Secure Your Secrets

Getting real about privacy and security

Lesson overview

Lesson 1	**But that wasn't me!**	Grades **2–6**
Lesson 2	**How to build a great password**	Grades **2–6**
Lesson 3	**Keep it to yourself**	Grades **2–6**
Lesson 4	**Interland: Tower of Treasure**	Grades **2–6**
Lesson 5	**What is digital privacy?**	Grades **4–6**
Lesson 6	**How is my data used?**	Grades **4–6**
Lesson 7	**Protecting your privacy online**	Grades **4–6**

Themes

Anyone who uses a device that's connected to the internet—a game, a phone, a digital assistant, a computer, etc.—needs to know the basics of online privacy and security. Protecting those devices and the personal information on them—all that stuff about you, your family and your friends—means thinking about what's incoming and outgoing and being smart about passwords, the information you share, and understanding the choices you have when it comes to protecting your privacy online.

Goals for students

- ✓ **Learn** why privacy and security matter and how they relate to each other.
- ✓ **Practice** how to create strong passwords and keep them to yourself (and the adults who watch out for you).
- ✓ **Review** the tools and settings that protect against scams, hackers and other threats.
- ✓ **Gain** a basic understanding of personal data and see the importance of caring about their online privacy.
- ✓ **Understand** some of the roles AI plays in personal data.

Standards addressed

ISTE Standards for Educators: 1a, 2c, 3a, 3b, 3c, 3d, 4b, 5b, 6a, 6d, 7a
ISTE Standards for Students 2016: 1c, 1d, 2b, 2d, 3d, 4d, 6a, 6d
AASL Learning Standards: I.a.1, I.b.1, I.b.2, I.c.1, I.c.2, I.c.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, II.d.3, 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.2, IV.b.3, V.a.2, V.a.3, V.c.1, V.c.3, V.d.1, V.d.2, V.d.3, VI.a.1, VI.a.2, VI.d.1, VI.d.3

Secure Your Secrets Vocabulary

Lessons 1–4

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

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

Lesson 1

Digital footprint: 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 too.

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

Lesson 2

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

Password or passcode: A secret combination used to access something. It can take different forms; for example, you may have a numbers-only code that you use for your phone lock and much more complex passwords for your email and other accounts. In general, it's important to make your passwords as long and complex as you can while still being able to remember them.

Lesson 3

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

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.

Lesson 5

Algorithm: A set of instructions in software code that tells a computer, robot, etc. what to do—the way instructions on a cake mix box tell you how to make a cake.

Cookie: A bit of text that an app or website puts on your phone, tablet or computer when you visit or use the app. It's used for lots of things, including convenience, like "remembering" if you've been there so you don't have to log in again or helping apps track your activity so you don't have to start over. It also helps websites know what people buy so they can show ads they'll like.

Machine learning: A form of AI that includes instructions to do things but also keep doing them better as it gets new data that helps it figure out how to—like a digital assistant in someone's kitchen that can tell the difference between a kid's voice and an adult's.

Tracking: What the software of apps, sites, etc. and other online services does after they've placed a cookie on your device—basically, follow your activity on the Web as you go from site to site.

Transparency: The way a window helps people see what's going on outside, transparency is what helps everybody know what apps, games and sites do with their data. It's where privacy is going. It's a right that people have—to know how businesses and governments are using our data. One way companies show transparency is by having a Privacy Policy their users can read, but these policies are usually really hard even for adults to understand, not just kids.

Lesson 6

Artificial intelligence (AI): Software that makes machines like a computer, robot or digital assistant learn, make guesses, solve problems and talk, kind of like we humans do. There are different kinds of AI that can do things like recognize faces, notice patterns like illegal hacking, tell people's voices apart and learn what songs you like so it can recommend new ones to you.

Lesson 6-7

Data: "Information" that's digital so it can be seen, used and shared online. It can take lots of forms: your name or phone number, a photo, a "like" you give the photo, a game score, friends lists, someone's location, etc. Each of those is called a "data point," and just like more information about a person helps us know them better, more data points about them helps an app, game or site guess what they want to see, play or buy.

Secure Your Secrets: Lesson 1

But that wasn't me!

Students explore outcomes of sharing their passwords and the impact those actions can have.

Goals for students

- ✓ **Learn** that sharing your password gives others control of your digital footprint.
- ✓ **Consider** what can happen when someone logs in as you.
- ✓ **Understand** how someone else's actions can affect your digital footprint…and **you**!

