

Module 6

Session 13



Fraud and Social Media

Lesson summary

As you build financial independence it's important to be aware of the threat of fraudsters, particularly in online channels. This session builds understanding of the dangers of oversharing on social media and the impact this can have, as well as outlining steps we can take to keep our social media usage safe.



Learning Objectives

- To be able to understand the different types of social media scams and frauds.
- To discuss how these could impact us in the real world.
- To build awareness of good social media practices.

Lesson preparation

1. HSBC PowerPoint slides to facilitate lesson: Module 6 Session 13: Fraud and Social Media
2. HSBC Worksheet M6W13 used to complete activity
3. HSBC Stretch Challenge M6SC13 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 1: Fraud and social media – 1 min

Explain that today we will be looking at how fraud shows up in social media.

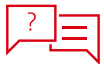


Ask the group: What is the difference between 'fraud' and a 'scam'?

Fraud is generally used to describe a suspicious activity on your bank account that you didn't authorise.

A scam is where you have authorised the payment yourself but it's a trick. You've been persuaded to buy a fake item, hand over a security code or transfer a sum of money, not realising you've been conned by a criminal.

Over 75% of the world's population uses social media.



Ask the group: How many people do you think that is?

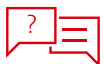
Answer: Over 4.5 Billion

Slide 2: The world of social media – 3 mins



Ask the group: How do you think social media helps us in our day to day lives?

Connectivity, entertainment, games, sharing.



Ask the group: What are the age restrictions on social media?

Most social media providers require you to be 13 before using their services.



Ask the group: Why do you think these rules are in place?

To protect young people from those who would try to defraud or manipulate them. To ensure people are old enough to handle the responsibility.



Ask the group: How long do our posts stay online?

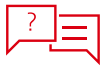
Forever – even if you delete a post later the server will still hold that information. Equally other people may have taken screen shots.

People have lost their jobs from things they have posted on social media as young people and as adults.

Slide 3: Protect your identity – 6 mins

Video (sound needed): Introduce the video which shows the dangers of leaving social media settings public. If the video fails to play you can load this manually via YouTube:

[Data to Go | CIFAS Film | Fraud & Security | HSBC UK – YouTube](#)



Ask the group: CLICK to reveal the discussion questions:

1. What is your reaction to the video?
2. What personal information do you think a fraudster could find on people's social media profiles?
3. What is the difference between public and private social media settings?
4. How would you feel if you lost a job because of something you posted on social media years earlier?

On the following slides take a look at some social media profiles to see how easy it would be to defraud the users.

Slide 4: Lauren's profile – 8 mins



Group work (Worksheet M6W13): Review Lauren's Profile on the new social media platform SnoopBook. Read out the bio and the three social media posts. Ask the group to review these on the worksheet (M6W13) and discuss the follow up questions.

Q1: What do we know about Lauren?

Answers: DOB; town she lives in; picture of front door – her address; her job; where she went to university; her hobbies; her favourite places; the number plate on her car; details of her friends; her friend's job; that she will be travelling this summer; name of her dad.

Q2: What could a fraudster do with the information?

Answers:

- Use of hashtags can make it easier for Lauren and her details to be found
- Lauren's personal details (eg address) could be used as security questions for other online or bank accounts
- Personal details (eg hobbies) could be used to create a fake friend or romance scam
- Details of Lauren's car/house/job – makes it easier to be targeted in the real world
- Giving away details of friends and family – make it easier for them to be targeted too
- Talking about holidays – tells burglars that the house will be empty over the summer

Q3: What advice would you give to her to secure her account?

Answers:

- Check her privacy settings to control who can see her account/her posts
- Make sure she does not post pictures with important information on them like her address or car registration
- Never post about a holiday that you are about to go on/whilst you are on holiday as it lets burglars know you are not at home (add them when you get back)
- Never post information that could give clues to your passwords/personal information
- Be careful who you connect with on social media
- Remember if you tag friends you could be exposing them to a fraudster so be careful with what you are posting

Slide 5: Jas' profile – 8 mins



Group work (M6W13) continued: Review Jas' profile on the new social media platform SnoopBook. Read out the bio information and then the three social media posts. Ask the group to review these on the second part of the worksheet (M6W13) and discuss the follow up questions in their groups.

Q1: What do we know about Jas?

