

The internet is a place that has a gazillion (well, billions and billions of) pieces of information. Internet search, sometimes called a search engine, helps us narrow down that crazy amount of information that comes from all over the world. It's a software tool that people use to find information on all kinds of topics.

You might already know that, to use this tool, you type a few key words about a topic you want to know more about into the search bar (the empty box on a search engine page) or in your browser window (where you also type web addresses). Then, when you're ready, you hit the Return or Search key, and—voila!—the search engine works its magic (in about a half second), and you get your search results. Ok, so it's not **actually** magic. Internet search uses algorithms, which is a fancy way of saying people at the search company taught the software how to find and turn up information for you. Don't worry about how algorithms work for now. You just need to know that Search does the "searching" for you.

It's also good to know that search results aren't necessarily answers to a question. They're just collections of information you're interested in or looking for. If you do have a question that you're taking to a search engine, you can often find an answer in your search results, but sometimes it takes a few queries to get to the answer you're looking for. That's called "refining" your search.

So let's practice how search works by pretending to be a search engine together...



• pizza

• tornado

airplane



2. Distribute a copy of the worksheet to each student.

3. Share a search topic with the class. Here are some possibilities:

solar system

Materials needed:

• Worksheet: "If we were a search engine" (one per student)

- volcanoes
- basketball

• soccer

• farmer

- cooking
- sharks
- dentist
- construction

**4. Students work with their partners** to create possible "search results" in each category on the handout: "Website," "Image," "Map" and "Video." Their results can be in the form of words or drawings, as appropriate.

Encourage students to be creative, and make sure they know there are no "wrong" answers. For example, if the topic is "sharks," students might brainstorm the following search results:

- Website: information about different kinds of sharks
- Image: a drawing of a shark
- Video: sharks swimming through the ocean
- Map: the location of a beach where people saw a shark

**5. When students finish** all four search result categories for the given topic, pick which category (website, image, video or map) to talk about as a class.

6. Have one student from each pair share out their example of one of the search results.

For example, let's say the topic is "pizza." You can decide to have each group share their image results for pizza. Students can hold up their drawing and explain what they created. This allows students to see all the different search results that can be generated from a single query.

### 7. After students share examples, ask the class the following discussion questions:

- · About how many different results did we have?
- About how many results were similar?
- If I changed my topic to \_\_\_\_\_\_, how do you think that would change your results? For example, if the search topic was "pizza," how would the results change if I changed my query to "pepperoni pizza"?

Suggestion: Complete 4 rounds in total...

- Choose a different topic from each round and repeat the same steps as listed above.
- Complete 4 rounds so you can have discussions about the 4 main types of search results.

### Takeaway

Internet search is a tool you can use to find information online. The info can be in the form of text on a website, videos, images, maps and more. The key words you type into a search engine determine what results you get.

Worksheet: Lesson 5

# If we were a search engine

Search Topic	Website
Image   Video   Map	

### Don't Fall for Fake: Lesson 6

## **Practicing Internet search**

Using an Internet connection, students explore using a search engine and practice creating ever more effective search queries.

### **Goals for students**

- Navigate a search engine.
- Practice searching for information about a topic.
- **Create** search queries.
- Change keywords and notice differences in search results.

### Let's talk



Search is a tool that helps you find information on the internet. To use search, you can go to a search engine and type a query—a question or keywords—into the search bar to get info on a topic you want to know more about. Sometimes using keywords works better than just asking a question. That's because, first, **the words you use** in your query and, second, **the order you put them** in are really important. If you just ask a question, it may not have the words and the order that help the search engine turn up the results you're looking for. But—no worries—it's perfectly fine to start with a question if you like.

The important thing is, just start, because lots of times it takes more than one query to get to the information you want. So type your question into the search engine, look at the search results and—if they're not good enough—you can use those results to guide you on how to create a better query and get even closer to what you're looking for.

**For example:** Let's say I want to start a garden. I want to grow vegetables I can use to cook in my kitchen.

- I have no idea how to do this, so I'm going to do an Internet search to find out how.
   I go to a search engine and type in the question, "How do I start a garden?"
   Display your computer screen so students can see you searching.
- Ok, let's take a look at these results. Review the results with your class. Be sure to point out that there are websites, images, videos and other types of results. Also point out search results that are not relevant to helping you grow a garden for vegetables and spices for cooking.
- I'm noticing that a lot of these results are about all kinds of gardens, but I need information about creating a garden at home, in my own yard. Also, I only want to grow stuff I can eat. I should probably include a keyword about vegetables, right? Ok, let's try searching this: "home garden vegetables".

Display your computer screen so students can see you searching.

• Take a look at these results. What do you notice? Allow the students to share what they notice in the search results.

Both sets of search results gave me information about starting a garden, right? But the first set was about all kinds of gardens. It showed me I had to add a couple of important keywords to my original query to get the search results I needed to learn how to start a garden for cooking (BTW, did you know that's called a "kitchen garden"?). The more you practice creating search queries, the easier search gets. You can always start with a question, and if you don't get your answer, the search results will give you keywords you can try to get closer to what you need to know. If you want to start with keywords and aren't sure which ones to use, just know that there are no wrong keywords. Just try some! You can always try a different query if you're not seeing the results you were hoping for. Let's try it out...

# Activity

#### Materials needed:

- Worksheet: "Practicing Internet search" (one per student)
- Internet-connected device

### 1. Create the first search query

Explain to students that they are going to explore using a search engine and practice creating search queries. On the handout, they'll find four different characters, each character thinking (in a thought bubble) about something they want to learn more about. Then have your students...

- Type the original search query (provided on the handout) into the search engine, and explore the search results.
- Record 4–5 search results on their handout.

### 2. Create their own (second) search query

Have students look again at what the character wants to know (in the thought bubble). Ask students, did the original search results give enough information relevant to this topic?

• Direct students to change the original query to include keywords that will get them more useful search results.

Hint: Students can look for keywords they found in the first search results or in the character's thought bubble.

- Have them type this second search query into the search engine and explore the search results.
- Have students record 4-5 results on their handout.

### 3. Discuss

Have students find a partner and ask them to share with their partners how they changed the original search query and the types of results they got from that revised search query. Ask them to share what they discovered in a brief class discussion.

### 4. Repeat Steps 1-3 for the remaining characters

### **Takeaway**

The more you practice creating search queries, the easier it will get to find the information you are looking for in a search engine.

### Worksheet: Lesson 6

## **Practicing Internet search**



### **Original search query**

Books about imaginary characters and mystery

### **Search results**

**Revised search query** 

### **Search results**

I want to make a cake for my sister's birthday. She doesn't like chocolate but loves fruit. I wonder what kind of cake I can make.



### **Original search query** No chocolate cake with fruit

**Search results** 

**Revised search query** 

### **Search results**

### **Original search query**

Video game jobs

### **Search results**

**Revised search query** 

### **Search results**

Original search query

What do I need to fish?

Search results

### **Revised search query**

### Search results

I love playing video games. I wonder what it would be like if I grew up and worked for a video gaming company. It would be so cool if that was my job someday!





# Don't Fall for Fake: Lesson 7 Interland: Reality River

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

Open a web browser on your desktop or mobile device (e.g., tablet), visit g.co/RealityRiver.

### **Discussion topics**



Have your students play Reality River and use the questions below to prompt further discussion about the lessons 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 on these lessons 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?