



Personal
Finance
Society

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



- 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

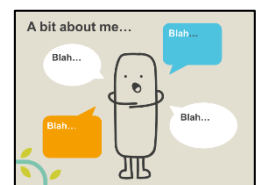
All state schools in England will have received copies of Your Money Matters textbook published by the Young Money charity. The chapter on “security and fraud” focuses on a number of the points discussed in this session and could be referred to during the session. There are many more activities, case 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.





Personal Finance Society

MY PERSONAL FINANCE SKILLS



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.

Learning objectives...
By the end of the session you will be able to:

- Recognise different types of financial scams
- Identify possible characteristics of scams
- Take steps to prevent being a victim of scams

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.

Starter Activity
In pairs you have 5 minutes to list types of scams that you know.

What do the scammers hope to achieve?

To steal your identity – so they can...?

Access your personal details – so they can...?

What is their ultimate goal?

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)

Phone scams (vishing)

Vishing involves fraudsters cold calling you at home or on your mobile pretending to be from a trusted organisation – like your bank, the police, a utility provider or a computer company. The fraudsters:

- May already have some of your details, which they will use to convince you they are genuine
- May ask you to confirm account numbers, PIN or passwords

Activity – Phone scams

Read the text and answer the questions.

You receive the following unsolicited phone call:

"You can win a fantastic prize and I can help you claim it. All you need to do is give me your account number and PIN. It's completely safe and you'll be able to claim it online. Don't worry, we're from the bank."

Q1 How would you identify that this may be a scam?

Q2 How do you think the scam operates?

Q3 What steps could you put in place to prevent falling victim to this situation?



MY PERSONAL FINANCE SKILLS




- Text message scams (smishing)

Activity – Phone scams

You receive the following automated phone call:

“Hi, we’re from the National Customer Satisfaction and Customer Satisfaction and Customer Satisfaction team and I’m calling you because you may have been a victim of a recent scam. We’re sorry to hear that and we’re here to help you. Please call 07704 79035 now.”



Q1 How would you identify that this may be a scam?


Q2 How do you think the scam operates?

Q3 What steps could you put in place to prevent falling victim to this situation?

Text message scams (smishing)

These messages are sent to your mobile phone and:

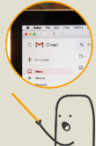
- Usually claim to be from your bank or a company that you have an account or subscription with (e.g. Netflix, Apple, Pepsi).
- May state there is a problem with a recent purchase, suspicious activity on your account, need to verify account details.
- Will either contain a link or a number to call.



- Email scams (phishing)

Email scams (phishing)

- Typical scam emails come from banks or other trusted companies and can look very convincing.
- Other scam emails do not include contact details and the email address may not look genuine.
- Poor spelling and grammar can give away the scam.
- Phon graphics or odd formatting can also be an indicator that it is a scam.
- Never click on any links or download any attachments unless you can guarantee that they are genuine.



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

Your account has been locked because of suspicious activity. To unlock your account, please click on the link below to verify your account details.

Secure link: [https://www.bankofscotland.co.uk/securelink/verify-account](#)

Expires: 23/03/2024 12:00:00

If you do not receive this email, please contact your branch manager.


Bank of Scotland

Dear Sir,

We are pleased to inform you that you have been selected to win a £10,000 cash prize. To claim your prize, please click on the link below to complete your details.

Claim your prize: [https://www.bankofscotland.co.uk/claim-prize](#)

Bank of Scotland



- Pop up scams

Pop ups - Genuine or fake?

Pop ups usually inform you that you’ve won a competition or 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 £10,000 cash prize.

Click here to claim your prize: [https://www.bankofscotland.co.uk/claim-prize](#)

Warning!

Your system has a security problem. Please click on the link below to update your software.

Update software: [https://www.bankofscotland.co.uk/update-software](#)



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

Money Mules


- Money mules transfer illegally gained money on behalf of others, usually through their bank accounts.
- Criminals contact people in need of money through job adverts on social media.
- They then transfer the ‘dirty’ cash into the victim’s bank account.
- They tell the victim to transfer the money to another bank account.
- Victims get a ‘fee’ for transferring the money.

Money muling can carry a 14 year prison sentence

Read All The Details

Money mules are people who transfer money on behalf of others. They are often young people who are contacted by criminals through job adverts on social media. They are then asked to transfer the money to another bank account. This is illegal and can result in a prison sentence.

For more information, visit: [https://www.bankofscotland.co.uk/money-mules](#)






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.

Activity 1
Do you know your phishing from your vishing?

Look at the **key terms** on your handout and match them to the correct definitions.



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

Activity 1
Do you know your phishing from your vishing?

Answers

Smishing	This is when someone tries to trick you into giving them your private information via a text or iMessage.
Money Mule	A person who lawlessly illegally get well money on behalf of others, usually through bank account.
Fraud	Intentional or negligent deception intended to result in financial or personal gain.
Hacking	When criminals succeed in guess or decipher your passwords, security questions, and/or Personal Identical Numbers (PINs).

Activity 1
Do you know your phishing from your vishing?

Answers

Vishing	Involves hackers deceiving people into believing they are speaking to a member of bank staff or a representative of another trusted company or agency.
Phishing	Attempts to trick your email inbox or computer, through can send fake emails or pop up messages to get you to reveal your personal information.
Identity Theft	The fraudulent practice of using another person's name and personal information in order to obtain credit.
Action Fraud	UK's national fraud and cyber crime reporting centre.

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.


How private is your personal information?

Watch the video and afterwards be prepared to discuss...

- What mistakes did the customers make?
- What are the implications for the customers?
- How would you make sure that you would not make these mistakes with your online presence?
- List 5 things you can do to protect yourself online.



Activity – Protecting yourself online



Click and play video. If video does not play, please follow the following link [here](#)

If you are delivering this session virtually, please copy and paste the video link so that the class can watch this in class and not via screen share.

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.

Top tips to protect yourself online

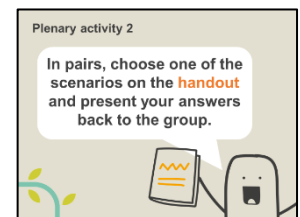
- Never disclose your security details with others
- Use strong passwords/PINs
- Do not use the same password/PIN for more than one account
- Never write your passwords down
- Only save passwords on private devices
- Keep firewalls and anti-virus software up to date on all devices
- Limit the amount of personal information you provide on social media
- Make sure you have strong security settings on social media
- Only accept online friend requests from people you know
- Don't do online banking on public Wi-Fi

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



Remind the students of the “ABC” of online security. 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 - slides 23-24 (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.





Personal Finance Society

MY PERSONAL FINANCE SKILLS



Conclude by asking students to complete their feedback form remembering to keep it anonymised.



Slide 25

At the end of the session to signpost for more information on the My Personal Finance Skills website. Please highlight what is available and ask students to share what themes they would like to know more about so we can create relevant content.

Ideas to be emailed to skills@thepfs.org or a member of the team.



Slide 26

Should you have extra time, we have a slide containing 2 x bitesize learning videos that could be played in the class. These videos consolidate learning already taken place.

If you are delivering this session virtually, please copy and paste the video link so that the class can watch this in class and not via screen share.