Answers: Year of birth; town he lives in; the industry he works in; he is married; he has a son; he visits local cafes; he visits the local park; he is training for a marathon

Q2: What could a fraudster do with the information?

Answers:

- Jas' personal information is reserved only for friends keeping the fraudsters out
- Fraudsters would find this profile more difficult as we have no specifics that could be used to scam or defraud Jas

Q3: What are the differences between Jas and Lauren's accounts?

Answers:

- The information on Jas' profile is more general and of limited use to a fraudster whereas Lauren gives more detailed information on herself which could be used by criminals
- Jas' profile has privacy settings in place so he is still able to share some information with his friendship group
- Jas takes care not to tag others in his profile – avoiding bringing them into view of fraudsters

Q4: Who is the easier target for a fraudster? Jas or Lauren?

Answer: Lauren as she has been very open with all of her personal information and doesn't have any privacy settings in place making it easy to access her information.

Slide 6: Fake friends and romance scams – 2 mins

Having a lot of personal information available online makes us easy targets for fake friends or romance scams.

1. The fraudsters can create a perfect persona that we would have lots in common with.
2. This may mean we build a strong friendship or relationship quickly.
3. They will sometimes ask for your phone number to talk away from the social media page.
4. However, there will always be a reason why they cannot video chat or meet in the real world. They may give believable reasons at first to stop you getting suspicious.
5. Next, they will start to ask for money. Sometimes it can be small amounts to get you used to the idea of gifting them money. They may then build up to larger amounts so that they can come & visit you or to help with a family emergency etc.
6. As we think we are in a friendship or relationship with this person it can make it difficult to say no. Our emotions may cloud our ability to think critically about what is being asked.

For example, a Japanese Widow was scammed by a man claiming to be a Russian Astronaut. She gave him over £27K in a month so he could get home from space and marry her. This is an extreme example, but it just shows you how manipulative these fraudsters can be.

If anyone you've only met online asks you for money or your financial details this is a red flag. You should block them and report them to the site immediately to help protect other users as well.

Slide 7: SnoopBook games wall – 2 mins

Ask the group to imagine we are back on our SnoopBook social media platform and are visiting the games wall to find something to do whilst we wait for a train.

- I will guess your favorite musician with 15 easy questions!
- This quiz will predict your future!
- Which film / TV character are you?
- What is your dream job based on your personality?
- The impossible quiz !
- 10 Questions to find out your superhero identity!



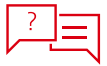
Ask the group: Which, if any of these quizzes would you be tempted to play to pass the time?

Explain that it's important to be careful as quizzes and apps on social media can be used to harvest our personal data. They usually include terms and conditions which allow the data you enter to be sold to third parties. The answers we give to quizzes may also allow fraudsters to build up information they can use to target our online banking security or be used to help create those fake friends.

Slide 8: Who wants to be a data leaker? Q1 – 2 min



Group work: Introduce the 'Who wants to be a data leaker' quiz. In table groups they need to decide which would be the safest option for each slide.

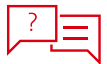


Ask the group: What question would be safe to answer?

Answer: B – Doesn't give away any personal details and only a 50/50 choice.

(A/C/D have all been used for online banking security questions)

Slide 9: Who wants to be a data leaker? Q2 – 2 min

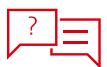


Ask the group: What question would be safe to answer?

Answer: C – Your teacher's description will just be an adjective to describe your personality.

(A/B/D have all been used for online banking security questions)

Slide 10: Who wants to be a data leaker? Q3 – 2 min



Ask the group: What question would be safe to answer?

Answer: A – It would just be your own opinion.

(B/C/D have all been used for Online banking security questions)

Slide 11: Who wants to be a data leaker? Q4 – 2 min



Ask the group: To see your quiz results, would you provide?

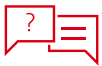
Answer: D – None of the above, quizzes looking for contact details may be trying to sell you additional products and services or in the worst-case scenario allowing a fraudster to get in contact.

Slide 12: Fake quizzes: Remember! – 4 mins

Whether you are completing an online quiz or registering for an app, be mindful of the personal information you may be revealing:

- Are the answers to the quiz important for the security of another online account?
- Do I trust the website or app with my personal data?
- Are they selling this data on afterwards?
- What if this data fell into the wrong hands, could it be used to target you in the real world?

