



Personal  
Finance  
Society

# MY PERSONAL FINANCE SKILLS



## Identify Theft & Scams Assembly– Presentation Guide

### Introduction

This assembly session has been developed for Key Stage 4 and/or 5 students, to help them and their family & friends avoid identity theft and scams

Schools and colleges may choose to follow up this session through their PSHE or enrichment curriculum or book a My Personal Finance Skills free financial education workshop (with up to 35 students).

### 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:

- I know what steps to take should I fall victim to financial fraud or identity theft
- I know about different types of financial fraud and identity theft, such as phishing, vishing and smishing.
- I can stay informed about the changing nature of financial fraud and identity theft so that I can stay one step ahead.
- I understand it is my responsibility to protect myself from financial fraud and identity theft, and their financial and emotional impact

### Session Outline

The focus of this session is to help young people to understand the need to keep their personal information safe and to recognise and avoid a number of common scams.

### Learning Objectives:

By the end of the session the students should be able to:

- identify some of the different types of financial scams
- recognise possible characteristics of scams
- reduce their chance of falling victim to a scam

### In advance

Before you arrive at the school/college



Personal  
Finance  
Society

# MY PERSONAL FINANCE SKILLS



- Check with the school/college whether PowerPoint will be available for you and the rough number of students likely to be present. (The assembly can be presented from these notes alone if PowerPoint is not available or the group will be too large for it to be practicable)
- Ensure you have read through the notes (and slides if you are using them), are comfortable with the content and have noted the timings
- When preparing for your visit, make sure you have something prepared to say on Slide 3 (a bit about me...)
- Should you wish to use the handout, check whether copies will be provided by the school or if you need to bring them 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:

- this presentation guide
- PowerPoint presentation
- optional: Spot a Scam handout
- to ask the school to have access to either a PC or laptop and projector, regardless of whether you are using the PowerPoint (see final bullet point below)
- Internet access – this assembly includes a link to a YouTube video. Where something is conducted virtually please ensure that students can see/hear the video. If necessary, send the video link to the school to play directly.
- Where a session has been scheduled with the My Personal Finance Skills team, the PowerPoint will be sent over to the teacher upon confirmation and 1 week before the session is due to take place.

## Length of session

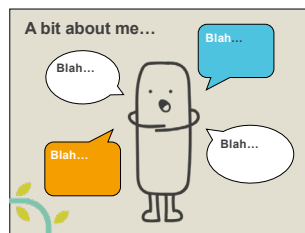
This session is expected to take approximately 30 minutes to deliver. There is a 5-minute float in the timings to allow for slippage.



## Session Guidance

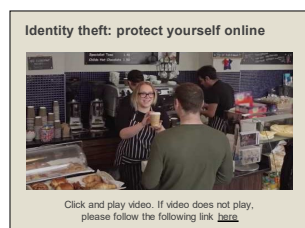
### General Introduction – slides 1-3 (5 minutes)

Introduce the session topic and the learning objectives.



Explain a little bit about yourself, your job, the role of the Personal Finance Society and the My Personal Finance Skills programme. Students are curious about visitors and what they do.

### Identity Theft - slides 4 and 5 (5 mins)



Explain that scammers might want to steal their identify and pretend to be them...so they can...

- Commit some sort of fraud, e.g.: credit card fraud, bank fraud, tax rebate fraud, benefit fraud & telecommunications fraud.
- Identity thieves can also use your identity when they commit other crimes; e.g. entering (or exiting) a country illegally, trafficking drugs, smuggling, committing cybercrimes, laundering money etc.

To avoid identity theft, they should be careful about the information they allow other people to access. It is a good idea to shred or otherwise destroy any paper document that contains sensitive information such as your bank account number.

It is now very common for identity theft to happen on-line



Personal  
Finance  
Society

# MY PERSONAL FINANCE SKILLS



Show the video full screen at: <https://www.youtube.com/watch?v=yriT8m0hcKU> The video only lasts for just over 1½ minutes. **NB** – If you are using the PowerPoint please make sure you ‘enable content’ when you open the presentation so that the video plays. You should be able to play the video directly in presentation mode. However, if you are unable to, you can find the direct link to the video below the video itself.

## How private is your personal information – slide 6 (2 mins)

**How private is your personal information?**

- You might want to think about the mistakes those customers had made about keeping their personal information safe.
- Once someone has details of your name and date of birth etc. they could easily pretend to be you
- Is your online information safe? If not, what can you do to protect it?
- Only post information publicly if you would be happy to stand on a busy street and hand out copies to passing strangers. Once something has been published online you no longer have control over it.



Suggest that students might want to think about the mistakes the customers had made about keeping their personal information safe

Explain that once someone has details of your name date of birth etc someone could easily pretend to be you. Is their online information safe? If not, what can they do to protect it? Stress that they should only post information publicly if they would be happy to stand on a busy street and hand out copies to passing strangers. Once something has been published online you no longer have control over it!

