Strong Passwords

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

Estimated time: 45 minutes

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**

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

Strong Passwords

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.

Strong Passwords

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

Password Tips

Name(s) _____ **Class** _____ **Date** _____

Directions

Read the tips below on how to make and use strong passwords. Then read stories about Jessie and Krystal and answer questions about their passwords. Use the tips to make new passwords for Jesse and Krystal.

DO'S

- **DO** share your password only with your parents.
- **DO** create passwords with at least eight characters.
- **DO** use combinations of letters, numbers, and symbols, which are harder to crack than just words.
- **DO** change your password regularly – at least every six months.

DON'T'S

- **DON'T** give a password to anyone else – not even your friends.
- **DON'T** use passwords that are easy for people you know to guess, like your nickname or your pet's name.
- **DON'T** use any private identity information in your password.
- **DON'T** use a word in the dictionary as a password.

Use Common Sense!

Know what the kinds of private identity information not to include in your password:

- Full (first and last) name
- Email address
- Passwords
- Credit card numbers
- Mother's maiden name
- Postal address
- Phone numbers
- Calling card numbers
- Social Security number

Password Tips

Smart Passwords?

Directions

Read the following stories and answer the questions.

Jesse lives in Lawrence, Kansas – the home of the University of Kansas. He has a pet rat named "Phil" and is a big fan of the Kansas Jayhawks men's basketball team. Jesse chose "jayhawks" as his password. Did he make a safe choice? Why or why not?

_____

_____

Krystal lives in Miami, Florida. Her birthday is August 4, and she swims on a team. Her password is "krswim84." How did Krystal choose her password? Was it a safe choice? Why or why not?

_____

_____

You Try It!

Directions

Using the tips above, make new passwords for Jesse and Krystal. Explain how Jesse and Krystal can remember their passwords.

Jesse _____

Krystal _____

STUDENT HANDOUT grades 6-8

Password Challenge

Name(s) _____ **Class** _____ **Date** _____

Directions

You will 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. Use the "Do" tips from the **Password Tips Student Handout** to create the strong password, and use the "Don't" tips from the same handout to create the weak password.

Example for Abraham Lincoln:

Strong: 4score7yrs ("Four Score and Seven Years Ago ...")

Weak: HonestAbe

YOUR HISTORICAL FIGURE: _____

FACTS OR INFORMATION YOU LEARNED ABOUT YOUR HISTORICAL FIGURE: _____

_____

_____

STRONG PASSWORD: _____

WEAK PASSWORD: _____

Directions

Place check marks in all of the boxes that describe your answers to the questions below.

1. How did you come up with your strong password? What strategies did you use?

- ☐ I chose something that was connected with my person, but not too obvious.
- ☐ I replaced certain letters with numbers and symbols.
- ☐ I abbreviated words.
- ☐ Other: _____

Password Challenge

2. What makes your weak password less secure than the strong one?

- ☐ I didn't use any numbers.
- ☐ I used whole words that were commonly associated with my person.
- ☐ I used the person's name or an obvious nickname.
- ☐ Other: _____

3. How could the weak password be more secure without changing it a lot?

- ☐ Abbreviate words.
- ☐ Replace letters with numbers/symbols.
- ☐ Spell out words in number form (A-1, B-2, C-3, D-4 ...).
- ☐ Other: _____

Lesson Assessment

Name _____ **Class** _____ **Date** _____

1. Read the sentences below. Write either DO or DON'T in each of the spaces to show rules for creating strong passwords.

_____ change your password regularly.

_____ use a word from the dictionary as your password.

_____ tell your password to your parents.

2. Some of the passwords below are strong passwords that are difficult to guess. Others are weak passwords that are easy to guess. Read the passwords below and circle whether they are strong or weak.

a) gRe@tj0b	Strong	Weak
b) Luv2sw!m	Strong	Weak
c) anna99	Strong	Weak
d) June111998	Strong	Weak

3. Noah wants to make a password by combining his name and his favorite sport. He chooses NoahSoccer. Khali wants to make a password by combining the first letter of her name with her cat's name, Snowball. She chooses KSn0wb@ll. Whose password is stronger?

a) Noah's password
b) Khali's password
c) They are both equally strong

Lesson Assessment

1. Read the sentences below. Write either DO or DON'T in each of the spaces to show rules for creating strong passwords.

Answer feedback

DO change your password regularly.

