Strong Passwords

grades 6-8 Lesson Plan

Estimated time: 45 minutes

Essential Question: How can a secure password help you protect your private information?

Learning Overview and Objectives

Overview: Students learn how to create secure passwords in order to protect their private information and accounts online.

Students learn tips for creating safe passwords. They explore scenarios in which two characters choose passwords, and they use the tips they have learned to create secure new ones for those characters. They then create posters to communicate password tips to their families and other students.

objectives

Students will:

- Identify the characteristics of strong passwords
- Apply characteristics of strong passwords to create new passwords
- Create secure passwords with their family members

Materials and Preparation

Materials

- **Password Tips Student Handout**
- **Password Challenge Student Handout**
- Poster paper
- Colored markers
- Chalkboard or white board

Preparation

- Copy the **Password Tips Student Handout**, one for every student
- Copy the **Password Challenge Student Handout**, one for every student

Parent Resources

- Send parents the **Security Parent Tip Sheet**
- Send parents the **Internet Safety for Middle School Parent Tip Sheet**
- Send parents the link to the ***Internet Safety Tips for Middle School Video***

Key Vocabulary

- **Password Protection**: The requirement that visitors use a password when they access a website so that only certain people can view the site and participate in its online activities
- **Random**: Having no pattern

- **Security**: Freedom from danger. Online, “security” refers to protecting one’s private information and protecting a computer from viruses or “malware”
- **Screen Name**: The online name you choose to log in with or to post on a website

teaching plans

Introduce

ASK *What are some of the non-electronic security devices that people use to protect their possessions from being stolen or used by others?*

Sample Responses:

- *Lock on a gym locker*
- *Apartment and house keys*
- *Bicycle locks*

ASK *What are examples of how you use passwords when you use electronic devices?*

Sample Responses:

- *Logging on to a computer*
- *Signing into online accounts*
- *“Unlocking” a cell phone*

EXPLAIN that passwords protect your online accounts from being stolen or used by others. Point out that the older students get, the more important password security will become to them. Choosing good passwords will help them protect their social networking profiles when they are in high school, keep their grades private when they are in college, and protect their bank accounts and online store accounts when they are adults.

ASK *What do you think could happen if someone got hold of your password?*

Sample responses:

Someone could:
- *Access my online accounts*
- *Steal my money*
- *Pretend to be me and hurt my reputation*
- *Find out things about me that I don’t want anyone else to know*

Teach 1: No Guesswork

DISTRIBUTE the **Password Tips Student Handout** and review each of the eight security tips for managing passwords.

INVITE students to explain why each tip is effective. If they are not sure, offer some of the following tips:

- **Only your parents should know your password.** Never give a password to anyone else – not even your friends. They could unknowingly share it with someone who could use your password to pretend to be you or to harass other people.
- **Don't use passwords that are easy to guess, like your nickname or your pet's name.** People who know you well can guess these kinds of passwords.
- **Never use any private identity information in your password.** Identity thieves can use this information to pretend to be you.
- **Don't use a word in the dictionary as a password.** Hackers use programs that will try every word in the dictionary to guess passwords.
- **Create passwords with at least eight characters.** The fewer the characters, the easier it is for hackers to try every combination of characters.
- **Use combinations of letters, numbers, and symbols.** They are harder to crack than just words because there are more combinations to try.
- **Change your password regularly – at least every six months.** The longer you use the same password, the more likely it is that someone will guess it or use a program to find it.

Make sure that students are familiar with the forms of private identity information listed in the "Use Common Sense!" box. Remind students of an important safety and security rule: Do not give out private identity information without the permission of a teacher or parent.

Teach 2: Password Remix

Students should now read and discuss the "Smart Passwords?" scenarios about Jesse and Krystal, also in the **Password Tips Student Handout**.

DISCUSS Jesse's password choice with students.

ASK *Did Jesse make a safe choice? Why or why not?* (Jesse's password is too obvious a choice, easily guessed by people who know him, and therefore not secure.)

HAVE students identify the password tips Jesse's password did and didn't follow.

GUIDE students to discuss the scenario about Krystal.

ASK *How did Krystal choose her password?* (She chose her password by combining part of her name (kr), her favorite activity (swim), and the numbers of her birth month (8) and day (4).)

HAVE students evaluate Krystal's password.

ASK *Was it a safe choice?* (It is a safer choice because she used no complete personal identity information, and she combined at least eight letters and numbers.)

ASK *What are some other password tips Krystal could follow?*

HAVE students follow the directions for the "You Try It" activity at the bottom of the handout. Invite them to write new passwords for Jesse and Krystal, then share their new passwords with the class. Write the new passwords on the board and ask students to share their suggestions for how Jesse and Krystal could remember them.

Teach 3: Pass the Word?

CHALLENGE students to create posters that will communicate the password tips and help their families and other students keep their online identities secure. You may wish to assign one tip to each student, resulting in a series of tip posters that can be displayed together or rotated throughout the year.

Wrap Up and Assess

Use the posters that students created in **Teach 3** and/or the questions below to assess students' understanding of the lesson objectives. Evaluate students' learning by having them read and explain the reasoning behind each of their poster tips.

ASK

- *What are some tips for having strong passwords? Which ones do you think are most important to follow?* (Encourage students to recall as many of the eight tips as they can. Have students explain why they think particular tips are important.)
- *Which tips are easiest to follow? Which are hardest?* (Have students explain their reasoning. Answers will vary.)
- *How can we remind ourselves, other students, and our families to keep passwords secure?* (Answers will vary.)

REVIEW with students that passwords protect their online accounts and identities. Remind students that hackers and identity thieves try hard to guess passwords so they can steal people's online information. Tell students that creating a good password will make it hard for people to guess it.

Extension Activity

Students practice designing strong and weak passwords. Using the **Password Challenge Student Handout**, students create one strong and one weak password for an important historical figure. Both passwords should indicate something that is special or unique about that person. However, the strong password should be created using the "DO" tips from the **Password Tips Student Handout**, and the weak password created by using the DON'T'S from the handout. Remind students to do a little historical research to learn something about their historical figure before they begin. Optional: Students can write down the weak password and bring it to school. Students then physically exchange passwords with a partner and try to guess each other's historical characters. Students can give hints when needed.

Homework

In-school pre-activity: Teach students how to create a random password. Explain that although they are harder to remember, random combinations of letters, numbers, and symbols are the safest passwords. Obtain three number cubes. Use stick-on labels to replace the numbers on one cube with six letters. Replace the numbers on another cube with six keyboard symbols. Leave the third number cube as is. Have students put the three cubes in a paper bag and choose one at a time, roll the cube, and record the character. Do this eight time to get a random password with eight characters. Have students do online research to learn about random password generators at http://www.freepasswordgenerator.com/. After students explore the sites, discuss the pros (very hard to crack) and cons (can be hard to remember) of using random passwords.

Home activity: Students then work with their parents to create two new passwords for themselves using the random password generator: http://www.freepasswordgenerator.com/. Students should also teach their parents about the DO'S and DON'T'S of creating passwords from the Password Tips Student Handout.

Alignment with Standards – National Educational Technology Standards for Students© 2007

(Source: International Society for Technology in Education, 2007)

2. Communication and Collaboration

a. interact, collaborate, and publish with peers, experts or others employing a variety of digital environments and media
b. communicate information and ideas effectively to multiple audiences using a variety of media and formats

3. Research and Information Fluency

b. locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media

5. Digital Citizenship

a. advocate and practice safe, legal, and responsible use of information and technology
b. exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity