LESSON 3

Passwords

LESSON OBJECTIVE

Students will learn how to keep their online information more secure by using and maintaining strong passwords. Students will learn about the principles of strong password design and the potential problems of password sharing. They will also learn how to keep their passwords safe and how to take steps to prevent unauthorized access to their accounts.

ESSENTIAL QUESTIONS	To what extent can passwords keep your information secure online?
AGE	11-18
MATERIALS	"Learning about passwords" Handout
PREPARATION	Print one handout per student
ISTE DIGCITCOMMIT COMPETENCY	ALERT: I am aware of my online actions and know how to be safe and create safe spaces for others online

SUPPORT MATERIALS

Visit ***facebook.com/fbgetdigital*** to access resources for parents and young people that can complement the lesson students took on Foundations today.

Password basics

Part 1

TELL YOUR STUDENTS

We often don't think a lot about the passwords we use for websites, apps and services. However, how good your passwords are determines how secure your information will be.

CLASS INTERACTION

Engage students in a discussion using the following questions. Please remind students that it's important not to share their actual passwords during this or any other exercise.

ASK YOUR STUDENTS

- How many passwords do you have?
- Do you have different passwords for each of your email and social media accounts?
- Are they very different or are they a variant of a single password?
- If you have more than one password, how do you remember which one belongs to which account?

ASK YOUR STUDENTS

- How often have you forgotten an important password?
- What have you done when you have forgotten your password?
- How do you make your passwords easy to remember?
- Is there a password you use every day?
- What would happen if—without your knowledge—someone found out what your password is?
- Would it depend on who it is?
- What kind of information might someone learn about you if they used your password to get into your account?

Part 2

CLASS INTERACTION

Organize students into pairs.

TELL YOUR STUDENTS

Along with your partner, discuss what might happen if someone who wanted to cause trouble learned the password to your favorite social media platform.

CLASS INTERACTION

Give students 5 minutes to discuss. And ask the groups to share out.

TELL YOUR STUDENTS

Now talk with your partner about what would happen if a hacker learned the password to your parent's/caregiver's online banking account.

CLASS INTERACTION

Give students 5 minutes to discuss. Then, ask the groups to share what they discussed.

Part 3

TELL YOUR STUDENTS

You might be wondering how a hacker could learn a private password. There are a few ways; one way is through social engineering—or tricking someone into sharing their password. A hacker can do this by sending an email that looks like it legitimately came from a platform or website where someone has an account. The email might ask the person to click on a link and log in with their username and password; when the person logs in, this information is now available to the hacker.

Hackers sometimes try to guess passwords by using common phrases like "password123," "test," or your first or last name.

Another way that hackers learn a private password is through what is called a "Brute Force" attack. A brute force attack occurs when a hacker tries to log in to your account by repeatedly trying various passwords. While a hacker can conduct a "Brute Force" attack by hand, it is often done by running a computer program that rapidly and automatically tries every possible combination of passwords it can think of. For example, a list of likely passwords or a set of passwords consisting of combinations of different letters and numbers, until they find the right passcode.

Of course, some "Brute Force" attacks are more sophisticated. If your password is on a list of likely passwords, like "fido123" or "password," then some programs can guess it faster by trying those options before less likely ones or randomized possibilities. The attack can also be more refined if the hacker knows information about you. If, for example, the hacker knows your pet's name is Toby, they may try "Toby" with different variations of numbers at the end (e.g., "Toby629," or "Toby3020").

Design principles

ASK YOUR STUDENTS

- Who knows what it means to have a "strong" or "stronger" password?
- Why is this a good idea?

TELL YOUR STUDENTS

A strong password helps protect your information. While having a strong password doesn't guarantee that your account won't be hacked, having a weak password makes it much easier for someone to access your information.

Password Exercise

ASK YOUR STUDENTS

- What are some examples of weak passwords?
  - Some examples include: Password, 12345, Hello!, a birth date, a nickname.
- Why do you think these are weak?
  - Answer: They could easily be guessed by another person and/or a computer running a "Brute Force" attack.
- What are some ways you can make a password stronger?
  - Some examples include: Adding numbers, upper and lowercase letters, symbols, making the password longer and avoiding common phrases and words on their own.

CLASS INTERACTION

After students provide their input, write these instructions on the board:

1. Include at least one number.
2. Include at least one symbol.
3. Include at least one uppercase and one lowercase letter.
4. Passwords should be at least 7 characters.
5. Passwords should be easy to remember (unless using a password manager).
6. A password manager is a website/app that helps users save and organize their passwords.
7. Passwords should not be a single common word or personal information (birth date, parent's name, etc.).
8. Passwords should not be shared between websites.

TELL YOUR STUDENTS

There are two approaches to creating strong passwords. The first is to follow a "password recipe" like this one on the board. Using such a recipe encourages you to include harder-to-guess elements in a text/numerical password, making the password itself harder to guess. The drawback of this approach is that it makes passwords harder to remember.

