LESSON FOUR
SOCIAL ENGINEERING

Key Stage 04

PSHE Association Quality Assured Resource

CONTEXT

This is the second in a series of two lessons developed by Cifas, the UK's leading fraud prevention agency. These key stage 4 lessons are designed to extend and build upon two foundational lessons at key stage 3. The lessons aim to 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 lesson raises awareness about 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).

The lesson plan is based on a one hour lesson. The timings given are the minimum time required to deliver the activities. Whilst it is always important for PSHE education lessons to be pacey, it is equally important to meet the needs of your students. More may be gained from spending longer on an in depth exploration of an activity that has fired up discussion and imagination, so long as you are comfortable leading the discussion and feel students are progressing towards the lesson objectives. When this is the case, it may be more appropriate for your group to extend the lesson plan across two lessons.

Neither this, nor any of the other lessons, is designed to be taught in isolation, but should always form part of a planned, developmental PSHE education programme.

Resources required

BOX OR ENVELOPE FOR ANONYMOUS QUESTIONS

RESOURCE 1: EXPLAIN TO AN ALIEN

RESOURCE 2: KEY TERM CARD SORT

(optional resource)

RESOURCE 3: SOCIAL ENGINEERING PROBLEM PAGES

RESOURCE 4: SENTENCE STARTERS AND KEY TERMS

(optional resource)

RESOURCE 5: TIPS FOR DEFENDING AGAINST CYBER CRIME AND FRAUD

[Extension Activity 2]

Key words

Learning objectives

- We are learning about the risks of identity fraud
- We are learning how to recognise and challenge social engineering

Intended learning outcomes

- I can explain the importance of protecting my identity and the risks involved in revealing personal information
- I can describe how to protect my online identity, both at home and at work
- I can explain how malware is used to commit online crime and how to protect devices from malware threats
- I can explain what social engineering is, how to recognise it and how to respond to social engineering techniques
- I can describe how and where to seek help if I am concerned about cyber crime

Climate for learning

- Establish or reinforce existing ground rules. Add or emphasise any ground rules that are especially relevant to this lesson. Local and national support groups or helplines should be signposted.
- Invite students to write down any questions they have anonymously at any time, and collect them using an anonymous question box or envelope, which should be accessible both in and after every lesson. To ensure that students do not feel self-conscious about being seen to be writing a question, you can ask all students to write something: either a question or 'no question' if taking anonymous questions during the lesson. You may wish to set aside some time at the end of each lesson for this.

Baseline assessment/reconnecting activity

BASELINE ASSESSMENT ACTIVITY

Revisit ground rules and remind students of the importance of keeping personal stories private.

Hand out **Resource 1** and ask students to imagine that they are going to explain what identity fraud means to an alien who has never been to planet Earth before. There are five specific questions, ask students to try to write something down for each of them, even if they are not sure or are making a guess. Wherever possible, they should give as much detail as they can because the alien doesn't know anything about our planet. Tell students not to worry about spelling or grammar as it is more important to record all of their ideas.

Collect these worksheets and explain that they will have an opportunity to return to them at the end of the lesson. The ideas recorded on these sheets will help to inform questioning throughout the lesson.

INTRODUCTION

Share the learning objectives and outcomes with students. Explain that today the class will be thinking about how fraudsters use cyber technology and social engineering techniques to manipulate people into disclosing personal information.

Core activities

KEY TERM CARD SORT

Explain to students that there are a range of complex terms used to describe different fraudulent techniques, and that being aware of these will help them to recognise if someone were trying to use them. Encourage them to work in pairs to complete a key term card sort (**Resource 2**) by matching the terms to their definitions.

For a non-printing alternative, the table below could be displayed on a smartboard in a 'mixed up' order and as a class the students could reorder the terms and definitions to match. Take feedback and ensure everyone has the correct definitions and understands all the terms.

KEY TERM	DEFINITION
Social Engineering	A method of manipulating people to reveal personal information about themselves
Cyber crime	A type of crime that is committed using information technologies such as a computer and a network
Phishing	An attempt to gain personal information through the use of email communications
Smishing	An attempt to gain personal information through the use of text message
Vishing	An attempt to gain personal information over the phone
Malware	Software which is specifically designed to disrupt or damage a computer system

For those students who may need support:

'provide students with a completed set and ask them to identify which (if any) they have heard of before, and to guess which they think is the most common form of cyber attack.

For those students who may need further challenge:

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

Core activities (cont.)

PROBLEM PAGES

As a class, read the four problem pages (**Resource 3**) of people who have experienced social engineering techniques. Identify which case study matches each form of social engineering. Take feedback from the whole class and collate ideas on the board:

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

For those students who may need support:

To support students in this discussion, you may wish to hand out **Resource 5**, which introduces ten tips for defending against cyber crime and what to look out for in order to recognise a social engineering scam.

Through discussion, draw out the key learning that the characters have become targets of social engineering techniques (phishing, vishing, smishing and malware respectively). It is possible that their details may now be used to commit fraudulent crimes, such as taking out loans or other financial services, or even creating false identities. The characters have a responsibility to report what has happened to Action Fraud and should inform their bank if they have revealed financial details like account numbers. In the case of Josh, he must inform his boss and finance department in order to secure the business from further fraudulent acts.

This may also be an appropriate time to signpost websites dedicated to supporting victims of fraud, including:

www.actionfraud.police.uk – reporting fraud when it happens

www.victimsupport.org.uk – supporting victims of crime through next steps

www.takefive-stopfraud.org.uk – raising awareness of how to prevent fraud

www.moneymules.co.uk

Core activities (cont.)

UNDERSTANDING RISK

5'

In pairs, ask students to consider for all four scenarios what the risks and consequences are of becoming a target of fraud. Students should list for each case, what risks there are to the individual involved, and what potential risks (if any) there might be to the organisation they work for.

For those students who may need further challenge:

If time allows, encourage students to suggest how these risks could be minimised.

Take feedback from the pairs, which could be recorded on the whiteboard at the front of the room. Ensure that the discussion highlights that the potential risks include:

For the individual – 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 debtors), maybe losing their job

For the organisation – getting into debt, reputational damage, hard to retrieve the funds which could impact on profit and therefore being able to pay staff, having to change security details or software

GIVING ADVICE

10'

Using the advice collated on the board and through discussion, encourage students to select one of the characters and write a response to them, explaining what the consequences of their actions might be, how they can seek support, how they might recognise social engineering techniques and what they should do differently in the future.

For those students who may need support:

For those who may struggle with extended writing, provide students with a selection of sentence starters or key phrases (**Resource 4**) that they may choose to use in their writing.

For those students who may need further challenge:

Ask students who require further challenge to list as many reasons as they can 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 fraud.

Plenary / Assessment *for* and *of* learning

ASSESSING (DEMONSTRATING) PROGRESS

Return **Resource 1** 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 have the opportunity to add to, change or edit their original answers in order to demonstrate their learning in this lesson.

Extension activities / Home learning

EXTENSION ACTIVITY 1

Ask students to write a diary entry for one of the characters in the problem pages. This diary entry should be in 2 months' time, explaining what has happened since they followed the students' advice and how the situation has begun to resolve itself. Where possible, students should try to include consequences for both the target of the fraud and the perpetrator.

EXTENSION ACTIVITY 2

Ask students to return to the list of tips for protecting against cyber crime and social engineering scams (**Resource 5**). 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 cyber crime.