LESSON 56

Strong vs. Weak Passwords

40 minutes | Cyber Safety

WHAT THIS LESSON DOES

Learn how to protect your online accounts by understanding the difference between strong and weak passwords. Follow simple steps to explore password basics, identify weak examples, and create secure passwords using length and varied characters.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Understand the importance of using strong passwords for online security.
- Identify the characteristics of weak passwords and why they are easy to guess.
- Understand the components of a strong password and how to create one.
- Comprehend how the length and complexity of a password affects its security.
- Analyze the strength of different types of passwords based on their composition and length.
- Apply the learned knowledge to create and use strong, secure passwords in real-world contexts.

BEFORE THE LESSON

- Open and test the interactive activities in steps 4, 8 and 9 on your own device beforehand, and check none are blocked by the school filter.
- One device per pupil or per pair for the interactive password checker and the Password Power Playground.
- Have a projector or large screen ready to work through the length and strength examples in steps 6 and 7 together.

Strong vs. Weak Passwords

HOW THE LESSON RUNS

- Introduction
- Weak Passwords
- Strong Passwords
- Strong Vs Weak Passwords
- Most Commonly Used Passwords
- Understanding Password Length and Security
- Comparing Password Strength
- Create Your Strong Password
- Password Power Playground
- Reflection

TEACHING MOVES

- 1. Introduction. Frame a password as a secret key to a locked door. Ask what could happen if someone else got the key to their game or school account, and draw out privacy and impersonation.
- 2. Weak Passwords. Read the weak examples aloud and ask pupils why each is easy to guess. Steer them off using their name, birthday or pet in any real password.
- 3. Strong Passwords. Put the four rules on the board: eight or more characters, upper and lowercase, a number, a special character. Keep them visible for the rest of the lesson.
- 4. Strong Vs Weak Passwords. Let pupils sort each password before clicking, then read the feedback. Ask them to say which rule a weak one breaks.
- 5. Most Commonly Used Passwords. Stress that hackers try these first. Ask pupils to raise a hand if they have ever seen one used, without naming their own accounts.
- 6. Understanding Password Length and Security. Work one digit example together on the board so pupils see how adding one character multiplies the combinations by ten. Keep the maths concrete.
- 7. Comparing Password Strength. Compare two eight-character passwords, one digits only and one mixed, and show how mixing character types explodes the guessing time even at the same length.
- 8. Create Your Strong Password. Have pupils build a password and watch every check turn green. Remind them this is a practice password to type here, never a real one they use.
- 9. Password Power Playground. Before anyone types, say clearly and twice: pretend passwords only, never a real one. Let pupils vary length and character types and watch the crack time change.
- 10. Reflection. Talk through the key points aloud. Ask each pupil to say one thing they will do differently when setting a password from now on.

WHAT TO WATCH FOR

- Pupils think a password made only of numbers is safe as long as it is long, such as 12345678. Use step 7 to compare a digits-only password with a mixed one of the same length, and show the mixed one takes far longer to crack.
- Pupils believe a familiar word or their own name is fine because they will remember it easily. Point back to the common passwords list in step 5 and explain that anything easy to remember and personal is also easy for others to guess.
- Pupils type a real password into the checker or playground to see how strong it is. State firmly that these tools take pretend passwords only, and explain that a real password should never be typed anywhere except its own login.

DIFFERENTIATION

- Emerging: Keep the four strong-password rules on the board and let the pupil check their attempt against them one rule at a time in step 8.
- Developing: Ask the pupil to explain to a partner why a given weak password is weak, naming the exact rule it breaks.
- Proficient: Challenge the pupil to design the shortest password they can that still passes all four checks, then use the playground to compare it against a longer one.