Show: Slide 1: Authentication Title Slide
Say: "Today we are going to go over authentication specifically how it relates to password safety"

Show: Slide 2: Passwords - Good or Bad?
Say: "To start off, we are going to do an exercise on whether you think the following passwords are good or bad"

Show: Slide 3 - Example 1
Say: Raise your hand if you think this is a good password. (Count the Student Responses)
Say: Now raise your hand if you think this is a bad password. (Count the Student Responses)

Show: Slide 4 - Example 2
Say: Raise your hand if you think this is a good password. (Count the Student Responses)
Say: Now raise your hand if you think this is a bad password. (Count the Student Responses)

Show: Slide 5 - Example 3
Say: Raise your hand if you think this is a good password. (Count the Student Responses)
Say: Now raise your hand if you think this is a bad password. (Count the Student Responses)

Show: Slide 6 - Example 4
Say: Raise your hand if you think this is a good password. (Count the Student Responses)
Say: Now raise your hand if you think this is a bad password. (Count the Student Responses)

Show: Slide 7 - Example 5
Say: Raise your hand if you think this is a good password. (Count the Student Responses)
Say: Now raise your hand if you think this is a bad password. (Count the Student Responses)

Show: - Slide 8: - Why are Passwords so Important?
Say: "Now I want you to think about why passwords are so important to us"

> # Warm Up:
> # Why are passwords so important?
>
> 1. Silently think about the question above.
> 2. Turn to your neighbor and discuss what your ideas.

Show: Slide 9 - Warm Up
Ask: Why do we think passwords are so important?
Say: "First think in your head why they are important and then turn to your neighbor and compare answers. When you are finished face back towards the front so that I know we are ready to move on"

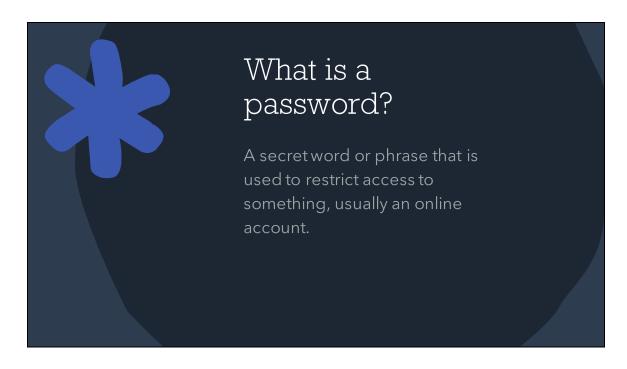Discuss as a Class

Show: Slide 10 - Class Discussion
Say: "Can I have a couple of volunteers to share why they think passwords are so important to us?"
Make sure as a teacher you discuss what can happen if an attacker gets into their account. Examples are stolen information like name, birthday, credit card numbers, addresses, etc.

Show: Slide 11: Learning Objectives
Say: "Today we are going to go over three main objectives. First, we will go over three different types of password attacks. Next, we will discuss how to make strong passwords to defeat these attacks. Finally, we will practice creating strong passwords that are memorable"

What is a password?

A secret word or phrase that is used to restrict access to something, usually an online account.

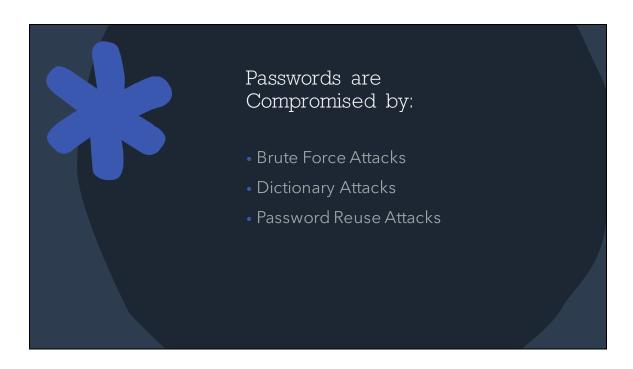**Show**: Slide 12: What is a Password?
Say: "The dictionary definition for a password is 'A secret word or phrase that is used to restrict access to something, usually an online account.'
Say: All of you have a password for your school email account and potentially for any social media or other websites that you have to log into"

Show: Slide 13: Three Deadly Password Attacks
Say: "There are three password attacks that we have to be aware of when we are creating our passwords"

Passwords are Compromised by:

- Brute Force Attacks
- Dictionary Attacks
- Password Reuse Attacks

Show: Slide 14: Passwords are compromised by:
Say: "These three attacks are Brute Force, Dictionary, and Password Reuse"

Let's break it down:
Brute Force Attack

Show: Slide 15: Let's break it down: Brute Force attacks
Say: "First we are going to look at what a brute force attack is, we'll break it down into pieces."

