Online Frauds: Learning From Victims Why They Fall For These Scams

Mark Button

Centre for Counter Fraud Studies, University of Portsmouth

Carol McNaughton Nicholls, Jane Kerr, Rachael Owen

National Centre for Social Research

Abstract

Online frauds have become a major problem in many countries with millions of victims from a wide diversity of scams committed in full or part online. This paper explores the extent and nature of this problem. Using data from depth interviews with 15 online fraud victims, 6 focus groups with a further 48 online fraud victims and interviews with 9 professional stakeholders involved in combating this problem. The paper explores why victims fall for online scams. It identifies a range of reasons including: the diversity of frauds, small amounts of money sought, authority and legitimacy displayed by scammers, visceral appeals, embarrassing frauds, pressure and coercion, grooming, fraud at a distance and multiple techniques.

Keywords

online fraud, scams, victims, fraudster techniques

Introduction

Fraud committed online against individuals has become a global problem (Levi, 2008; Smith, 2010; Button, 2012). The advent of the internet and related technologies has created huge advantages for society, but it has also spawned multiple opportunities for frauds (and other crimes) to be perpetrated on an industrial scale (Jewkes and Yar, Levi, 2008; 2010a; Sandywell, 2010; Buchanan and Whitty, 2013; McGuire and Dowling, 2013a). All over the world millions of people are targeted with scams via the internet and related technology everyday by thousands of fraudsters operating within and beyond the borders of the victim's country (Office of Fair Trading, 2006; Karstedt, and Farrall, 2006; Federal Trade Commission, 2007a; Australian Bureau of Statistics, 2012). The revolution in communications has created huge opportunities to perpetrate 'old' frauds on an industrial scale at low cost as well as develop completely new scams (Wall, 2007; Smith, 2010). It has created daily risks of victimisation to many people who previously would have been rarely openly targeted with such crimes. It has also created the means for scammers to connect with victims in other countries far away from where they reside who previously they would have little chance of targeting. Despite this substantial shift in the nature of criminality and a growing body of research, one area which has received relatively little attention are the growing number of victims of mass marketing fraud and particularly online fraud (Shover *et al*. 2003). Indeed victims of fraud in general have been neglected by researchers in comparison to other crime victims (Levi, 2001; Croall, 2007; Button *et al*. 2009b and forthcoming).

This paper draws upon research on victims of online frauds in England and Wales to examine in the victims own words how they fell for the online scams. These findings, however, also have relevance beyond England and Wales to other English speaking countries such as Australia, New Zealand, USA, Canada etc where many of the same online scams occur, often targeted by the same fraudsters (Cross, 2012; Consumer Sentinel Network, 2012). There are also examples of substantial numbers of online frauds in non-English speaking countries. For example ethnic Koreans in China targeting South Koreans with phishing scams and 'one click' frauds in Japan, where users think they are downloading

pornography, but instead malware which causes potential embarrassment with pop up explicit pictures, unless they agree to pay for it to go away (China Daily, 2013; Hamada, 2011). Online fraud is a global problem and as such these findings will be of interest beyond England and Wales. There are of course limitations to victims understanding: they may not know what happened, they may wish to hide the reasons out of embarrassment, but as the findings will show later much can be gleaned from their experience of why they fell victim. The paper will examine the techniques used by the fraudsters to perpetrate successful frauds. Before we embark upon this, however, a brief overview of the internet revolution and how this has spawned new opportunities for fraud will be explored, combined with evidence of the nature and extent of the problem.

The Internet Revolution and Implications for Online Fraud

> It is an incontrovertible fact that the Internet has brought with it major changes in the life of industrialised nations (and is increasingly doing so in the 'developing world') (Jewkes and Yar, 2010b: 1).

In December 1995 across the globe there were estimated to be 16 million users of the internet (Jewkes and Yar, 2010b). By 2000 there were around 361 million users of the internet worldwide (Internet World Stats, 2012). This had grown to almost 2.5 billion in 2011, amounting to 35 per cent of the world's population using the internet, compared to 18 percent in 2006 or just over 1.1 billion. The means to access the internet have expanded from desk based computers, to laptops, to tablets, to televisions to mobile phones. Indeed global mobile phone subscriptions in the four years prior to 2011 had been growing at the rate of 45 percent annually with 87 percent of the global population or 5.9 billion having one and within that a doubling of those subscriptions with access to mobile broadband to 1.2 billion (International Telecommunications Union, 2012). Smart phones, which have advanced computing and internet access facilities, have also been growing substantially (Think Insights with Google, 2012).

Completely new forms of social interaction have emerged through social networking sites such as Facebook, Myspace and Linkedin. Indeed Facebook, which was only launched in 2004 in the USA, has grown to over a billion users (Facebook, 2013). Social networking sites dedicated to people seeking love have also emerged and research by YouGov in the UK found that 1 in 5 relationships now begin online (Nolan, 2012). New forms of undertaking shopping have grown from nothing to the norm in less than a decade with Amazon and Ebay some of the most prominent examples. Online banking services are also now used by half the UK adult population, but 76 percent of 25 to 34 year olds (Office for National Statistics, 2013a).

The statistics above provide some, of potentially many more indicators, to illustrate the revolution across the globe in the way we interact with one another and buy goods and services. These changes have also provided exponential new opportunities to commit crimes and frauds have formed a significant component of these (Jewkes and Yin, 2010).