## Types of Scam – slides 7 -8 (4 mins)

**Types of Scam...**

**Impersonation Scams**  
Scammers pretend to be from a well-known trusted organisations. They often threaten you into handing over money or personal details.

**Support and Account Scams**  
These messages often appear to come from a "Webmail Team" or "Customer Support". The scammers might offer to repair an issue with your computer and ask you to provide your email username and password to confirm, cancel, or upgrade your account.

**Order and Delivery Scams**  
Scammers send a message that asks you to click a link to verify or check your order. They often spoof the organisation's real communication templates.

**"Windows" Scams**  
If you didn't enter a competition or a draw, then you definitely didn't win! These scammers aren't going to give you free money; they are out to steal it from you.




**Types of Scam...**

**Funds Transfer or Money Muling Scams**  
You receive a message saying that someone wants to transfer a large sum of money to you for "safe-keeping," but they need your bank account details to do so. The scammer plans to overdraw your account or use you to help them launder money from illegal activity.

**Sexortion/Exploitation Scams**  
Someone threatens to share embarrassing pictures or videos of you with your friends, family and/or online unless you pay them a ransom.

**Social Media Scams**  
These often look genuine, using official brand logos etc. Clicking on the links sends your personal information on to someone else and may also trigger a "take" with friends & family... who are then more likely to fall for the same scam as they are probably going to assume that you meant to send them the link. **Mystery Shopper** and **Work from Home Job Scams** are common on social media; these are usually an attempt to steal money and/or your personal information.



Explain that there are many different types of scams.

Depending on the size of the group and the timing, you could ask students to stand up if they have received a scam email or message...and/or if they are aware of each of the different types.



Personal  
Finance  
Society

# MY PERSONAL FINANCE SKILLS



## **Impersonation Scams**

Scammers pretend to be from a well-known trusted organisation. They often threaten you into handing over money or personal details.

## **Support and Account Scams**

These messages often appear to come from a "Webmail Team" or "Customer Support". The scammers might offer to repair an issue with your computer and ask you to provide your email username and password to confirm, cancel, or upgrade your account.

## **Order and Delivery Scams**

Scammers send a message that asks you to click a link to verify or check your order. They often spoof the organisation's real communication template.

## **"Winner!" Scams**

If you didn't enter a competition or a draw, then you definitely didn't win! These scams aren't going to give you free money; they are out to steal it from you.

## **Funds Transfer or Money Muling Scams**

You receive a message saying that someone wants to transfer a large sum of money to you for "safe-keeping," but they need your bank account details to do so. The scammer plans to overdraw your account or use you to help them launder money from illegal activity.

## **Sextortion/Sexploitation Scams**

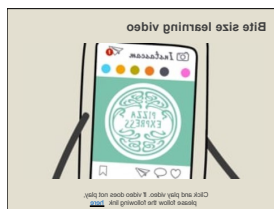
Someone threatens to share embarrassing pictures or videos of you with your friends, family and/or online unless you pay them a ransom.

## **Social Media Scams**

These often look genuine, using official brand logos etc. Clicking on the links sends your personal information on to someone else and may also trigger a "share" with friends & family...who are then more likely to fall for the same scam as they are probably going to assume that you meant to send them the link. **Mystery Shopper** and **Work from Home Job Scams** are common on social media, these are usually an attempt to steal money and/or your personal information.



## slides 9 – 14 (5 mins)



**Phone scams (vishing)**

Phone scams involve 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.


- 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



**Text message scams (smishing)**

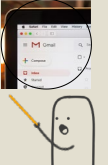
These messages are sent to your mobile phone and:

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



**Email scams (phishing)**

- 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 often gives 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



**Pop ups - Genuine or fake?**

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. You should immediately be suspicious because it looks unprofessional and lacks contact details.

Congratulations! You have been selected as a winner for a £10,000 prize. Please click here to claim your prize before it expires.




**Money Mules**

- A money mule is a person who transfers illegally gained money on behalf of others, usually through their bank account.
- People often get drawn in through job adverts on social media.
- Illegally gained money is put into the victim's bank account and they are asked to move it to another account for a fee

**Red flag warnings**

- Job advert offers a generous payment over time
- Job advert offers an opportunity to work from home
- Job advert offers a commission or bonus based on sales
- Job advert offers a commission or bonus based on sales
- Job advert offers a commission or bonus based on sales

Money mules can carry a 14 year prison sentence



Slide 9 – play video. If conducting session virtually, make sure you copy and paste the link into the chat box for the class to watch it in the class.

