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**

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.

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.

Standards addressed

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

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.

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?