The diversity of online fraud: not just 'old wine in new bottles'

Wall (2007) has distinguished between 'computer assisted' and 'computer orientated' crimes. The former are crimes which pre-date modern technology which have been given a boost and a new dimension by the internet, such as the selling of bogus goods and services. The latter are new forms of crime linked to the new technologies, such as malicious software. Most online frauds fall into the first category, but as this section will show there are also a wide range of new 'computer orientated' frauds. There are also a growing number of 'computer orientated' crimes. Smith (2010) has distinguished between syntactic (technical), semantic (social engineering) and blended (both). The syntactic involve the scammer exploiting technical weaknesses to secure personal data through malware such as viruses, keyloggers, worms, spyware, trojan horses to name some. Semantic

involves social engineering where individuals are tricked into revealing personal information most commonly by phishing (false websites and spam e-mails), SMShing (texts messages), social phishing (social network sites) and vishing (phonecalls). Sometimes individuals also leave personal data online, which can also be exploited. Blended uses both and invariably involves a problem created on a computer which the scammer then creates a situation where the victim is contacted and provides the 'solution' in return for their gain (money and/or personal information). Such processes are most commonly used to gather personal information which can then be sold and used to facilitate mass marketing scams or to commit identity fraud (Smith, 2010). The latter can range from using the victims' banking details to purchase goods and services, take over their accounts, apply for credit to using he identity to engage in criminal acts (Pontell, 2009). More detail on the types of online fraud which are common, will shortly be explored, but before this is undertaken it would be useful to gauge the extent of victimisation.

The extent of online fraud: the dark figure of crime

Consumer frauds (bar identity frauds) for a variety of reasons have low rates of reporting. This is attributed to victim's feelings of self-blame, not knowing who to go to, embarrassment, the contested nature of the crime, the low value, to name some (Schichor *et al*. 2000; Button *et al.* 2009a; Croall, 2009, Webb, 2010, Hache and Ryder, 2011; McGuire and Dowling, 2013b). These same issues arise with online fraud and one study in the UK of cybercrime victims found only 44 per cent of 655 victims surveyed had reported this to the police (Goucher, 2010). Large-scale prevalence surveys are the only way to capture the extent of this problem, and unfortunately nuanced data on experiences of online fraud have rarely been gathered in such surveys.

There have, however, been a number of studies to start to uncover this 'dark figure'. For example Karstedt and Farrall (2006) in England and Wales, Germany and Eastern Germany found 80 percent of those surveyed had been victims of 'crimes of everyday life' at some time, most of which could be considered frauds in their broader sense, although not all online. Growing sophistication in prevalence surveys of crime conducted on a regular basis has emerged in several industrial nations. Unfortunately their coverage of fraud is generally weak to non-existent. Some countries have also commissioned one off pieces of research. In table 1 below some of the evidence from Australia, England and Wales, Scotland and the USA is presented. Much of this research does not distinguish whether the frauds were committed online or by traditional methods (McGuire and Dowling, 2013b). However, research on scams by the Consumer Sentinel Network (2012) suggests a significant majority occur online in some form. The evidence shows very large numbers of people in the countries concerned who have fallen victims to frauds.

Table 1. The prevalence of fraud: evidence from selected countries

Country	**Type of Research**	**Findings**
Australia	Regular Prevalence Survey	2010-11 6.7% of population over 15 at least victim of one personal fraud in previous 12 months. Above includes 3.7% victim of credit card fraud 0.3% victims of identity theft

		2.9% victims of scam
England and Wales	National Fraud Authority commissioned survey	2012 8.8% victims of identity fraud in previous 12 months
	Annual Crime Prevalence Survey	2011-12 4.5% of plastic card holders victims of fraud in previous 12 months 56% targeted with unsolicited communication, less than 1% sent money.
	Specific Office of Fair Trading Report (UK Wide)	2006 48% targeted 8% a victim
Scotland	Annual Crime Prevalence Survey	2010-11 4.5% of plastic card holders victims of fraud in previous 12 months 0.5% of adults victims of identity theft
USA	National Public Survey on White Collar Crime	2010 24% of households had at least one person experienced a fraud related crime in past 12 months
	National Crime Victimisation Survey	2010 7% of households had experienced at least one incident of identity theft of those 12 and over in this year
	Specific Federal Trade Commission Report 2005	2005 13.5% of adults victims of a consumer fraud
	Specific Federal Trade Commission Report 2005	2005 3.7% of adults victims of identity theft

Source: Australian Bureau of Statistics (2012), National Fraud Authority (2013), Office for National Statistics (2013b and c), Scottish Government (2011); Huff *et al*. (2010); US Department of Justice (2011); Federal Trade Commission (2007a and b);

The variety and extent of different types of online frauds is difficult to determine for a number of reasons. First, there is a lack of reporting. Second, there is a lack of internationally agreed categories of frauds. Third, many frauds use a mix of methods to occur, including the internet. Fourth, many national bodies don't publish the information or seek to professionally deconstruct the data. It is clear from the literature, however, that there is a very diverse range of frauds (OFT, 2006; Button, 2009a; CIFAS, 2012; Cross, 2012). The latest Crime Survey in England and Wales did ask questions relating to mass marketing fraud (which goes beyond online). The most common unsolicited communications are listed in table 2. Unfortunately there is no data on actual victimisation and it would seem the different scenarios were presented to interviewees, which does not reflect the full diversity of mass marketing fraud. For example communications which trick the respondent into downloading malware, foreign property scams, slimming products, Viagra scams, fake charities to name some could also have been offered. It does not account either for victims who searching on the internet for products and services that become victims, as opposed to those targeted by unsolicited mail. At best the results should be treated as a barometer of *some* of the most popular scams been perpetrated.

