

Strong vs. Weak Passwords

40 minutes

Cyber Safety

WHAT THIS LESSON DOES

In this lesson, you will explore what passwords are and why they matter for keeping your accounts safe. Learn to spot weak passwords that are easy to guess, and create strong ones that mix uppercase and lowercase letters, numbers, and symbols. Practise with quizzes, tools, and reflections to build secure habits.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Understand the purpose and importance of passwords in protecting online accounts.
- Identify characteristics and examples of weak passwords that are easy to guess.
- Recognise features and examples of strong passwords that enhance security.
- Differentiate between strong and weak passwords through practical assessment.
- Apply principles to create and evaluate secure passwords using length and character variety.

BEFORE THE LESSON

- Open and test each interactive yourself first: the strong-vs-weak sorter (step 4), the password builder (step 8) and the Password Power Playground (step 9), so you know what green checks and the power meter look like.
- One device per pupil or per pair; the sorting and building activities are done on screen.
- Set the ground rule out loud before pupils start typing: never type a real password into any of these, only a made-up practice one.

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. Lead with the key analogy: a password is a secret key. Ask who they would trust with the key to their house, then link that to who should know a password.
- 2. Weak Passwords. Draw out why the listed passwords are weak by asking pupils to guess each one aloud. If the class can guess it in seconds, that is the point made for you.
- 3. Strong Passwords. Fix the four ingredients on the board: length, upper and lower case, numbers, symbols. Pupils will reuse this checklist in steps 8 and 9.
- 4. Strong vs Weak Passwords. Have pupils commit to weak or strong before tapping, then read the feedback reason together. Slow the pace so they connect the verdict to the rule.
- 5. Most Commonly Used Passwords. Stress the twist: these are dangerous because they are popular. Ask why a hacker would try common passwords first.
- 6. Understanding Password Length and Security. Walk the numbers-only examples slowly so pupils see the count jump with each added digit. Let the growth surprise them rather than just stating it.
- 7. Comparing Password Strength. Keep the fixed 8-character, 1,000-guesses-per-second setup so pupils compare like with like. The only variable is character variety, and that is the lesson.
- 8. Create Your Strong Password. Repeat the practice-password rule, then challenge pupils to turn every check green. Circulate to spot anyone typing something real.
- 9. Password Power Playground. Let pupils change the guesses-per-second setting and watch the crack time shrink. Ask what this shows about a faster computer facing the same password.
- 10. Reflection. Take this as a spoken discussion. Ask pupils to name one thing they will do differently next time they make a password.

WHAT TO WATCH FOR

- Pupils think a password using their name, pet or birthday is safe because it is hard for a stranger to know. Point out that this personal information is often easy to find or guess, and that a computer trying millions of guesses does not need to know them personally.
- Pupils believe swapping a letter for a lookalike symbol on a common word (like p@ssword) makes it strong. Test it in the Playground in step 9. Show that it is still short and still a known pattern, so the crack time stays low.
- Pupils treat length and variety as either-or, choosing a long simple password or a short mixed one. Return to step 7 and show that strength comes from combining both. Have them build one in step 8 that is long and mixes all four character types.

DIFFERENTIATION

- Emerging: Sit them with a partner for the interactives and let them read each feedback message aloud together before moving on. Keep the four-ingredient checklist visible on the board so they can tick it off while building in step 8.
- Developing: Ask them to say why a password is weak or strong in their own words before they tap an answer in step 4. Have them predict whether their step 8 password will pass all checks, then confirm on screen.
- Proficient: In step 9, challenge them to find the shortest password that still takes a long time to crack, and explain the trade-off. Ask them to invent a memorable but strong practice password and explain to you why it is hard to guess but easy for them to recall.