cifas
Leaders in fraud prevention

LESSON TWO
IDENTITY FRAUD AND DATA PROTECTION

Key Stage 03

PSHE Association Quality Assured Resource
PSHE Association

CONTEXT

This is the second in a series of two lessons developed by Cifas, the UK's leading fraud prevention agency. These key stage 3 lessons also have corresponding lessons designed to extend learning at key stage 4. 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 focuses on the importance of protecting personal details, in order to minimise the risk of identity fraud. In particular, this lesson will encourage young people to think about the risks of sharing personal information on social media.

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

CIFAS – DATA TO GO VIDEO

BARCLAYS DIGITAL SAFETY VIDEO

RESOURCE 1: SAFE OR UNSAFE SCENARIOS

(printed or displayed on board)

RESOURCE 2: DIAMOND 9 OF TOP TIPS

(1 set between 2 or 3 students)

RESOURCE 3: GIVING ADVICE

Key words

IDENTITY FRAUD
-
SOCIAL MEDIA
-
ONLINE DATA
-
FIREWALL
-
ANTIVIRUS

Learning objectives

- We are learning about the importance of online safety strategies to protect us from fraud
- We are learning how to keep our online data secure

Intended learning outcomes

- I can classify information that is private and that which is safe to share publicly online
- I can explain the risks of oversharing personal information on social media
- I can suggest a variety of ways to keep online data secure

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

INTRODUCTION

Revisit ground rules and remind students of the importance of keeping personal stories private. Explain that today the class will be thinking about identity fraud, how it is committed and the importance of protecting personal information online.

BASELINE ASSESSMENT ACTIVITY

Present students with **Resource 1** (either printed for each student or projected on the board), which lists a range of scenarios about online activities. Ask them to decide if they think in each case, the action is 'safe', 'unsafe' or 'it depends'.

Encourage students to then move into pairs and compare their answers with a partner to see if they made the same decisions about the safety of these examples. Take some feedback from the pairs, asking them to explain the reasons for their choices. Use this feedback to gauge students' starting point and to adapt teaching accordingly.

NB: The key message to get across during feedback is that we should always think before posting and be prepared for anyone (family, teachers, a fraudster) to see what has been uploaded. It is important to understand the risks of sharing too many distinguishing features, such as school logos, addresses, location check-ins and to understand how someone might use this information to build up a picture of a person's identity. It is especially important to be wary when using public computers or internet access or if friends online with people we haven't met offline.

Teachers may wish to ask students to suggest their idea of what identity fraud is, building on the learning of the previous lesson. This could be done by the teacher taking ideas through questioning or by all members of the class writing ideas on a post-it note and sticking them on the wall at the front of the classroom. Teachers should then ensure students are familiar with the definition:

Identity fraud is when a fraudster uses someone else's identity (or creates a fake identity) to access a product or service so they get out of paying for it themselves.

Core activities

WHAT IS MY IDENTITY?

Ask students to list (or mind-map) all of the elements that make up their identity.

For those students who may need support:

To encourage students to think widely during this activity, teachers may choose to use some of the following prompt headings:

- Personal details and information e.g. name, DOB, address
- Skills and qualifications e.g. what school you go to, exams you've taken
- Interests and hobbies e.g. football team, favourite singer
- Friends and family
- Cultural and religious heritage

For those students who may need further challenge:

Encourage students to group these features of their identity into 'public' and 'private'; those they would be willing to share with other people/online and those that they would only share with people they know and trust.

When students have finished creating their lists, ask them to highlight those parts of a person's identity that they think a fraudster might use to impersonate them to a bank or company.

NB: During discussion, it is important for teachers to emphasise that someone trying to commit fraud is interested in lots of different pieces of information about a person, not just their date of birth and address. Fraudsters will also use information about a person's interests and hobbies to befriend a target and trick them into giving over more information. So the more that someone shares publicly online, the more at risk they are of being susceptible to fraud.

Core activities (cont.)

DATA TO GO

As a class, watch the Data To Go video which demonstrates how a hacker or fraudster might be able to access personal information online.

https://www.youtube.com/watch?v=sq-0tjv4_BA

Develop thinking about this video by asking students:

- How did people react in this video when they were presented with their information?
- What parts of their identity were the team able to find out about them?
- What could these people have done to protect their information?
- What do you think a fraudster would use this information for?
- What might be the consequences of having this information publicly available?

