



Session overview

This lesson, focused on money attitudes, common money-related mistakes and best practice for keeping financial information safe, is one of four Money Skills lessons for young people aged 11-14.

Time	Key learning outcomes	Resources
90 mins	By the end of the activity students will be able to: Highlight some of the influencers on our attitudes to money and how we form good and bad habits	 Dealing with financial dilemmas presentation slides Make It Through the
	 Recognise common financial mistakes and threats, and understand how to improve financial health Understand the different ways they could be affected by fraud and how to keep financial information safe 	Month interactive tool



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. Each lesson has 90 minutes of core activities, along with suggested extension activities and signposting to supporting LifeSkills content and relevant external links. 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: Icebreaker – Money and me	20 mins	2
Activity two: Managing money	30 mins	3
Activity three: Fraud and identity theft	30 mins	5
Summary	10 mins	8

There is Money Skills content to suit a range of ages and abilities – take a look at our 7-11, 14-16, 16-19 and 19+ resources, which focus on topics such as attitudes to money, money management and risk, and financial independence.

Please note that this lesson includes figures used in calculations such as student loan thresholds, NI contributions or similar. These figures were correct at the time of publication but may have changed by the time you use the resource as they are usually updated by the Government on a yearly basis.

© Barclays 2023. Modification of this lesson plan is not permitted. Use of this lesson plan is governed by the LifeSkills terms and conditions which can be found at barclayslifeskills.com/terms-and-conditions



Activity one

Icebreaker - Money and me

1. Discuss attitudes to money



- Explain that attitudes to money and financial behaviours can be influenced by many factors. Display **slide 2** and ask students to spend a few minutes in pairs discussing each statement
- Ask students to present back their ideas, but emphasise that there is
 no right or wrong answer. For example, borrowing money in the form of
 a student loan or for a mortgage on a house is not 'bad' if you can afford
 to make the repayments; or, it's sensible to put some money aside on
 payday so that you have savings for emergencies. Remind the group
 that it's important to understand how we can change our decisions and
 behaviour to avoid potentially negative consequences from our actions

Who or what do they think influences these opinions?

Explain that we develop our attitudes to money at a young age, and this is influenced by messages around us.





Activity two

Managing money

1. Explore Sam's habits and influences



Use slide 3 to read through Sam's story and ask students to discuss his
financial habits and influences using the questions below as prompts.
If you have completed Recognising your money personality or Value
for money lessons, refer to the activities on budgeting and money
personalities to guide their answers

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?

 Ask students what they know about fraud, and the ways that online criminals can use your personal details to make purchases or open accounts in your name. Use the terms on page 8 of this lesson plan to prompt if needed. Do they think Sam is at risk from fraud?

2. Create an action plan

• Once the group can recognise Sam's bad habits, ask them to come up with a brief action plan using **slide 4** to help Sam improve his money management and online security. As an extension, you could add that Sam would like to buy a car. How could an action plan help him adjust his spending and saving behaviours to achieve this goal?

Use the suggestions below if they need prompts:

- Setting up alerts through his bank that tell him when his balance reaches a certain amount
- Change his PIN and make sure they are not all the same
- Keep his PIN secret by memorising them and not recording them anywhere
- Removing his personal information (e.g. date of birth) from his social media accounts, and check privacy settings –
 fraudsters could use this information to access his bank
- Shredding or storing securely any financial paperwork or personal documents to protect himself from identity theft
- Open a savings account and put money aside on pay day, then create a budget using his remaining balance
- Only spend what he can afford to pay back each month
- Research a car that he could afford and work out how long it would take for him to save up

Extension

Students can complete the 'Make It Through the Month' quiz (tool on slide 5) as a class, in small groups on laptops/tablets, or individually with printed copies of the questions.

Activity three

Activity three

Fraud and identity theft

1. Exploring online financial safety

As technology changes the way we communicate, shop, and transfer money, fraud is becoming increasingly
sophisticated and it's important that students understand how to keep personal information safe. Safe online
habits can help protect the whole digital community

Contents

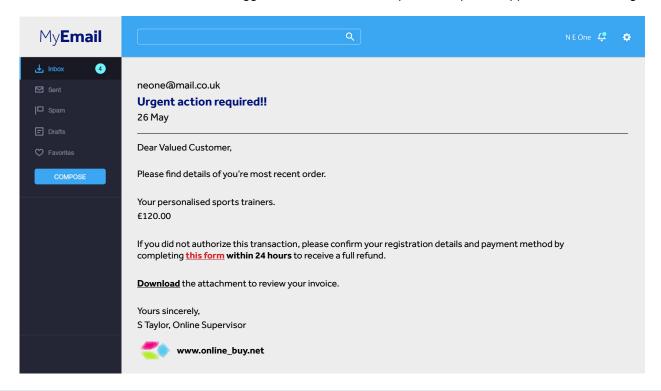


Sources: Cifas Fraudscape Reports 2020 and 2021 (fraudscape.co.uk)

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 <u>'Take Five' campaign</u>

2. Spot the faker

- Display the email using **slide 6**, or print copies for students. Challenge them to find all the features that can provide clues to spotting a fake, or that may suggest a fraud risk
- After a few minutes, collate their suggestions, and as a class explore the tips that appear on the following slide