DON'T use a word from the dictionary as your password.

DO tell your password to your parents.

You should change your password every six months. Don't use a dictionary word for your password, because some computer programs are designed to guess them. Share your password with your parents to keep it safe.

2. Some of the passwords below are strong passwords that are difficult to guess. Others are weak passwords that are easy to guess. Read the passwords below and circle whether they are strong or weak.

Answer feedback

a) gRe@tjOb	(Strong)	Weak
b) Luv2sw!m	(Strong)	Weak
c) anna99	Strong	(Weak)
d) June111998	Strong	(Weak)

Passwords gRe@tjOb and Luv2sw!m are strong passwords because they contain capital and lowercase letters, numbers, and symbols. Passwords are weaker when they are a dictionary word, or when they are an important date.

3. Noah wants to make a password by combining his name and his favorite sport. He chooses NoahSoccer. Khali wants to make a password by combining the first letter of her name with her cat's name, Snowball. She chooses KSn0wb@ll. Whose password is stronger?

a) Noah's password

b) Khali's password

c) They are both equally strong

Answer feedback

The correct answer is **b**. Khali's password is stronger because it contains numbers, letters, and symbols. Noah's password is not as strong because it contains only letters, and shows his first name.

Common Sense on Security

Some Facts

- Nearly 2 million households suffered ID theft in the previous year (*Consumer Reports*, 2009).
- The number-one piece of malware detected around the world infected more than 27 million files in the course of 30 days (McAfee Labs, 2009).
- 52 percent of teens have given out personal information online to someone they don't know offline (McAfee and Harris Interactive, 2008).

Staying safe and secure in a digital world

Technology makes it so easy for kids to connect and share things with friends and family no matter where they are. But these connections can come with a huge cost if kids aren't careful. Learning to protect personal identity information, creating strong passwords, and being cautious when downloading programs and files are crucial to the safety and security of the digital devices kids use, as well as the information those devices store. Otherwise, kids can expose themselves and their families to digital threats like computer viruses, data and identity theft, and hacking.

What is digital safety?

To understand digital safety and security, you'll need to learn some new words: *phishing*, *malware*, *spyware*, *spam*, and yes, even *junk*. These greedy little programs attach themselves to respectable-looking software – for example, a downloadable game that looks really cool – and then wreak havoc once installed on your computer. Security programs can block them, but one of the most important weapons is teaching kids to treat their devices and information as the truly valuable things they are.

Why it matters

If kids don't protect their personal information, there are many potential risks: damage to the hardware, identity theft, or financial loss. But children may not realize they are putting their information in jeopardy, because the warning signs aren't always obvious.

A friend might ask for your child's computer password to play a game, and then access your child's private email account. Or your child might use a file-sharing program that passes along a virus to your computer. To participate in an online contest, your tween might be asked to provide personal identity information such as a home phone number, address, date of birth, or your Social Security number, all of which opens up the family to the risk of identity theft. Just like in real life, kids have to know who to trust with information. It's as true in the digital world as the real world.

Common Sense on Security

common sense says

Parent tips for all kids

Remind your children to follow these important security tips.

Master the fine art of password creation. It can actually be fun to develop really good passwords. (See more details on how to do this below.) Strong passwords are a key defense against unauthorized access to your information, as well as identify theft.

Know the difference between information worth sharing and private information. There are many ways you can share your ideas and creativity online, but personal information should remain private. Never input personal identity information such as phone numbers, addresses, or your date of birth in order to download something. And never, ever give Social Security numbers or credit card information.

Be very careful with what you download. Don't download free games or videos to your computer. These programs often come with spyware and viruses that will land your computer in the shop – and you in hot water.

Password protection

Protect yourself – and your stuff – with strong passwords that safeguard your digital data. Use these tips to help you do it:

Don't use passwords that are easy to guess – such as your nickname or your pet's name. People who know you well can guess these kinds of passwords.

Don't 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.

Do use combinations of letters, numbers, and symbols. These are harder to crack than regular words because there are more combinations to try.