



MY PERSONAL FINANCE SKILLS



Staying Safe – Presentation Guide

Introduction

This session has been developed for Key Stage 4-5 pupils, predominately for those who are in the process of considering life beyond school. It can also be used to support Sixth Form students transitioning from school or college into the wider world.

Schools and colleges may choose to integrate this session into the PSHE or enrichment curriculum.

Financial Education Planning Framework

The Financial Education Planning Framework is a national framework that aims to support the planning, teaching and progression of financial education by setting out the key areas of financial knowledge, skills and attitudes. This session aims to develop the following skills and attitudes:

- *I can stay informed about the changing nature of financial scams and identity theft so that I can stay one step ahead.*

Session Outline

The focus of this session is for students to gain an understanding about how to recognise financial scams and identity theft and to identify steps that could be put in place to prevent falling victim in the future.

Learning Objectives:

By the end of the session all students will be able to:

- recognise different types of financial scams
- identify possible characteristics of scams
- take steps to prevent being a victim of scams

In advance

Before you arrive at the school/college

- ensure you have read through the slides, are comfortable with the content and activities and have noted the timings



Personal
Finance
Society

MY PERSONAL FINANCE SKILLS



- ensure any materials and resources required to deliver the session are provided by the school or brought yourself.
- ensure that you have viewed the relevant training webinar and have passed the financial education sign off process with the My Personal Finance Skills team.

What you will need

For this session you will need:

- the presentation guide, the PowerPoint presentation and copies of the staying safe handout for each student
- to ask the school to have access to either a PC or laptop, projector, paper and pens for the students
- Internet access – this lesson is linked to a YouTube video

Length of session

This session is expected to take approximately 1 hour to deliver.

Links to Your Money Matters Textbook

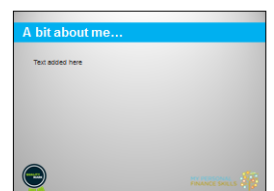
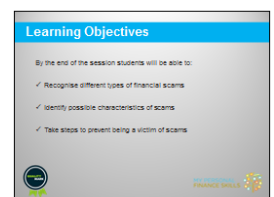
All state schools in England will have received copies of Your Money Matters textbook published by the Young Money charity. The chapter on “security and fraud” focuses on a number of the points discussed in this session and could be referred to during the session. There are many more activities, case studies and questions in the book to help further develop the student’s understanding of these topics.

Session Guidance

***where an activity is numbered, this means that this activity takes place on the student handout**

General Introduction – slides 1-3 (5 minutes)

Introduce the session topic and the learning objectives.



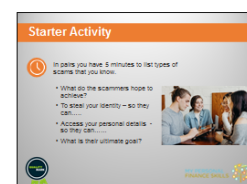


Explain a little bit about yourself, your job role and the role of the Personal Finance Society. Students are often inquisitive about visitors and what they do so ask students if they have any questions about your job.

Starter Activity – slide 4 (7 minutes)

Ask students, in pairs, to complete the starter activity. They should make a list of different scams that they might know about.

After 5 minutes ask for student feedback and if appropriate, share your own professional experiences of staying safe online with the students. Discuss what scammers hope to achieve using the remaining questions on slide 4.

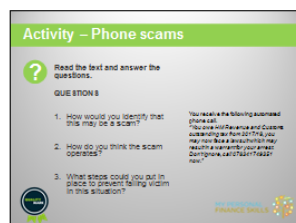
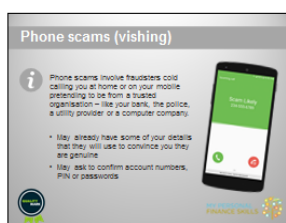


Different types of financial scams – slides 5 – 12 (20 minutes)

Using the slides discuss the different types of financial scams and ask students to complete the activities. After each section, ask students to discuss the questions with the person next to them and make notes. For the first section on phone scams, you may want to work together as a group to give students examples of the kind of answers and detail that you want. During the sections, students may want to share their experiences of online safety with you so encourage them to focus on how the situation was resolved or how they could have resolved a situation better if it didn't have a positive outcome.

At the end of each section, take answers from around the room and try to make sure that each group contributes to the feedback. See if other groups can add more details or give different responses so that the students have a range of answers. A range of answers are provided for the volunteers on the slide notes.

- Phone scams (vishing)





Personal
Finance
Society

MY PERSONAL FINANCE SKILLS




- Text message scams (smishing)

Text message scams (smishing)

i These messages are sent to your mobile phone and:

- usually claim to be from your bank or a company that you have an account or subscription with (e.g. Netflix, Apple, PayPal)
- may involve a problem with a recent purchase, suspicious activity on your account, need to verify account details
- will either contain a link or a number to call



FINANCE SKILLS

Activity – Text message scams

? Read the text message and answer the questions.