Strong passwords

TELL YOUR STUDENTS

Another approach to creating strong passwords is connected to password length. Because password strength is related to password length, using a string of four or more unrelated words makes passwords much harder to guess for humans and "Brute Force" attacks. This method has the added benefit of resulting in passwords that are easier to remember than the recipe method.

Lastly, one can use a combination of these two methods by coming up with a string of four or more unrelated words, also including symbols and numbers.

The goal of these different methods is the same: developing passwords that are unique and difficult for other people to guess.

CLASS INTERACTION

Organize students into pairs.

TELL YOUR STUDENTS

In pairs, try to create a strong password using the instructions you wrote on the board earlier. Remember that a password that is hard for a computer to guess randomly might still be easy for a human or a computer with a list of common long passwords to guess. The piece of paper with your password won't be collected at the end of the activity. You are encouraged not to actually use this password for one of your accounts, as those in the group will know it.

CLASS INTERACTIONS

Give students 5 minutes to do this. Then go around the room and ask students what they think their strongest password examples are. Ask students if they can remember the passwords they generated without looking at them directly.

TELL YOUR STUDENTS

While some websites will require your password to meet a few (or all) of these conditions, others have no such restrictions. You can also create passwords using a string of random common words.

CLASS INTERACTIONS

In the same pairs, have students create new passwords that are strings of words. Tell them there should be at least four words in the password to make it both strong and easy to remember. Give students 5 minutes to do this. Then go around the room and ask students what their password examples are. Again, remind students that the sheet of paper won't be collected at the end of the activity, nor should the password be used for any of their accounts.

TELL YOUR STUDENTS

Some websites use a system called multi-factor (or two-factor) authentication to verify your identity. These websites often use text messaging, an app or email to send a one-time code that must be entered along with the password.

This method can make your accounts much safer by adding an extra layer of security that is far more difficult to break. For instance, to log into your account, a person must have your password and access to the app, device or email address associated with the account.

Keeping passwords safe

TELL YOUR STUDENTS

Even if you create a password that is really tough for a computer or person to crack, there are other ways a password can be weak.

ASK YOUR STUDENTS

- What are some other ways that passwords can be weak?
  - Some examples include: reusing a password for multiple accounts, using a password that contains personal information, using the same password for many years, forgetting your password.
- How often do you think you should change your passwords?

TELL YOUR STUDENTS

Even good passwords can be compromised or stolen, but there are things you can do to protect yourself. If there is a data breach on a website where you have an account, make sure to change your password on that website as well as any other websites where you use similar passwords.

Remembering a lot of long and complicated passwords can be difficult.

ASK YOUR STUDENTS

- Do you think it's a good idea to write down your passwords on a piece of paper or in a document file on your computer? Why or why not?

CLASS INTERACTION

Mention possibilities like someone finding the piece of paper or noticing the file on your computer. Explain that one approach is to use a password manager, an application that helps users save and organize their passwords.

TELL YOUR STUDENTS

Every day, we use a lot of different accounts on different websites. It can get complicated to log in and sign out of every website every time.

ASK YOUR STUDENTS

- Have you ever used the "save password" feature in your browser to save a password for a website? Why or why not?
- Do you understand how the website remembers who you are?
  - Ask for explanations.
  - Then explain that websites can remember that you logged in by storing a cookie. Cookies are tiny files stored on your computer to help a website know who you and your computer are on future visits, without logging in again. However, cookies can also be used to track you as you go from website to website. That's one way that ads can target you.
- Is it okay to save a password if it's on your own computer?

ASK YOUR STUDENTS

- Does your computer have a login password? What if you share the computer with others?

TELL YOUR STUDENTS

In this case, even though your password in the password field may be hidden by black dots or asterisks, other people using your computer can potentially figure out what your password is. Just because you can't see what the password is on the screen doesn't mean it's not stored somewhere.

ASK YOUR STUDENTS

- Are there ever times when it's okay to share a password? When? Why?
  - Some examples might be that parents may want their passwords or that they have a joint/family account on a service like Netflix.
- Do you share your passwords with anyone? If so, with whom/why?
- If you are close friends with someone, would them saying "if you care about me" act as a motivator to share your password with them? Why or why not?

TELL YOUR STUDENTS

You may choose to share your password with someone you care about, but caring about them does not necessarily mean that they deserve full access to your online accounts.

Think carefully about your relationship with that specific person before you share, including how that relationship might change over time. For instance, sharing with a parent/caregiver is a very different choice than sharing with your best friend.

ASK YOUR STUDENTS

- What might happen to you if you share a password?
  - Some examples include: Someone could hack into your bank accounts, impersonate you online or learn some of your secrets.
- If you shared a password to an account, would you use that account differently?

ASK YOUR STUDENTS

- Are there things you wouldn't watch on Netflix or write in an email if someone else could see what you were doing?

CLASS INTERACTION

Students should reflect on their own behavior when using a shared account. They should consider that their online activity is on display for other users on the account.

