
Social Engineering

Key Stage 4 | Lesson 2





Resources Required

Box or envelope for questions

Resource 1: Key Term Card Sort (one set per pair, cut up)

Resource 2: Social Engineering Scenarios (one set per pair)

Resource 3: Top Tips for Avoiding Social Engineering and Cybercrime (one per student)

Resource 4: Sentence Starters and Key Terms (support option as required)

Key Words

Cybercrime
Social Engineering
Malware
Phishing
Smishing
Vishing
Quishing

Context

This is the second of two key stage 4 lessons developed by Cifas, the UK's leading fraud prevention service. These lessons build on two lessons for key stage 3 students and have a further lesson for key stage 5, along with a dedicated lesson for students with SEND. The lessons empower young people to protect themselves from fraud through building awareness of how to identify fraud and how to protect personal data online. This second key stage 4 lesson raises awareness of various forms of cyber-enabled crime, specifically social engineering techniques. In relation to fraud, social engineering refers to the techniques used by criminals to manipulate people to reveal personal information about themselves or to induce them to carry out an action (such as transferring a sum of money).

Learning Objective

To learn about the risks of social engineering, how to recognise and challenge it, and sources of support available.

Learning Outcomes

Students will be able to:

- explain what social engineering is and how to recognise its different forms
- explain the risks involved in revealing personal information and how to respond to social engineering attempts
- describe how and where someone can seek help if they are concerned about cybercrime

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 teacher subject knowledge about types of fraud and consequences of fraudulent behaviour.

Lesson Summary

Activity	Description	Timing Total: 60 mins
Baseline Assessment	Students answer five questions to establish their baseline knowledge and understanding.	10 mins
Introduction	Revisit ground rules and outline the learning objective and outcomes.	2 mins
Key Terms Card Sort	Students sort cards to define key terms for the lesson.	5 mins
Social Engineering Scenarios	Using four scenarios, students identify different forms of social engineering, considering the possible risks and what the characters can do to seek support.	15 mins
Understanding Risk	Students identify the possible risks posed by social engineering for individuals and organisations.	5 mins
Giving Advice	Students give advice to one of the characters, including where to seek support.	10 mins
Signposting Support	Signpost students to where they can seek information and support, including how to report fraud.	3 mins
Endpoint Assessment and Personal Reflection	Students revisit their baseline answers. They then complete a personal reflection activity about keeping safe from social engineering in their own lives.	10 mins

Baseline Assessment



Slide 2 and 3

Introduction



Slide 4

Core Activity



Slide 5

Baseline Assessment Activity

Revisit ground rules on [slide 2](#) and remind students of the importance of keeping personal stories private. Let them know they can use the question box to add a question, with or without their name, during the lesson.

Show [slide 3](#), which has five baseline questions. Ask students to try to write something for each of them, even if they are not sure. Wherever possible, they should give as much detail as they can.

Explain that they will return to these questions at the end of the lesson. The ideas recorded will help to inform questioning throughout the lesson. For example, if students cannot answer question 4 in detail (What should someone do if they are a target of identity fraud?), you may wish to spend longer on the final core activity: Giving advice.

Introduction

Introduce the lesson objective and outcomes. Tell students that they will be thinking about how fraudsters use cyber technology and social engineering techniques to manipulate people into disclosing personal information.

Key Term Card Sort

Explain that there are terms used to describe different fraudulent techniques, and being aware of these will help them recognise if someone is using them to manipulate behaviour. In pairs, ask students to match the terms with their definitions using [Resource 1: Key term card sort](#).

Take feedback and ensure everyone has the correct definitions and understands the terms.



Challenge:

After students have matched the correct terminology and definitions, ask them to create examples of each technique.

Core Activity



Slides 6-10

Social Engineering Scenarios

As a class, read the five scenarios on [Resource 2: Social engineering scenarios](#), showing social engineering techniques.

Ask students to identify which scenario matches which form of social engineering. Take feedback using [slide 7](#) to confirm answers, ensuring the key learning is covered:

1. *Carla's phone call claiming to be from a bank – this is an example of vishing.*
2. *Josh's email claiming he has won a games console and can join a lottery – this is an example of phishing.*
3. *Paulo's private chat online and being sent a malicious link – this is an example of a malware attack.*
4. *Amir scans a QR code on a poster that takes him to a fake login page – this is an example of quishing.*
5. *Nicki's instant message about parcel delivery – this is an example of smishing.*

Next, ask students to discuss the questions on [slide 8](#):

1. What might happen next to the characters in these scenarios?
2. What should these characters do now?
3. Where could they seek more help and advice?