Let's talk

What happens when you share your password?
Think about a password you've created for some sort of app or device you use. Maybe it was a password to unlock your phone or to log into your favorite game or video app. Have you ever shared a password with someone else? Ok, let's be honest, a lot of us have. But there's an important reason why you really should not share your passwords…

You have something called a digital footprint. A digital footprint represents you online. It's what all the things you leave online—likes, comments, your screen name, photos, messages, recordings, etc. add up to and give other people an idea of what you're really like. It affects your reputation, how people think of you. They make guesses, or assumptions, about you based on that footprint you leave. That's one thing really important to be aware of when you're online.

Another thing really important to know is that, when you share your password, you are giving someone else control of your digital footprint—you're actually allowing them to help create it and shape how other people think of you. Yikes, right?! Since it's your footprint, everybody believes you're the one creating it. So if someone with your password does something you don't like, people will think that was you doing it! That's why it's super important not to share your passwords.

For example: Let's say you share your password to a social media account with a friend. While logged in as you, your friend sends a message to someone in your class like, "Can you send me your homework answers?" The next day in class, the student goes to the teacher and says you were trying to cheat on your homework by asking for answers. Then they show your teacher the message your friend sent from your account. Who do you think your teacher will believe? How does this affect your reputation? What else might happen?

Brainstorm with the class possible outcomes. Examples: Teacher calls home. You lose points on an assignment. Your digital footprint shows that you tried to cheat in school. You get into a fight with your friend who sent the message.

Remember, your digital footprint represents you online. Any time you share your password with someone, you are giving them control of your digital footprint, which can impact how people see you on the internet and everywhere else. Let's explore this idea together.

Continued on the next page →

Activity

Materials needed:

- Worksheet: "But that wasn't me!" (one for each pair of students)

1. Help students partner up

2. Pick an account

Students choose what type of account they're sharing a password for and fill it in at the top of the worksheet: social media account, gaming account, phone, tablet/computer, or streaming service.

3. Pick an action

Partners fill in the first box with an action they choose from the choices below—or think up themselves. This is an action taken by someone who has been given the password to their account. They can draw or write what they come up with **or** choose from these possible actions:

- "Likes" all of your crush's recent posts.
- Buys $100 worth of clothes.
- Sends a message like, "Don't you think Carmen is so annoying?"
- Plays your favorite game but loses points.
- Downloads new apps.
- Shares an embarrassing picture on your social media page.
- Reads all your texts and shares them with someone else.
- Watches episodes of an inappropriate TV show.

4. Create an outcome

In the second box, students create a possible outcome to the action they chose or created.

5. Discussion

As a class, ask a few students to share out the action and outcomes that they created. Below are some questions you can ask partners after they share:

- Why did you pick (or create) that action?
- How did you decide on the outcome?
- If you knew this was the outcome, how would you change your action?

6. Digital Footprint

In the last box, students write one sentence of how this action and outcome impacts the feelings, life or digital footprint—any or all of those things. Guide students to think about how this affects their reputation, or how others view them. Ask for volunteers or choose pairs of students to discuss what they draw or wrote and what they think about the story they created.

Takeaway

When you share your password, you are giving someone else control of your digital footprint, but you're still accountable for whatever they do with it. If you want to be in the driver's seat when it comes to how people see you online, don't share your passwords with anyone but a parent or other adult you totally trust.

Worksheet: Lesson 1

But that wasn't me!

I shared my password to:

- ☐ social media account
- ☐ gaming account
- ☐ phone
- ☐ tablet/computer
- ☐ streaming service
- ☐ _____

Action

Outcome

Digital Footprint Impact

Secure Your Secrets: Lesson 2

How to build a great password

Students learn how to create a strong password—and then 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 screenlocks 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: texts, games, posts and messages; with words, pics, and videos; using phones, tablets, laptops and digital assistants. (How do you connect with **your** friends?)

But the same tools that make it easy for us to share information can also make it easy for hackers and scammers to steal that information and use it to damage our devices, steal our identities or hurt our relationships and 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 devices that are unlocked or used by lots of people (like at school) and, above all, building strong passwords—**and not sharing them!**

- 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," your dog's name, your address, etc.)

Who thinks these passwords are good? **;)**

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, line in a movie, 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.

Handout: Lesson 2

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 hard 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: Iw2We$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, IwenttoWestern).

