



Introduction to fraud and scams

Age range: 11-14

 **BARCLAYS** | LifeSkills



Session overview

This lesson belongs to a suite of Money Skills lessons for young people aged 11-14.

Time	Key learning outcomes	Resources
50 mins	<p>By the end of the activity students will be able to:</p> <ul style="list-style-type: none"> Understand the difference between fraud and scams. Recognise some different types of fraud and scams and perceive different financial mistakes and threats. Understand how to protect their data, keep their financial information safe and develop good online habits. Define what a money mule is and understand the negative consequences. 	<ul style="list-style-type: none"> Introduction to fraud and scams presentation slides.



The [Money Skills 11-14 lessons](#) support students to develop helpful financial skills for their future, prepare them for the world of work, and keep up to date with modern financial changes. They are accredited with the Young Money Financial Education Mark, recognising them as recommended financial education resources.

This lesson plan is designed to be used in tandem with a PDF containing interactive activity slides.

Contents

Activities	Time	Page
Activity one: Managing money and introducing fraud	30 mins	3
Activity two: Different fraud types, online fraud and money mules case studies	15 mins	3
Activity three: Protecting against fraud and scams	5 mins	7

Please note that the Spot the faker activity in this lesson plan needs to be run from a desktop or laptop. The activity isn't currently supported to be run from a mobile or tablet.

There is Money Skills content to suit a range of ages and abilities – take a look at our 5-11, 11-14, 14-16, 16-19, 19+ resources, which focus on topics such as attitudes to money, money management and risk, and financial independence.

Activity one

Managing money and introducing fraud

1. Explore Sam's habits and influences



- Start by introducing your students to Sam's story, using **slides 2-5**. You can print **slide 6** for your students to use if you would like them to make notes as they explore Sam's story.

What are Sam's bad habits? What are his good habits?

Do you think Sam has any savings?

How could Sam stay safe and avoid being a victim of fraud?

What could he do to improve his money management?

- Introduce your students to the concept of fraud, that it is when your account or card has been accessed, stolen or used without your knowledge (and that it can also be when a fraudster opens an account using your identity). Ask students what they know about the ways that online criminals can use your personal details to make purchases or open accounts in your name. Use the terms in the next activity to prompt if needed.

Do they think Sam is at risk from fraud?

Activity two

Different fraud types, online fraud and money mules case studies

1. Introduction to types of fraud

- This section introduces students to the most common types of fraud, what to look out for, and how to protect themselves from risk. You could coincide this lesson with national campaigns such as Cybersecurity Awareness Month or use the resources as part of the ['Take Five' campaign](#).
- Display **slide 7** to recap the fraud definition and introduce your class to what is meant by scams.
- Fraud is becoming increasingly sophisticated with changing technology along with criminals' use of that technology in addition to criminals getting better at tricking others into giving them the information they need to commit fraud and scams (called social engineering).

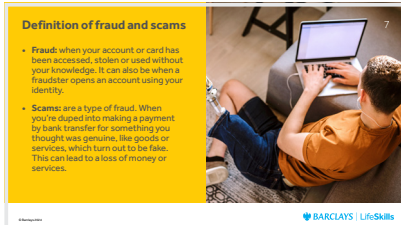
UK Finance reported that in 2023 there was a 34% increase in the reports of online purchase scams, where victims lost an average of £548 each. By comparison, there was a 1% rise in investment scams, with an average loss of £10,540 per victim.

For unauthorised mobile banking fraud, there was an increase of 62% in 2023 compared to the previous year, with an average loss of £2,270.

Source: ukfinance.org.uk

Activity two

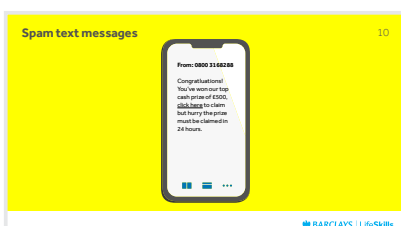
Different fraud types, online fraud and money mules case studies



- It's important that your students understand how to keep their personal information safe, as fraud and scams can take many forms, such as a text message, email, letter or phone call, and can have serious consequences including losing money, your bank account being closed down (which may affect the financial products and services you can access in future) and even facing criminal charges.
- Explain that it is important for students to understand the signs to look out for and that the most common type of scams for their age group now takes place on social media.
- Introduce your students to the difference between fraud and scams and some of the most common types, using the terms and definitions on **slides 7-9**.

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing	Fraudsters send emails that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, for example, due to an unauthorised payment.
Quishing	A scam to access valuable personal details by using QR codes which ask you to download an attachment or follow a link to a website containing malware, which can collect secure information.

2. Spot the faker



- Explain that fraudsters also use spam text messages to trick people out of money – this is called smishing. Divide your students into small groups and starting on **slide 10** ask them to decide if the texts could be spam, ask groups to look at the first example then come back as a group to discuss each of the tips which appear when you click on the slide, before moving onto the next text message. There are three text message examples in total.

Activity two

Different fraud types, online fraud and money mules case studies

Example 1

Phone number	A number you might not recognise, but sometimes they are created to look similar to a number you might recognise. This is called number spoofing.
Spelling mistakes	Spelling mistakes can be a sign it's not from a genuine sender. In this text, there is a spelling error in 'Congratulations'.
Offering a prize or reward	Tries to entice people in and excite them without thinking, regarding a competition they have not entered.

