AACPS Digital Citizenship

Lesson Title: Powerful Passwords

Grade 5

Time: 30 minutes

Overview: Students learn the benefits of using passwords and then play a board game to discover some strategies for creating and keeping secure passwords.

Objectives:

- Describe the functions of passwords.
- Identify strategies for creating and protecting secure passwords.

Materials:

Activity Sheets:

- *Powerful Passwords*
- *Password Game*
- *Strong Passwords*

- counters, dried beans, or other game pieces (1 per student)
- number cubes (1 for every group of two to four students)
- sheets of card stock (1 per student)
- rulers
- scissors

Maryland Technology Literacy Standards for Students (MTLSS):

Standard 2.0–Digital Citizenship:

Students will demonstrate an understanding of the history of technology, its implications on society and practice ethical, legal, and responsible use of technology to assure safety.

Activities:

- Invite students to share with the class all the online sites they like to visit where passwords are required to enter. Allow them to share some of the activities they most enjoy.
- **Ask:** *How would you feel if someone else used your password and pretended to be you on one of these sites?*
- **Distribute Activity Sheet -***Powerful Passwords.* Have students read and discuss the first two paragraphs. You may wish to add details about how adults use banks and other financial institutions, explaining that they can check their accounts, move money from one account or institution to another, and pay bills online.
- After students read **Hard to Put Together**, have them answer the question individually or in pairs. **NOTE: Postpone discussion until students have played the password game on Activity Sheet 2.**
- **Distribute ActivitySheet-** *Password Game* and discuss how to play the game with students.

- Divide the class into small groups and distribute one game piece per student and one number cube per group. Allow students to play, reminding them to pay attention to what they read each time they land on a space with directions.

- Once students have finished the game, have them list dos and don'ts for making powerful passwords. Guide them to include items such as these:
    - **Do** make passwords eight or more characters long.
    - **Don't** use your nickname as your password.
    - **Do** include letters, numbers, and symbols in your password.
    - **Do** change your password at least every six months.
    - **Don't** share your password with your friends.
    - **Do** give your password to your parent or guardian.
    - **Don't** use private identity information in your password.
    - **Don't** use your phone number as your password.
    - **Don't** use dictionary words as your password.
- Have students compare their dos and don'ts list to the answer they wrote on Activity Sheet 1. **Ask:** *Which tips did you know? Which ones surprised you?*

- **Distribute Activity Sheet -***Strong Passwords* and review each of the eight security tips for managing passwords.
- Have students infer why each tip is effective. If they are not sure, offer the following:
    - Only your parents should know your password. Never give a password to anyone elseð not even your friendsð because your friends can use your password to pretend to be you or to harass other people. They could also give it to other people.
    - Don't use passwords that are easy to guessð like your nickname or your pet's nameð because people who know you well can guess these kinds of passwords.
    - Never use any private identity information in your password because identity thieves can use this information to pretend to be you.
    - Don't use a word in the dictionary as a password because hackers use programs that will try every word in the dictionary to guess passwords.
    - Create passwords with at least eight characters because the fewer the characters, the easier it is for hackers to try every combination of characters.
    - Use combinations of letters, numbers, and symbols, which are harder to crack than just words because there are more combinations to try.
    - Change your password regularlyð at least every six monthsð because 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 students are familiar with the forms of private identity information listed in the Be CyberSmart! box, and discuss an important safety and security rule: Do not give out private identity information without permission of a teacher, parent, or guardian.

- Have students **read** and **discuss** the scenario about Jesse. They should recognize that 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 it does and does not follow.
- Have students **read** and **discuss** the scenario about Sondra. She chose her password by combining part of her first name (so), her favorite activity (swim), and the numbers of her birth month (8) and day (4). It is a safer choice because she used no complete personal identity information, and she combined at least eight letters and numbers. Have students evaluate

Sondra's password and describe the additional tips she could follow.

