Protecting against online fraud and scams

Age range: 14-16

BARCLAYS | LifeSkills

BARCLAYS | LifeSkills

Session overview

This lesson belongs to a suite of Money Skills lessons for young people aged 14-16.

The activities allow students to understand how to protect themselves and others against online fraud, scams and identity theft.

Time	Key learning outcomes	Resources
40 mins	By the end of the activity students will be able to: • Recognise different types of financial fraud and understand how to reduce the risks they pose. • Understand the ways in which identity theft occurs and how to prevent it.	• Protecting against online fraud and scams presentation slides. • 'Data to go' film from Cifas.

The Money Skills 14-16 lessons are designed to help student 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.

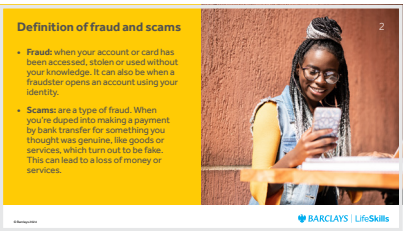
Contents

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

Understanding fraud and scams

1. Defining fraud and scams



This section highlights the most common types of fraud, what to look out for, and how students can 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**.

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**

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.

- Show **slide 2** and ask students to read through the two definitions before having a brief discussion about the difference between a fraud and a scam.
- 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.
- Reiterate that fraud 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), whereas a scam is when you have participated in activity that has led to a loss of money or services through payments that you know about but were duped into making or agreeing to.
- Show **slide 3** and ask your students to read the terms relating to different types of fraud and scams, and the definitions, before asking them to match up each term with the correct definition.
- Explain that in many instances when you are taken advantage of, provided you have followed all the rules for use of your account, your bank or financial institution may be able to help to return lost funds to you.
- This is also a good moment to explain that identity theft is a type of fraud in which personal details are stolen and used to open bank accounts or make purchases in that person's name.

Activity one

Understanding fraud and scams (cont'd)

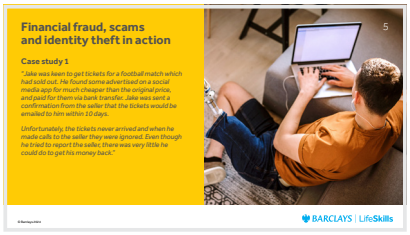
2. Watch a film about fraud

- Cifas has produced an engaging **short film** (1 min 30 secs) which exposes how much personal information is accessible to fraudsters via our social media accounts. Show this film to students and ask why they think they should be careful about the information they share publicly.
- Summarise the video by reminding students that they should check how much personal information is public on their social media accounts, e.g. birthday, home town, pet names, holiday dates, job title. Fraudsters can use this information to steal a person's identity and apply for bank accounts or buy products in their name.

Activity two

Exploring social media and smishing (text message) fraud case studies

1. Explore case studies



- **Slides 5** and **6** feature examples of an online purchase scam and a text message (smishing) scam.
- Split your class into two groups, where half of your students work through Jake's case study (purchase scam) and half work through Tom's case study (smishing). Ask students to discuss within their groups before asking each group to present back on the answers to the questions below, as well as any other observations they may have.

What type of scam is this?

How does this scam operate?

What could they do differently next time?
Examples could include: not revealing personal or financial data, verifying whether offers within online groups are legitimate by only purchasing from the company directly, not clicking on links from unknown sources.

---

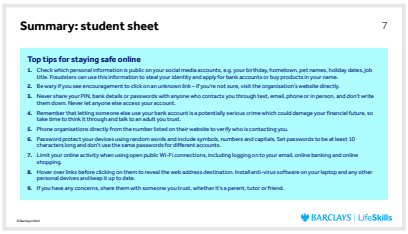
2. Ask students to present

- Ask each group to briefly present their opinions and key points back to the rest of the class. Encourage them to draw on the definitions and concepts they have discussed earlier on in this lesson.

Activity three

Identifying scams and staying safe online

1. Top tips for staying safe online


Summary: student sheet 7

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. Fraudsters can use this information to steal your identity and apply for bank accounts or buy products in 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 devices using random words and include symbols, numbers and capitals. Set passwords to be at least 10 characters long and don't use the same passwords 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. Install anti-virus software on your laptop and any other personal devices and keep it up to date.
9. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend.

BARCLAYS | LifeSkills

- In pairs or small groups, ask students to discuss some ways to identify scams and stay safe online. Explore suggestions before showing them the tips on **slide 7**.

Summary

- To close the lesson ask any willing students to share something they now know which they didn't know at the beginning of the lesson. Is there anything students may do differently going forward? You may want to print **slide 7** as a takeaway for your students.