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 think someone else knows it (besides a parent or guardian).
- Change your passwords every now and then.
- Always use strong screenlocks 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 or even a pet's name, etc.) in your password.
- Don't use a password that's easy to guess, like your nickname, chocolate, just the name of your school, favorite sports 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 parent or guardian.
- Never write passwords down where someone can find them.

Secure Your Secrets: Lesson 3

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 + 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 on your page or 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.

In addition to setting, a really important thing to think about it who can friend or follow you (that may or may not be in your Settings). The safest choice is to have only your offline friends and family following you or on your friends list. If you allow other people, don't forget that whatever you share can be seen by people you've never met. That can get a little creepy, and sometimes parents just don't allow it at all. Talk it over with an adult you trust to figure out what's best for you—what keeps you safe and gives you the most peace of mind.

Your parents or guardians should **always** be making these decisions with you. Plus, it can be fun to go through your privacy settings together (so they can see how smart you are!).

Activity

Materials needed:

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

Review options

I have this 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
- Making your page or online profile—including photos and videos—public or private (visible only to the family and friends you choose)
- Going through your location and other settings—which ones are best for you?
- Getting alerts if someone tries to log in to your account from an unknown device
- Getting an alert when somebody tags you

Continued on the next page →

- Enabling two-factor or two-step verification
- Setting up recovery information in case you get locked out of your account
- Reporting problems

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—as you grow up, more and more you'll be the one deciding how much of your personal info to share, when, and with whom. So it's important to get used to making these decisions right now.

Takeaway

Choosing a strong, unique password for each of your important accounts is a great first step. Now, you need to remember your passwords and keep them private too.

Secure Your Secrets: Lesson 4

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), visit **g.co/TowerOfTreasure**.

Discussion topics

Have your students play Tower of Treasure 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.

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

Secure Your Secrets: Lesson 5

What is digital privacy?

Students learn the basic concepts of digital privacy and how it applies to them specifically.

Goals for students

- ✓ **Understand** basic concepts of digital privacy.
- ✓ **Relate** digital privacy to their own lives and internet use so it's meaningful to them.

Let's talk

You know we're talking about digital privacy, but what **is** it exactly? It's not just privacy settings in an app. To really understand it, first let's make sure we're clear about what the **oldest** kind of privacy is—because it's a little different from the **online** kind. Privacy has been around since long before there was an internet or information about us in a place we call "online." It's more important now than ever, because people's photos, videos, info, opinions, etc. can go viral globally now. People who think a lot about our rights tell us that old-fashioned privacy is a basic human right that must never go away. (Do you agree? Why/why not?)

So think about what that means. Your private information is info about you that you don't want the whole world to know about. Maybe it's a secret you don't want to share. It can also be something that you only want people you totally trust to know about you—not people you've never met. Privacy means we can **decide** whether people see us or our information and how much they can see. If we have privacy, we can control it. Or we **should** have some control. That's our right.

So what is *online* privacy? It has two parts to it, both really important:
1. What we *can* control: The old-fashioned kind we just talked about—the part where we choose, or control, what information about ourselves we want to share (or not share) online and who we want to share it with. This is what apps' and sites' Privacy Settings are for. They give us that control.

2. What we *can't* control: The other part of online privacy is not about what **we** choose to do with our information. It's about what **the apps, games and sites we use** do with our information. It's really important for you to know about this part so that you can do as much as possible to protect your privacy—the information, or data, you (and all of us) put into apps, games and websites when we use them. Because it's **your** data. It's also important because online privacy is changing, and learning about it now will make you aware of changes so you can make them work for you as you grow up.

3. [Optional] Transparency: Transparency is an important thing to know about because it has a lot to do with what we can't control online. And it's part of the good direction privacy is headed in. So what does it mean? Well, when you look through a window, you can see what's going on outside, right? That's because the window is **transparent**. When apps, sites, games and other online services are transparent about what they

do with your data, they're letting you see what they do—they're showing their privacy practices—for example, whether they just use your data to make their app work better for you or whether they share your data with other companies. More and more internet users want their apps and other services to be transparent. More and more people feel this is good business. One way companies try to be transparent is by having a Privacy Policy, but these policies are usually really hard even for adults to understand, not just kids.

Activity

Materials needed:

- Worksheet: "What are we talking about here?" (one for each pair of students)
  - For teacher: Answer Key for worksheet which includes answers in Column 2
- Handout: "Your privacy cheatsheet" with definitions of "data," "cookie," "tracking," "artificial intelligence," and "algorithm" (one per student)

After class discussion, students pair up, read examples of everyday online activities and match each one up with the privacy term it describes. Then they share their thoughts with the class.

Note to teacher: *This first lesson teaches foundational concepts of digital privacy so that they're relevant to your students. It's designed to give them time and space to think out loud together about what these important terms mean to them in their everyday internet use. The "Your Thinking" column in the worksheet is the most important part—it will give your students time to think the concepts through and lay a solid foundation.*

While a student passes out the handout and worksheet, write the terms "data," "cookie," "tracking," "artificial intelligence (AI)" and "algorithm" on the board, then have the class look at the handout while someone reads the definitions aloud to the class. After hearing each definition, write key words about each term that will help students differentiate between the terms. For example, for the word "data" you might write "information, photos, your name, location." For the word "algorithm" you might write "set of directions." After each description, ask your students if they have any questions—encourage them to answer each other's questions if anyone would like to. After the discussion, have the students pair up.

Now, with the Worksheet you just got, you're going to do an activity with your partner. Using the terms on the board, go through the worksheet with your partner. With each example in the left-hand column. choose a word it describes—is it an example of data, cookie, tracking, AI or an algorithm? If you're not sure, that's definitely ok. Just try your best, based on what you know so far about online privacy. Write down a little about why you picked that term under "Your thinking" in the right-hand column. When you're finished, one of you raise your hand, and I'll ask one of you to share your thinking on how you two made your choice. Anyone can raise their hand if they have a question or comment.

Takeaway

Way to go! You now know more about online privacy than most grownups on the planet. You have really thought about what it means for you as an internet user—you're even more internet awesome! Next we'll talk about things like what apps, games and sites do with our data.

Worksheet: Lesson 5

What are we talking about here?

For each example below, decide if it is an example of **data**, a **cookie**, **tracking**, **AI**, an **algorithm**, or if it could be more than one. Then, share your thoughts on how you made your choice. Not sure? That's ok! Just try your best based on what you know so far about online privacy.

Example	Is this about **data**, a **cookie**, **tracking**, **AI**, or an **algorithm**?	Your thinking
1. You "Like" a photo posted from your friend's birthday party.		
2. Software that makes guesses about what we like and want to see online, and the guesses keep getting better		
3. A little bit of text an app or site puts on your phone that you can't see		
4. A robot in a car factory gets instructions on how to tell if something's wrong with a new car so it can get fixed before somebody buys it, and it keeps getting better at that.		
5. You go online to see the weather and it already has your location on the site.		
6. You go to log into one of your favorite gaming sites. Your login and password are already filled in for you on the login screen.		
7. Whatever makes the thermostat at your house turn on the heat when the temperature goes below 68 degrees in the winter		
8. You use your school email to create a new gaming profile		
9. You were just on a site with cute pictures of dogs, and now ads are showing up about where you can buy dog food.		
10. A site recommends a video that looks interesting to you, so you watch it. Then the next one it recommends looks even more interesting, and that keeps happening until you can hardly stop watching videos!		

Answer Key: Lesson 5

What are we talking about here?

For each example below, decide if it is an example of **data**, a **cookie**, **tracking**, **AI**, an **algorithm**, or if it could be more than one. Then, share your thoughts on how you made your choice. Not sure? That's ok! Just try your best based on what you know so far about online privacy.

Example	Is this about **data**, a **cookie**, **tracking**, **AI**, or an **algorithm**?	Your thinking
1. You "Like" a photo posted from your friend's birthday party.	Data	
2. Software that makes guesses about what we like and want to see online, and the guesses keep getting better	Artificial intelligence (AI)	
3. A little bit of text an app or site puts on your phone that you can't see	Cookie	
4. A robot in a car factory gets instructions on how to tell if something's wrong with a new car so it can get fixed before somebody buys it, and it keeps getting better at that.	Artificial intelligence (AI) and/or Algorithm	
5. You go online to see the weather and it already has your location on the site.	Tracking	
6. You go to log into one of your favorite gaming sites. Your login and password are already filled in for you on the login screen.	Cookie	
7. Whatever makes the thermostat at your house turn on the heat when the temperature goes below 68 degrees in the winter	Algorithm	
8. You use your school email to create a new gaming profile	Data	
9. You were just on a site with cute pictures of dogs, and now ads are showing up about where you can buy dog food.	Tracking	
10. A site recommends a video that looks interesting to you, so you watch it. Then the next one it recommends looks even more interesting, and that keeps happening until you can hardly stop watching videos!	Artificial intelligence (AI) and/or Algorithm	

Handout: Lesson 5

Your privacy cheatsheet

Here are 5 things that are really good for internet users to understand: "data," "cookie," "tracking," "artificial intelligence (AI)," and "algorithm." I'm going to give you time to ask any questions you have, then we're going to do an activity that will help you lock in what these terms mean.