QUESTIONS

1. How would you identify that this may be a scam?
2. How do you think the scam operates?
3. What steps could you put in place to prevent falling victim in this situation?

Text Message
Tuesday 17:22

Approve the online payment to Amazon for £729.99 now. Please reply 'Yes' or 'No'. If no, please call 08001234567 immediately. Thank you

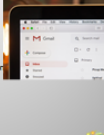
FINANCE SKILLS

- Email scams (phishing)

Email scams (phishing)

i Typical scam emails come from banks or other trusted companies and can look very convincing.

- Often scam emails do not include contact details and the email address may not look genuine
- Poor spelling, grammar and punctuation can give away the scam
- Poor graphics or odd formatting can also be an indicator that it is a scam too
- Never click on any links or download any attachments unless you can guarantee that they are genuine



FINANCE SKILLS

Activity – Is it a scam?

? Compare the two emails below and decide which one is genuine and which one is fake. How do you know this?

Security alert

Dear Kim,

Today you signed into your Apple iCloud account at 12:52 from an unknown device.

If this was not you please let us know by calling us on 0800 000 000 or by emailing us at apple-support@apple.com

Thank you

Mac Team

Head of Customer Service UK

FINANCE SKILLS

- Pop up scams

Pop ups - Genuine or fake?

i Pop ups usually involve winning a competition or to tell you that there is a system/browser problem. A pop up can appear on your phone, tablet, PC or laptop.

Look at the pop-up. In your opinion would you say that this is genuine or fake? What makes you think this?

Congratulations!

You have been selected as a winner for a free brand new iPhone

Please click [here](#) to claim your prize before it expires

FINANCE SKILLS

- Money mules/discuss the issues surrounding money mules for young people

Money Mules

i A money mule is a person who transfers illegally gained money on behalf of others, usually through their bank account.

- Criminals contact people in need of money through job adverts on social media.
- Criminal puts illegally gained money into the victim's bank account.
- They tell the victim to transfer the money to another bank account.
- Victim gets a 'fee' for transferring the money.
- Money muling can carry a 14 year prison sentence.

Real Life Examples

- Two men received different phone payments in their name.
- A victim reported that her statement by bank transfer.
- A friend who reported that she was concerned by the bank name.
- A friend who was a money mule.

They will receive about £1,000 per day and their money will be used to pay for their expenses.

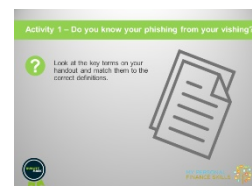
If you are interested [click here to become a money mule](#)

FINANCE SKILLS

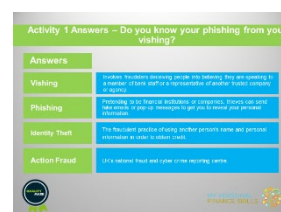


Activity 1 - Do you know your phishing from your vishing? – slides 13-15 and handout (3 minutes)

This is a recap activity to check students understanding of the key terms about the different types of financial scams. Students should match the correct term to the definition using their handout.



Once complete, take answers from the group and use slides 14 and 15 to show the correct answers.



How private is your personal information? – slides 16-18 (12 minutes)

The lesson now looks at how to protect yourself online. Ask students to watch the video and discuss the questions on slide 16.

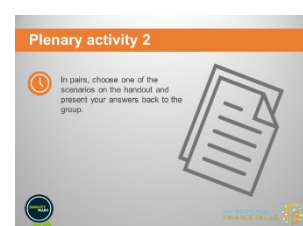


Take answers from the group and then discuss the top tips on slide 18. Using your own knowledge, you could explain how to set a strong password and explain why they should never do online banking on public Wi-Fi. You could also ask them if they have any more top tips that could be added.



Plenary/reflection activities – slides 19 -21 and handout (10 minutes)

On the handout provided, students should choose one of the scenarios and using their newly acquired knowledge, they should decide how best





to respond to the situation. If time, choose some pairs to present their ideas back to the rest of the group.

To conclude the session, inform the students that they should always query a call or message particularly if it is unsolicited. In their own time, they could create a list of 5 questions that they can use in the future to help them determine the authenticity of an email, text or phone call. You could give them a couple of ideas to get them going for example

- Are they asking to confirm sensitive details?
- Are they asking for money?
- Do I know who has sent the message?
- Is the email address genuine?
- Are there any mistakes in the correspondence?

Bring the session to an end and recap the learning objectives. Thank the students/teachers and that you hope they have learned some new things about staying safe.

Next Steps and feedback - slide 22 (1 minute)

Finally, suggest the next steps that the students could take to ensure their own online presence is safe and secure and if necessary, they could also change their passwords to make sure that their security is protected at all times. Conclude by asking students to complete their feedback form remembering to keep it anonymised.

