



Fraud in the Workplace

Key Stage 5 | Lesson 1



QUALITY
ASSURED
RESOURCE
PSHE ASSOCIATION



Resources Required

Box or envelope for questions

Resource 1: Case file (one per pair)

Resource 1a: Case study (support option – as required)

Resource 2: Problem pages (one per group)

Key Words

Application Fraud

Cyber Security

Social Engineering

Smishing

Phishing

Vishing

Malware

Context

This lesson for students in key stage 5/post-16 settings has been developed by Cifas, the UK's leading fraud prevention service. It extends the anti-fraud education lesson pack for secondary students, by exploring real-world examples of fraud in the workplace, and how students can prepare to enter the workplace through better understanding of cyber security. No lesson should be taught in isolation, and this lesson would work well as part of wider learning about digital safety or finance, careers and the workplace.

Learning Objective

To learn about cyber security and fraud risks in the workplace.

Learning Outcomes

Students will be able to:

- explain the risks of application fraud for individuals and workplaces
- identify common workplace scams and security systems in place to protect against them
- evaluate real-world responses to social engineering techniques

Climate for Learning

Refer to the Teacher guidance before teaching this lesson. This includes information about establishing a safe learning environment, such as setting out ground rules and language sensitivities. It also supports teacher subject knowledge about types of fraud and consequences of fraudulent behaviour.

Lesson Summary

Activity	Description	Timing Total: 60 mins
Baseline Assessment	Students complete a structured mind map to demonstrate what they already know about fraud and how it can occur in the workplace.	5 mins
Introduction	Introduce ground rules, learning objective and outcomes. Provide a brief introduction to types of fraud at work.	5 mins
Applying for Work: Application Fraud	In groups, students review a scenario involving application fraud, highlighting the individual and workplace consequences.	15 mins
At work: Workplace Fraud	Students read problem pages of young people who have encountered fraud in the workplace and consider what support might be in place in workplaces for reporting incidents.	10 mins
Protecting Workplaces	In pairs, students evaluate the effectiveness of a range of human and technological solutions to protect workplaces from fraud.	15 mins
Signposting Support	Make sure students are aware of where they can seek further information and support, including how to report fraud.	3 mins
Endpoint Assessment and Personal Reflection	Students revisit their mind map from the start of the lesson to demonstrate their progress. They respond to a personal reflection question.	7 mins

Baseline Assessment



Slides 2 and 3

Introduction



Slides 4 and 5

Baseline Assessment Activity

Show [slide 2](#) and remind students of the agreed ground rules for PSHE lessons. Remind them they can submit questions to the question box at any time, anonymously if they prefer.

Then show [slide 3](#) and ask students to complete a mind map focused on the term 'fraud', using the prompt questions and categories shown on the slide. They should do this individually and without discussing the topic, so you get an accurate reflection of what students already know, understand and believe about fraud before the lesson. This will help you to tailor your teaching and questioning throughout the lesson, for example to address misconceptions.

If time allows, take some feedback from students and collate a class mind map of key ideas.

Introduction

Using [slide 4](#), introduce the learning objective and outcomes for the lesson, and explain that this lesson will help them to think about fraud in the workplace, and why it is important for them to learn about, as young people entering the workforce.

On [slide 5](#), give the definition of fraud and the statistics which reflect the prevalence of some fraud types, so that those who haven't learnt about fraud before are supported to complete the lesson activities.

Core Activity



Slides 6 and 7

Applying for Work: Application Fraud

In pairs, give students [Resource 1: Case file](#). Ask them to read through the case, and discuss or write responses to the questions on [slide 6](#):

FACTS:

what type of fraud was committed?

MOTIVATIONS:

why did Jesse do what they did?

CONSEQUENCES:

what are, and what might be, the consequences for Jesse?

IMPACTS:

what might be the short- and long-term impacts of what they did?

EFFECTS:

are there any effects on others (e.g. the workplace, the applicants)?

Once students have considered all questions, take feedback and use [slide 7](#) to draw out the key learning points from this case study:

- *Jesse has committed application fraud (lying about previous work experience, academic grades, and using a fake reference).*
- *Jesse wanted the job, pay and holiday, and they felt it wasn't fair for them not to have the chance; they had already told everyone they'd applied so maybe felt extra pressure to do so.*
- *Jesse is clearly struggling to keep up with the demands at work and with the online learning courses. It's likely they won't be able to complete the apprenticeship or will be asked to leave by the employer, which could affect their self-esteem, motivation to apply for future roles, and their future employment chances.*
- *If the workplace finds out Jesse committed application fraud, this can be reported and they may get a criminal record. This can affect future job applications, mortgage applications and they may be considered less trustworthy by others. Even if Jesse is not caught, they are still in a difficult situation of working in a role they are not properly qualified for, struggling to keep up with the demands and getting into trouble at work; they are also likely to get a poor reference from this employer when they leave.*
- *The mentor, boss and other colleagues are probably under stress trying to manage and support Jesse with this apprenticeship. The clients have had incorrect calculations on their accounts so may have lost or mismanaged money as a result, and the company may face reputational risks if the clients complain. There are other applicants who would have been better suited to the apprenticeship who have missed out on the opportunity because it was given to Jesse.*



Support:

Give students Resource 1a: Case study as an alternative version.



