Passwords (beginning)

Even though it's one of the most important things you can do for your online security, creating and using strong passwords can be a tough sell for learners. Secure password advice can conflict, and it's hard to remember and implement when all you want to do is create an account and start using it! In this lesson, we'll look at ways to explain the "how" and "why" behind strong passwords.

Recommended Reading

- Creating Strong Passwords
- Animated Overview: How to Make a Super-Secure Password Using Dice
- Using Password Managers to Stay Safe Online
- XKCD comic about password strength and diceware passwords

Gotchas and Other Problems You Might Hit

- When making new passwords, there may be a few participants who will forget their new passwords. If people have changed the passwords for critical accounts or for their devices without memorizing their passwords, this activity may cause more harm than good.
- Consider suggesting people write down their passwords (on paper or in password managers). For those who write down their passwords, remind them to watch out for others peeking at their papers, and to keep these papers in a safe place!
- It is also worth looking into memory retention techniques for those who have trouble remembering their passwords, like mnemonics, creating illustrations or imagery to accompany the password in the course of their memorization, creating a funny story around the password, and so on.
- Some people may have trouble with typing long passphrases due to motor difficulties. If this is the case, provide accommodations for them to still participate, but perhaps loosen requirements on the exact number of words for the passphrase.
- Others may have trouble with a passphrase generated from the diceware or random dictionary word selection technique, perhaps due to issues with being

able to spell the word. Consider making an accommodation by helping them to choose another more familiar, but still sufficiently random, word.

Learning Objectives

Learners will:

- Be able to give examples of weak passwords.
- Be able to describe how weak passwords are easy for attackers to guess.
- Be able to describe why it's a risk to use variations of the same **password** across different accounts.
- Be able to explain the dangers of giving honest answers to "security questions."
- Be able to describe what makes a strong password.
- Be able to explain why the randomness of using dice or a book is effective at producing a secure **passphrase**.
- Produce a highly secure passphrase.

Prerequisites

- If you plan to have learners actually generate their own passwords and phrases, then they should bring their devices and have password managers installed on them (see module on password managers).
- Learners should have a general understanding of what a **web browser** is, and familiarity with logging into a website.

Ratio

Instructor: Learners
1:4 (Four people to one instructor)

Suggested Materials

A visible note-taking area, such as a whiteboard.

A computer and projector, if showing external resources to participants.

Lesson Content

Warmup: Partner Introduction

Write down three questions in a visible place, like on a board or in a slide:

1. Your name and pronouns
2. What you ate for breakfast
3. What was the first time you created an account for a website? Did you make a password? If you feel comfortable sharing that first password, what was it?

Pair everyone off and have them tell each other their answers to the questions. Then, go around the room and have everyone introduce their partner to the room; e.g.: “This is Naima. She ate eggs for breakfast. The first time she made a password was in 3rd grade for a website for going on adventures with a cartoon pet. The password was ‘iamcool.’”

Things you’ll learn from this ice breaker:

- How social the participants are; how much they enjoy working in groups.
- Whether they all know what passwords are.
- How good they are at following instructions and remembering details.

Part of what’s fun about this icebreaker is that people are better at remembering than they think they will be. When you’re explaining how to remember a passphrase later on, you can remind them how easy it was to remember random details about their partners.

Activity: What is a Weak Password?

The facilitator can use a whiteboard for this activity, or jot comments down on a piece of paper during this activity.

Narrow View: If Someone Knows You, What is a Weak Password?

The facilitator can allot between 2-4 minutes for each discussion item. We recommend giving a specific time limit to contain the discussion.

Facilitator: “In your pairs over the next [X] minutes, I’d like you to take turns answering the following questions:”

1. “Have you been able to guess someone’s password before, based on things you knew about them, like when they were born, what their favorite animal is,

what their favorite song is, or their interests?"

2. "Has someone ever shared their password with you, and you were completely unsurprised about what their password was?"
3. "Think about someone you know very well. Would you be able to answer their security questions on their behalf?"

After the pairs have discussed, the facilitator can check back in with the group. The facilitator can ask for volunteers to (without disclosing the password itself), share an anecdote of an "easy" or "unsurprising" password.

Facilitator: "Still in your pairs, I'd like you to discuss the following over the next [X] minutes: If someone was to do a Google search about your friend in that scenario, or to look at their social media accounts, or look around their desk for hints, would they be able to guess that friend's interests? Would any of those interests lead them to hints for their passwords? Would any of those interests lead them to hints for their security questions?"

After the time allotted, the facilitator can check back in with the group.

The facilitator can ask participants to raise their hands in response to a question, or have them stomp their feet or clap.

Facilitator: "Show of hands: How many of you would be able to find out information about your friend's passwords, based on the type of information that they are unaware they share about themselves?"

Wide View: If Looking at the Data, What is a Weak Password?

Facilitator: "What's your guess: What are some of the most common passwords? In your pairs, over the next [X] minutes, I'd like for you to come up with at least five passwords that you feel the majority of people will pick. Which passwords do you think other people are likely to pick?"