Table 2. Percentage of adults experiencing unsolicited mass marketing communications in England and Wales during 2011-12.

Type	Percentage
A big win in a lottery, prize draw, sweepstake or competition you haven't entered	40
The chance to make an investment with a guaranteed high return	16
A loan on very attractive terms	15
Someone who invites you to get to know them with a view to a possible friendship or relationship	13
Help in moving large sums of money from abroad	12
A job offer, a franchise offer or other business opportunity	10
Help in releasing an inheritance	9
An urgent request to help someone get out of some sort of financial trouble	8
Adopting or buying a pet	3
Some other type of similar request	7
No communication received	44

Office for National Statistics (2013c: 4)

The reasons victims fall for scams

Given the extent of the problem there has been a paucity of research over why victims fall for scams based upon contact with actual victims. (see for example, Shichor *et al*. 2000; Lagenderfer and Shimp, 2001; Office of Fair Trading, 2009; Button *et al*. 2009a; Whitty and Buchanan, 2012; Whitty,

2013). The research by Office of Fair Trading (2006) and Whitty and Buchanan (2012) are the only studies based on the UK and were undertaken by psychologists. In the UK the Office of Fair Trading commissioned research undertaken by psychologists at the University of Exeter (Office of Fair Trading, 2009). This involved 30 victims and near victims of mass marketing frauds. It is not clear from the report on the type and nature of victimisation, particularly whether the internet was involved. However, it is clear for some it was. The research found two main reasons victims responded to scams, which were: appeals to trust and authority and visceral triggers. As will shortly be shown these were also important in this research.

The Exeter research also identified a series of error inducing triggers and some of the most significant were: scarcity cues (emphasising a personal offer with a time limit to respond), induction of behavioural commitment (series of small steps towards victimisation), disproportionate size of reward (a high value reward for small investment), and a lack of emotional control (some were less able to control their emotions and were more open to persuasion). Some of these triggers were also found in the research conducted for this paper.

The Whitty led research focused purely upon romance scams perpetrated online using analysis of victim data, posts on the internet and interviews with victims. The findings noted those with high romantic beliefs as being at greater risk of victimisation. Among other findings some of the persuasive techniques were also noted such as: profiles of fraudsters providing stereotypical traits likely to appeal to prospective lovers, fictitious authority figures were used to persuade the victims and gradual grooming of the victim, amongst others. The Whitty research provides an important contribution to understanding scammers, but of one type of online fraud amongst dozens of others (Whitty and Buchanan, 2012, Whitty, 2013; Buchanan and Whitty, forthcoming). There is therefore a gap in research relating to the wide variety of online frauds, their victims and why they fall for them.

Methods

The research methodology comprised three phases. Phase one, an evidence review, involved detailed scoping of the existing literature, focusing on the ways in which the fraud offences in the scope of the research are being committed, factors relating to their seriousness and the culpability of the offender and the impact on the victims involved. Phase two therefore explored the same issues using face to face interviews with nine key stakeholders who were working at the forefront of fraud prevention. Interviews lasted about an hour, were audio recorded and fully transcribed verbatim.

Phase three involved primary research with victims of online fraud and adopted two distinct strands. Six focus groups with 48 members of the public who had been directly affected by the two types of fraud in scope for this study, conducted completely or partially over the internet. The focus groups were used to explore experiences of how online fraud is committed and perceptions relating to the seriousness of online fraud offences, the culpability of the offender and what should be the key aggravating and mitigating factors. Impacts of online fraud were also explored. Focus groups lasted around 2 hours, and were audio recorded, and transcribed verbatim. Depth interviews with 15 participants who had been victims of online fraud were also conducted. Depth interviews were specifically used with participants who had experienced particularly sensitive or extensive frauds, such as romance scams or long term investment scams facilitated via email contact; or participants that could be considered vulnerable. Interviews facilitated an approach that was responsive and tailored to individual experiences. The interviews focused particularly on the way that the fraud had been committed and the type of harm and impacts they had experienced.

Characteristics of the participants were monitored to achieve diversity across and within the groups in terms of their gender, age, whether they lived with other people or alone, employment and health. The breakdown of participant characteristics is presented in the table below.

Table 3. Achieved sample characteristics for focus groups and depth interviews – participants who had experienced online fraud

	Focus Groups	Depth Interviews
Gender		
Female	25	8
Male	23	7
Total	*48*	*15*
Age		
16 – 24	6	0
25 – 40	21	3
41 – 59	15	5
60 +	6	7
Total	*48*	*15*
Household		
Live alone	8	4
Live with others	40	11
Total	*48*	*15*
Socio-economic activity		
Full time or part time work	36	9
Education or training	2	0
Unemployed	2	2
Retired	7	2
Other	1	1
Unknown	0	1
Total	*48*	*15*
Health		
Visual or hearing impairment	3	0
Limited physical activity	1	5
Learning difficulty	0	1
Long-standing physical/psychological condition	4	1
None	40	10
Unknown	5	0
Total	*53*	*17*

Note: Disability do not add up to totals due to some participants reporting more than one disability.

