Authentication- Passwords Teacher Guide

Disclaimer – This was prepared as a guide to the slides. If it does not suit your students learning style feel free to change it up. It is intended to help lead the discussion around password safety

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

Slide 2: "To start off, we are going to do an exercise on whether you think the following passwords are good or bad"

Slides 3-7: "Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands."

Slide 8: "Now I want you to think about why passwords are so important to us"

Slide 9: "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"

Slide 10: "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.

Slide 11: "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"

Slide 12: "The dictionary definition for a password is 'A secret word or phrase that is used to restrict access to something, usually an online account.' 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"

Slide 13: "There are three password attacks that we have to be aware of when we are creating our passwords"

Slide 14: "These three attacks are Brute Force, Dictionary, and Password Reuse"

Slide 15: "First we are going to look at what a brute force attack is"

Slide 16: "Can anyone tell me what brute means?" Click Slide

"It means something that does not have any reasoning or intelligence"

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

Slide 18: "Lets put it all together now" Click Slide "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"

Slide 19: "So how do we defeat a brute force attack?" "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"

Slide 20: “Next we are going to go over a dictionary attack”

Slide 21: “Now I know you all know what a dictionary is so who can raise their hand and tell me?” Click Slide “That is right it is a book that has words and their definitions”

Slide 22: “But how does that work with a password attack you ask?” Click Slide “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”

Slide 23: “Well how are we going to keep safe from a dictionary attack. 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”

Slide 24: “Our last password attack is a password reuse attack. Can anyone guess what this means?”

Slide 25: “To reuse means to use something again or more than once”

Slide 26: “_____ 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”

Slide 27: “So how do we avoid these attacks? 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”

Slide 28: “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”

Slide 29: “One thing to remember is to NEVER share your passwords with anyone”

Slide 30: “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 “tiohernan” 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” “That was a lot of information do we have any questions”

Slide 31: “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”

Slide 32: “Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands.” (click slide) “You guys were correct this was a bad password. 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.

Slide 33: “Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands.” (click slide) “You guys were correct this was a good password. Can anyone raise their hand and tell me why?” Expect answers like it has uppercase, lowercase, symbols, numbers, length, etc.

Slide 34: “Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands.” (click slide) “You guys were correct this was a bad password. Can anyone raise their hand and tell me why?” Expect answers like it is too short.

Slide 35: “Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands.” (click slide) “You guys were correct this was a bad password. 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.

Slide 36: “Raise your hand if you think this is a good password. Okay lower your hands. Now raise your hand if you think this is a bad password. You may now lower your hands.” (click slide) “You guys were correct this was a good password. Can anyone raise their hand and tell me why?” ?” Expect answers like it has uppercase, lowercase, symbols, numbers, length, etc.

Slide 37: “I am going to handout 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”

(not online version) “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”

Slide 38: “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”

Slide 39: “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”