Scams awareness report
December 2022
Citizens Advice Exeter

Back ground and information:

The annual cost of fraud in the UK is £190 billion each year. The Office for National Statistics (ONS) say that people are more likely to fall victim to fraud or cyber offences above any other crime.

Investment fraud, Identity theft, Romance fraud, Ticket fraud, Payment in advance fraud are among the multitude of frauds taking place in the UK and elsewhere regularly. Fraudsters have become increasingly sophisticated and it can be very difficult to detect that the situation is not a genuine one. (1)

Many studies have been done to try and determine, through looking at case studies and victims, what the trends are and what the factors are that influence vulnerability to scams and fraudsters, but this is a highly complex picture with different reports showing conflicting results. (2) The complexity is massively increased because different scams are targeted at very different audiences, making trends extremely difficult to establish.

Methodology

Our research and campaigns team designed a questionnaire to assess the level and range of scams people had experienced, and to assess the level of knowledge in the Exeter region in respect to the level of scams, how to report scams, and how to get scam alerts.

Staff and volunteers took turns to ask the public to complete the questionnaires with us at the RESPECT festival in Exeter, and we have analysed the results using Survey Monkey.

We distributed Citizens Advice Scams awareness leaflets to over 100 members of the public, informing them about how to report scams and how to receive fraud alerts, and we asked people if they would be happy to give us further details about their scam experience if we contacted them on the phone.

We contacted the people who were happy to give us permission, and took details of the scam and the impact the scam had had on them.

Using our database (Casebook) we have also analysed data relating to clients who have, or who are worried they have experienced scams, and endeavoured to see if any trends or vulnerabilities could be identified within our client base.

Survey Monkey results

Survey Monkey analysis reveals that **100 % of the people we surveyed had been targeted by a scam in the previous year**, and some had fallen victim to either one or more scams during that period of time.

The greatest proportion of people in our survey were targeted by phone, the second largest group was by email and third largest was by text. Some victims had encountered scams whilst browsing and using the internet. 55% of the people we surveyed did not know how to report a scam and did not know about action fraud alerts.

Categories of scams encountered

Through this research we encountered many of the fraud and scam categories which are known, from cloned investment companies to romance fraud, crypto currency, HMRC, identity theft, police, and individual fraudsters calling on peoples' doorsteps.

Our research and campaigns team have outlined the stories of several victims of scams below. The people are anonymised, and the focus is on the circumstances and any vulnerabilities of the victim, also detailing the impact on them moving forward from the scam.

Some of our stories along with the impact on the victims are outlined below:

1. *Male aged 56, lives alone. Wheelchair bound after rapid progression of MS. Marriage breakdown subsequent to this. Had a professional career but unable to work now due to illness. Targeted by online dating scam leading to online romance with person claiming to be overseas female. Transferred almost entirety of life savings to this person, who subsequently did not communicate any further. Eventually reported to police after a period of feeling ashamed and gullible, but too late to recover any of the money. This person was already at a low ebb due to the challenges outlined above, and this has caused an immense loss of self-confidence as well as severe financial hardship.*

2. In May 2022 Moira attempted to open a Coop account but was advised that there was a CIFAS marker against her name and they couldn't open an account for her and advised her to contact Halifax. Halifax duly confirmed that there was a CIFAS marker against her name and that her accounts would be frozen on 9 Jul 2022. Moira understands the CIFAS marker has been put in place because of suspicious activity with her Barclays account, where money has been deposited and withdrawn, without the client's knowledge. Moira has lost no money, but is at risk of having her existing Halifax accounts frozen, and is not able to open another account. Moira is very concerned and anxious about the future financial implications for herself.

3. *A 73-year-old, Jay, found a voicemail on her landline purporting to be from Amazon Prime saying that £1000 had been taken from her bank account and that she should call a number to resolve the issue. When she got home she thought she better check with her bank, Barclays, and found an old "fraud number" that she called. She was asked for extensive personal information but did not give her pin or account numbers. She was told they could not help further without more information and client ended the call in tears.*

4*. Sasha, aged 26, has a grandmother, who lives in Bangladesh, has cancer which requires expensive treatment. She wanted to contribute to the cost of her grandmother's care, and was seeking to grow her capital. Sasha became aware of a woman, who was advertised by several social media influencers, who facilitated crypto-currency investment. Sasha initially invested £650, increasing to a total of around £20,000 in all. This is made up of Sasha's and her parent's money. Sasha was sent screenshots of the valuation of the crypto she had invested and was encouraged to invest more. She was subsequently prevented from accessing her funds, and was told that she had to pay tax on the fund, and then she discovered that she had been blocked by the Crypto currency provider. The only forms of communication used were Snapchat and WhatsApp. Now Sasha is unable to contact her. Victim is suffering anxiety and shame about the fraud and about her parents finding out as well*.