Show: Slide 16: What does brute mean?
Ask: "Can anyone tell me what brute means?" Pause for student answers. Click Slide
Say: "It means something that does not have any reasoning or intelligence"

What is Force?

To make a way through or into by physical strength

Show: Slide 17: What is Force?
Ask: "Now can anyone tell me what force means (and I don't mean in relation to Star Wars)?" Pause for student responses. (Click Slide)
Say: "That's right it is to make your with through or into something using physical strength"

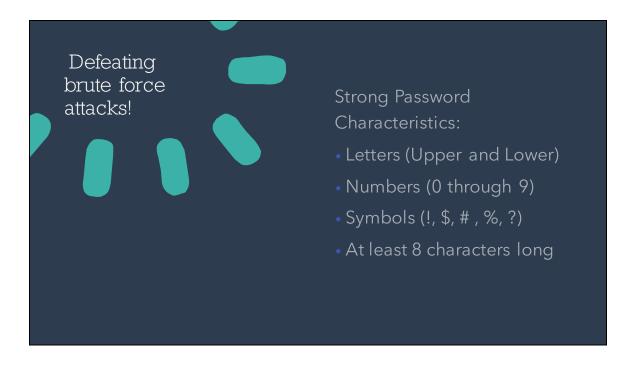**Putting it back together: Brute Force Attack**

An attack that relies on the strength of modern computing to try all possible combinations to find the correct password.

Show: Slide 18: Putting it Back together: Brute Force attack
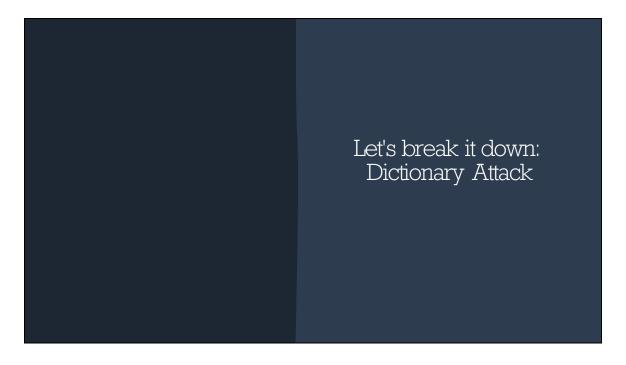**Say**: "Lets put it all together now" (Click Slide)
Say: "A Brute Force attack is an attack that relies on the strength of modern computing by trying all of the possible combinations (a-zA-Z0-9 plus symbols) to find the correct password"
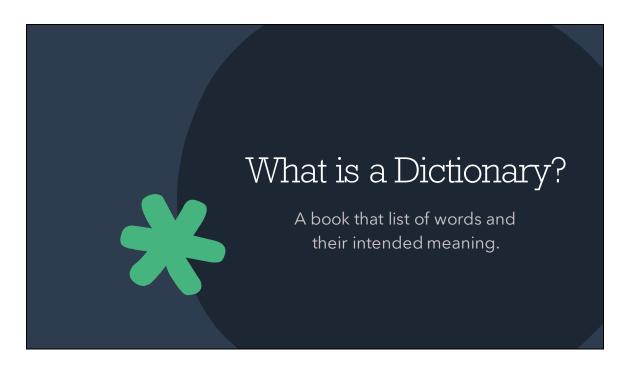
Defeating brute force attacks!

Strong Password Characteristics:

- Letters (Upper and Lower)
- Numbers (0 through 9)
- Symbols (!, $, # , %, ?)
- At least 8 characters long

Show: Slide 19: Defeating Brute Force attacks

Ask: "So how do we defeat a brute force attack?"

Say: "There are 4 different characteristics that make our password strong. These are using Upper and lower case letters, using numbers, using symbols, and making your password at least 8 characters long"

Show: Slide 20: Let's break it down: dictionary attacks.
Say: "Next we are going to go over a dictionary attack"

Show: Slide 21: What is a Dictionary?

Ask: "Now I know you all know what a dictionary is so who can raise their hand and tell me?" (Click Slide)

Say: "That is right it is a book that has words and their definitions"

Putting it back together: Dictionary Attack

An attack that uses dictionary words and a list of commonly used passwords to guess to correct password.

