



Spotting online shopping scams

Age range: 16-19

 **BARCLAYS** | LifeSkills



Session overview

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 some of the most common types of fraud, scams and identity theft. Explore the different contexts where fraud and scams take place, and how to protect themselves from becoming victim to them. 	<ul style="list-style-type: none"> Spotting online shopping scams presentation slides.



The [Money Skills 16-19 lessons](#) are designed to help students 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.

Always start the sessions by agreeing ground rules with the group. This lesson plan is designed to be used in tandem with a PDF containing interactive activity slides. For advice on this and other ways to establish a safe learning environment, download the [content guide](#).

Contents

Activities	Time	Page
Activity one: Fraud, scams and identity theft	10 mins	3
Activity two: Exploring phishing (fraudulent emails)	15 mins	3
Activity three: Rental scam case study	15 mins	5
Activity four: Top tips for protecting against fraud	10 mins	5

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 and 19+ resources, which focus on topics such as attitudes to money, money management and risk, financial independence and fraud.

Activity one

Fraud, scams and identity theft

1. Defining fraud and 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.

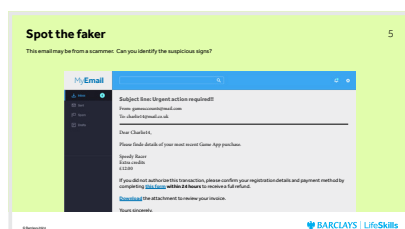
Source: ukfinance.org.uk

- Start the lesson by showing **slide 2** and outlining the difference between fraud and scams.
- Next put students into small groups, and ask them using the **slide 3** to match up the correct term to the right definition. Once they have matched up definitions to each term, come back as a group and go through the correct answers on **slide 4**.
- Remind students 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.

Activity two

Exploring phishing (fraudulent emails)

1. Spot the faker



- Start by having a discussion around how your class currently use emails, and that in the workplace it is a primary form of communication.
- Explain that emails may also be the first point of contact that students will have with a work experience or volunteering placement, and with prospective employers. Their email address may be the first thing that an employer will see. They are also likely to use it regularly as an employee or business owner in the future.
- In small groups, have them consider emails they have received and what elements within them made them reliable and trustworthy.
- Display the email on **slide 5**. The email features several signs that suggest it may not be real and may be from a scammer.
- Continuing to work in small groups, ask them to find all the features in the email that can provide clues to spotting that it is fake and may suggest a fraud risk.

Activity two

Exploring phishing (fraudulent emails) cont'd

What can you spot that looks suspicious in this email?

Make a list of the signs. What are the potential consequences of receiving this email to a personal account and what could happen if it was sent to a work account?

- Allow some time for the class to look at the email and make a list of the things they think are suspicious.
- Collate their suggestions, and then click each slide and discuss the tips that appear. There are seven in total, and the copy within each point is also shown in the table below.
- If you want to extend this activity, you could ask groups to write a list of the things to look out for and produce a poster to go on display to warn other people.

Look out for	Why
Imagery or design that looks familiar but doesn't feel right	Email design, fonts or imagery that don't look as you'd expect can be a sign that it's not from a genuine sender.
Message subject line	Be suspicious of urgent requests or something that sounds too good to be true. Fraudsters often use these tactics to encourage a quick response.
'To' line	Watch out for emails that refer to you in an unusual way, such as the first part of your email address. A trustworthy organisation is more likely to use your full name.
Request for personal details/completing a form	Trustworthy 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	Be careful if you are asked to click on a link or download an attachment. 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. Hover over hyperlinks without clicking to display the destination and evaluate whether it looks real.
Sender	Look at the sender to see if the email address is suspicious. For example, it might not match who the sender says they are or it may be from an email address like Google or Yahoo which anyone can create instead of a business email address.
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 genuine sender.

Top tip

- Remind students that fraudsters use spam messages to gain access to information within workplaces and that this can increase risk to a company or business if they reveal confidential information.
- Add that fraudsters also use spam text messages to trick people out of money or information, and that many of the same features discussed in the Spot the faker email can apply to spam text messages too. For example, an unknown number, spelling and grammar mistakes, hyperlinks and requesting personal information. Quite often if an email or text seems too good to be true, it isn't genuine.

Activity three

Rental scam case study


1. Case study – house hunting

Financial fraud, scams and identity theft in action

Case study – House hunting

"Mia has been looking online for flats to move into with her friends. She has been having a hard time on rental and property websites as properties are not out very quickly. She finds a three bedroom flat in a housing group on a social media app, and enquiries about its availability. The landlord asks Mia to transfer one month's deposit to hold the property. Mia transfers the money via bank transfer. Mia doesn't really want to do this but she is so desperate for this flat she transfers the money via bank transfer."

However, after she transfers the money she doesn't hear from the landlord again."



- Now explain to your class that you are going to explore a case study which details a type of scam that can affect young people looking for rental properties.
- Ask your class to explore Mia's case study either in groups or independently using **slide 13**, before using the questions below to come back together as a class to discuss, giving time for the questions and any answers to be noted down.

What signs could Mia have spotted to stay safe?

What could she do differently next time?

What might the consequences be? (e.g. she loses the money she transferred for the holding deposit)

What should Mia have done instead to avoid this situation?

Activity four

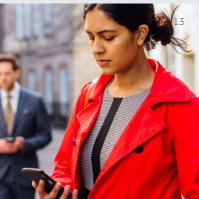
Top tips for protecting against fraud

1. Summary

Top tips for protecting yourself from fraud, scams and identity theft

14

1. Check which personal information is public on your social media accounts, e.g. your birthday, hometown, pet names, holiday dates, job title. Scammers can use this information to steal your identity and apply for bank accounts or hire products in your name.
2. Be wary of free money or prizes to claim online. If you're not sure, visit the organisation's website directly.
3. Beware of offers that sound too good to be true, particularly if they are offering higher return on investment in foreign currency, stocks and shares or cryptocurrency.
4. Never share your PIN, bank details or passwords with anyone and never let your phone, email, phone or person and don't enter text alone. Never let anyone take your account.
5. Remember reporting a scam or abuse your bank account is a potentially serious crime which could damage your financial future, so take time to think it through and ask for an adult you trust.
6. Please report any offers to claim the number listed on their website to verify who is contacting you.
7. Remember protect your device using security tools 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.
8. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping.
9. Never use the public Wi-Fi in your phone to access the online banking details.
10. Remember to be careful of your phone and any other personal devices and never let it be stolen.
11. If you are a victim of fraud, you should leave your understanding and contact your bank. From there, you should make a list of the fraudulent transactions and report them to the relevant authorities (e.g. the police).
12. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend.



- Now ask students in pairs to come up with a few ways to protect themselves against fraud that they can share with their families.
- Once they have come up with their ideas, have each pair share a suggestion before showing them the list on **slide 14**.
- Facilitate a discussion around how some of these ways to protect against fraud could extend into the workplace.

Summary

- Recap the lesson and 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 14** as a takeaway for your students.