5. Jim searched online for "Citizens Advice". However, instead of being taken to the Citizens Advice website, Jim was sent to another website which directed him to Just Ask for which he had to pay £5 from his PayPal account. After Jim had paid the £5, he checked his PayPal account, only to find that another payment of £50 was going to be taken the following month. Jim then cancelled the £50 payment that had been mysteriously set up to go from his PayPal account.

6. Female, 99yrs, lives alone. She opened her front door to a caller who looked 'official' who was dressed in a dark jacket, flat cap, and sunglasses. He claimed to be from a water company dealing with a leakage nearby and said he needed to check her upstairs radiators. She allowed him to go upstairs and do what was necessary while she remained alone in the sitting room. He left, she assumed by the back door, without her being aware he had gone, but the next day she discovered her jewellery box had disappeared. She didn't mention this to anyone until a week later when she very diffidently told her daughter about the visit. The elderly woman was sheepish and embarrassed as she realised she should not have been so trusting as to let a stranger into her house. This caused her much stress and loss of confidence.

Current scam issues and proposed imminent action by Citizens Advice Exeter:

More recently, we have been alarmed by scams targeting the sections of society who are currently hardest hit financially:

A report from the Office for National Statistics (ONS) (3) said anti-fraud squads had identified new trends as phishing attacks – when perpetrators attempt to trick users into clicking a bad link and have started to target those in difficult financial situations.

The types of messages being sent by email and text include the promise of energy and council tax rebates or encouraging people to apply for a "cost of living payment", mimicing genuine government support packages.

The emails use the Ofgem logo and colours and have the subject header "Claim your bill rebate now".

Cifas, a UK fraud prevention service, https://www.cifas.org.uk/ said there was a "real concern due to the rise in living costs, criminals will look to target loan products and deferred credit services".

Common campaigns they have encountered include fraudsters posing as utility providers offering deals on energy bills or competitions to win fuel vouchers.

Actions Proposed:

To make our advisers aware of these scams so that they can advise all potentially vulnerable clients. We have already done this via our morning briefing, but will continue to emphasise this.

To supply the Exeter foodbank with leaflets to be put into the food parcels. This will help to inform a proportion of our most vulnerable clients who are being targeted by these scams.

In the longer term, we will continue to attend public events and distribute scam awareness literature during these difficult times.

References

1. https://www.actionfraud.police.uk/what-is-fraud
2. https://journals.sagepub.com/doi/full/10.1177/0963721421995489
3. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26

Appendix 1 **Scams Resources**

1.Age UK (Cheshire East)

Scams awareness and aftercare plus monthly bulletins
https://www.ageuk.org.uk/cheshireeast/search/?q=scams+awareness&qid=35736

2. National Trading Standards

Scams Team, Friends against scams – online learning
https://www.nationaltradingstandards.uk/work-areas/scams-team/

3. Journal article

Current Directions in Psychological Science
The scams among us – who falls prey and why
https://journals.sagepub.com/doi/full/10.1177/0963721421995489

4. Which? Consumer Rights

Spot and protect yourself from scams

https://www.which.co.uk/consumer-rights/advice/how-to-spot-a-scam-alFiz5h8mnJ9

a. How to spot a fake, fraudulent or scam website

https://www.which.co.uk/consumer-rights/advice/how-to-spot-a-fake-fraudulent-or-scam-website-aUBir8j8C3kZ

b. Phone scams

https://www.which.co.uk/consumer-rights/advice/phone-scams-aL1Yy5L9Utl4

c. Email scams

https://www.which.co.uk/consumer-rights/advice/how-to-spot-an-email-scam-au5Lt0O3EgcPd.

