Passwords

Created: March 2016
Last Updated: July 2018

Estimated time:	95 minutes ● [20 minutes] Activity #1 ● [20 minutes] Activity #2 ● [20 minutes] Activity #3 ● [15 minutes] Activity #4 ● [20 minutes] Assignment Depending on the time you have allotted for each group meeting, we suggest you engage in the final two exercises of this learning experience ("Activity #4" and "Assignment") in your second group convening.
Group or individual activity:	Group
Ages:	11-18 years old
Grades:	Grades 6-12
Online / offline elements:	This learning experience contains links to online resources to help facilitate a group-based discussion, with an offline writing assignment.
Areas:	Main area: Security Additional areas: Content Production, Information Literacy, Privacy and Reputation
License:	

Learning Goal

Participants will learn how to keep their online information more secure by using and maintaining strong passwords. Participants 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.

Materials

- [One per participant] Handout: Learning About Passwords
- [For educator - optional] Computer with Internet access
- [Optional] Projector and projection screen
- Flip chart (or poster)
- Marker
- [One per group of 2 participants] Paper
- [At least one per participant] Colored pens or pencils

Resources

- Lesson: Strong Passwords (3-5) - by Common Sense Education
- Article: Tips for Strong, Secure Passwords & Other Authentication Tools - by ConnectSafely.org [© 2015 ConnectSafely. All Rights Reserved.]
- Scratch Project: Password Strength Calculator - by thebriculator (Scratch)
- Blog Post: Example Controlled Assessment Report - by Dan Gardner
- Comic: Password Strength - by xkcd
- Multi-factor authentication and password management tools:
    - Google 2-Step Verification - by Google
    - RSA SecurID - by RSA
    - LastPass - by LastPass
    - RoboForm - by RoboForm
    - KeePass - by KeePass
    - 1Password - by 1Password

Activity #1: Password Basics

SAY:

- We often don't think a lot about the passwords we use for websites, apps, and services. However, the strength of your passwords is a key factor in terms of how secure your information will be.

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

ASK:

- How many passwords do you have?
    - Are these passwords different from each other?
    - 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?
- 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 one of your accounts?

[Organize participants into pairs.]

SAY:

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

[Give participants 5 minutes to discuss. Then ask the groups to share out.]

SAY:

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

[Give participants 5 minutes to discuss. Then, ask the groups to share what they talked about.]

SAY:

- 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 also try to guess passwords by using common passwords like "123456," "password," "12345678," "password123," "test," or your first or last name. A quick online search for "most common passwords" can give you an idea of other very common passwords.
- 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's more 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 than others. If your password is on a list of likely passwords (e.g., "welcome" or "password"), then some programs can guess it faster by trying those options before less likely passwords or randomized possibilities. The attack can also be more refined if the hacker knows information about you. If, for instance, the hacker knows your pet's name is Toby, they may try "Toby" with different variations of numbers at the end (e.g., "Toby123456" or "Toby2004").

Activity #2: Design Principles

ASK:

- Who knows what it means to have a “strong” or “stronger” password? Why is having a strong password a good idea?

SAY:

- 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.

ASK:

- What are some examples of weak passwords? [Some examples include “password,” “123456,” “Hello!,” a birth date, a nickname.]
    - Why do you think these are weak? [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? [Adding numbers, upper and lowercase letters, symbols, making the password longer, and avoiding common phrases and words on their own.]

[After participants provide their input, write these instructions on the flip chart / poster:

- Include at least one number.
- Include at least one symbol.
- Include at least one uppercase and one lowercase letter.
- Passwords should be at least seven characters.
- Passwords should be easy to remember (unless using a password manager). [A password manager is a website / app that allows users to store their passwords. One example of a popular password manager is LastPass. Feel free to project the site on the projection screen and briefly review some of the site’s features.]
- Passwords should not be a single common word or personal information (e.g., birth date, parent’s / caregiver’s name, etc.).
- Passwords should not be shared between websites.]

SAY:

- There are two approaches to creating strong passwords. The first is to follow a “password recipe” like this one on the flip chart / poster. 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.