Globally, over 1 million young people become victims of fraud each year, with an average loss of £400 per person.



Ask the group: How much money could we save as a class by being more mindful of our online activities?

(Number of young people in classroom) X £400 = answer

For example if there is 30 in the group

$$30 \times £400 = £12,000$$

If no access to a calculator:

Calculate the number of people in classroom X 100 then double the answer twice.

For example $30 \times 100 = £3,000$

$$\times 2 = £6,000$$

$$\times 2 = £12,000$$

Slide 13: Fact or fake? Dubious links and fake apps – 4 mins

We are back on our SnoopBook social media platform and are now looking at posts coming up from other users. In tables ask each group to decide which of the 3 posts are safe, dangerous, or are legal but beware.

1. Download the "My Most Used Words" app. Find out your most popular words by connecting us to your account.
 2. Don't forget to sign up for 2-Factor authentication. Log in and activate this by visiting your settings.
 3. Be the first to sign up for our exclusive shopping app. 30% off most items and free delivery for the next hour. Download at www.Easyspend.972365.ru
-
1. **Legal/beware:** 18 million users downloaded this app on a popular social media platform. The app then recorded IP address, profile picture, age, friends list, posts, posts you are tagged in, education history, likes, photos and more. On this occasion the data was not sold but should be a warning to check the terms and conditions of other apps that you let talk to your social media.
 2. **Safe:** Message from the social media platform encouraging you to review your security by visiting the settings page. No link.
 3. **Dangerous:** Suspicious link, time pressured deal, too good to be true.

Slide 14: Fact or fake? – Fake goods – 4 mins



Group work: Now look at some posts for people looking to sell items online. In table groups decide which of the 3 posts selling items are safe, dangerous, or legal but beware.

1. Selling old phone to earn money for new laptop. Comes with protective case but no charger. PayPal verified.
2. Ultra HD Projector and Screen M8ssive r3duction Noe only £25 whilst st8cks last Please prvide crd details
3. Hair straighteners. Never been used. Unwanted Christmas gift. Will post first class once you pay £40 into my online account.

1. **Safe:** Using a reputable third party to manage the payment means you have a point of contact if there are any issues with the purchase. Also a third part payment system means your details are not shared with the seller directly.
2. **Dangerous:** Poor spelling and grammar with an unrealistic price for an expensive item. Fraudsters use social media profiles to advertise the 'sale' of discounted goods to consumers. When a customer goes to buy the product, the fraudster then uses the customer's card details to purchase the items from a legitimate source and then keeps the payment from the customer.
3. **Legal/beware:** It is legal to sell items like this on social media, many may be genuine but beware you will have no legal protection and you will struggle to get a refund if anything goes wrong.

Slide 15: Fact or fake? Fake jobs – 4 mins



Group work: Next go through some posts for people advertising jobs online. In table groups decide which of the 3 posts are safe, dangerous, or legal but beware.

1. Urgent need for support staff at hospitals in your local area. To progress your application pay £75 to cover DBS checks and processing.
 2. Payment Processing Operative. Flexible Hours. Earn commission on each payment. Great way to earn fast.
 3. Interested in weekend work at our family run restaurant? Please visit our careers page to find out more and start the application process.
-
1. **Legal/beware:** Agencies and recruitment firms may advertise jobs online and they may charge you additional fees to register with them. Be aware that you may be able to find the same jobs yourself for free on job search engines. They may also overcharge for services like DBS checks. Shop around and consider all the options.
 2. **Dangerous:** This job advertisement would be a red flag for money muling. The fraudster is looking for people to help them launder money through their own bank account. The victim may not realise this is a fake job until the crime has been committed. Assisting with money laundering results in being blacklisted with all financial services for 6 years and potentially a prison sentence.
 3. **Safe:** No link to click on instead the advertisement advises the user to visit their careers website to start the application process.

Slide 16: Summary: Staying safe on social media – 2 mins

Read through summary slide encouraging your group to think about their own social media presence:

- Make it hard for criminals to get hold of your personal details – be careful what you share online
- Be mindful of your posts – future employers or colleges may look at your profile
- Review your settings, who can see your personal information?
- Be vigilant of quizzes and games that gather personal information, especially questions that may relate to online banking security
- Be wary of fake friends adding you, what are they trying to get from you?
- Take the time to review links, job postings and adverts you may see on your social media
- If you think you have been a victim of a fraud, tell your bank and report the social media account immediately.

Slide 17: Stretch Challenge

This can be used as you see fit for a homework, group project or additional lesson during school hours. Use the Stretch Challenge worksheet provided to record answers.

Stretch Worksheet M6SC13

Our emotional reaction to posts, links and direct messages are the weak spots that fraudsters use to get round the security of social media companies.

- Describe 3 actions you will take following this fraud and social media session
- Create a set of instructions for a young person setting up a social media profile for the first time

6

Module 6
Session 13 M3SC13



Stretch Challenge: Fraud and Social Media

Taking Action

People with social media accounts face a 46% increase in the chance of becoming a victim of identity theft.

Our emotional reaction to posts, links and direct messages are the weak spots that fraudsters use to get round the security of the social media companies.

Describe 3 actions you will take to make sure that you do not become a victim of fraud.

1.

2.

3.



Essex Year of



 **HSBC UK**

Name: _____

Helping others

Create a set of instructions for a young person setting up a social media profile for the first time.

Remember to include guidance on privacy settings, information oversharing and how to avoid social media scams and attempted fraud.



1.

2.

3.

4.

5.

M3SC13

Name: _____

Worksheet

Worksheet M6W13

Review Lauren's profile on the new social media platform SnoopBook. Read out the bio and the three social media posts. Ask the group to review these on worksheet (W6W13) and discuss in the follow up questions in groups.

- What do they know about Lauren?
- What could a fraudster do with the information?
- What advice would you give to Lauren to secure her account?

Review Jas' profile on the new social media platform SnoopBook. Read out the bio and then the 3 social media posts. Again in groups review the next section of the worksheet M6W13 discussing the follow up questions for Jas.

- What do they know about Jas?
- What could a fraudster do with the information?
- What are the differences between Jas and Lauren's accounts?
- Who would be an easier target for fraudsters?

Module 6
Session 1 MBW13

Worksheet: Fraud and Social Media

In your table groups look through Lauren's social media profile and posts and then discuss:

What personal information have you discovered?

What a fraudster could do with this information?

What advice you would give to her to secure her account?

© HSBC UK

Lauren's social media profile and posts

Profile:

- **Username:** @lauren1992
- **Location:** Solihull, Birmingham
- **Job:** Senior Accountant at Birmingham Accounting Ltd
- **Marital Status:** Single
- **Education:** Accountancy at University of Birmingham
- **Hobbies:** Reading, Gardening, DIY, Socialising with friends
- **Favorite Place:** France, Mexico, Asia

Post 1:

So excited to be moving into my new house!

Can't believe I am moving into my own house after 10 years of renting. Looking forward to making Solihull my home and meeting all the new neighbors. #NewStart #HouseWarming #Birmingham

Post 2:

Thank you to my amazing friend @jane123 for help with unpacking. Love it!

So happy to have this friend in my life. She is always there when I need help and I would do anything to help her too. Can't wait to see her in 10 years time when you can take a well earned break from working.

Post 3:

Time to plan my next project. Need inspiration!

My mom mentioned this about me but I was 10! I used to play with my mom's wheelbarrow that she gave me around the house. Super funny how my mom plans to decorate the front garden really bright. #mom #DIY #Birmingham

Now let's look at Jas's social media activity. In your table groups look through Jas's social media profile and posts. Consider:

What personal information have you discovered?

What a fraudster could do with this information?

What are the differences between Jas and Lauren's accounts?

Who would be easier for the fraudster to target?

Jas's social media profile and posts

Profile:

- **Year of Birth:** 1990
- **Location:** London
- **Job:** Finance professional at Financial Institute
- **Marital Status:** Married
- **Partner:** @james123
- **Hobbies:** @golf @tennis @hiking
- **Favorite Place:** @switzerland @japan
- **Just Visited Page:** @london @paris

Post 1:

Nothing new to a week at the new club in town. 5 Stars would recommend!!!

So nice to get this new regular and a happy meal, looking forward to a fun weekend with lots of laughs.

Post 2:

Amazing weather as a quick guest of hotel and week is needed before lunch. So nice when you will be home next year at the kids.

Post 3:

Our marvelous looking house! Don't put off to tomorrow what you can do today!!

If you feel like you can donate, you can do so immediately on our charity page. Link is in my bio.

#Charity #Donation #Birmingham