In addition diversity was also achieved in terms of individuals' self reported internet usage and confidence with financial matters. Fieldwork for phases two and three took place between July and October 2012. The participants had experienced a diverse range of frauds perpetrated online including: :

- romance scams ,

- fake online auctions
- downloading/discovering they hadmalware
- malicious spam (for example fraudulent emails advising the recipient they had been recorded as accessing indecent images of children online and should pay a fine to avoid further action)
- purchasing of goods found to be counterfeit or faulty on arrival
- purchasing goods or service that did not exist/arrive
- employment scams (for example online websites advertising employment which required registration fees)
- investment scams
- identity theft (fraudsters purchasing goods or services or opening accounts online using stolen personal details)
- account takeover (money being taken by fraudsters from existing online bank account)

The complex nature of fraud made it difficult to put the fraud experienced into clear categories. Often a number of different types of fraudulent activity may be undertaken before the fraudster successfully obtained money from the victim. For example, what began as a romance scam with the victim meeting the fraudster on an online dating site, could become an investment fraud if the victim was convinced to send money for bogus shares.

Why Victims Fall for Online Scams

As noted in the previous section, the frauds experienced across interview and focus group participants involved a range of different types of contact occurring between the participants and the perpetrators. The internet played one of three roles to facilitate the fraud: as the central medium for the fraud, to support other offline methods such as a website to reassure a victim contacted in person or on the phone or as an enabling tool to lure victims for the fraud to occur by other means.

Generally speaking, participants who had experienced confidence frauds were usually able to explain how the fraud had occurred. The realisation that they had been defrauded occurred at the point where the goods or services they had purchased did not arrive or were faulty and the seller was unresponsive to their communications. There were also participants who were able to explain the workings of more complex frauds such as malware as illustrated by the case of 'Bob' (see later). Some participants (who had experienced a range of different types of fraud), were only partially aware or appeared to have very little knowledge of how the fraud occurred. For example, participants understood that people's details were passed between fraudsters but had little or no understanding about how the fraud against them had actually been committed and in particular how their personal details had been gained by the fraudster in specific instances:

> *"And I think that's one of the scary things is that I haven't got a clue how they've managed this, to have all those details, you know" (Interview participant).*

Even when participants offered some explanation of how elements of the fraud occurred, in some cases they were still unable to explain the whole story. One for example, admitted to having the same password for all their internet banking and social networking sites. They understood that the fraudsters were likely to have found out their password when there was a security breakdown on one of the sites, but was unaware of how they then managed to locate the bank accounts they held and access them with the password.

This section will now unpick the main reasons victims fall for scams drawing upon the interviews and focus groups with victims, interviews with stakeholders and broader literature. Some of the previous research has also indentified certain psychological traits which make some more likely to fall victims (Office for Fair Trading, 2009; Whitty and Buchanan, 2012). This was beyond the remit of this research, but is clearly an area which requires further investigation for the wide range of scams that occur. It is important to note that in many cases fraudsters utilise multiple strategies and the different techniques below should not be considered in isolation. Many of the techniques are not new and have been noted in previous research with other scams. However, as this section will reveal the internet provides for the amplification and more easy use of these tactics.

Small amounts and mass targeting

Many of the frauds perpetrated online work on the principle of large number of victims losing relatively small sums of money. This has a number of advantages for the fraudster. First the small amount of money lost means that many victims will be reluctant to report the fraud, which is often a time consuming process (1). Second, for those that do report it they are unlikely to receive much interest from the authorities who generally have high thresholds before they consider an investigation. Buying goods, entering lotteries, purchasing tickets for concerts and sporting events which never transpire are all common types of frauds perpetrated online where relatively small sums of money are sought. Linked to this is also the tactic of mass targeting with a business model built on the basis a small percentage will respond. The phishing scams with spam e-mail also work on this basis. The internet has revolutionised the ability of fraudsters to do this on an industrial scale cheaply and makes much smaller sums of money secured from victims more viable as a business model. By contrast telephone and mail methods of targeting have much higher costs. This means many more people are exposed to potential scams more frequently. This was illustrated by comments from one group participant.

> *"You look at your account and you think, oh two pee's gone out, I'm not going to do anything about it; but if there's a million people who do that… and it wasn't actually PayPal [taking the money] it was a fraud thing, it was a scam" (Group participant).*

Authority and legitimacy

Authority and legitimacy was a key trigger for victims falling for scams as has also been found by the Office for Fair Trading (2009) and Whitty and Buchanan (2012). Perpetrators tapped into participants' need to find the fraud legitimate by assuming a professional or legitimate façade. This was achieved by having a professional looking website and making reference to well known legitimate companies. That this could be successful is evidenced by the fact that participants had believed the fraudulent website they accessed to be legitimate because they used well known logos of existing legitimate companies. For the technically adept it is relatively easy to create a professional looking website or copy a legitimate one. The legitimate façade was also created by the perpetrator pretending that they were making a financial contribution like the participant or by having a 'real person' available to speak to the participant in order to reassure them every time they made contact.

> *"So I was looking on the internet this day and I come across this particular site … and there was a price I could afford, just about. So I looked into it as best as I could, rung the company up, spoke to the people, seemed, perfectly alright…there was a number on the website which has now disappeared" (Interview participant).*

In these instances the person the participant was directed to, claimed to be in a position of authority offering further credibility to the fraud. Lastly, appearing legitimate was facilitated by the

perpetrators being able to utilise legitimate sales techniques as part of the fraud, for example advertising items on well known bidding and social networking sites.

