

The Dangers of Sharing Passwords

40 minutes

Cyber Safety

WHAT THIS LESSON DOES

In this lesson, you will explore why passwords protect your online accounts like a secret key. Learn the risks of sharing them, such as account takeovers or privacy breaches. Discover who to never share with, how to respond to requests, and tips for creating strong, unique passwords to stay safe.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Understand the purpose of passwords in safeguarding online accounts and personal information.
- Recognise the risks and potential consequences of sharing passwords with others.
- Identify individuals and situations where passwords must never be disclosed.
- Develop strategies for responding to requests for passwords and seeking appropriate support.
- Adopt practical habits for creating and protecting strong, unique passwords.

BEFORE THE LESSON

- Open and test the chat simulator interactive in step 7 on your own device beforehand, and check your school filter does not block it.
- Devices ready for pupils to reach the simulator, or a large screen if you plan to run it as a whole-class activity.
- Have your school's report-a-worry procedure to hand so 'tell a trusted adult' points somewhere concrete.

The Dangers of Sharing Passwords

HOW THE LESSON RUNS

Introduction

Why do we have passwords?

What can happen if we share our passwords?

Who Should You Never Share Your Password with?

What if someone asks for your password?

How can we protect our passwords?

Chat Simulator

Conclusion

TEACHING MOVES

- 1. Introduction. Open with the house-key comparison and let pupils extend it: what else has a key, and what happens if a stranger gets one? Keep it quick, it frames the whole lesson.
- 2. Why do we have passwords? Draw out the lock idea, then push past it: passwords protect messages, settings and identity, not just entry. Ask what could a stranger do if the lock were off.
- 3. What can happen if we share our passwords? Land the point that sharing means losing control, even with a friend. Name impersonation and being locked out as the two big real consequences.
- 4. Who Should You Never Share Your Password with? Handle the 'but they're my friend' objection head on. Stress that online contacts may not be who they claim, so the rule holds for everyone.
- 5. What if someone asks for your password? Have pupils say the refusal aloud: 'No, I don't share my password.' Model that they owe no explanation and should tell a trusted adult after.
- 6. How can we protect our passwords? Turn the four habits into a checklist pupils can repeat: keep secret, make strong, use different ones, don't leave written down where others see.
- 7. Chat Simulator. Let pupils work the simulator and notice the pressure tactics, prizes, guilt, threats. Afterwards ask which felt hardest to refuse and why.
- 8. Conclusion. Close on the secret-key message and check retention: ask three pupils to name someone they'd never share with and what to do if asked.

WHAT TO WATCH FOR

- Pupils think it is fine to share a password with a best friend or to log in 'as a joke'. Stress that sharing hands over control regardless of trust, and that a joke can still get someone locked out or impersonated.
- Pupils believe an online friend is safe to trust because they chat often. Point out that online, anyone can claim to be someone else, so you cannot really know who is asking.
- Pupils feel they must give a reason or apologise when refusing a request. Rehearse a short, firm 'No, I don't share my password' and confirm no explanation is needed.

DIFFERENTIATION

- Emerging: Give the sentence to say word for word and let them practise it with a partner before the simulator.
- Developing: Ask them to run the simulator and then name aloud which pressure tactic was used on them.
- Proficient: Have them write or say a strong-password rule of their own and explain why it makes an account safer.