



Module 6

Session 12 M6SC12



Fraud and Your Money

Lesson summary

One of the biggest threats to managing our money is fraudsters, both in person and online. This session provides guidance on how to recognise fraud across a wide range of channels to protect yourself, your identity and your money.



Learning Objectives

To be able to understand the common red flags in popular types of fraud.

To be able to apply your fraud knowledge in identifying fake messages.

To be able to create a strong password.

Lesson preparation

1. HSBC PowerPoint slides to facilitate lesson: Module 6 Session 12: Fraud and Your Money
2. HSBC Worksheet M6W12 – used to complete activity
3. HSBC Stretch Challenge M6SC12 – to further embed learning as homework or a class project
4. Prepare examples to share where you or someone you know has been targeted or fallen victim to a fraud. What was the impact financially/emotionally etc?

Slide 2: What is Fraud? – 5 mins

Years ago, criminals used to try and rob banks to steal your money. However, with advanced security measures this is no longer effective. Instead, fraudsters find it easier to trick people into giving away access to their money.



Group work: Ask the young people to work in groups to discuss frauds they are familiar with. Friends/family may have been a victim or it may have been something that they have seen on the news.

Allow 2-3 minutes and then take examples of what has been discussed from each group.

CLICK to reveal the answers:

In the mind map with the common types of frauds – see which ones the groups identified and the other types of fraud mentioned that nobody has experienced.

Set the expectation that all of these fraud types will be covered in Module 6. For this first session the main financial frauds of Phishing, Smishing, Vishing, ATM Fraud and Card Not Present fraud will be covered.

Slide 3: How much did criminals try to steal through fraud in 2023? – 3 mins

We know that fraudsters work incredibly hard to try and get access to people's hard earned money.



Ask the group: How much did criminals try to steal through fraud in 2023? (Answer options on the slide)

CLICK to reveal:

The answer is £2.42bn, although the banks managed to block £1.2bn of this - that's 50p in every £1.

What do you think we could buy for £2.42 billion pounds?

Take some answers first before revealing the stats.

- Around £36 for each of the 67 million UK residents
- 11,025 Ferrari F8 Spiders each priced at £219,500
- 167 five bed mansions each priced at £14,500,000

How do we feel about that?

Slide 4: Spot the signs of fraud: Email – 3 mins

Give the class time to read the message on screen.



It is recommended that you put your presentation into presenter mode and click the magnifying glass to zoom closer into the email example.



Group work: Fraudsters send emails to people to encourage them to give access to their bank accounts and money. It's hard to tell the difference but there are some clues. Can you spot them?

Give the class time to read the message on screen and discuss in groups then run through their thoughts.

CLICK to reveal answers:

'Dear customer': This is the first clue - your bank will know your name and include it when it writes to you.

Sender's email address: Always hover over this to reveal the actual sender's email address which may look suspicious.

Check grammar and spelling mistakes: Your bank is unlikely to say 'slight error' – either there has been an error or there hasn't.

Do you recognise the web link? Don't click on any web links that you don't recognise.

CLICK and read out the 'Look for the detail' box.

Slide 5: Spot the signs of fraud: SMS – 3 mins

It's even harder to tell if a text message is real or attempted fraud as you may have less information to help you decide.



Group work: Give the class time to read the message on screen to spot the signs of fraud and discuss in groups.



Again if you can, put your presentation into presenter mode and click the magnifying glass to zoom closer into the email example.

CLICK to reveal answers:

- Check spelling / grammar
- Have you visited the store?
- Large amount to create fear and panic
- Asking you to ring not text
- Graphics look odd

CLICK and read out the Stop and Think box.

- Do you remember buying what's described?
- Don't call the number in the text message
- Call the bank's usual phone number (such as the number on the back of your card) not the number in the message

Slide 6: Spot the signs of fraud: SMS – 3 mins

Fraudsters can manipulate messages, so they appear in a thread with genuine messages or with the company's name included. The first message in the thread was legitimately sent by the retailer John Lewis.



Ask the group: What are the differences between message 1 and 2? What red flags can you see?

Answers:

- Check spelling / grammar
- No personal details/card number
- Suspicious looking link

Slide 7: Design your own scam – 10 mins



Group work: Use worksheet M6W12 to create your own fraudulent message.

- Which company are you impersonating?
- What are you trying to get your victim to do?
- Will you use scare tactics to get them on the phone or a suspicious link to get into their device?
- Don't forget to include a few errors like spelling, grammar, and unusual links to help us know it's a scam

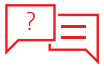
Young people to complete their worksheets individually whilst discussing ideas in their groups / tables before sharing examples with the rest of the class.

