
Identity Fraud & Data Protection

Key Stage 3 | Lesson 2





Resources Required

Box or envelope for questions

Cifas video: Data to Go

Resource 1: Safe or Unsafe?
Scenarios (one per student)

Resource 2: What is Personal
Identity? (support option, as
required)

Resource 3: Diamond 9 of Top
Tips (one per group)

Key Words

Identity Fraud

Social Media

Online Data

Firewall

Antivirus

Context

This is the second of two key stage 3 lessons developed by Cifas, the UK's leading fraud prevention service. This series also has lessons designed to extend learning at key stages 4 and 5, along with a lesson for students with SEND. The lessons teach young people to protect themselves from fraud through building awareness of how to identify fraud and how to protect personal data online. This lesson focuses on the importance of protecting personal details online to minimise the risk of identity fraud.

Learning Objective

To learn about the importance of online safety strategies to protect people from fraud and keep online data secure.

Learning Outcomes

Students will be able to:

- identify information that is private and that which is safe to share publicly online
- explain the risks of sharing personal information online
- describe a variety of ways to keep online data secure

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 the development of teacher subject knowledge into types of fraud and consequences of fraudulent behaviour.

Lesson Summary

Activity	Description	Timing Total: 60 mins
Introduction	Revisit ground rules and outline the learning objective and outcomes.	5 mins
Baseline Assessment	Students consider whether different online activities are 'safe', 'unsafe' or they are 'unsure' to establish their starting points.	5 mins
What is Personal Identity?	Define identity fraud and in pairs, students decide what makes up someone's personal identity, considering which aspects of this are private and public.	10 mins
Data to Go	Students explain the risks of over sharing personal information online.	10 mins
Top Tips	Based on their learning, students create top tips someone could use to protect from identity fraud when posting online.	10 mins
Giving Advice	Students decide if opinions about identity fraud are correct and then give correct advice or additional information about these.	10 mins
Signposting Support	Signpost students to where they can seek further information and support, including how to report fraud.	5 mins
Endpoint Assessment	Students work in small groups to complete a recall relay, identifying learning from this and the previous lesson.	5 mins

Introduction



Slides 2 and 3

Baseline Assessment



Slide 4

Introduction

Revisit ground rules using [slide 2](#) and introduce the lesson objective and outcomes on [slide 3](#). Let students know they can use the question box to add a question, with or without their name, during the lesson. Explain that today they will be thinking about identity fraud, how it is committed and the importance of protecting personal information online.

Baseline Assessment Activity

Give students [Resource 1: Safe or unsafe scenarios](#). Ask them to decide if they think the action in each scenario is 'safe', 'unsafe' or 'it depends'.

After students have responded individually, ask them to compare their answers with a partner to see if they made the same decisions. Take some feedback from the pairs, asking them to explain the reasons for their choices. Use this feedback to gauge students' starting point and to adapt teaching and questioning throughout the lesson accordingly.

Core Activity



Slides 5-7

What is Personal Identity?

Ask students to suggest what they think identity fraud is by thinking back to the learning from the previous lesson. Then share the definition on [slide 5](#). Show students the list of elements that make up a person's identity on [slide 6](#). In pairs, ask students to give examples of the types of information that might come under each heading on the slide, using the first one to model this:

Personal details and information – examples include name, date of birth, address, previous addresses, etc.

Briefly feedback some examples for each element of personal identity, using the animations on [slide 6](#). Next, ask students to group these features of personal identity into 'public' and 'private'; those they think are suitable to share with other people/online and those that should only be shared with people they know and trust.

When students have finished sorting their lists, ask them to highlight those parts of a person's identity they think a fraudster might use to impersonate them to a bank or company.

Take feedback and emphasise that someone trying to commit fraud is interested in lots of different pieces of information about a person, not just their date of birth and address. Fraudsters will also use information about a person's interests and hobbies to befriend a target and trick them into giving over more information. So, the more that someone shares publicly online, the more at risk they are of being susceptible to fraud.



Support:

Give students **Resource 2: What is personal identity?** which has the elements of personal identity and examples on for students to match up.



Challenge:

Ask students to discuss why a fraudster might be interested in finding out each element of a person's identity and ask them to share some ideas during the feedback session for this activity.

Core Activity



Slides 8 and 9

Data to Go

Show the '[Data to go](#)' video on [slide 8](#), which demonstrates how a fraudster might be able to access personal information online:

In small groups, ask students to discuss the following questions:

- How did people react in this video when they were presented with their information?
- What parts of their identity were the team able to find out about them?
- What could these people have done to protect their information?
- What do you think a fraudster would use this information for?
- What might be the consequences of having this information publicly available?

