TECH for Tomorrow

CLASSROOM ACTIVITY

Hashing and Cracking: Password Essentials

Objectives

Students will be able to:

- **Assess** password strength based on probability.
- **Develop** and **research** password recommendations and create passwords based on these best practices.
- **Develop** their own innovative and secure password system.

Overarching Question

How can I create safe and secure passwords?

Activity Summary

In this activity, students will pretend they are entrepreneurs about to begin their own company website, and they want their login system to be as secure as possible. In order to accomplish this, students will investigate the probability behind passwords and read about current password recommendations. They will then apply what they have learned as they create a secure emoji-based password system for their new customers.

Grades

4–6

Timing

50–60 minutes

Materials

- Device with the ability to project, one for the teacher
- Station 1: ABCD1234 handout, one per student
- Station 2: Expert Tips handout, one per student
- Station 2: *How Does a Password Get Hacked?* article, one per student
- Design a Password System handout, enough for ¼ of the class
- Lined paper, for the class to share
- Scissors, for the class to share
- Glue, for the class to share

Activity Directions

Premise | 10 minutes

- Begin class with a quick poll. Ask: Through a show of hands, who uses the same password for more than one login system? Convert this number to a rough percentage based on the number of students in your class, and write the percentage on the board.
- Then share the following statistics and continue to write the percentages on the board:
    - 50% of people worldwide polled by an internet security company use the same password to protect more than one of their online accounts.
    - 83% of Americans use weak passwords that are easy to crack.
    - 25% of people worldwide have never changed their passwords.
- Ask students to evaluate these statements and share some of the key takeaways that come to mind.
- Next, explain that the students are about to take on a challenge related to password security: For the rest of class, students will be acting as entrepreneurs who are creating a company website. They want their login system to be as easy and as safe as possible for their new customers, so they will be investigating how passwords work so they can eventually develop a secure login system!

Investigate | 30 minutes

- Think-Pair-Share: Based on what you already know, what makes a password secure?

  Note: In a think-pair-share, students think about the question independently, discuss their answers with a partner, and then share their thoughts with the larger class.
- Tell the class that before they develop their own password system, they will further investigate recommendations for secure passwords as well as why these recommendations exist!
- Divide students into pairs and explain that each pair will complete this investigation in two stations:
    - Each pair will begin with Station 1. Pass out a Station 1: ABCD1234 handout to each student, and explain that in a moment, pairs should find an area in the classroom to read the directions and complete this work together.
    - Once pairs finish Station 1, they should move on to Station 2. Show students where to find the Station 2: Expert Tips handout and the Station 2: How Does a Password Get Hacked? article, and explain that they should pick up the work for this station once they have completed Station 1.
    - Pairs will have about 25 minutes to complete the two stations.
    - Remind the class that this training will give them the background they need to create a strong password system for their new customers, and then instruct them to get to work!
- When about 12 minutes have passed, ask students to begin wrapping up Station 1. Once 15 minutes have passed, instruct all groups to move on to Station 2 if they have not done so already.

Solve | 10–20 minutes

- Bring the class back together and take a few minutes to summarize the password tips that the students compiled.
- Then ask:
    - Do you think password systems must be limited to letters and numbers? Why or why not?
    - Why might a password system that goes beyond letters and numbers be stronger and harder to crack?
- Bring students back to their original task (to develop a secure password system for their new company website) and add one additional challenge: The cofounder of the students' new company would like to include facial emojis in their password system to make it more secure.
- With this in mind, it's time for the class to create their company's password system! Complete the following to prepare students for this activity:
    - Place each pair of students with another pair to make groups of four.
    - Distribute one Design a Password System handout to each group.
    - Instruct students to follow the handout's instructions to create the new password system for their company.
    - Remind students to apply what they learned in their station work as they develop this system and then encourage them to get to work!
- If time allows at the end of the class session or at the beginning of the next class session, encourage students to exchange password systems with each other, follow their instructions, use their keyboard to create a password, and provide suggestions for improvement!

Standards

Common Core Mathematics Standards

- CCSS.MATH.PRACTICE.MP1: Make sense of problems and persevere in solving them.
- CCSS.MATH.PRACTICE.MP3: Construct viable arguments and critique the reasoning of others.
- CCSS.MATH.PRACTICE.MP4: Model with mathematics.

Common Core English Language Arts Standards

- Speaking and Listening
    - CCSS.ELA-LITERACY.CCRA.SL.1: Prepare for and participate effectively in a range of conversations and collaborations with diverse partners, building on others' ideas and expressing their own clearly and persuasively.

Standards for Technological Literacy (ITEAA) Standards

- Standard 8. Students will develop an understanding of the attributes of design. In order to comprehend the attributes of design, students should learn that:
    - D. Requirements for a design include such factors as the desired elements and features of a product or system or the limits that are placed on the design.
    - F. There is no perfect design.
    - G. Requirements for a design are made up of criteria and constraints.
- Standard 9. Students will develop an understanding of engineering design. In order to comprehend engineering design, students should learn that:
    - H. Modeling, testing, evaluating, and modifying are used to transform ideas into practical solutions.
- Standard 13. Students will develop the abilities to assess the impact of products and systems.
    - As part of learning how to assess the impact of products and systems, students should be able to:
    - C. Compare, contrast, and classify collected information in order to identify patterns.