Challenge:

Ask students to discuss what advice they would give to someone considering committing application fraud and summarise this in one or two sentences.

Core Activity



Slides 8-10

At Work: Workplace Fraud

On [slide 8](#) check students' familiarity with key terms by showing the names of different social engineering techniques and asking students to match them to the definitions.

Then, show [slide 9](#) and give small groups or pairs [Resource 2: Problem pages](#), which each describe young people affected by a different type of workplace fraud. Ask students to read all the workplace issues young people have encountered, and to discuss: What should someone do if they think they might have been targeted by fraud at work?

- Who could they tell?
- What could they say?
- Why is it important?

Use [slide 10](#) to emphasise the key learning that:

- *It is essential to tell someone at work straight away if they think they have been targeted by fraud. This will usually be their line manager, could be someone in charge of IT or cyber security at their workplace, or if appropriate, someone in senior leadership.*
- *Phrases like "I got a strange email/message earlier..." "I'm worried I've been targeted by a fraud attack..." "I think I've clicked a link I shouldn't have..." "Has anyone else had an unusual email?" "I think I've made a mistake, but I wanted to tell you straight away and help to put it right however I can..." are all helpful ways of raising the alarm.*
- *Even if it feels worrying or they think they might get in trouble, the sooner someone tells their workplace, the less damage is likely to be done by the fraud attack. If they have been targeted, it is also possible other people in the same workplace have been or will be approached, so everyone needs to be alert to the risk.*



Challenge:

Ask students to discuss what factors might make fraud hard to spot, especially for a young person who is new to the workplace?

Students might suggest: Wanting to impress the boss, worried about challenging requests, not being clear on systems or policies, not provided with training to spot fraud attempts, afraid to ask questions or be seen to not know what they are doing.

Core Activity



Slides 11 and 12

Protecting Workplaces

Next, explain that workplaces have a range of strategies in place to help keep their data and information safe from fraud attacks. These often involve a range of technological solutions and human responses. Show the range of strategies on [slide 11](#), and check students understand what each of these means.

Then ask them to work in the same small groups to rank these strategies from the one they think is the most helpful strategy, down to the least helpful. Can they give reasons for these judgements?

Finally, show [slide 12](#) and ask students to choose one of the characters they met in [Resource 2: Problem pages](#), and to write a paragraph of advice on what the character should do next.

- What should they do now?
- Who could they tell?
- What might help them or their workplace in the future?
- What should they do differently next time?



Support:

During the ranking activity, ask students to select their top solution and explain their reason why this is the best solution.

Signposting Support



Slide 13

Plenary/ Assessment for and of learning



Slide 14 and 15

Extension Activity Slide 16

Signposting Support

Remind students where they can access support if concerned about fraud or cyber security, both at home and at work, this includes organisations such as:

- Cifas: www.cifas.org.uk/youngpeople
- Report Fraud: www.reportfraud.police.uk
- Take 5 to Stop Fraud campaign: www.takefive-stopfraud.org.uk

If they think they have been targeted by fraud at work, they should tell their employer immediately.

If they are concerned about any online behaviour, including fraud in a personal context, they can always speak to trusted adult at home or at school.

Endpoint Assessment

Show [slide 14](#) to revisit the mind map students created at the start of the lesson. They should now use a different colour pen to add new learning from today's lesson. This might include; new information, key terms or systems they have learnt about, changing their initial ideas if they were incorrect or inaccurate, giving further detail on their initial ideas. This will help to demonstrate individuals' progress.

Personal reflection:

Finish by asking students to reflect privately on the question shown on [slide 15](#): What do you think is the most important thing you've learnt today for your future in the workplace?

As this is a personal reflection question, students do not need to share their responses with the rest of the group.

Extension Activity

If time allows, or to extend the thinking of specific students in your group, ask them if they can suggest any other solutions they think workplaces could introduce to protect against fraud in the future. They can consider both human or technological strategies, and should explain what their solutions are, and why they think these would be helpful.