- 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, and 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.

[Organize participants into pairs.]

SAY:

- In pairs, try to create a strong password using the instructions I wrote on the flip chart / poster 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.

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

SAY:

- While some websites and platforms will require your password to meet a few (or all) of these conditions, others have no such restrictions. Now let’s create passwords using a string of random common words. [One example would be “correcthorsebatterymoon” consisting of the words correct, horse, battery, and moon.]

[In the same pairs, have participants 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 participants 5 minutes to do this. Then go around the room and ask participants what their password examples are. Again, remind participants 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.]

SAY:

- 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.

Activity #3: Keeping Passwords Safe

SAY:

- 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:

- 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, or forgetting your password.]
- How often do you think you should change your passwords?

SAY:

- While the recommended rate at which you should change your passwords is debated, even among security professionals, generally, you shouldn't need to change your passwords if they are sufficiently complex to begin with, unless there is a suspected data breach on the website(s) / platforms where you have an account.
- While even good passwords can be compromised or stolen, there are things you can do to protect yourself. If there is a data breach make sure to change your password on that website / platform as well as any other websites / platforms where you use similar passwords.
- Remembering a lot of long and complicated passwords can be difficult.

ASK:

- 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?

[Mention possibilities like someone finding the piece of paper or noticing the file on their computer. Note that it's important to consider: at what level does protecting information become inconvenient? As soon as protecting information becomes inconvenient, this form of protection will likely be avoided, which may contribute to reduced security (e.g., if a password is too complex, someone might write down the password on a piece of paper by their computer). Explain that one approach to organizing passwords is to use a password manager, a website / app that allows users to store their passwords (e.g., LastPass).]

SAY:

- 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:

- 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 note 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?
- Does your computer have a login password so only you and the people who know the password can use it?
- What if you enter your password on a computer you don't trust / a shared computer? 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:

- Are there ever times when it's okay to share a password? When? Why? [Some examples might be that parents / caregivers may want their passwords or that they have a joint / family account on a media streaming service.]
- Do you share your passwords with anyone? If so, with whom and 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?

SAY:

- 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:

- What might happen to you if you share a password? [Someone could hack into their bank accounts, impersonate them online, or learn some of their secrets.]
- If you shared a password to an account, would you use that account differently?
- Are there things you wouldn't watch on a media streaming service or write in an email if someone else could see what you were doing? [Participants 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.]
- 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? [Discuss the possibility of someone pretending to be them and sending messages to their friends, and the possibility that they may lose access to their account as letting others use it might be prohibited by the platform's terms of service.]
- Do you allow any of the devices you use to store your passwords? Why or why not? Does that mean it's 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?

[Organize participants into pairs.]

SAY:

- 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.]

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

Activity #4: Unauthorized Account Access

[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 if you have already engaged in Activity #1, or skip it.]

SAY:

- It’s 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.

ASK:

- Raise your hand if you have ever forgotten your password to a website.
- What happens when you click on “I forgot my password?” [The website usually asks for answers to security questions or will try to contact someone 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, 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? [Text message, email, etc.]
- Who else might have access to your points of contact?

- How could a stranger learn the personal information associated with your answers to security questions? [Social media posts, online searches of public information, guessing multiple times, contacting their friends, etc.]
- What are some examples of social media posts with personal information? [For example, a photo of their cat with its name in the caption, public birthday posts, or a photo of them and their friends with a location tagged.]
- How can you use Google to learn more about someone and hack their password? [If a search engine shows them someone's ninth-grade class photo in a school newspaper online, they could figure out that individual's ninth-grade teacher's name.]

SAY:

- 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 (a website / app that allows users to store their passwords, such as LastPass) 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:

- 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? [The reset password link method is safe most of the time, but if they share an account or password with someone else, it exposes them to risk.]

SAY:

- 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. Social hacking 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 don't know.

Assignment

[Ask participants to answer the following questions and add their responses in the form of text or visuals to the Learning About Passwords Handout.]

SAY:

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

Learning About Passwords Handout