What is data? It's basically another word for "information," but it has lots of forms that we don't always **think** of as information. It's bits of info like your name, phone number, birthday or location. It can also be your level in an online game, a "like" you give a photo of a puppy, a video of you with friends, a photo of you that a relative shares, etc. (does anyone have another example?). Each is called a "data point."

There's data about us all over the internet, from everything we do and everywhere we go online—thousands of data points about us all over the place. When we like, click, buy, share or say something online, that's data that an app, site, company or government has about us. In fact, the world is absolutely swimming in data—more and more of it all the time. It's used in lots of ways by businesses, schools, banks, hospitals, governments—to make using their products better or easier, to make money, to solve problems, to catch criminals, to make games more fun, etc. It's used for good and not so good things.

What's a cookie? Of course you know we're not talking about the oatmeal or chocolate chip kind, right? Cookies are little bits of text that an app or website puts on your phone, tablet or computer when you visit or use it. They're used by the apps and sites for lots of reasons: to let them (or their software) know you've been there before so you don't have to log in again, to see where you go next so their software can guess what you like and show you ads it thinks you'll like or make your experience better—or both (more on this in Lesson 6). Mostly, cookies help companies customize their service for us. Some people don't like this tracking and customizing, though, because they feel it reduces their privacy. These cookies weren't designed with kids in mind, and a lot of adults feel kids' online privacy should be protected better. What do **you** think about that?

What does "tracking" mean? It basically means what the software of apps, sites and other online services might do after they've placed a cookie on your device—also what they do as you use their site, play their game, like something or post a comment. The software tracks all that so the apps or sites can get a sense of who you are—what you like, share and do—so they can make their videos or advertising work better for you, keep your attention and, sometimes, sell your data.

What is artificial intelligence, or AI? It's the software that makes sense of all that information collected about us. It makes guesses about what we like or want from the data it gets from cookies and our online activities to make our experience in a game, an app or a site work really well for us, give us the search results it "thinks" we're looking for or to show us videos, profiles or ads we might like. You may have heard of "machine learning," well that's what AI uses to make those guesses based on our likes, views, comments, wins and losses, cookies, app registration info and other data points the apps gather from us. And AI is used for so much more. It helps people find places, catch criminals, make movies, correct mistakes, design things, etc.

What is an algorithm? It's part of what AI runs on. It's a set of instructions, like a recipe for making pancakes, only made up of computer code not words. That's the most basic kind of algorithm, the kind that helps a computer or robot make something or do the same task really well over and over again. The other kind, a machine-learning algorithm, is what makes artificial intelligence **intelligent**. It's instructions plus data—**tons** of data that keeps getting fed into the algorithm. So instead of doing the same thing over and over again, it keeps "learning" so whatever it does gets better. Like a cook whose pancakes get tastier with every new recipe they find, a machine-learning algorithm can make better and better guesses, designs, solutions, games, etc.

Secure Your Secrets: Lesson 6

How is my data used?

This is both a guessing and role-playing game, where students pretend to be artificial intelligence and guess things about a person based on the data points provided. Class discussion follows.

Goals for students

- ✓ **Gain** a basic understanding of what AI does and how.
- ✓ **Grasp** how challenging it is for AI to be completely accurate.
- ✓ **Understand** some of the roles AI plays.

Let's talk

An app or online game where we set up an account usually has software that puts all the information we gave it when we registered (like our name, address, phone number or birth date) together with what the software "learns" about us as we use the app, game or site. As we learned in Lesson 5, the software is called artificial intelligence, or AI. It keeps getting new data from us—our likes, game moves, comments, chats, videos we watch, sites we visit, photos we share, searches we do—and makes better and better guesses for what we might want to do, see or buy. We might forget what we've shared, but the software doesn't forget that data. This is good for everybody to know, including kids (if you set up an account with an adult in your family, you might be able to help them understand).

Apps, games and sites might...