Closure:

- Have students follow the directions for the activity at the bottom of their sheet. Suggest that they make up a sentence that is meaningful to them or use the first line in a favorite saying or song. For example, Jesse could use ñGo Jayhawks basketballòto make the password ñg0jHkz#bllòand Sondra could use ñshe sells three sea shells by the seashoreòto make the password ñs$3CshxtCshrò
- Remind Students not to use the examples used in class as their real password.

Extension: Take Action (Optional)

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

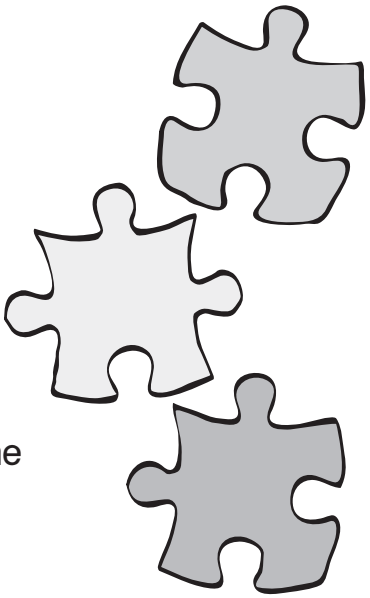
Name _____ Date _____

CyberSmart! 21st century skills for education

Powerful Passwords

Powerful passwords protect private possessions. Can you say that five times fast? It's a tongue twister, but it's true. Passwords stop other people from seeing your private information or pretending to be you. They are the keys to unlocking your special stuff on computers and online. For example, your password allows you to save your points after playing an online game.

When you're older, you'll use passwords to keep track of your money. You'll also use them to shop online. Knowing how to create powerful passwords will help keep your money safe.



Hard to Put Together

Creating a powerful password is like putting together a puzzle. The best ones are made of small pieces put together in a way that only you can remember. Good passwords are hard for your friends to guess. They are also hard for a criminal to figure out. Experts have come up with tips for making strong passwords. The more tips you follow, the harder your password will be to guess.

What do YOU think makes a powerful password?

_____

_____

_____

Be CyberSmart!®

It's okay to write down passwords. But don't carry them with you or tape them on your computer. With your parent or guardian, find a safe place at home to keep them.