Through feedback, draw out the key learning:

Scenario 1:

The fraudster tries to create a sense of panic and urgency for Carla, but a bank will never ask a customer for their PIN number. In this situation, Carla should hang up and call her bank using the official bank phone number (shown on the back of a bank card and the bank's website).

Scenario 2:

If Josh clicks the link, the fraudster is likely to try to get him to reveal personal information and/or send money. Josh should look for signs of phishing – this email was not expected, he hasn't entered any competitions, there are grammatical errors, a sense of urgency and that something isn't quite right. He should report the email as a scam to his email provider and then block and delete. If Josh was unsure whether the email was genuine, he could speak to a trusted adult at home or school about it.

Scenario 3:

Fraudsters can befriend people over time, to encourage them to feel trust. It is important Paulo doesn't click on links shared, as they could include malware. He should make sure his device is fully up to date with any prompted updates and could also install virus protection.

*Continued on next page

Core Activity



Slide 11

Scenario 4:

Amir should avoid entering any details after scanning an unexpected QR code, as it could take him to a fake site designed to steal his information.

If someone in a scenario like any of these shares personal details or clicks on malicious links, it's possible their details might be used to commit fraudulent crimes. So, it's important to report what has happened to Report Fraud and their bank if they have revealed financial details like account numbers.

Scenario 5:

It is important that Nicki doesn't reply to the message or click on the link as this could include malware or encourage her to share personal information. She should take a screen shot of the message and report it in the app and then block the number before deleting the message. Some networks might delete the message automatically when it's reported.

Nicki can also forward the message for free to 7726 (it spells out SPAM on the keypad) and then she can block and delete. This is a service from the National Cyber Security Centre and it will report the message to the mobile phone provider.

Give students [Resource 3: Top tips for avoiding social engineering and cybercrime](#), which is also summarised on slides [9 and 10](#), and ask them to consider whether there are any strategies here they think would help the characters that they had not already considered.



Support:

Hand out [Resource 3: Top tips for avoiding social engineering and cybercrime](#), at the start of this activity to support students in responding to the questions.

Understanding Risk

In pairs, ask students to consider what the risks and consequences are of becoming a target of fraud, in all four scenarios. For each scenario, students should list what risks there are to the individual involved.

Take feedback highlighting potential risks, including:

- *emotional stress in dealing with the problem, needing to change bank and/or personal details, getting into debt, reputational damage (organisations thinking they are unreliable customers)*



Challenge:

Ask students to suggest how these risks could be minimised.

Core Activity



Slides 12 and 13

Signposting Support



Slide 14

Giving Advice

Show [slide 12](#), which include various sources of support for people targeted by fraudsters.

Using this information and their understanding from the lesson, show [slide 13](#) and ask students to select one of the characters from the social engineering scenarios and write to them, explaining what the fraudsters might be attempting to do, how they might recognise social engineering techniques and how they can seek help and support.



Support:

Give students **Resource 4: Sentence starters and key terms**, to support their responses.



Challenge:

Ask students to list reasons why some people might not report incidents of fraud. For each reason, they should try to suggest what could be done to make it easier for people to report.

Signposting Support

Using [slide 14](#), revisit the sources of support shared in the last activity, reinforcing that if someone is worried about fraud or want to find out more.

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
- Victim Support: www.victimsupport.org.uk
- UK Finance – Take 5 to Stop Fraud: www.takefive-stopfraud.org.uk
- Stop! Think Fraud: www.stophinkfraud.campaign.gov.uk

Plenary/ Assessment for and of learning



Slide 15

Extension Activity

Slide 16

Endpoint Assessment

Revisit the baseline questions and ask students to consider the key terms, examples and advice they have explored during the lesson. Using a different coloured pen, students should now add to, change or edit their original answers to demonstrate their learning in this lesson.

Ask students to complete a '3, 2, 1' activity for personal reflection. They should consider three ways they could spot social engineering, two things they could do if they ever receive what they think might be a fraudulent email or message and one source of support they could access for help. Students should not be asked to share these personal reflections.

Extension Activity

Ask students to return to the list of tips for protecting against cybercrime and social engineering scams shown on Resource 3: Top tips for avoiding social engineering and cybercrime.

They should design a logo, diagram or image to represent each of the ten top tips. These diagrams could be collated and used to form a display around school about fraud prevention and cybercrime.