Facilitator will check in with the group after the time is up. "What did you come up with in your pairs?"

Facilitator will write down the passwords on the board. The facilitator can occasionally ask: "Did anyone else have this password as one of their most common password guesses?" and highlight it. The facilitator can choose to a star next to the word each time someone raises their hand.

Learners will likely come up with variations on the spelling of “password”, common placements of keys on the keyboard (“qwerty”), sequential numbers “123456”, commonly used phrases in pop culture like “open sesame” or something less appropriate, maybe even words included on the webpage like “admin”, and “Facebook.”

The facilitator can prompt the learners. “What about favorite sports? Favorite colors? Popular names? Quotes from a movie or book? Song lyrics?”

Facilitator: “In your pairs, I’d like you to discuss over the next minute: How do you think people are able to determine what the most common passwords are?”

Facilitator will check back in after the allotted time and ask for volunteers. “What did you come up with?” Facilitator will wait for participants to come up with the idea of a leak, or the breach of a website’s databases.

If there is a major database breach in the news (e.g. Yahoo! In 2013, Adobe in 2013, and LinkedIn in 2012), the facilitator can use it as a discussion point for why strong passwords are important, and why it’s important to have unique passwords across accounts.

Activity: What Can You Do With Weak Passwords?

The facilitator can then show the live site for https://haveibeenpwned.com/, which has a huge database of passwords obtained from major breaches.

Facilitator: “Breaches can be very valuable sources of information in revealing people’s password habits. Unfortunately, the vast numbers of passwords show us that we are all quite predictable in how we choose these secret and valuable codes.”

Facilitator explains: “Let’s say that you just learn about a breach of a major social networking site, and the passwords, security questions, and answers, and the associated emails of a couple million users are now suddenly available as a downloadable file. And oh no! The website did not use strong **encryption** for this sensitive data. This is a *lot* of information. Let’s say, in this scenario, *you* are an attacker looking to make some money.”

Facilitator: “In your pairs, you have [X] minutes to discuss: What could you do with all these emails, security questions, and passwords? I’d like for you to come up with a few scenarios. What value would this information hold for you?”

The facilitator checks in after the time allotted, and asks the question again: “What did you come up with? How will you use those emails and passwords? How will you use those security questions and answers?” The facilitator waits for participants to respond. They may have a variety of answers, ranging from “look out for usernames of note,” “try to find someone valuable,” “share that information with a network of other attackers,” “try all these password combinations on other associated accounts,” and so on.

The facilitator can feel out where the discussion goes, and give participants the opportunity to think about how a malicious actor views their account details when it is at scale.

Facilitator: “Let’s talk a little bit about the capabilities of an attacker. This is a numbers game, and the attacker in this scenario is counting on humans being fairly predictable. Many people use the same password across different websites, maybe adding a few numbers at the end, or swapping a letter with a number. It is a fairly common practice for attackers to “brute force” their way into as many accounts as possible: that is, the attackers use passwords from these leaks across as many associated emails in different websites as possible. They’re able to do so fairly quickly with their computers plugging in the account information for them. They’re able to write a script for their computers to add those numbers at the end of passwords, or to swap numbers with letters, and so on. They’re able to pull from known common words, from common quotes and phrases.”

Facilitator: “You might remember *[insert hack where millions of account passwords, IDs, and associated information were taken here—facilitator can browse news sites and share a screenshot of the headline, or browse around the breaches in HaveIBeenPwned]*. When something like this breach happens, what can you do?”

Participants’ responses may range from: “nothing” and “delete your account,” to the more proactive suggestions of “monitor account information,” “set up **two-factor authentication**,” or “change your password.” The facilitator can encourage the latter three behaviors, and mention that users can take advantage of the three options if they are available for a given service.

Facilitator can use the suggestion of “change your password” to prompt the discussion of: “What could you change your password to?”

Knowledge Share: What is a strong password?

Facilitator: “Let’s say that you’ve decided to change your password. Keep in mind that you’ve learned:

- We may pick passwords that are personally relevant to us and can be guessed by learning about our interests or histories,
- Humans are fairly predictable in choices of passwords even when they aren't directly related to our personal experiences,
- We have a tendency to make predictable variations of the same password,
- We tend to use the same or similar password across many sites,
- The shorter a password is, the easier it is for a computer to guess."

Facilitator will write the above constraints on the board, as a slide, or in another visible way.

Facilitator: "Considering these common weak experiences with passwords...What qualities might a strong password have? You have a minute to chat in your pairs."

Facilitator checks back in with the group. Hopefully, participants arrive at similar conclusions: "long", "random," and "unique" are the keywords to look out for.

Facilitator should then write these qualities in a visible way:

- **Random**
- **Unique**
- **Long**

"Passwords should be random, long, and unique for every site."

The facilitator can show the XKCD comic illustrating this point. https://xkcd.com/936

Audience members may ask "But how am I supposed to possibly remember these random, unique and long passwords?" That serves as an excellent transition to teaching about password managers.