Another example of this technique was illustrated by the case of 'Mary', a middle-aged married woman with children, who regularly used the internet for online shopping and researching topics of interest. She wanted to buy a satellite navigation system and did a Google search on 'tom tom'. She clicked on the link for a bidding site which was selling a tom-tom and bought £15 worth of points so she could try and bid for one. The website looked legitimate, especially as it had the PayPal logo on display and she was used to buying items using other well known bidding sites. When she had almost won the item her computer froze. When she refreshed her screen she had to start bidding for the item again. In the end she lost £26 before realising that the website was fraudulent.

> *"And then the thing about it (the fraudulent website), what makes it look trustworthy is, there was like a symbol saying [name of well known e-commerce business] verified"* (Interview participant).

At other times the perpetrator had made use of legitimate sites in order to commit the fraud, for example selling and buying goods via sites such as Ebay. In some instances the financial third party had assumed a degree of responsibility for the fraud and had reimbursed the participant any money lost as a result. However, this was not always the case and other participants described how the financial third party had distanced themselves from the fraudulent activity on account of the perception that the fault lay with the 'participant' for not following their terms and conditions.

Visceral appeals

Visceral appeal was another key finding in the Office of Fair Trading (2009) research as well as some other studies which have explored scammers (Langenderfer and Shimp, 2001; Kienpointner, 2006). Appeals to basic needs such as money, sex, love, pain, sorrow etc are made. Such appeals had been experienced by participants, emotionally, for example offering the participant hopes of a romantic relationship, or financial security and what that would change in their lifestyle. For example participants had been offered a financial incentive for engaging in the fraud such as an investment recently maturing, a lottery win or a steady income through employment.

> *"They completely inundate you with it [the emails] and you're very tempted, in moments of weakness, to fall for it, and you think that it's going to happen" (Interview participant).*

An example of a positive reward was financial gain described above through a lottery win or job as one participant noted who had been offered easy money.

> *"You've had that big carrot dangled in front of you and you thought you were going to make some money to live an easy life. But there's no such thing as a free lunch" (Interview participant).*

Related to this is the often disproportionate relation between size of alleged reward and cost of obtaining it ('too good to be true'). On entering the fraud participants had felt that they were getting a 'good deal' and would come out of the experience better off. In one example, the participant had initially agreed to pay £125.00 for a deposit for a phone but then the 'seller' had told him to pay just £50.00.

> *"Initially, he (the perpetrator) said, oh, send me half, I think it was £125, and I thought, I would have done that, but then he said, I'll tell you what, look, just send me £50, I don't want*

to mess you around, just send me £50, and once the phone arrives, then as long as you're happy with it, send me the rest. You've got my address, I've got your address and details, and everything like that, and let's just do it sensibly. So, you know, it was only £50; I took a bit of a punt on it. Low and behold, obviously the phone never turned up" (Interview participant).

Embarrassing frauds

Many perpetrators create frauds which are embarrassing and make it less likely the victim will report to the authorities. Romance scams particularly fall into this category as many victims are reluctant to reveal they have been duped and in some cases have even been encouraged to participate in sexual activities online, which they will not want to discuss (Whitty and Buchanan, 2012). Other examples included when a parent paid for a photo shoot for their child to enter the modelling world but then never heard back, or when a woman applied for an escort job. Stakeholders noted how in such examples the victim would be too embarrassed to follow it up with the perpetrator or report the fraud.

"we've come across this where, young women presumably who are in need of a bit of extra cash, are invited to join, a, some kind of, what is it, a network or something for, providing escort services and they pay some kind of fee to be, put on the books and they never get any work sent to them. You know, and I suppose, to some extent, that it's difficult for these people to complain because they may not want their friends and family to know that they're doing that work…So, I think those sorts of things where it is difficult to complain 'cause it's embarrassing, you know, there's things around ,for men, you know, around sexual services which don't turn up or are not as described is I'm sure an area which is ripe for exploitation" (Stakeholder interview).

The internet allows for a much wider group to be reached who can be targeted with potentially embarrassing frauds.

Pressure and coercion

Some of the participants had been intimidated to go along with the fraud. This occurred in a number of ways from coercion that something bad might happen, such as going to the police, time pressures to bombardment of the victim. Such tactics were also noted by the Office of Fair Trading (2009) and Langenderfer and Shimp (2001). Examples reported by participants included being placed under time pressure so they would comply with the fraud and carry out the perpetrator's request quickly, receiving threats from the perpetrator, being made to feel responsible for solving a specific problem and the perpetrator implying that they were involved with non–legal activities to prevent them from reporting the fraud. In one example 'Tom', a middle-aged married man with children, regularly used the internet for both work and personal reasons. He had recently experienced a virus on his laptop at home. One morning when he switched on his laptop he was faced with a message which read '[name of local police], you are in violation of a Great Britain law for looking at illegal child abuse images ('child porn')'. The message went on to explain how if he paid a £100 fine then no further action would be taken. Tom had not been accessing illegal pornography but was going to pay the fine due to the concern he had that further action would be taken regardless. He became suspicious and reported it to the fraud department at the local police. He found his laptop had also been infected with a virus when he had opened the email, which took time and effort to remove. Tom felt this was annoying, but the email accusing him of accessing illegal pornography had a particularly negative impact:

"The other viruses, they were annoying as well but they hadn't got that shock element 'cause they didn't involve the police. They didn't involve being accused of child porn."