- Track where we've been (online and our physical location history) to figure out what we'll want to do or see next and make our time online better, more fun or more convenient.
- Use our data to analyze and categorize us to show us ads about stuff their artificial intelligence "thinks" we (or other people like us) will buy.
- Use info our friends or family share to make guesses about us and what we like (because it figures out who people's friends are).
- Share our personal information with other companies to make money or buy our data to show us ads.
- Find patterns of bad online behavior that a human being would take forever to notice—like criminals trying to get into banks' computers, threatening to shut businesses down to get their money, spreading false information or trying to steal someone's identity.

Activity

Materials needed:

- Worksheet: "How is my data used?" (one per student)

It's the AI behind the apps or games that makes these guesses about us. In this activity, you will pretend to be AI. See if you think it's easy or hard to be AI—and why it likes to gobble up more and more information!

On the worksheet, you'll have four data points on three different internet users. That's not much information, right?! But AI analyzes any information it can get and makes guesses about who these people are and what they like so the apps and websites it

Continued on the next page →

works for can do things like show them ads of things they might want, recommend videos to watch and suggest products for them to buy.

The four data points will give you hints about the person so you can guess what they're like. For example, in the first data point on Person 1, notice the part about "50th high school reunion." What might that say about that person—or about someone in the photo the person posted (if there's only one reunion a year)? That's the kind of thing you'll want to think about to help you fill in a mental picture about the person.

After you describe the person, you'll get to be AI and guess what types of products they might like to buy, what type of company would love to have them as a customer, etc. Have fun with this! See how creative you can be as you think about what AI would "think."

The fourth person on the worksheet is you! You'll think up four data points about what you do online, then write what you think AI will guess about you.

Note to teacher: *Have students fill out their worksheets, taking about five minutes each for the first three "persons" and maybe a little more time to think about their own data points. Discuss it all as a class, especially eliciting students' thoughts on why they made their guesses and choices.*

Takeaway

Just because the word "intelligence" is in its name doesn't necessarily mean that artificial intelligence knows everything. It makes guesses. The more data it gets, the better its guesses get—so it's pretty hungry for data, **everybody's** data.

Worksheet: Lesson 6

How is my data used?

Remember! As you read these data points—or hints—about the person they're describing, there's no perfect answer. You don't know who this person is because you're artificial intelligence, so you're just guessing. Have fun fleshing out these people!

Person 1

Data point 1 ⟶ Posted a picture on social media from a 50th high school reunion.
Data point 2 ⟶ Visits a pet store once a week.
Data point 3 ⟶ Buys dog toys online a few times a year.
Data point 4 ⟶ Walks to local park every day.

Write 2-3 sentences describing this person:

What type of company might want this person to be their customer? Why?

Person 2

Data point 1 ⟶ Watches skateboard videos every day.
Data point 2 ⟶ Browses popular shoe shopping sites.
Data point 3 ⟶ Listens to music on phone app each day around 3:30 P.M.
Data point 4 ⟶ Posts pictures at the beach.

Write 2-3 sentences describing this person:

What types of ads do you think this person will see on their social media? Why?

Continued on the next page ⟶

Worksheet: Lesson 6

How is my data used?

Person 3

Data point 1 ⟶ Visits local grocery store multiple times a week.
Data point 2 ⟶ Orders kitchen supplies from popular site.
Data point 3 ⟶ Commented "Delicious dinner!" on social media post.
Data point 4 ⟶ Attended a neighborhood food festival last weekend.

Write 2-3 sentences describing this person:

What types of stores or businesses might want this person to shop with them? Why?

Person 4 (Challenge): This person is YOU

Think about your online activity and create four data points about yourself.

Data point 1 ⟶

Data point 2 ⟶

Data point 3 ⟶

Data point 4 ⟶

Do you think these data points accurately describe who you are? Why or why not?

Secure Your Secrets: Lesson 7

Protecting your privacy online

Students consider their options in various privacy scenarios, think about what they decided and discuss their thinking together as a class.

Goals for students

- ✓ **See** the importance of caring about their online privacy.
- ✓ **Understand** they have choices to make in protecting their privacy.
- ✓ **Recognize** they have an important role—but not complete control—in protecting their privacy.

Let's talk

As you learned in Lesson 5, there's no such thing as total privacy in today's world, including online. And there's no such thing as total control over your data—not anytime soon, anyway. But there are concrete things you can do to make your privacy as solid as possible.