Show: Slide 22: Putting it back together: Dictionary attack
Ask: "But how does that work with a password attack you ask?" (Click Slide)
Say: "It means that an attack uses the entire list of dictionary words and a list of common passwords in order to guess the correct password. This is similar to the brute force attack except it uses words instead of random letters and numbers"

Show: Slide 23: Defeating Dictionary attacks.
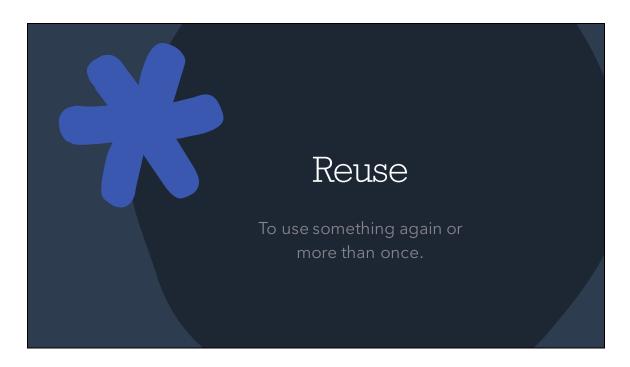**Ask**:"Well how are we going to keep safe from a dictionary attack?
Say: There are a few simple rules to follow. We should avoid using words that are in the dictionary. We should not use common passwords. And we should not use any sentences. What we should do however is to break up our words with numbers and symbols. It also makes a dictionary attack harder if we remove all the vowels from the word. And finally you can replace letters of your words with different symbols or numbers"
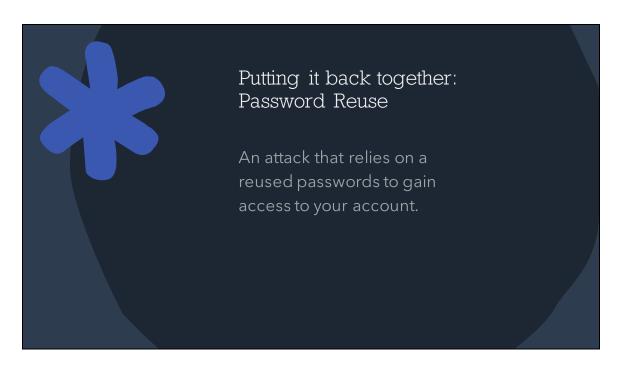
Let's break it
down:
Password Reuse
Attack

Show: Slide 24: Let's break it down: Password Reuse attack
Say: "Our last password attack is a password reuse attack.
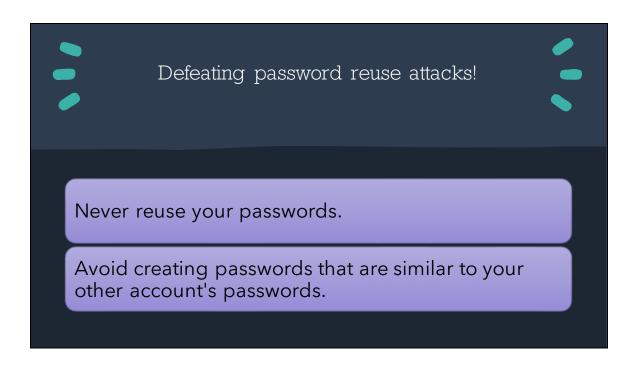**Ask**: Can anyone guess what this means?"

Show: Slide 25: Reuse definition
Say: "To reuse means to use something again or more than once"

Putting it back together:
Password Reuse

An attack that relies on a reused passwords to gain access to your account.

Show: Slide 26: Putting it back together: Password Reuse
Say: "_____ you were right. This is an attack where they rely on you to reuse your password for more than one account. Once they have it for one account they would then have access to all of the accounts with the same password"

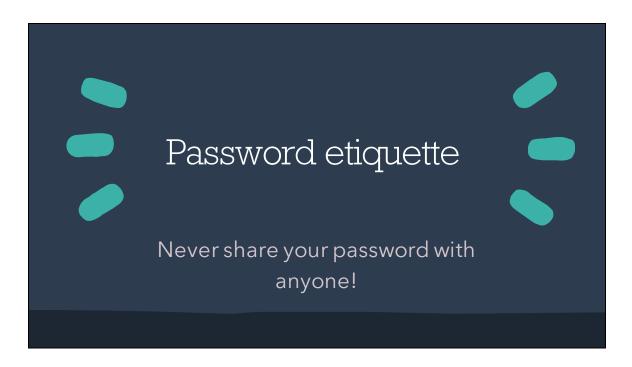**Show**: Slide 27: Defeating password reuse attacks.
Ask: "So how do we avoid these attacks?
Say: The most obvious answer is to never reuse your passwords. You also want to avoid using passwords that are similar to passwords that you have for other accounts"

Password complexity

A Bad password:	A Good password:
• Contains personal information (pet names or birthdays) • Has repeating letters, numbers or symbols • Is similar or the same as a password from another account • Has unbroken full words or sentences	• Has a good variety of letters, numbers and symbols • Breaks up words with letters or symbols • Is always 8 characters or longer • Is Unique

Show: Slide 28: Password complexity
Say: "Overall there are characteristics of a good password and a bad password. Take a minute to read the slide and think about how your passwords relate to this password complexity"

Password etiquette

Never share your password with anyone!

Show: Slide 29: Password etiquette
Say: "One thing to remember is to NEVER share your passwords with anyone"

Ensure students understanding that sharing a password could compromise the security of even the most secure passwords. The only person who should know a students password is them and their parents.