Grooming

Whitty and Buchanan (2012) found evidence of grooming in romance fraud and there was also evidence of this in this research. Some participants described how a process of grooming had taken place during the fraudulent activity. One way in which this has occurred was that the fraud had started with smaller, less noticeable, amounts before escalating to a larger amount. This process was reiterated in the stakeholder interviews where it was described how in some frauds, for example romance scams, perpetrators would initially ask for small amounts of money to test the victims and then gradually increase this. Stakeholders also reported on the various strategies perpetrators could use to facilitate the grooming process such as sending the 'victim' gifts like flowers or an e-card.

Enterprising fraudsters: diverse frauds

The entrepreneurial flair of fraudsters has been noted by Levi (1981) in his classic study of long firm fraud. Fraudsters engaged in mass frauds have also been described as 'enterprising' ,'vocational predators' with 'entrepreneurial bent' and 'scampreneurs' (Levi, 1998; Shover *et al*. 2003; and Button *et al.* 2009a). The participants' descriptions across the interviews and focus groups of how the fraud occurred illustrated a range of techniques which perpetrators had used in order to maximise the effectiveness of the fraud. There was also evidence of enterprise, innovation and business skills amongst some fraudsters confirming the research of Levi (1998), Shover *et al*. (2003) and Button *et al.* (2009a). These skills are clearly illustrated with the diversity and professionalism of many of the scams victims fall for and the constantly evolving nature of them to target new victims. As already discussed, there is huge diversity in frauds. The Office of Fair Trading (2006) identified a variety of frauds men, women, the old and young tend to fall for. Earlier the wide range of frauds were noted which are common. A perusal through the Action Fraud (2) website scam alerts also reveals the huge diversity, with each scam tailored to a particular type of victim. For instance trial scams for budding footballers, bad debt calls for those with loans, bogus rare metal investments for those with spare money, the fake census calls from the Office of National Statistics to secure personal information, the 'undelivered parcel' that requires a call to a premium number, and even Action Fraud has been impersonated to try an con victims out of more money in order to receive a reward. The ingenuity and innovation of the fraudsters is extensive and ongoing there seems to be a scam for almost every demographic group.

Fraud at a distance

Duffield and Grabosky (2001) have identified the importance of distance for the committing of frauds for the offender, as they are less likely to feel any empathy for the victims. Distance also serves other purposes. It presents challenges for many victims to confront the offender. They can't just pop into a local office to complain. They may find it difficult to actually contact the fraudster and if they do secure a telephone number or e-mail address, the former may have cost implications and they may also be ignored. There is also the additional factor that for a fraudster it makes law enforcement intervention less likely as there is often a reluctance to become involved in expensive overseas investigations and this may also act as a deterrent to report or for the report to be accepted by law enforcement. The internet and modern forms of communication are very well suited to enabling frauds to take place at a distance.

Conclusion

This paper has highlighted the significant numbers who fall victims to fraud and the huge diversity in online fraud. The paper used victims in England and Wales as the basis of this research, but it is clear that the same types of frauds and principles of these scams are occurring in many other countries who share the same language, such as Australia, Canada, New Zealand and the USA; but also beyond the English speaking nations, where access to the internet is common and there are wealthy citizens to be targeted, such as Japan and South Korea. This research has also highlighted the sophisticated ways in which online fraud occurs and how victims fall for it. Although not all participants were able to describe the inner workings of the fraud, the accounts indicated highly organised frauds and illustrated a range of perpetrator strategies at play. The centrality of the internet to the fraud experienced varied. In some cases it was the central medium for the fraud occurring, in others it was used alongside other methods of communication, to create the impression that the fraud was genuine (legitimacy) or as an enabling tool to lure the victim in (such as a website being seen as evidence the fraudulent goods were real). This may be indicative of the way in which computer mediated communication is integral to the day to day activities many people engage in.

Many of the reasons online fraud victims fall for online scams are similar to other mass marketing frauds, but clearly the internet does facilitate for the fraudster an easier way to utilise the traditional scamming techniques. Mass targeting is cheap and easy; impersonation and the authority that provides is undemanding for those with the technical skills; pressure, coercion and grooming can all take place at a distance from the keyboard of a laptop, without having to meet or speak with the victim. With the internet, the longstanding techniques used by fraudsters therefore become easier to apply on a larger scale meaning more people are targeted, more regularly, with regularly changing and often innovative scams and ultimately more falling for them.

The lessons for countering these scams are for another paper, but clearly these findings provide some insights for prevention, such as: educating and regularly alerting the public to the risk of scams, not to accept the word of unsolicited contact without further verification, to not be rushed into decisions and the closing down of fake websites as quickly as possible to name some. There also needs to be more regular and nuanced surveys of the prevalence of victimisation for fraud amongst the general public. This could provide better information on trends in different types of fraud, the modus operandi of fraudsters, the characteristics and needs of victims. Such surveys of appropriate depth would also provide data on any changes in why victims might be falling for such scams. This wide range of data would not only aid investigatory activities but also the prevention work of anti-fraud bodies. More depth research should also be conducted on some of the more common scams, for it is clear the underpinning technological revolution which has occurred in recent times is likely to further increase the risk of more people becoming victims as access to and ease of use of the internet continues to rise all over the world.

Funding

This research was commissioned and funded by the Office of the Sentencing Council for England and Wales.