During discussion and feedback from these questions, teachers should try to draw out the key points that everyone should be careful what they share on social media and that there are lots of ways to protect personal information, from thinking carefully about what is appropriate to publicly share (with strangers), to making sure that electronic devices are protected using anti-virus software and strong passwords, to not accessing personal information on public Wi-Fi networks (for example doing online banking using a café's free Wi-Fi). While in this video the personal information was only being accessed in order to demonstrate an important security point, a fraudster might use this type of information to apply for loans, credit cards, or to befriend and trick someone online into revealing even more about themselves. Having this information publicly available could make people more likely to be targeted by fraudsters which can lead to long lasting reputational damage, problems getting credit in the future and to being unable to retrieve stolen money.

TOP TIPS

As a class, also watch the Barclay's digital safety advert.

https://www.youtube.com/watch?v=w2tW50CD6Aw

Thinking about both videos and the starter activities, create a class mind-map on the board about the sort of 'tips' students would recommend to ensure safety from identity fraud when posting online.

Once students have made their initial suggestions, provide pairs or small groups with **Resource 2**: Diamond 9 top tips and ask them to prioritise these tips into a diamond shape, demonstrating what they believe to be the most important tip to the least important.

For those students who may need support:

Teachers may prefer to offer students a Diamond 5 sorting activity of 5 top tips to protect themselves from identity fraud, using the top 5 cards.

For those students who may need further challenge:

Ask students to explain why it is important that people follow each of these tips when protecting themselves from identity fraud.

Core activities (cont.)

GIVING ADVICE

Present students with **Resource 3**: Giving advice and ask them to look at the statements made by the character who is confused about identity fraud. Students should first decide if the statement is true or false, and then give some advice or additional information in response to each statement.

Take feedback, identifying that:

Your bank will sometimes call and ask you for your PIN or passwords

FALSE – Your bank will never under any circumstances ask you for your full PIN or password and you should never give these details out to a caller

If you have been a victim of identity fraud once you won't be a victim again

FALSE – Fraudsters share stolen personal details with each other. A fraudster may try to use your identity to commit another type of crime

Identity Fraud is a victimless crime

FALSE – Identity fraud can be very distressing for the target. They may struggle to get all their money back, and the emotional and reputational damage can be very harmful. Someone who has been a victim should seek advice and help from victim support organisations

If you are a target of identity fraud you should report it as soon as possible

TRUE – The sooner it is reported, the easier it is to resolve and the less damage a fraudster can do. Fraudsters move quickly when impersonating someone, the quicker you contact the organisation concerned the faster they can freeze your account or prevent fraudsters ordering goods in your name

Plenary / Assessment *for* and *of* learning

ASSESSING (DEMONSTRATING) PROGRESS

Organise students into teams and ask each team to stand in a row in front of a large sheet of paper (which should be stuck to a wall). Give the first person in each team a marker pen. Ask them to write down one thing they have learnt from today's lesson. They should then pass the pen to the next person in their team and join the end of the row. Tell each team that they will be timed and that the team with the most ideas at the end of the time will be the winners.

Continue the activity for 2–3mins, allowing all members of the team to write at least one thing on the sheet. As a class, read through the ideas written at the end of the task.

(Depending on the size of the class and resources available, it may be beneficial to carry out these key messages relays with several teams, for example 4 or 6 groups, so that more members are able to participate).

Extension activities / Home learning

EXTENSION ACTIVITY 1

Ask students to design a television advert to warn people about the risks associated with identity fraud. Students should create a storyboard showing what would be included in their advert, in particular highlighting ways to keep personal information safe online.

EXTENSION ACTIVITY 2

Ask students to create a step-by-step action plan of what someone should do if they think they might have become a target of identity fraud, considering what they should do first, etc.

If computers and internet access is available, encourage students to conduct further research to complete this task, using the following websites:

https://www.actionfraud.police.uk/ID

https://www.victimsupport.org.uk/help-and-support/what-you-can-do