Example 2

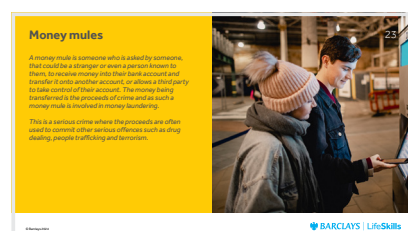
From	Can appear to be from a professional company, even one you might recognise.
Details about your parcel	This is designed to spark your curiosity to see what the package is.
Click here	Be careful if you are asked to click on a link as you might be directed to a fake website where your login and personal details are requested and stolen, or your device could be infected by a virus.

Example 3

Closed permanently	Fraudsters can make you panic in an attempt for you to respond quickly without thinking.
Spelling/grammar mistakes	Spelling mistakes can be a sign it's not from a genuine sender. In this text, there is a grammar error ('two' rather than 'to').
From	Can seem like it's from a company you know and trust.
Call 0800 6817277	Be careful if you are asked to call a number, you could potentially be directed to speak to the fraudsters who would try to get login or personal details in an attempt to steal money.

- Highlight that sometimes fraudsters will claim the spam text message is from a family member or friend saying that they have lost their phone for instance to explain why you don't recognise the number. Remind your students that if something sounds too good to be true then it probably is.

3. Case studies



- Now show **slide 23** and read out the definition of a money mule. **Slides 24 and 25** feature case studies which discuss money mules. Print a copy of each of the case studies or display them on tablets/PCs. Small groups should read through Priya's case study. Explain that this is an example of a mule scam called 'deets and squares', a common scam affecting young people.
- Use the questions below to discuss the case study as a class, making sure that they understand that in this instance Priya has acted illegally, and that there are serious implications.

Activity two

Different fraud types, online fraud and money mules case studies

Can students identify the red flags from the case study?

(e.g. approached by someone, easy way of making 'quick' cash, was asked to share her bank details, offered money with unknown origin, moving money and being complicit in the crime).

What signs could she have spotted to stay safe?

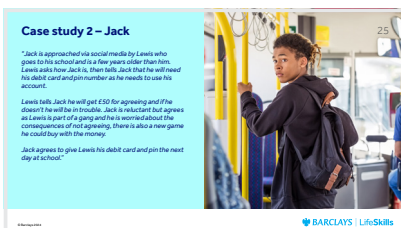
(e.g. she was approached unexpectedly, it sounds too good to be true, being asked to share her bank details).

What could she do differently next time?

What might the consequences be?

(e.g. your bank account can be closed down, which may affect the financial products and services you can access in future, and you can receive a prison sentence).

Where could she have gone to for help when she was approached?



- Now ask students to work through the same questions, giving time for them to note them down, in small groups to discuss Jack's case study on **slide 25**. Ask each group to present their opinions and key points back to the rest of the class.
- Split students into small groups and display **slide 26**. Ask them to discuss what they would do if they were approached via the different methods displayed on the slide? How could they protect themselves in future? Each group to share views around one channel with the rest of the class.
- Discuss what an approach on social media might look like. Display **slide 27** to highlight that fake opportunities can be marketed as 'jobs with no experience necessary' and the chance to make 'quick cash'.

4. Quick quiz

- Recap your students' knowledge by asking the class to answer the quiz questions on **slide 28** in groups. Then go through the answers below.

1. What is the most common way 12- 18 year olds are approached by scammers?

Social media.

2. What is an attempt to get sensitive information by texts or SMS called?

'Smishing'.

3. What is fraud?

Transactions carried out by a third party which are not authorised by the customer.

4. What is a scam?

Transactions in which the customer has been convinced or coerced to make the transaction.

Activity three

Protecting against fraud and scams

Summary: student sheet

29

Top tips for staying safe online

1. Check which personal information is public on your social media accounts, e.g. your birthday, hometown, pet names, holiday dates, job title. Think about how you use this information to share your identity and safety for bank accounts or your products or your name.
2. Be wary if you see encouragement to click on an unknown link – if you're not sure, visit the organisation's website directly.
3. Never share your PIN, bank details or passwords with anyone who contacts you through text, email, phone or in person, and don't write them down. Never let anyone else access your account.
4. Remember that letting someone else use your bank account is a potentially serious crime which could damage your financial future, so take time to think it through and talk to an adult you trust.
5. Phone organisations directly from the number listed on their website to verify who is contacting you.
6. Password protect your device using random words and include symbols, numbers and capitals. Set passwords to be at least 10 characters long and don't use the same password for different accounts.
7. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping.
8. Hover over links before clicking on them to reveal the web address destination.
9. Install anti-virus software on your laptop and any other personal devices and keep it up to date.
10. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend. Remember not to talk to strangers in person or online, even if they send follow-up messages. Report the user to help.

BARCLAYS | LifeSkills

- Ask your students to suggest some ways which they can protect themselves against online fraud before going through the ways shown on **slide 29**.

Extension

Task students with creating a poster or short film that shares top tips about how to keep personal and financial information safe when paying or managing money using digital methods.

For inspiration and research, you could signpost students to [Explore Get Safe Online](#) for relevant content.

Summary

- Ask your students to put forward the key learnings from the session, using the information on **slide 29** to help. You may want to print this slide as a takeaway for your students.