ACKNOWLEDGEMENTS

We are grateful to Emma Marshall and Trevor Steeples from the Sentencing Council for their advice, support and assistance for the duration of this research. Thank you also to Mehul Kotecha, Steven Coutinho, Jasmin Keeble and Sarah Dickens for their input to the project.

We would like to thank the key stakeholders and the participants in this research for sharing their views, and we would like to thank the staff of organisations that provided their time to assist with the recruitment of participants, especially Rebecca Lambot at Action Fraud. We would also like to convey special thanks to those who shared their personal experiences of fraud offences and provided valuable information on factors which should be taken into account when sentencing fraud offences.

Notes

1. As the research was been conducted (Summer 2012) the process of reporting for victims of fraud in the United Kingdom was undergoing a period of change. Action Fraud (see Note 2 below) was in the process of becoming the central reporting body for all frauds. This may make the reporting of frauds in the future less time consuming as there are online and telephone facilities.
2. Action Fraud is the central UK report receiving body for all frauds which was established in 2010, which from April 2014 will fall under the control of the City of London Police, which is the national lead force on fraud. Prior to this it was run by the Government body, the National Fraud Authority, which has been abolished. See http://www.actionfraud.police.uk/

References

Amazon (2013), 'Press Release.' Retrieved 5 February 2013 from http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-newsArticle&ID=1779040&highlight=

Australian Bureau Of Statistics (2012), 'Personal Fraud Costs Australians $1.4 billion.' Retrieved 5 February 2013 from http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument

Bossler, A.M., And Holt, T.J. (2009), 'On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory (RAT)', *International Journal of Cyber Criminology,* 3: 400—420.

Buchanan, T. And Whitty, M. (Forthcoming), 'The Online Dating Romance Scam: Causes and Consequences of Victimhood', *Psychology, Crime and Law*.

Button, M. (2012), 'Cross-Border Fraud and the Case for an 'Interfraud'', *Policing: an International Journal of Police Strategies and Management,* 35: 285-303.

Button, M., Lewis, C. And Tapley, J. (Forthcoming), 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families', *Security Journal.*

Button, M., Lewis, C. And Tapley, J. (2009a), *Fraud Typologies and the Victims of Fraud Literature Review*. London: National Fraud Authority.

Button, M., Lewis, C. And Tapley, J. (2009b), *A Better Deal for Victims*. London: National Fraud Authority.

Button, M., Tapley, J. And Lewis, C. (2013), 'The 'Fraud Justice Network' and the Infra-structure of Support for Individual Fraud Victims in England and Wales', *Criminology and Criminal Justice,* 13: 37-61.

China Daily (2013) Two Stand Trial for Major Phone Scam in Shanghai. Retrieved 12 December 2013 from http://usa.chinadaily.com.cn/epaper/2013-09/11/content_16961084.htm

CIFAS (UK Fraud Prevention Service) (2012), *Fraudscape: Depicting the UK's Fraud Landscape.* London: CIFAS.

Consumer Sentinel Network (2012), *Databook for January to December 2011*. Retrieved 8 February, 2013 from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf

Croall, H., (2009), 'White Collar Crime, Consumers and Victimisation', *Crime Law and Social Change* 51: 127-146

Croall, H., (2007), 'Victims of White Collar and Corporate Crime', in Davies, P. Francis, and C. Greer, eds., *Victims, Crime and Society* , 78-108. London: Sage.

Cross, C ., (2012) *The Donald Mackay Churchill Fellowship to study methods of preventing and supporting victims of online fraud.* (Unpublished)

Duffield, G ., And Grabosky, P. (2001), *The Psychology of Fraud. Australian Institute of Criminology: Trends and Issues in Criminal Justice*. Canberra: Australian Institute of Criminology.

EBAY (n.d.), *The Company*. Retrieved 5 February, 2013 from http://pages.ebay.co.uk/aboutebay/thecompany/companyoverview.html

Facebook (2013), *Key Facts*. Retrieved 6 February 2013 from http://newsroom.fb.com/Key-Facts

Federal Trade Commission (2007b), *Consumer Fraud in the United States: The Second FTC Survey*. Retrieved 7 February 2013 from http://www.ftc.gov/opa/2007/10/fraud.pdf

Federal Trade Commission (2007b), *FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005*. Retrieved 7 February 2013 from http://www.ftc.gov/opa/2007/11/idtheft.shtm

Hache, A. C., And Ryder, N., (2011), 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminal on the Web lurking to scam shoppers this Christmas: a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud', *Information and Communications Technology Law,* 20: 35—56

Hamada, J. (2011) One-Click Fraud Targeting Smartphones in Japan. Retrieved 12 December 2013 from http://www.symantec.com/connect/blogs/one-click-fraud-targeting-smartphones-japan

Huff, R. , Desilets, C., Kane, J. (2010), *The 2010 National Public Survey on White Collar Crime*. Fairmont (WV): National White Collar Crime Center.

Internet World Stats (2012), *Internet Usage Statistics*. Retrieved 5 February 2013 from http://www.internetworldstats.com/stats.htm

Jewkes, Y. And Yar, M. (2010a), 'Histories and Contexts', in, Y. Jewkes and M. Yar, eds., *Handbook of Internet Crime,* 9-16.. Cullompton: Wiley.

Jewkes, Y. And Yar, M. (2010b), 'Introduction: The Internet, Cybercrime, and the Challenges of the 21st Century', in, Y. Jewkes and M. Yar, eds., *Handbook of Internet Crime,* 1-8. Cullompton: Wiley.