We're going to go through those concrete steps together, and I'm passing out this worksheet so you can fill in the blanks as someone reads each step. That way, you'll each have your own list of privacy steps to take home. I'm going to ask for volunteers to read them and, while they do, please write the title of each step. If any of you have any questions, raise your hand, and we'll see if I or one of you can answer.

Note to teacher: *Distribute the Privacy Steps handout before discussing the steps. This will help students keep track of all the different steps and will help them complete the activity later. As you introduce a new step, direct students to fill in the title of that step in the appropriate box in the handout.*

1. **Get help in setting things up.** If you set up an account in a game or app, be sure to set it up with an adult you trust and go through the privacy policy together. Every site and app should have one. If it doesn't, or if the policy seems pretty sketchy or super hard to read, be sure the person helping you knows that. That app or game probably isn't something you want to use.
2. **Make two lists:** As you and your adult helper get ready to set up an account or set privacy settings, it might help to make a list 1) about what you should never share publicly (because you don't know who can see it) and 2) about what **is** ok to share. That can help you remember these things that help you protect yourself and your privacy. It's also really good to think about what something you post could say about you if someone you don't know saw it.
3. **Consider keeping your account private.** That's so it's harder for people to find your account. If you don't know how to keep it private, ask a parent or relative for help with that.
4. **Play only with people you already know offline. That's how most kids play online games**—especially kids your age, but also teens—because (you know) it's a great way to hang out with friends when you can't in person. It's also much safer, because you have each other's backs if someone creepy shows up in the game.

Continued on the next page →

5. **Keep the game chat about the game.** It's good to keep in mind that it's not safe to talk about personal stuff if people you don't know might be in the game or app. Ignore anyone you don't know who asks personal questions like your age or location.
6. **Be sure to give your actual age** when you register, because honest apps, sites and internet companies give kids extra protections.
7. **Check Privacy Settings.** Privacy settings can change, so check your device and app settings every now and then to give yourself as much privacy control as possible.
8. **Don't just check the box.** If an app or game asks you to agree to something, work with a parent, teacher or other trusted adult to check out what you're agreeing to.
9. **Notice that apps get old, too.** Only have apps on your device that you actually **use**. If you don't use an app, consider deleting it—but before you do, delete your account before you delete the app. The privacy is about your account—what you registered and created when you started using the app—not the app.
10. **Do a search for yourself online** and see what "the Internet" knows about you (because what your search turns up is what other people on the internet see about you).
11. **If something upsets you, ask for help.** Talk with the parent or other adult you trust. Whether it's something bad you or a friend ran into, it's important to get help for dealing with it. We know kids are smart. You may have a lot of tech experience but you don't have as much **life** experience as grownups. So even if an adult who cares about you doesn't know much about online privacy (or safety), they can find out what you and they need to know, and they will be motivated to figure out where to get answers.
12. **Report privacy violations** in apps, games and sites you use and, if nothing happens, tell your friends and relatives about it. You could even talk with them about whether you all want to delete the app, or even spread the word together and be privacy activists.

Not all apps, games and internet companies protect kids' privacy as well as you'd like, but privacy's getting better all the time, and the more you practice this stuff, the more you can protect yourself, help your friends and kids younger than you—also the more you can stand up for kids' privacy rights!

Activity

Materials needed:

- Worksheet 1: "Privacy Steps" (one per student)
- Worksheet 2: "How Can I Protect My Privacy Online?" (one per student)

Note to teacher: *After passing out worksheets, have students choose an option for each scenario, then think through why they made that choice by writing out why they made it. They can use their "Privacy Steps" handout from the earlier discussion. Then, in a class discussion, see if different students chose different options and talk about why.*

Be sure to tell students that the goal is not to have all the right answers on a paper but to think about their privacy when they're online and learn to make choices that protect their privacy as much as possible.

Takeaway

Nobody can have total control over their online privacy (yet, anyway), but there are steps you can take to make your privacy as good as possible, and the more you try them out, the better it'll get and the more you can help others with theirs.

Worksheet 1: Lesson 7

Privacy Steps

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

Worksheet 2: Lesson 7

How Can I Protect My Privacy Online?

Directions:

1. For each scenario below, select which option will better protect your data and privacy.
2. Answer the questions to explain your thinking, then we'll have a class discussion.

Scenario 1

You are creating a new account on a gaming site.

☐ **Option 1:** Ask an adult to help you create the account.
☐ **Option 2:** It is a gaming site for kids, so you complete the account on your own.

Which option did you choose? Why?

Scenario 2

You and your dad are registering a new account in an app and have to enter your age.