d. Other types of scams

https://www.which.co.uk/consumer-rights/scams/types-of-scams

e. Campaigns

https://campaigns.which.co.uk/tech-giants-responsibility/

5. National Cyber Security Centre

https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

6. Metropolitan Police

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/prevent-personal-fraud/

7. Super Easy

https://www.supereasy.com/track-down-someone-who-scammed-you/

8. Independent Age

https://www.independentage.org/pounds-shillings-and-pensions/whats-the-scam/impact-of-scams-on-mental-health

9. Love Money

https://www.lovemoney.com/news/118715/scams-mental-health-victims-anxiety-trust-confidence

10. Lifepath Counselling

https://www.lifepathscounseling.com/emotional-support-fraud-scams/

11. Psychology Today

https://www.psychologytoday.com/gb/blog/metacognition-and-the-mind/202104/fool-me-once-why-scams-leave-people-feeling-foolish

12. Dochas psychological Services

https://www.dochaspsych.com/blog-coping-after-being-scammed-or-hacked/

Appendix 2

A selection of some of the stories we encountered through this research.

We have used fake names to ensure anonymity

Bogus companies

1. Brian (70) has recently received a marketing letter addressed to him as the director of a company, xxxxx Ltd. Upon investigation, client discovered that someone has fraudulently created this company using his name, address etc. The company was registered on 10/9/21 and since then Brian has been removed as a director, but remains as a 'person with significant control.' The company is no longer registered at the client's address. Brian has already been in contact with Action Fraud, Companies House and HMRC. Action Fraud have given advice to him which has been acted upon, namely the completion of Companies House pro-forma 'Report suspicious company activity.'

2. Roger believes he has been the victim of an email scam and as a result, has not been paid £2,100 (approx.) by a company xxxx, to whom he sold scrap cars. xxx say it is not their fault, as they allege Roger's email account has been hacked. xxx are refusing to reimburse him as they have not been able to recover the money from the bank. Citizens Advice explained that ultimately, xxx owes the money for the goods he sold, so Brian may have to go to the Small Claims court if he cannot recover the money any other way.

Internet fraud

1. Neli lives with her partner. She says that in 2022, the had debts of £17,000. Neli tried to contact Citizens Advice and is unsure how she got through to the 'Debt Expert Team.' Neli has no paperwork or emails, but spoke to someone named Vinnie, who took details of their joint debts and then referred them to xxxx Insolvency. Vinnie spent time going through the questions Neli would be asked by xxxx and specifically told her to answer 'no' as to whether she had a bank overdraft, as 'it would complicate matters.' Neli is worried about this and concerned that she has been scammed.

2. Damien's daughter recently moved out of the family home and someone used client's bank details to make multiple purchases on eBay, which have been delivered to an address in Cambridge. This emptied his bank account and he reported the theft to his bank, which refunded about £2,000. The bank investigated and found a longer pattern of similar purchases on eBay, and now say they no longer believe that the recent spate was fraudulent, because Damien did not report previous ones. They have written to Damien telling him that they intend to take the money back from his account in the next few days. Damien has not reported this to any other agency.

Crypto currency/investment fraud

1. Maud is 79 years old. She explained that she and her husband made the decision to transfer £25,000 of savings to a company called xxxx Standard Investments. Maud saw an advert for the company in a newspaper and looked online. Maud also contacted the FCA before making investment to make sure they were bona fide. Maud transferred the money by bank transfer from Nationwide to xxx Services Ltd. When they did not receive acknowledgement, cl. spoke to xxxx Standard, who agreed to send them a certificate which details the £25,000 placed in a 'strategic bond.' This appears to be a clone of the xxxx Standard firm. Maud is aware that it may not be possible to retrieve their funds, but wishes to prevent the same thing happening to someone else. Maud has reported the case to Action Fraud, who have added their report to others, but are not offering any further help.