Activity three

Fraud and identity theft (cont'd)

Message subject	Be suspicious of urgent demands – fraudsters often use scare tactics and threats to encourage a response without thought.
'To' line	Be wary of emails that use generic greetings, or refer to you in an unusual way, such as the first part of your email. A legitimate organisation is more likely to use your full name.
Request for personal details/ completing a form	Reputable organisations will never request that you provide your PIN, password, or online banking login details, or ask you to transfer money to another account.
Hyperlink to follow or attachment to download	The email is designed to impress on you the importance of clicking this link or attachment right now, even if the link to what could be your account looks genuine. Hyperlinks can direct you to a hoax website where your login and personal details are requested, or your computer or smartphone is infected by viruses. Hover over hyperlinks without clicking to display the destination and evaluate whether it looks legitimate. Never open attachments from someone you don't know or weren't expecting, as these can download spyware or malicious programmes onto your smartphone or computer.
Sender/signature	A signature that is generic or doesn't follow the usual format could indicate a suspicious sender. Look whether the email address matches their name or signature and beware of unexpected emails from public accounts like Google or Yahoo.
Poor grammar/ mistakes	Poor grammar, unusual style, and mistakes in the wording of the message can be a sign that it is not from a legitimate sender.
Intriguing statement	Financial rewards are offered in exchange for personal details or following a link – if something sounds to good to be true, it probably is. People are naturally curious, and phishers take advantage by promising something new or exciting to encourage them to click on a link.
Web address/ organisation logo	Phishers can use branding and links to websites of companies that you may know and trust, but they may be poor quality or stretched. Compare previous messages you may have had from companies they are trying to imitate or look their sites up online and look for subtle differences.

• **Slides 7-12** feature case studies of fraud and identity theft. Print a copy of each of the case studies or display on tablets/PCs. Small groups should read through one of the case studies and consider:

How do you think the person felt?

Are there any terms you don't understand?

What type of fraud or practice is this?

What signs could they have spotted to stay safe?

What information would a bank or reputable company ask for? (e.g. they would never ask for a full PIN or password)

How convincing was the fraudster? What did they do to make themselves more convincing?

What could they do differently next time? Examples could include: not revealing personal or financial data, verifying whether links in emails are legitimate by contacting the company directly, not opening email attachments from unknown sources.

• Each group could present their opinions and key points back to the rest of the class. If you'd like to cover some fraud terminology, use the descriptions below or look at 'Do you know your phishing from your smishing?'



Activity three

Fraud and identity theft (cont'd)

3. Terms for teachers

Money mules (Case study 1)	A "witting" mule assists the crime by providing the bank account where the proceeds of any fraud or scams can be paid to. Fraudsters and scammers can open an account themselves using fake ID, or can convince someone who already has a bank account to receive money on their behalf. The mule has acted illegally, even if they didn't know the extent of the fraduster's actions.
Online scams (Case study 2)	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 (Case study 3 and 4)	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing (Case study 3 and 5)	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 and smishing (Case study 6)	A scam to access valuable personal details by sending emails or texts, that ask you to call a number, download an attachment or follow a link to a website containing malware, which can collect secure information. Messages often appear to be from your bank, or company you are registered with.

- Take a look at the short films on the '8 ways to stay safe online' page
- You could also watch an engaging short film produced by Cifas (1 min 30 secs), which exposes how much personal information is accessible to fraudsters via our social media accounts. Show this film to students by searching online for 'Cifas data to go'
- CIFAS have worked with the PSHE Association to create four anti-fraud lesson plans for 11-16 year olds. These offer more detail on fraud, scams and protecting personal data, and can be downloaded here

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

- Recap the session aims and outcomes, and ask students to put forward the key learnings from the session, using the information on **slide 14** to help. You may want to print this as a takeaway for students
- Explain that as they reach an age where their income increases, they will need to consider how to manage
 their own budget and make independent decisions about what they can afford. Aside from keeping their
 money safe, they need to be aware of how their financial decisions will affect other elements of their lives

Further links and activities

To supplement this lesson, you could look through the following links with the class, or suggest that students spend some time exploring the articles and tools on the LifeSkills website in their own time.

NB: Students need to be over 14 to register to use the LifeSkills website independently.

Articles

8 ways to stay safe online

Do you know your phishing from your smishing?

Tools

Make It Through the Month Quiz

Lessons

This is one of four Money Skills lessons for 11-14 year olds. Consider delivering the other lessons:

Recognising your money personality

Value for money

Next steps on your financial journey

There is Money Skills content to suit a range of ages and abilities – take a look at our 7-11, 14-16, 16-19 and 19+ resources, which focus on topics such as attitudes to money, money management and risk, and financial independence.

External links

Digital Wings

You & Co (Victim Support's youth site)

Take five (campaign website, resources and films)

National Debt Line (credit factsheet including advice for victims of fraud and identity theft)

CIFAS (anti fraud lesson plans)

Get Safe Online (advice on online and tech safety and fraud protection)

© Barclays 2023. Modification of this lesson plan is not permitted. Use of this lesson plan is governed by the LifeSkills terms and conditions which can be found at barclayslifeskills.com/terms-and-conditions