☐ **Option 1:** Put in your real age so that the app can apply special protections for kids.
☐ **Option 2:** Put in a fake age so the app thinks that you are an adult.

Which option did you choose? Why?

Scenario 3

You have apps on your device you no longer use.

☐ **Option 1:** Delete the apps, which will then delete your account information.
☐ **Option 2:** Delete your account information first, and then delete the app.

Which option did you choose? Why?

Continued on the next page →

Worksheet: Lesson 7

How Can I Protect My Privacy Online?

Scenario 4

You just updated all the privacy settings on your device with a parent.

☐ **Option 1:** You are good to go! You only have to do this one time.
☐ **Option 2:** Check your privacy settings again in a few months to make sure nothing has changed.

Which option did you choose? Why?

Scenario 5

A game asks you to agree to an update to its Terms and Conditions to keep playing.

☐ **Option 1:** Ask a parent to look at the new terms with you to make sure you understand what you are agreeing to.
☐ **Option 2:** You can go ahead and click Agree. There isn't usually any important information in those updates.

Which option did you choose? Why?

Scenario 6

You are deciding whether to make your account public or private.

☐ **Option 1:** Make your account public so it is easier to connect with friends.
☐ **Option 2:** Always keep your account private to make it harder for strangers to connect with you online.

Which option did you choose? Why?

Answer Key: Lesson 7

How Can I Protect My Privacy Online?

Note to teacher: *The answers in red below are written so that you can read them to your students in a class discussion if you'd like.*

Directions:

1. For each scenario below, circle which option will better protect your data and privacy.
2. Answer the questions to explain your thinking, then we'll have a class discussion.

Scenario 1

You are creating a new account on a gaming site.

☐ **Option 1:** Ask an adult to help you create the account.
☐ **Option 2:** It is a gaming site for kids, so you complete the account on your own.

Which option did you choose? Why?

Option 1 is the better option. Whenever you are asked to create an account, it's always best to create the account with an adult. Even if it is a site for kids, you are still sharing lots of data points about yourself to create the account. So, you want to make sure you are still protecting your privacy.

Scenario 2

You and your dad are registering a new account in an app and have to enter your age.

☐ **Option 1:** Put in your real age so that the app can apply special protections for kids.
☐ **Option 2:** Put in a fake age so the app thinks that you are an adult.

Which option did you choose? Why?

Option 1 is the better option because, just as it says, when you put in an accurate age, the app might have special protections for children and teens. If you put in an age that is not correct, you are taking the risk of not protecting your privacy **and safety** because the app doesn't know you are a kid.

Scenario 3

You have apps on your device you no longer use.

☐ **Option 1:** Delete the apps, which will then delete your account information.
☐ **Option 2:** Delete your account information first, and then delete the app.

Which option did you choose? Why?

Option 2 is the better option. When you delete an app, your account still exists and will still have your data connected to it. If you delete your account first, you are making sure that the app no longer has your personal data.

Continued on the next page →

How Can I Protect My Privacy Online?

Scenario 4

You just updated all the privacy settings on your device with a parent.

☐ **Option 1:** You are good to go! You only have to do this one time.
☐ **Option 2:** Check your privacy settings again in a few months to make sure nothing has changed.

Which option did you choose? Why?

Option 2 is better. Apps, websites, devices, programs, etc. often change the privacy settings they provide. Sometimes you don't even know when the settings change. Check your privacy settings at least once a year to make sure you are doing everything you can to protect your data and your privacy.

Scenario 5

A game asks you to agree to an update to its Terms and Conditions to keep playing.

☐ **Option 1:** Ask a parent to look at the new terms with you to make sure you understand what you are agreeing to.
☐ **Option 2:** You can go ahead and click Agree. There isn't usually any important information in those updates.

Which option did you choose? Why?

Option 1 is better. Terms and Conditions are often really long and wordy, and they're definitely not written for kids. It is easy to miss important information. If you look at them with an adult, you are more likely to see information you need to know to protect your privacy.

Scenario 6

You are deciding whether to make your account public or private.

☐ **Option 1:** Make your account public so it is easier to connect with friends.
☐ **Option 2:** Always keep your account private to make it harder for strangers to connect with you online.

Which option did you choose? Why?

Option 2 is better. This is one of the easiest ways you can protect your privacy. It might take a few more steps to connect with friends, but it is worth it to protect your information and activity from people you don't know—people who should not know anything about you.