Take feedback, drawing out the following key learning:

- *People in this video were surprised and shocked at how much the coffee shop staff knew about them, just from interacting with a social media post.*
- *The team could find out anything they had shared online: phone number, email address, mother's maiden name, bank, addresses, whether they have children, job, schools they went to, religion, nationality, etc.*
- *To protect themselves these people could:*
 - *Think carefully before sharing information online as it then becomes public, including to strangers. If someone shares information online, they need to be prepared for anyone (family, teachers, future employers, strangers, a fraudster) to see that content.*
 - *Avoid sharing too many distinguishing features, such as school logos, addresses, location check-ins, as a fraudster might use this to build up a picture of a person's identity.*
 - *Make sure that electronic devices are protected using anti-virus software, strong passwords and by turning off location tracking.*
 - *Don't access personal information on public Wi-Fi networks (for example doing online banking using a train or café's free Wi-Fi) - these are not secure networks and others may be able to access someone else's device.*
- *While in this video the personal information was only being accessed to demonstrate an important security point, a fraudster might use this information to apply for loans, credit cards, or to befriend and trick someone online into revealing even more about themselves.*
- *Having this information publicly available could make people more likely to be targeted by fraudsters, which can lead to long-lasting emotional and reputational damage, problems getting credit in the future and to being unable to retrieve stolen money.*

Core Activity



Slide 10

Core Activity



Slide 11

Top Tips

Thinking about their learning so far, ask each small group to create a list of 'tips' students would recommend, to help protect from identity fraud when posting online.

Once students have made their initial suggestions, give each group **Resource 3: Diamond 9 top tips** and ask them to prioritise these tips into a diamond shape, demonstrating what they believe to be the most important tip to the least important. Ask for feedback, including the reasons for their choices.



Support:

Give students five cards from **Resource 3: Diamond 9 top tips** and ask them to rank them, demonstrating what they believe to be the most important tip to the least important.



Challenge:

Ask students to explain why it is important that people follow each of these tips when protecting themselves from identity fraud.

Giving Advice

Show **slide 10** and ask them to look at the statements made by the character who is confused about identity fraud. Stress that all the statements are incorrect and ask students to give some correct advice or additional information in response to each statement.

Take feedback, identifying:

'I thought that your bank might call and ask you for your PIN or password sometimes.'

INCORRECT:

A bank will never under any circumstances ask someone for their full PIN or password and people should never give these details out to a caller.

'I heard that if you have been a victim of identity fraud once you won't be a victim again.'

INCORRECT:

Fraudsters share stolen personal details with each other. A fraudster may try to use someone's identity to commit another type of crime.

'I heard that identity fraud is a victimless crime – is that right?'

INCORRECT:

Identity fraud can be very distressing for the target. They may struggle to get all their money back, and the emotional and reputational damage can be very harmful. Someone who has been a victim should seek advice and help from victim support organisations.

'People say there's no point reporting it if you think you might have been a target of identity fraud, unless you're sure.'

INCORRECT:

The sooner it is reported, the easier it is to resolve and the less damage a fraudster can do. Fraudsters move quickly when impersonating someone, the quicker someone contacts the organisation concerned, the faster they can freeze an account or prevent criminals ordering goods in their name. So even if someone is not sure if they have been targeted, it's important to report it as soon as possible.

Signposting Support



Slide 12

Plenary/ Assessment for and of learning



Slide 13

Extension Activity Slide 14

Signposting Support

If someone is worried about fraud or wants to find out more, explain where they can seek further support.

They can speak to:

- a parent/carer or other trusted adult outside of school
- a tutor, pastoral lead or other trusted staff member in school

And/or visit:

- Report Fraud: www.reportfraud.police.uk
- Childline: www.childline.org.uk | 0800 1111

Endpoint Assessment

Organise students into teams and ask each team to stand in a row in front of a large sheet of paper (which should be stuck to a wall). Give the first person in each team a marker pen. Ask them to write down one thing they have learnt from this or the previous lesson. They should then pass the pen to the next person in their team and join the end of the row. Tell each team that they will be timed and that the team with the most ideas at the end of the time will be the winners.

Continue the activity for 2-3mins, allowing all members of the team to write at least one thing on the sheet, trying not to repeat anyone else's answers. As a class, read through the ideas written at the end.

(Depending on the size of the class and resources available, carry out these key messages relays with several teams, for example 4 or 6 groups, so that everyone can participate in the time allowed.

Extension Activity

Ask students to design a television advert to warn people about the risks associated with identity fraud. Students should create a storyboard showing what would be included in their advert, including ways to keep personal information safe online.