Karstedt, S. And Farrall, S. (2006), 'The Moral Economy of Everyday Life', *British Journal of Criminology*, 46 : 1011-1036.

Kienpointner, M (2006), 'How to present fallacious messages persuasively: The case of the 'Nigeria Spam Letters', in, P. Houtlosser, and M. A. van Rees, eds., *Considering Pragma-Dialectics*, 161-173. Mahwah, N.J./London: Lawrence Erlbaum Associates.

Langenderfer, J., And Shimp, T. A. (2001), 'Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion', *Psychology and Marketing, 18: 763-783*.

Levi, M. (2008), 'Organized Frauds and Organising Frauds: Unpacking the Research on Networks and Organisation', *Criminology and Criminal Justice* 8: 389-419.

Levi, M. (2001), 'White Collar Crime Victimisation', in, N. Shover, and J., P. Wright, eds., *Crimes of Privilege*. Oxford: Oxford University Press.

Levi, M. (1998), 'Organising Plastic Fraud: Enterprise Criminals and the Side-Stepping of Fraud Prevention', *The Howard Journal of Criminal Justice,* 37: 423-438.

Levi, M (1981), *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud*. London

McGuire, M. and Dowling, S. (2013a) *Cybercrime a Review of the Evidence. Research Report 75.Chapter 2: Cyber-enabled Crimes: Fraud and Theft.* Retrieved 16 December 2013 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

McGuire, M. and Dowling, S. (2013b) *Cybercrime a Review of the Evidence. Research Report 75. Chapter 4: Improving the Cybercrime Evidence Base*. Retrieved 16 December 2013 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf

National Fraud Authority (2013), *Annual Fraud Indicator*. London: National Fraud Authority.

Nolan, S. (2012), *Huge Spike in Online Dating After Christmas as Holiday Spirit Encourages Thousands to Cure their Loneliness*. Retrieved 5 February 2013 from http://www.dailymail.co.uk/news/article-2254968/Online-dating-statistics-Huge-spike-Christmas-holiday-spirit-encourages-thousands-cure-loneliness.html#axzz2K7uODPCt

Office Of Fair Trading (2009), *The Psychology of Scams: Provoking and Committing Errors of Judgement*. London: Office of Fair Trading.

Office Of Fair Trading (2006), *Research on Impact of Mass Marketed Scams.* London: Office of Fair Trading.

Office for National Statistics (2013a) *Internet Access – Households and Individuals, 2013*. Retrieved 16 December 2013 from http://www.ons.gov.uk/ons/dcp171778_322713.pdf

Office for National Statistics (2013b), *Crime in England and Wales, Year Ending September 2012 Statistical Bulletin*. Retrieved 5th February 2013 from http://www.ons.gov.uk/ons/dcp171778_296191.pdf

Office for National Statistics (2013c) *Chapter 4: Mass Marketing Fraud*. Retrieved 16 December 2013 from http://www.ons.gov.uk/ons/dcp171776_309772.pdf

Randall, C. (2010), *E-Society*. London: Office for National Statistics.

Rege, A., (2009), 'What's love got to do with it? Exploring online dating scams and identity fraud' *International Journal of Cyber Criminology,* 3 : 494—512

Sandywell, B. (2010), 'On the Globalisation of Crime: The Internet and New Criminality', in, Y. Jewkes and M. Yar, eds., *Handbook of Internet Crime,* 38-66. Cullompton: Wiley.

Scottish Government (2011), *Scottish Crime and Justice Survey: Main Findings*. Retrieved 5th February 2013 from http://www.scotland.gov.uk/Resource/Doc/361684/0122316.pdf

Shichor, D., Sechrest, D., And Doocy, J., (2000), 'Victims of Investment Fraud, in, H. Pontell and D. Shichor, eds., *Contemporary issues in crime and criminal justice: Essays in Honor of Gilbert Geis,* 87–96. New York: Prentice Hall.

Shover, N., Coffey, G., S. And Hobbs, D. (2003), 'Crime on the Line. Telemarketing and the Changing Nature of Professional Crime', *British Journal of Criminology*, 43: 489-505.

Smith, R., G. (2010), 'Identiy Theft and Fraud', in, Y. Jewkes and M. Yar, eds., *Handbook of Internet Crime,* 273-301. Cullompton: Wiley.

Think Insights With Google (2012), *Key Market Report: Trends in Digital Device and Internet Usage*. Retrieved 6 February 2013 from http://www.thinkwithgoogle.com/insights/library/studies/trends-in-digital-device-and-internet-usage-2012/

Treadwell, J. (2011), 'From the Car Boot To Booting It Up? Ebay, Online Counterfeit Crime and The Transformation Of The Criminal Marketplace', *Criminology and Criminal Justice*, 12: 175-191.

US Department Of Justice (2011), *Identity Theft Reported by Households 2005-2010*. Retrieved 7 February 2013 from http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf

Wall, D., S. (2007), *Cybercrime*. Cambridge/Malden, MA: Polity.

Webb, R., (2010), 'A New Approach To Online Consumer Protection In The UK', *E-commerce Law and Policy,* April 2010.

Whitty, M. (2013), 'The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam', *British Journal of Criminology*, 53: 665-884.

Whitty, M., And Buchanan, T. (2012), *The Psychology Of The Online Dating Romance Scam.* Leicester: University of Leicester.