2. Audrey lives with husband and two boys, aged 13 and 10. In January 2018, she invested £24,000 in Bitcoin through xxxx International Ltd. Audrey then left for an extended stay in India with family and did not return to the UK until April. Audrey was contacted by the 'broker' GVIL to say that they had tried to invest the money, but it had been lost. Audrey said she called GVIL and it was suggested that if she gave them more money, they might be able to retrieve the original amount. The matter lay unresolved as Audrey had difficulties in her family life and returned to India from June to October 2018. Audrey has been too frightened to contact xxxxx, or anyone else since then. However, last week, she was cold called by someone from Blockxxxx, a 'crypto currency blockchain explorer service', who advised Audrey that GVIL were trying to access her money from Blockxxxx and, if she had given authorisation to the broker, they might get it. Blockxxx offered to get Audrey's money back for her and said they would take a £2,000 commission if successful.

HMRC/National Insurance scams

1. Nazeem is 67 years old and has been receiving phone calls saying that her NI number has been compromised and action would be taken – press 1 to talk to someone. She has received multiple calls. She thinks they are scams, but not sure. Nazeem contacted Citizens Advice to know if this was a scam. She had done nothing so far. CA advised that there are many scams and that she should not give her details to anyone who cold calls, without being absolutely sure who they are. CA directed Nazeem to gov.uk websites that give examples of scam phone calls and suggested she read them to see if they fit her calls.

2. Andrew aged 36, received a call from someone claiming to be from HMRC. They were asking for payment of £1800 as payment for unpaid taxes. They threatened Andrew that he would be arrested if he did not pay, so he panicked. He told them that he could not pay that amount over the phone. Andrew was directed to the local post office, where he was instructed to purchase £500 worth of Google play cards. Just as he had bought them, he was cut off from his phone call, so is now left with the play cards.

Courts/police contact fraud /scams

1. TV licence – Susan has received a letter from the magistrates' court fining her £374 for not having a TV licence. Susan Insists she has a TV licence and is paying £15.90 per month by direct debit, though the usual monthly amount would be £13.25. Susan has confirmed with TV Licensing who agree she has a valid licence. It seems that this is the second time this has happened to her and £125 was deducted from her Income Support last year by the court, when she also had a valid licence. This may be a breakdown in communication between the courts and TVL.

2. Anna described having been contacted by the police on three occasions. Firstly, by the Domestic Violence Unit, because they said they are concerned for her welfare, due to her partner's behaviour with his ex-wife. In addition, it had been alleged that she fraudulently used her partner's ex-wife's credit card, and on another occasion that she stole a bottle of wine. Both were disproved, but she is concerned about the effect it could have on her career as a nurse. She doesn't know how the police would have her contact details and wants to know if these contacts are genuine.

Identity theft

1. Sharon has had the same mobile number for the last twenty years. Her provider for the last two years has been O2. She renewed her contract in December 2020 for two years. Sharon has never had any problems until about three months ago, when things started to go wrong. Sharon thinks some sort of scam has taken place and her number is being used in a rogue way. People are receiving texts and phone calls from this number, but Sharon has not sent the texts or made the calls. Sometimes these messages can be rude and vulgar, because people on her contacts list have asked her why she has sent such awful messages. Sharon should be paying £18 per month for the contract, but has received a bill of £4,600 for the month of May. She confirmed that there is no way that she has racked up such a bill in one month. Sharon has been in touch with O2 on numerous occasions, trying to sort out the issue and has demanded to speak to managers for itemised bills. She is struggling to get anyone to return her calls. On Monday the Sharon spoke to someone and a manager did call back on the Tuesday and apologised and said that she did not have to pay the £4,600. But on Wednesday, she received an email stating that she owes £4,574, which needs to be paid by July. Sharon is very anxious about this issue and is very getting frustrated. She has tried to change her sim card (but kept the same number). This did not help. She does not have any other debts.

2. Chris states that he has been a victim of fraud. He had requested a credit check and found that he had a County Court judgement against him. He applied to the court to see the claim. The claim had been issued to a false address and so he was never served with the claim. Chris has subsequently found another claim issued in his name to a different false address. Chris had not been able to respond within the fourteen days' timescale because he had never received the paperwork. He has spoken to the police and Action Fraud, who were unable to help him. He has hired a solicitor to deal with the claims that have been issued. Chris. states that the claims are being served by a ghost company called xxxxxx Magazine Ltd, who have a London mailing address, but no one works from this address. Chris cannot believe that the court can issue a claim without cross-referencing the address and is concerned that he is going to receive further claims. He is anxious about having to pay a solicitor and the fact that he may receive more claims.

Final version 20.12.22 KD/MB