ASK YOUR STUDENTS

- If your account is a virtual representation of you, like a social media profile, is it okay to allow other people to use your account?

CLASS INTERACTION

Discuss the possibility of someone pretending to be you and sending messages to your friends.

ASK YOUR STUDENTS

- Do you allow any of the devices you use to store your passwords? Why or why not? Does that mean it is safe to save your passwords on your personal phone or computer? What happens if you let a friend borrow your phone or computer?
- Are there any devices you share with others, such as family or friends? Do you share an account on that device or does each person have their own?
- Do you ever use a "public" device, such as one at the library, at school or somewhere else? Do you do the same things on that device that you might do elsewhere?

CLASS INTERACTION

Organize students into pairs.

TELL YOUR STUDENTS

In your pairs, discuss whether you have ever logged onto a computer at school, at a library or in another community setting and saw that someone else was still logged on to their social media or email account. Ask them to consider if they would look around the account or do anything else.

CLASS INTERACTION

Give students 5 minutes to discuss, then ask them to share. Engage the group in a discussion about such unauthorized use.

Unauthorized account access

Part 1

Please note: Part of the content of this activity has been covered in "Activity #1: Password Basics." We defer to your judgment regarding whether or not you would like to go over this material again or skip it.

TELL YOUR STUDENTS

It is possible for others to access your account, even without already knowing or succeeding with a random guess of your password. If someone knows enough personal information about you, they might be able to make educated guesses about your password or they might convince someone at a company to hand over your information. Because they're not using technology to break into your accounts, this kind of attack is called social hacking or social engineering.

ASK YOUR STUDENTS

- Raise your hand if you have ever forgotten your password to a website. What happens when you click on "I forgot my password?"
  - Some examples include: The website usually asks for answers to security questions or will try to contact you using a phone number or email.
- What are some security questions the website asks for?
  - Explain how some of these are questions that friends or acquaintances could answer or guess. Things like: the name of their pet, where they were born, their mom's maiden name, the name of their favorite teacher, the name of their best friend, their favorite sports team.
- Who else might know this kind of information about you?
  - How does a website contact you when you've forgotten a password? Who else might have access to your points of contact?

ASK YOUR STUDENTS

- How could a stranger learn the personal information associated with your answers to security questions?
  - Some examples include: Social media posts, online searches of public information, guessing multiple times, contacting your friends, etc.
- What are some examples of social media posts with personal information?
  - For example, an Instagram of your cat with its name in the caption, a photo with a location tagged or public birthday posts.

- How can you use Google to learn more about someone and hack their password?
  - Some examples include: If a search engine shows you someone's ninth-grade class photo in a school newspaper online, you could figure out their ninth-grade teacher's name.

Part 2

TELL YOUR STUDENTS

Posting information that contains the answers to your security questions can be very unsafe. Make sure to choose security questions that have answers only you know.

You can also make up answers to security questions, as long as you save them in a password manager or they're easy to remember.

Websites might contact users using a phone number or email associated with the user's account. If a user forgets their password, websites often provide a temporary password or hyperlink that the user can use to reset their password.

ASK YOUR STUDENTS

- Is this a safe way of ensuring that the person requesting the new password is the user?
- What if you share the email address associated with the account?
  - Some examples include: The reset password link method is safe most of the time, but if you share an account or password with someone else, it exposes you to risk.

TELL YOUR STUDENTS

Social hacking can be accomplished by people contacting you directly and trying to trick you into giving them your information. Sometimes, people will send you an email pretending to be someone else (such as a friend, a family member or someone from the bank) and ask you to share important information with them (such as your birth date) to verify your identity. This can also be more subtle, like if someone hacked your friend's social media account and messaged you (and potentially many others) asking about your birthday or where you grew up. If you receive any messages from your friend that appear odd, you may first want to reach out to your friend (outside of the social media platform) to determine if they are actually sending the content.

Attacks that use a real-looking email or website are called phishing and can lead to identity theft. For instance, an identity thief may open up credit cards in your name and use them, which could make it hard for you to get a credit card when you're older.

Phishing can allow the thief to impersonate you and access more information, allowing them to snoop through your emails, message your friends while pretending to be you or steal your money. This process could also allow the thief to block you from your account by creating a new password that you do not know.

Assignment

Ask students to answer the following questions and add their responses in the form of text or visuals to the "Learning about passwords" Handout.

9. What are three insights from this session you will apply the next time you have to create a password?
10. What is one instance where you feel that it is okay to share your password with someone else?
11. What are three strategies you can use to safely share your password with someone else?
12. What are three examples of what might go wrong if a password gets into the wrong hands?

HANDOUT

Learning about passwords

1. **What are 3 insights from this session you will apply the next time you have to create a password?**
   -
   -
   -
2. **What is 1 instance where you feel that it's okay to share your password with someone else?**
   -
3. **What are 3 strategies you can use to safely share your password with someone else?**
   -
   -
   -
4. **What are 3 examples of what might go wrong if a password gets into the wrong hands?**
   -
   -
   -