Slide 8: Spot the signs of fraud - 4 mins

Some fraudsters will cold call you to convince you to move money or get you to reveal your passwords.



Click to play: Short fraud TikTok.



Ask the group: What should you do if you are suspicious about a phone call?

Discuss thoughts of the young people and then click to reveal top tips:

- Stop! Don't continue with the call
- Clear the line by ringing another person first
- Check with the genuine company using confirmed contact details
- Report the number to Action Fraud

Slide 9: Types of fraud - 2 mins

The messages we have just looked at were all different types of fraud.

'Phishing' is a type of financial fraud where criminals trick people by email to get their details or to get access to their money.

It's name sounds like fishing as they are trying cast a long net and see who gets caught. The phishing link could ask you to give information through what you think is a reputable site or it could trick you into giving access to your computer and all that you have stored on it!

'Smishing' is where text messages (SMS messages) are sent trying to trick people into paying some money or to click on suspicious links, sometimes by pretending they are from a company that you trust.

The smishing link could trick you into downloading malware onto your phone giving cyber criminals access to your phone and data. Or the link could take you to a malicious site which looks like a company you trust – then tricking you into giving information and sending it to the criminals.

Lesson commentary

'Vishing' is over the phone phishing where scammers will try to persuade people to share information by pretending to be from the bank or another organisation that you trust. Often they will say it's urgent and sound very official to try and get you to do what they want.



Ask the group: So with all these fraudsters about what can we do?

CLICK and reveal answers:

1. Never give your PIN to anyone
2. Never let anybody use your bank cards
3. Don't tell anyone your passwords for your bank account – even bank staff
4. Never transfer money to another account that you don't know/own to keep your money safe

Slide 10: Card not present fraud - 2 mins

"Card Not Present" transactions occur when the payment card is not in the same place as the retailer.

This could be through:

Online order/telephone order: A fake retailer could be selling items with prices that are too good to be true. You never receive the item, but the card details you have provided are then used to buy something for the fraudster at the same price which helps them avoid suspicion.

Card already on account: Fraudster could hack into the account of your streaming service which has already approved your card and take over that service for themselves changing all the other details on the account.

Things to consider.

- Think about if the deal seems too good to be true
- Use a secure payment method on a reputable site
- Consider using a credit card for additional protection
- Read online reviews of the retailer
- Check with the manufacturer if they are a legitimate seller

Slide 11: ATM fraud - 3 mins

Shoulder Surfing

Watch out for people standing too close to you when you are using the cash machine. They may be looking to see your PIN.

CLICK to reveal icon: Don't be afraid to:

1. Ask people to stand back
2. Use a different machine if you don't feel comfortable
3. Use the cash machine inside if the bank is open

Distraction Tactics

CLICK to reveal icon: Make sure you don't get distracted by someone – They may be looking to grab your card whilst you are distracted.

1. Keep your eyes on your cash and your card at all times
2. Tell the person talking that you will talk to them in a moment
3. If they persist end the transaction and alert a member of staff

CLICK to reveal: Skimming or Retention Devices

Skimming: A device over the card entry slot of an ATM copies the details from your magnetic strip. The fraudster can use this to make payments through making fake cards.

Retention: If a fraudster has used a device to trap your card in the machine, report it to the bank immediately and put a stop on the card.

Read the Devices Top Tips

- Do not try and remove the device
- Don't use the ATM
- If your card is captured, call your bank and cancel it
- Report the suspicious device to the bank or the police immediately
- Keep bank helpline numbers saved in your phone for emergencies

Slide 12: Making a payment - 5 mins

Banks are continuously improving their security to protect your money. However, you still play an important role in keeping your money safe whilst making online payments.



Ask the group: What details do you need to know to make an online bank transfer?

Options for answers:

- Full name
- Sort code
- Account number

You may also need address and specific information for international payments. Each country may have different regulations.

Banks now protect customers with the confirmation of payee service. Every time you make a payment, they will check with the other bank that the name you have typed in matches the name on the account. If it doesn't match, then you will receive a warning before sending the money. The choice will then be yours if you want to continue with the payment.



Ask the group: What would you do if you received an email asking you to change the account details you pay your rent to?

Discuss answers and then reinforce that we shouldn't change account details such as these until we have confirmed it with a member of staff at that organisation.