Show: Slide 30: Memorize your Password!
Say: "Another key aspect to password safety is to memorize your password. You should not write your password down on a notepad or your phone etc. Some easy ways to memorize your password are to create a story for your password. For example if my story is "Please Excuse My Dear Aunt Sally!" Then I can take the first letter of each word to remember it is "pemdas!".

The next strategy is to relate your password to the website it is being used for. An example of this is if I am logging into my school email I might choose "math15myFavorite".

And finally, you could choose a phrase or a quote. This could be from a TV show, a movie, or maybe your favorite book. From the wizard of oz "Toto I don't think we are in Kansas anymore" to make this a password you could choose to use the second letter of the words "Oiohernan" and then add a numbers or symbols to strengthen it.

Making passwords can be a daunting task especially when we have so many accounts. One option you could try is a password manager like LastPass. To login to these you use one strong password to unlock the passwords to the rest of your accounts"

Say: "That was a lot of information do we have any questions"

Show: Slide 31: Passwords Good or bad

Say: "We are now going to do the same exercise we did at the beginning of class and see if your answers have changed after everything we have learned so far"

Show: Slide 32: Example 1
Say: Raise your hand if you think this is a good password.
Say: Now raise your hand if you think this is a bad password.
(click slide)
Say: If you guessed this was a bad password you are correct!
Ask: Can anyone raise their hand and tell me why?" Expect answers like it is a common word or could be found in a dictionary attack.

Ex. 2
!@9YAt#f3h

Show: Slide 33: Example 2
Say: Raise your hand if you think this is a good password.
Say: Now raise your hand if you think this is a bad password.
(click slide)
Say: If you guessed this was a good password you are correct!.
Ask: Can anyone raise their hand and tell me why?" Expect answers like it has uppercase, lowercase, symbols, numbers, length, etc.

Show: Slide 34: Example 3
Say: Raise your hand if you think this is a good password.
Say: Now raise your hand if you think this is a bad password.
(click slide)
Say: If you guessed this was a bad password you are correct!.
Ask: Can anyone raise their hand and tell me why?" Expect answers like it is too short.

Show: Slide 35: Example 4
Say: Raise your hand if you think this is a good password.
Say: Now raise your hand if you think this is a bad password.
(click slide)
Say: If you guessed this was a bad password you are correct!.
Ask: Can anyone raise their hand and tell me why?" Expect answers like it is a common word or could be found in a dictionary attack.

Show: Slide 36: Example 5
Say: Raise your hand if you think this is a good password.
Say: Now raise your hand if you think this is a bad password.
(click slide)
Say: If you guessed this was a bad password you are correct!.
Ask: Can anyone raise their hand and tell me why?" Expect answers like it has uppercase, lowercase, symbols, numbers, length, etc.

Group Activity – Create a Password

& Worksheet

Show: Slide 37:
Say: "I am going to hand out a worksheet. On this worksheet there will be a list of passwords."
(online version) "I would like you to get into groups of _____ and use your chromebooks to go onto passwordmonster.com and fill out the worksheet. Make sure you discuss as a group and write down one word as to why you decided if each password was usable or not usable. Do not go based soley off the time. Then after you have completed the first section work with your group to come up with a password that you think is usable. After you write down your password check it on password monster and record the time. Reminder do not use any of your personal passwords"
(unplugged version)
Say: "I would like you to get into groups of _____ and fill out the first section worksheet. Make sure you discuss as a group and write down one word as to why you decided if each password was usable or not usable. Then after you have completed the first section work with your group to come up with a password that you think is usable. Reminder do not use any of your personal passwords"
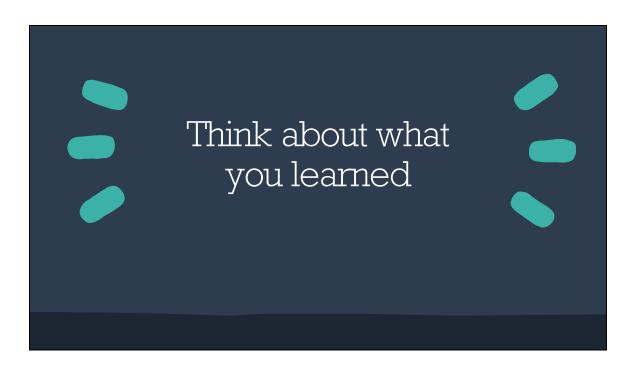
Show: Slide 38:

Say: "Today we learned three main objectives. First, we went over three different types of password attacks. Next, we discussed how to make strong passwords to defeat these attacks. Finally, we practiced creating strong passwords that are memorable"

Show: Slide 39:

Say: "I am going to hand out another worksheet so that you can connect what we learned in class today to your passwords at home. Fill out the worksheet to the best of your knowledge"