IMPORTANCE OF STRONG PASSWORDS

Lesson Description:

In this lesson students will discover what makes a strong password, as well as the importance of having strong, unique, passwords for each website/app that they use. The students will then create an algorithm for how to create strong and unique passwords that are also easy to remember.

Prerequisite Knowledge:

- Vocabulary:
  - ASCII
  - URL
  - Algorithm

- Encryption using Caesar or other ciphers is not necessary, but could be a lesson extension.

Length of Completion: Approximately 40 minutes

Level of Instruction: 9th - 12th Grade

Applicable Concepts and Standards:

- **GenCyber Cybersecurity Concepts**
  - Defense in Depth
  - **Confidentiality -** Discussion of strong passwords used to access confidential information
  - Availability
  - **Think Like an Adversary** - Discussion of how passwords can be cracked.
  - **Integrity -** Discussion of how to make passwords strong

  - **Keep it Simple -** Creation of an algorithm to make strong, but easily remembered, unique passwords

- **NYS State Computer Science and Digital Fluency Standards**
  - **9-12.CY.2** Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information.
  - **9-12.CY.5** Recommend multiple actions to take prior and in response to various types of digital security breaches.

- **AP Computer Science Principles**
  - **IOC-2.B.1** Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.
  - **IOC-2.B.2** A strong password is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.

Resources that are Needed:

- Google Slides Presentation - Link here
- Guided Notes Sheet - Attached
- https://www.security.org/how-secure-is-my-password/

Sources

- UTeach CS Password Generator Project
- Code.org Keys and Passwords Worksheet

Accommodations Needed:

Accommodations for this lesson should be the normal accommodations that students receive in their class. A text to speech or speech to text translator may be helpful for visually impaired students.

LEARNING OUTCOMES

At the end of the lesson students will be able to:

- Explain what makes a password strong and apply knowledge to creating a strong password.
- Explain the importance of strong passwords.
- Create strong, unique passwords that are easily remembered but difficult to guess/crack.

LESSON DETAILS

Interconnection:

Prior lessons may include:

- Encrypting messages using simple ciphers such as a caesar cipher. There will be an opportunity for this to be a lesson extension for students who grasp the content quickly.

Further lessons may include:

- The need for two factor authentication
- Encrypting data, including asymmetrical encryption.
- SQL Injections and the importance of unique passwords for each website.

Assessment:

Formative assessment may include individual discussion with students while they are working on the activities as well as whole-class discussion on the overall concepts at the end of each activity.

Summative assessment may include a test at the end of the unit or a final exam. This content is also relevant to the AP Computer Science Principles course and the AP exam could be used as a summative assessment.

The teacher may have the students submit the worksheet or their algorithm from Activity 2 and use that as either a formative or a summative assessment.

Extension Activities:

During the lesson students create an algorithm for how to create strong passwords. An extension of this could be to have students write a program in which the user inputs some information and a strong, unique, and easily-remembered password is generated.

If the passwords that your school uses are generated in a specific way, discuss whether or not they are secure. If they are not, discuss a way for those passwords to be generated easily, and for students to remember them, but so that they cannot be easily guessed by other students.

If you have extra time, this website shows how the strength of passwords has changed over time.

Differentiated Learning Opportunities:

For examples where the students are asked to generate possible passwords, the teacher could create examples for students to try and either present them or provide a completed version of the guided notes.

For students who may struggle creating their own password algorithm, the teacher could ask students to use a pre-created algorithm to generate passwords for several websites or apps that students frequently use. Alternatively, the teacher could have students add extra steps to their password generator, such as using a caesar cipher to encrypt the letters from the website url.

LESSON

Warm Up: (5 - 10 minutes)

Ask the students to answer questions 1 and 2 on the provided notes sheet. They will create a fake password and test it's strength at the website: https://www.security.org/how-secure-is-my-password/

The goal of this is for students to see how strong the passwords they already use are. Expect some students to have easily cracked passwords and others to have strong ones. In the next activity students will discover what makes a password strong.

Note: Be sure to tell students not to use actual passwords that they use, as they will be sharing them with the class.

After students have answered the questions, have them share with the class how long it would take to crack their passwords. Ask which password(s) took the longest to crack.

Activity 1: What makes passwords strong? (10 - 15 minutes)

In this activity, students will answer questions 3 through 8 on the worksheet. They will start by creating passwords that are all lowercase, and testing their strength with two different lengths. Then they will create passwords using any characters on the keyboard to try and find what makes a password strong. After they answer these questions, have a discussion with the class to determine what a strong password should have. Specifically, a strong password should include multiple types of characters (uppercase, lowercase, digits, symbols) and should be at least 10 characters long.

Activity 2: Generating Strong Passwords (15 - 20 minutes)

In this activity students will create an algorithm that they can use to create strong passwords that are unique to each website or app that they use. An example algorithm would be to choose 3 random ASCII characters that stay the same, type every other letter from the website or app URL, capitalizing every other one, and choose 3 more random ASCII characters to put at the end. This should generate a password of at least 10 characters that is unique and difficult to guess.

Name: ________________________________ Period: _________ Date: ______

Worksheet: The Importance of Strong Passwords

<u>Warm Up</u>: Testing Password Strength

1. Create a strong password, and write it below. *Do not write a password that you actually use, as we will be sharing our passwords with the class*.

2. Go to the website https://www.security.org/how-secure-is-my-password/ and test your password.

   How long would it take a computer to crack your password? Is it a strong password?

<u>Activity</u>: What Makes Passwords Strong?

3. Create and write three passwords using 8 lowercase ASCII characters (a-z) and test their strength. What's the longest amount of time-to-crack you can generate?

4. Create and write three passwords using at least 12 lowercase ASCII characters (a-z) and test their strength. What's the longest amount of time-to-crack you can generate?

5. Try creating a password with 20 of the same character in a row. How long would it take to crack?

6. Using any characters on the keyboard, create and write a few passwords. What's the longest amount of time-to-crack you can generate with an 8-character password?

7. What seems to be the single most significant factor in making a password difficult to crack? Why do you think this is?

8. Opinion: Is an 8-character *minimum* a good password length for websites to require? Give your opinion, yes or no, and explain why you think that. What other requirements should a strong password have?

Activity 2: Generating Strong Passwords

9. Why might it be important to use unique passwords for each website or app that you use?

10. Why would someone create one, or only a few passwords that they use for all of their logins?

11. Create an algorithm (set of steps) that people can use to create passwords that are secure, unique to each website or app, and easily remembered. Your algorithm should be complex enough that it generates strong passwords, but not so complex that you cannot remember it or how to use it.

    Example: Type every other letter/character in the site URL and capitalize every other. Pick 6 - 8 ASCII Characters (that will always stay the same) and put half before and after your password.

    So the password for wikipedia.com could be $a1WkPdA!7B. I would use $a1 and !7B before and after every password, and the middle part would change.

    Below, write your algorithm and an example of how it can be used: