Excessive Spending and Financial Scams

Overview

In this guide, you'll find a range of activities that can be used to engage and inform people on this topic through conversations and insights.

Each section can be used independently or alongside sections from other topic areas. For more tips on how to use the resources in a session see **'How to use Bee Smart online safety resources'**.

A short definition

An online financial scam is a fraudulent scheme that is conducted over the internet. The goal is to steal money or personal information from the victim. Online financial scams can take many different forms, but they often involve the use of phishing emails, fake websites, or social engineering techniques.

Fast Facts

1. What percentage of online shopping scam victims lost money from their attacks worldwide in 2022?
   - **a.** 35%
   - **b.** 45%
   - **c.** 24%
   - **d.** 72% ✔
2. True or False? Around 200,000 people a year are thought to have been tricked into online subscription scams. **[FALSE]**
3. True or False? Women are more likely than men to encounter suspicious content online. **[FALSE]**

Questions to ask

- Were you surprised by the findings or statistics?
- Have you come across any of these issues before?
- Do you know anyone who has had experience of these issues?

Take away

Summary actions to tackle the issue

Excessive spending and financial scams – What is it?

Nearly 43 million UK adult internet users have encountered suspected scams online. One in five victims lost over £1000.

Some key risks exist in online shopping, online banking and online payments:

- Counterfeit goods
- Fake or cloned websites
- Gift card scams
- Subscription traps
- Online stores may offer products at a much reduced price.
- Jobs can be advertised that don't exist.
- Get rich quick schemes that look too good to be true but that are nonetheless attractive.
- A personalised message from a modelling agency saying they've seen your social media posts and would like to discuss some work with you.

Here are some tips you can use to help tackle these issues.

Prevent

- Never click on a link in an email or text message you suspect.
- Always double check the URL (web address) that you are using – browse to the website yourself rather than clicking on a link within an email.
- If something sounds too good to be true, then it probably is. If something is far cheaper on one site than on all of the others be wary.
- Look to see if sites are using a 'trust mark' of some sort– but remember that these can be spoofed too.

Protect

- Never agree to pay for something by bank transfer. Any reliable website or online service will have a secure payment portal. Challenge anyone who asks for a bank transfer instead.
- Check a returns policy on any online shopping site or app that you are using.
- Look to see if a site is using a secure URL (https://) and see if it is showing a padlock sign which means that it is encrypted and that any transactions cannot be intercepted.

Resolve

- If you have been a victim of online fraud then report this to your bank or payment provider.
- You should also make a report to Action Fraud
- Scam/phishing emails should be passed on to report@phishing.gov.uk
- Scam text messages should be forwarded to 7726

Explore

Signpost participants to these resources to learn more and get support.

- Which - How to report a scam
- Action Fraud – information on cyber fraud
- Get Safe Online - shopping and banking advice
- Get Safe Online - Check a website tool
- NCSC - Avoid and report internet scams and phishing
- Ofcom- How to report scam texts and calls
- Internet Matters - how to tackle online scams
- Childnet - help with phishing and scams
- UK Safer Internet Centre - A guide to protect against common online scams
- Internet Matters - social media scams advice hub

Interact

Quiz to learn and test understanding of the topic

1. Which of these is a typical strategy used in online scams?

a. Sharing terms and conditions for the platform.

b. Using a secure and encrypted URL (https:// and the padlock sign).

c. Using emotive language telling you that there is a time limited deal. ✔

d. Clearly publishing a returns/refund policy.

2. Which of the following could be a sign of an online scam?

a. An unsolicited contact with an offer that seems too good to be true.

b. A request to share personal information early on in a transaction.

c. Pressure to make a decision quickly – or lose out on a deal.

d. All of the above. ✔

3. What is the best course of action if you suspect an online scam? Tick all that apply.

a. Play along with it to waste their time – never parting with any personal information or money.

b. Carry out some background checks in order to confirm your suspicion. ✔

c. Report it and block whoever sent it. ✔

d. Respond by challenging whoever made the original post.

4. Which of the following do you think is the most common type of online scam?

- **a.** Impersonation scams. ✔
- **b.** Counterfeit goods scams.
- **c.** Investment or get rich quick scams.
- **d.** Ransomware scams.

5. What percentage of online scams take place on social media platforms?

- **a.** 29%
- **b.** 77% ✔
- **c.** 94%
- **d.** 43%

Play quiz using Kahoot learning platform

Kahoot!

Discussion scenarios

Use these scenarios to spark conversations around the topic and help participants consider different the consequences that can happen when taking different actions to respond to the scenario.

Scenario A

Holiday scams

Mishal and Charlie are looking to buy a much needed holiday but are struggling to find something to suit their budget as they have noticed the cost-of-living crisis making an impact on what they can afford. Charlie finds a website that seems reputable offering a deal which is significantly cheaper than any others and substantial discounts for paying directly via a bank transfer rather than through the website, stating that this is a legitimate way to reduce costs for both parties. Mishal is unsure about whether this is safe or not.

Actions to take

What should Charlie and Mishal do?

1. Check that the website has the ABTA (Association of British Travel Agents) logo and if it does then it's worth taking a risk for the savings that are on offer. **(Negative as the logo alone is no guarantee of anything)**
2. Steer well clear – it looks dodgy and seems odd that the site would offer something so much cheaper. **(Positive)**
3. Do some research to see if it is genuine – look at reviews – what have others said about it? **(Positive)**
4. Get in touch and see if it's possible to pay with a credit or debit card but still receive the discount. **(Positive)**

Potential consequences

1. You should be wary of any site or deal where they are asking you to pay by bank transfer. If something goes wrong then it can be very difficult to trace and would not be refundable. Using a credit or debit card brings a degree of protection. You should never pay by bank transfer if you are using sites such as Airbnb or Holiday lettings – these sites have secure payment methods within their platform. You should carry out all communications and transactions related to your holiday through the official sites otherwise you lose the protection that these services offer. Just because a platform is displaying an ABTA logo doesn't mean that it's genuine, it's easy for anyone to create a website which uses logos or even links to official sites. Never click on a link in an email – always browse to the site yourself.
2. This is safest option – if it looks too good to be true then it probably is!
3. Be wary of positive reviews on a site that you haven't used before or heard of. These can be fake reviews and may not give you the insights or information that you need.
4. Again, be wary of communicating directly with anyone connected to one of these sites – they are likely to reinforce the claims made on the site and try to persuade you to take advantage of the offer which may not be genuine.

Other questions to ask and potential answers

How do I know that I'm dealing with a reputable website/organisation?

- Many holiday companies are ATOL registered. ATOL stands for Air Travel Organisers' Licensing and is a scheme from the Civil Aviation Authority to give financial protection to people who have bought a package holiday or flight from members of the scheme. You can search to see if your provider is genuinely part of this here hwww.caa.co.uk/atol-protection/check-an-atol/
- Similarly many companies will be part of ABTA (Association of British Travel Agents) and you can use this link to see if the company you are dealing with is a member www.abta.com/abta-member-search

What if a bank transfer is the only option for paying?

- This should be a red flag and it will be safer not to use the site. You won't have any protection from your bank if something goes wrong.

How do I know if I can trust reviews for a website?

- This is a difficult area but the following could give cause for concern:
  - Many reviews are similar – they use similar language or styles
  - The reviewers haven't posted many reviews already and seem new
  - There should be a good mix of factual information (things you might be able to check) and personal thoughts and reflections on what something was like.
  - There are only a small number of reviews.
- Some sites will provide "verified reviews". For example Airbnb do this.

Summary highlight
The internet has made it very easy for people to book a holiday themselves without the need of using travel agents or other third parties but this can also be exploited by bad actors who see it as an opportunity to make money through fraudulent activities. If something looks too good to be true then it probably is. Do your research, question things and check thoroughly before parting with any money. If in doubt don't do it.

Scenario B

Job/employment scams
Steve lost his job a couple of months ago and has been struggling to find something new. He's just received a text message which is offering a chance to work from home at hours that suit you and earn up to £300 per day. It says that they have filled most of the vacancies and so Steve should act immediately if he wants to take advantage of the opportunity. The text contains a link to click on in order to get more information. Steve has clicked this and it takes him to a website which looks legit where he is being asked to provide more information so checks can be carried out. He is very tempted as this could be the solution that he needs to solve his financial problems.

Actions to take

What should Steve do?

1. If the site that he has clicked through to looks legitimate then it's worth progressing a bit further, there's nothing to lose and Steve has heard of other people who are making a lot of money from these sorts of jobs – since COVID lots of people are now working from home on flexible contracts and he sees a lot of posts from people on social media who say it's brilliant. **(Negative)**
2. Be very wary – it sounds like a scam and seems a bit too good to be true. **(Positive)**
3. Share with some friends and see what they think. **(Positive as it could get some suggestions or support - but negative in that it could encourage them to get involved)**

Potential consequences

1. Even clicking on the link in the first place could have caused a problem – he could have inadvertently installed some malware onto his device which could already be mining his data or spying on his online activities. Quite often these scams will ask people to pay upfront for online background checks to be carried out – stating that provided these come back clear that they will be offered a job. After money has been paid nothing further will happen, the job doesn't exist.

2. It's best to always use reputable sites that will provide some protection from scams and fraud.

3. This is quite a good idea as friends can often provide the voice of reason and point out potential problems. Sometimes having someone else offer an opinion can be helpful in getting you to reflect on what is happening, particularly if it's someone you know and trust.

Other questions to ask and potential answers

Why do these scams exist? What do the scammers get out of it?

- Often these scams will say that you've been successful and offer you a post. They then ask you to provide bank details so that they are able to pay you. The information you have already shared about where you live, date of birth etc. can be used to take money from your account.
- If the job is going to involve you moving to a new location you might be put in touch with an "agency" who will be able to help you with the logistical arrangements for moving to a new place. Typically these agencies will ask for a fee in order to help you.
- Some fraudsters are simply after your data. If they have enough personal information about you they can use this to set up accounts in your name or to get into your own existing accounts.

What should I do if I think I'm a victim of an online employment scam?

- Stop any communication with the "agency", organisation or individual that you are speaking to.
- Keep any evidence, screenshots of text or WhatsApp messages you've received, websites that you've visited and the information that you've shared.
- If you disclosed any passwords then change these immediately.
- Set up two factor authentication on any apps and sites that you use where this is possible so you will be notified is someone else is trying to access them.
- If you have already given money away then contact your bank about this immediately.

What are some of the signs that this could be fraudulent?

- You should be way of any unsolicited message that you weren't expecting, particularly if it is a text or WhatsApp message.
- Look carefully at the spelling, punctuation and grammar in the post. If there are errors then this should raise suspicions. A reputable company would want to ensure that they are projecting the best possible image of themselves and incorrect spelling etc. could damage their reputation.
- If a point of contact is using a more generic email address such as a gmail account or a guerrilla mail account then this should cause concern. A genuine company would have a company email address protocol.

Summary highlight
There has been a significant rise in online recruitment scams in recent times partly as a result of COVID and a different attitude to working from home and partly due to the cost of living crisis. The scams look very attractive and can at the outset appear to hold no risk for someone signing up. Seemingly genuine testimonies from others who have already started to make money from them can be really effective in enticing people to take part or at least explore further. Whilst there are some individuals and even companies who are using social media to recruit, it is safer to use an established recruitment agency which will be able to offer some protection and safeguards from this type of scam.

Scenario C

Social scams
Sofia is finding that her salary doesn't quite stretch to the end of the month at the moment. Rent has gone up and so has everything else. She sees a post shared from a couple of friends on social media that suggests there is an opportunity to receive a £50 voucher for a local supermarket just by answering a few questions. There are a lot of posts/comments from other people saying that they've done it and it was true.

Actions to take

What should Sofia do?

1. Steer well clear – if something looks too good to be true then it probably is. **[Positive]**
2. Check with the supermarket website – if it is a genuine promotion then it should be highlighted there (or on their official social media channels). **[Positive]**
3. Get in touch with her friends to see if they really did get a voucher and if they knew they had shared the post. **[Positive]**
4. Go for it – there's nothing to lose provided that she doesn't part with any money. **[Negative]**

Potential consequences

1. This is the safest option – if it looks too good to be true then it probably is!

2. This is a sensible strategy and should prove very quickly whether the promotion is genuine or not.

3. Others will often be unaware that their account has shared this type of post. If they clicked on the original post to show their interest or find out more, they may well have compromised their account meaning that it can be used by others or that they have inadvertently given their permission (usually by clicking on something to give their consent) for this to happen.

4. Often clicking on these links will take you to another (fake) site where you will be asked to login to the social media platform – doing so will provide the scammers with your username and password. This is particularly problematic if you use the same password for lots of different things!

Other questions to ask and potential answers

What is there to lose by checking out some of these posts, provided I don't part with any money?

- Many of these scams are not trying to get you to part with money – they are more interested in your data and personal information which in turn can give them access to other things.
- Sometimes scams will ask a user to click on a link which will take them to another site where they are asked to login – e.g., to Facebook – when they do, the credentials that they use can be captured by the scammers.

What happens if you do fall for one of these scams and then find that the offer doesn't actually exist?

- Carry out a malware and virus check of your device.
- Change any passwords that you think might have been compromised. Not only for the site connected to the scam – but for anywhere you are using the same password. You can check to see if your email has been compromised here haveibeenpwned.com

What can I do in order to spot this type of scam?

- Look at the web address that the post is trying to send you to. Hovering your mouse/cursor over the link will often show you the actual address – which may be very different from what is written!
- Look at your timeline to see if you've received more than one similar post – if there are lots of them then this is a sign that it could be a scam.
- Check simple things like spelling, punctuation and grammar. Often (but not always) scams will not use correct spelling and grammar.

- Look carefully at logos – these can easily be taken from the internet and may not be up to date or using a quality image that you would usually expect from a professional organisation.
- Do contact the company if you're unsure – if it is a genuine offer or promotion then they will be pleased to tell you about it!

Summary highlight

It is very easy for people to create these online scams and use others to share them (often unknowingly) on social media platforms. Friends may well share something believing it to be genuine and research has shown that a recommendation from a friend or someone we trust is powerful and much more likely to be believed. Never click on a link you've received in a post or email or message, even if it says it is taking you to a particular website. It's always better to browse to this on your own rather than clicking a link. Equally, you should never share a username or password if you're asked to do so in an email or text or post. Banks and other organisations will never ask for this information like this. If in doubt, go to their official website yourself and check.