Depending on the timing you might want to go into a little more detail about some common types of scam. You can use some or all these slides, however, this section can be skipped if time is tight and/or you prefer to use the handout (see below)

### **Phone scams (vishing)**

Phone scams involve 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. They may already have some of your details that they will use to convince you they are genuine. They may ask you to confirm account numbers, PIN or passwords

### **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, PayPal), they often mention a problem with a recent purchase, suspicious activity on your account, or ask you to verify your account details and will either contain a link or a number to call.

### **Email scams (phishing)**

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 often give away the scam and 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 are certain that they are genuine.

### Pop ups - Genuine or fake?

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 and they can be difficult to get rid of! Pop ups can also hide a virus that access personal information on your phone or PC so always be very careful when clicking on them.

### Money Mules

A money mule is a person who transfers illegally gained money on behalf of others, usually through their bank account. People often get drawn in through job adverts on social media. Illegally gained money is put into the victim's bank account and they are asked to move it to another account for a fee. Money muling can carry a 14-year prison sentence

### Add-ons – slides 15 - 16 (3 mins)

**Add-ons**

- Although they're not a scam... it can be very easy to spend a lot of your money or someone else's without realising it, through add-ons such as gaming expansion packs.
- Once a new game comes out, the publishers often support it with downloadable content, which is usually for a price.
- In one infamous game you could purchase a diamond-tipped chisel, which would be very useful indeed...but the cost for it was three billion in-game coins equivalent to £34,000!

**Add-ons**

- Make sure you know whose card is associated with the gaming account and that you have their permission before buying anything extra.
- Ideally either turn off in-app purchases, ask for an extra level of security to be added, set up a separate gaming account with no card attached so you can't spend anything without really intending to!

"My son spent £100 over four days at the end of March. He brought me the name was the user name on the game the money was coming out of his account. Surely this was not the case."

"Our seven-year-old son managed to spend £30 in a couple of weeks ago. He thought it was game credits rather than actual cash."

Although they are not a scam...it can be very easy to spend a lot of your money or someone else's without realising it, through add-ons such as gaming expansion packs (also known as Downloadable Content or DLC). Once a new game comes out, the publishers often support it with additional DLC, and there is usually a charge.

In one infamous game you could purchase a diamond-tipped chisel, which would be very useful indeed...but the cost for it was three billion in-game coins equivalent to £34,000!

Explain to students that they need to make sure they know whose card is associated with the gaming account and that they have their permission before buying anything extra.



It is a really good idea to either turn off in-app purchases, ask for an extra level of security to be added, or set up a separate gaming account with no card attached so they can't spend anything without really intending to!

Quotes from parents: "My son spent £150 over four days at the end of March. He thought as his name was the username on the game the money was coming out of his account. Sadly this was not the case. "Our seven-year-old son managed to spend £80 a couple of weeks ago. He thought it was game credits rather than actual cash."

### Top tips to protect yourself online - slide 17 (2 mins)

- Never share your security details with anyone else
- Use strong passwords/PINs
- Use a different password/PIN for more every 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 and make sure you're using strong security settings on social media
- Only accept online friend requests from people you know
- Don't do online banking on public Wi-Fi



### Remember Your ABC - slide 18 (2 mins)

Stress that if you want to stay safe, then...

- **A**ssume something is a scam until you can confirm it is not
- **B**e careful with your personal information
- **C**heck before you take action/ respond



### What Next? - slide 19 (2 mins)





Personal  
Finance  
Society

# MY PERSONAL FINANCE SKILLS



**Next steps...**



- Ask a friend or a family member who you trust to search all of your social media profiles and see what information is public. If you are not happy with what others can see then tighten up your privacy settings.
- Think before you post any personal information
- Check your passwords for all the accounts that you have online – change them if you have not done this for a while and remember to use a different one each time

Bring the session to an end and suggest that after the session, students might like to:

- Ask someone they trust such as a close friend or family member to search all of their social media profiles and see what information is public. If they are not happy with what others can see, then they can tighten up their privacy settings.
- Think carefully before posting any personal information.
- Check their passwords for all the accounts that they have online – change them if they have not done this for a while and remember to use a different one each time

## **Thank you & Questions – Slide 20**

When ending the session, thank students & teachers for their attention and signpost to the [mypersonalfinanceskills.org](http://mypersonalfinanceskills.org) where students can find more financial education content.

Furthermore, please remind that the programme also delivers workshops in smaller groups.

**Thank you & Questions**

Find us online [mypersonalfinanceskills.org](http://mypersonalfinanceskills.org) for:

-  Bitesize learning videos (Scams & Social Media, your first payslip and what it includes)
-  A student money blog
-  On demand financial education sessions

To organise another assembly or workshop in smaller groups, please email us [skills@hepfps.org](mailto:skills@hepfps.org)

## EXTRA OPTIONS

Should you wish to bring it to life more, look up some recent scams to talk to students about. You could screen shot them and place them into a presentation to show.