Source

1 – Avast Security News Team. “World Password Day 2019: Is your password strong enough?” Avast Blog. blog.avast.com/strengthening-passwords-on-world-password-day.

Station 1: ABCD1234

Directions: : Decide who will be Partner A and who will be Partner B. Then complete the steps below:

Step 1: Password Creation

Partner A: Create a three-digit numerical password and write it below. For instance: 937
Partner B: Create a three-letter password and write it below. For instance: DTQ

Keep this password a secret from your partner!

My Password:

Character 1	Character 2	Character 3

Keep this password a secret from your partner!

Step 2: What Are the Chances?

Think about the probability (or chance) that your partner will guess one of your password's characters correctly on the *first* try.

To figure out the chance of this happening, count all of the characters that your partner *could* guess. In other words: If your partner knew that the first character in your password was 1–9 or A–Z, how many possible characters are there between 1–9 or A–Z? Write this number the blank below.

There is a 1 in ____ chance that my partner will guess one of my password's characters correctly on the first try.

Step 3: Crack the Password

Now take turns guessing each other's passwords! Make sure your partner knows if your password is made up of numbers or letters. Then go back and forth, guessing one number or letter at a time. Make a tally in the box below each time your partner takes a guess. When they guess correctly, tell them and then move on to the next character!

Password Guesses:

Character 1	Character 2	Character 3

Step 4: Discuss the Odds

Partner A: How many total guesses did it take for your partner to guess your password?
Partner B: How many total guesses did it take for your partner to guess your password?
(Or is your partner *still* guessing?)

Station 1: ABCD1234

Partners A and B:

- Why was there a difference in the number of guesses that it took to guess each password?
- What connection(s) can you make between the number of guesses *and* the chances that you each recorded in Step 2?
- What recommendations would you give to someone trying to create a strong password? Record your answer below.

  Tip: Think about how using letters, numbers, and/or letter *and* numbers may affect the chances of someone else cracking your password.

____

____

____

____

____

Station 2: Expert Tips

Directions: Complete the steps below with your partner.

Step 1: Be Informed

Read *How Does a Password Get Hacked?* aloud together. As you read, underline ideas that could help you create a strong password.

Step 2: Password Analysis

Use your annotations to develop three tips for creating strong passwords and write them below:

1.

2.

3.

Step 3: Password Creation

Use these tips, as well as what you learned in Station 1, to develop at least three model passwords.

Step 4: Strengthen & Improve

If you have time, share your passwords with another pair. Review their work and give suggestions to make their passwords even trickier to crack!

Station 2: How Does A Password Get Hacked?

Adapted for Grades 4–6 from How to Create a Strong Password

Cybercriminals use many password-hacking tricks, but the easiest one is to buy passwords off the dark web. The dark web is a part of the internet that needs special software to get into. Its users are anonymous so it is an easy place for crime to occur. People will pay a lot of money to buy log-in information on the black market. If you have been using the same password for years, there's a high chance that it can be found here.

But if you change your password often, and remember to make your password complex, cybercriminals won't be able to buy your passwords...they'll have to crack them instead! And if that's the case, they're likely to use one of the methods below.

Brute force attack

This attack tries to guess every possible combination until it hits on yours. The attacker uses automatic software to try as many combinations as quickly as possible. One hacker, for instance, developed a program that made 350 billion guesses per second. He could crack an 8-character password (that had upper case letters, lower case letters, numbers, and symbols) in less than six hours. And some brute force attacks can crack passwords even more quickly! Any passwords with less than 9–12 characters are at risk of being attacked.

Dictionary attack

This attack is exactly what it sounds like! While a brute force attack tries every combination of symbols, numbers, and letters, a dictionary attack tries different words that you would find in a dictionary. If your password is a regular word, you'll only survive a dictionary attack if your word is very uncommon **or** if you use many words together, like *LaundryZebraTowelBlue*. Passwords with several words can outsmart a dictionary attack.

Design a Password System

Directions: Work as a group to follow the steps below and create a strong facial emoji password system for your new company!

Step 1: Discuss & Jot Notes

Do you think a password system would be stronger if the user could select an emoji that was already created *or* if the user could create their own emoji? Why?

____

____

If people could create their own emoji, what should the emoji include? Picture the different parts of an emoji's face, and make a list below:

EYES, ____

____

What else should a strong password include? (Think about what you learned in your stations!)

____

____

Step 2: Create

Create a password keyboard below that your customers will use to create their password. It should include every letter, number, shape, or emoji facial feature that your customers may need:

Step 3: Explain

Finally, write step-by-step instructions that tell your customers how to use your keyboard to create a strong password. Write these on a piece of lined paper, and then cut out your keyboard and glue it to the bottom of these instructions.