The company may have been infected by spyware which is looking out for key words like "payments" and will email you changing account details to the account of the fraudster. This often means the customer and the company aren't aware of the fraud until several months later. Fraudsters especially like to target organisations that transfer large amounts of money on their customers behalf like estate agents/ solicitors etc.



Ask the group: What do we mean by two factor authentication?

Two separate confirmations of your identity. Like having two locks on your front door

If your password was compromised, the fraudster would still not be able to get into your account without your fingerprint, face scan or your security code

Slide 13: Creating a strong password - 10 mins

Fraudsters can obtain passwords from data breaches, your use of unsecured Wi-Fi or by social engineering through looking at your social media profiles and guessing your security answers.

This can give them access to our finances and personal data and give them the ability to commit fraud without restriction.



Ask the group: How many of you use the same password for multiple accounts? What is the risk?

CLICK to reveal answers:

Using the same password makes it easy for the fraudster to try that same username and password on other popular web sites to see if you have an account with them. It would literally be a domino effect of account takeovers.

If you don't have 2 factor authentication set up. They could empty your bank account or blackmail you to return access!!

CLICK and reveal the importance of secure passwords:

Research shows that longer passwords are easier to remember than short ones. We recommend using random phrases that have no link to your personal life to ensure that the password can't be guessed by a scammer.

CLICK to reveal the ideal way to build a password:

- Word 1
- Word 2
- Word 3
- Number
- Punctuation

Lesson commentary

Or

Word 1 – Jolly

Word 2 – red

Word 3 – cloud

Number – 4

Punctuation – ?

Make it clear that there should be no relationship. between the words and your own personal experiences. Making it different enough will also make it memorable later.



Group work: Use the remaining time to generate some random passwords. You can work in groups to generate one word of the password each or individually. Ask for examples of random passwords the group have built.

Slide 14: How to protect you and your money from financial crime - 2 mins

Read through how to protect yourself from financial crime:

- Be careful using ATMs
- Don't tell anyone your banking security details
- Be vigilant of calls, emails, social media and text messages
- Use strong, separate passwords for each account that no one else can guess
- Be wary of unsecured WIFI
- Use two factor authentication
- Be alert if payment details suddenly change

Remember: Just because someone says they are calling from HSBC or any other bank does not mean that they are.

Slide 15: Stretch Challenge

This can be used as you see fit for a homework, a group project or additional lesson during school hours. A Stretch Challenge worksheet has been provided to outline the challenge.



Group work: Stretch Challenge M6SC12. Research one of the frauds discussed during session 12 which introduced us to fraud and keeping your money safe. Create a list of top ten tips to protect yourself and others from that fraud.

You should include information that covers the following points:

- How to spot the fraud?
- How to stay safe from the fraud?
- How it could impact your finances if you are a victim?
- What you should do if you think you have been a victim of the fraud?

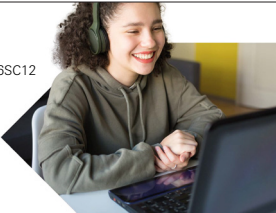
Think carefully about how you will display the information to make it easy to read. You can use appropriate images and statistics to support your top tips.

Slide 17: Stretch Challenge

Stretch Worksheet M6SC12

6

Module 6
Session 12 M6SC12



Protection from fraud

Research one of the frauds discussed during session 12 which introduced us to fraud and keeping your money safe. Create a list of top ten tips to protect yourself and others from that fraud.

You should include information that covers the following points:

- How to spot the fraud?
- How to stay safe from the fraud?
- How could it impact your finances if you are a victim?
- What should you do if you think you have been a victim of the fraud?

Think carefully about how you will display the information to make it easy to read.
You can use appropriate images, statistics to support your top tips.

Name: _____

Slide 18: Worksheet

Worksheet M6W12

6

Module 6
Session 12 M6W1



In the shoes of a fraudster: SMS

To help us better understand the world of a fraudster, try creating your own fraudulent message. How compelling can you make it so that people click on the link or give you the information that you are after?

Consider:

Who is the fraudster imitating?
Who is the target audience?
What does the fraudster want from their target?

Techniques that the fraudster might use:

- Scare Tactics (e.g. limited time only, act now to avoid losing money etc)
- Links that look like another company/feel safe to click

Extra clues that make it obvious this is a fraudulent message:

- Spelling mistakes or grammatical errors
- No personal details of the person you are contacting
– remember the fraudster won't have this information



Essex Year of NUMBERS |  HSBC UK Name: _____