Activity

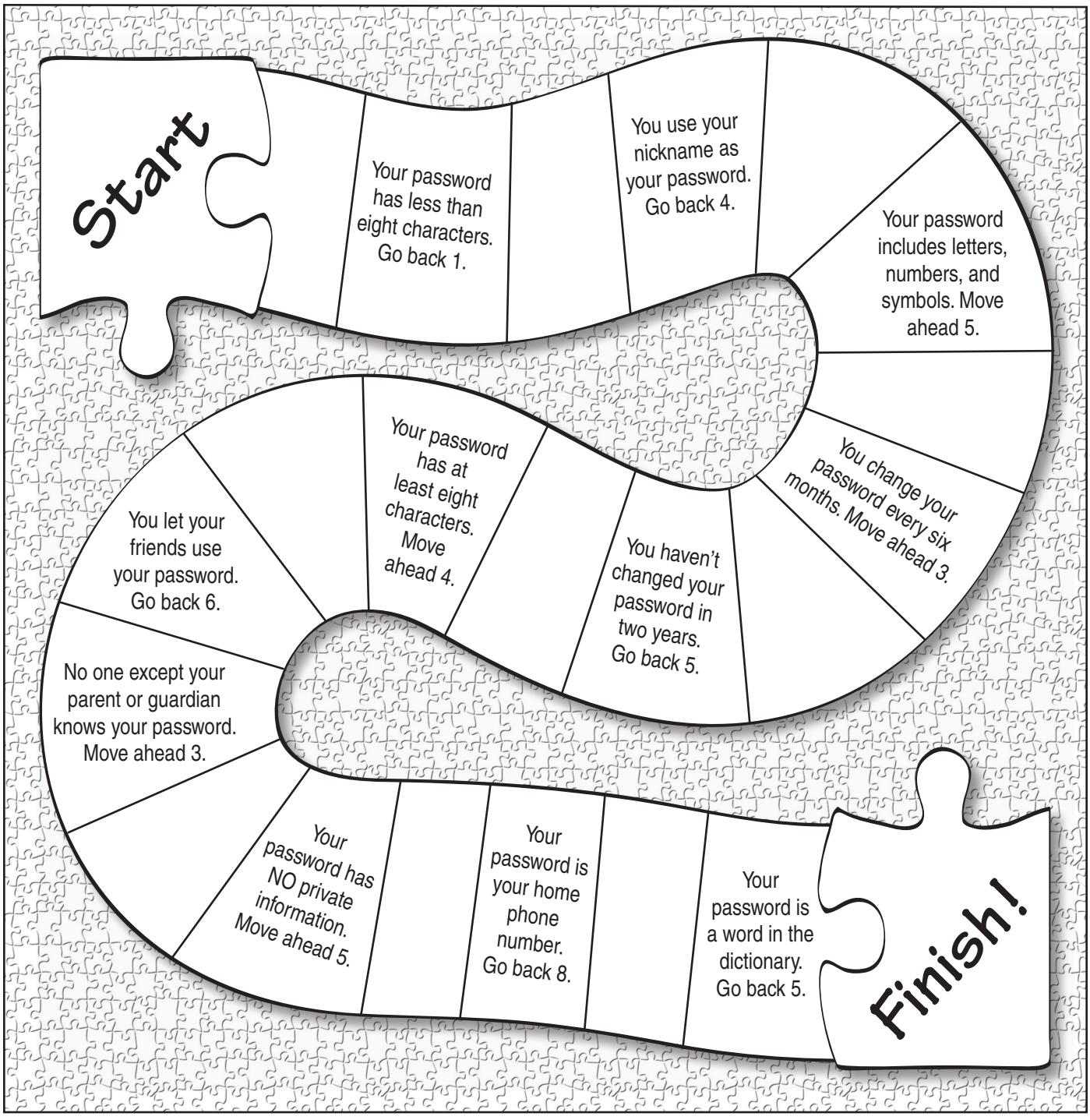
Use the game board on Activity Sheet 2 to play the password game. Use a counter or a bean as a game piece. When the game is over, try listing all the tips for making powerful passwords.

Name _____ Date _____

CyberSmart! 21st century skills for education

Password Game

Take turns rolling a number cube. Move the number of spaces you roll.
If you land on a space with directions, follow them. The first to Finish wins!



Name _____ Date _____

CyberSmart! 21st century skills for education

Strong Passwords

Strong passwords help protect your computer, your files, and your school and online accounts from being tampered with.

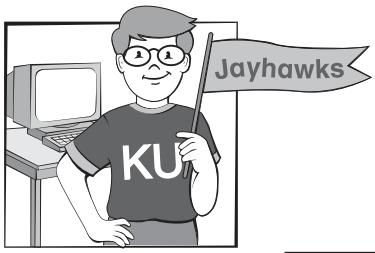
You can avoid many hassles by following these security tips.

- ☑ Only your parents should know your password.
- ☑ Never give a password to anyone else—not even your friends.
- ☑ Don't use passwords that are easy to guess—like your nickname or your pet's name.
- ☑ Never use any private identity information in your password.
- ☑ Don't use a word in the dictionary as a password.
- ☑ Create passwords with at least eight characters.
- ☑ Use combinations of letters, numbers, and symbols, which are harder to crack than just words.
- ☑ Change your password regularly—at least every six months.

Be CyberSmart!

Know the kinds of private identity information:

- full (first and last) name
- postal address
- e-mail address
- phone numbers
- passwords
- calling card numbers
- credit card numbers
- Social Security number
- mother's maiden name



Jesse lives in Lawrence, Kansas—the home of the University of Kansas. He 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?

Sondra lives in Miami, Florida. Her birthday is August 4 and she swims on a team. Her password is "soswim84." How did Sondra choose her password? Was it a safe choice? Why or why not?

Activity Using the tips above, make new passwords for Jesse and Sondra. Try making up a sentence and changing it into a series of letters, symbols, and numbers. Explain how Jesse and Sondra will remember their passwords.

Jesse _____

Sondra _____