Understanding the UK Public Perception of Cyber Fraud

Dhara Letu

21012489

Supervised by John De-Hayes

FORE60375 Project in Policing and Criminal Investigation

BSc Hons Policing and Criminal Investigation

Word Count: 10,061

Acknowledgments

I would like to thank all the professors I have had over the course of the three years for everything they have taught me, and every participant that has participated in my survey.

I would like to express my sincere gratitude to my mentor John De-Hayes for helping me throughout the whole process of writing this dissertation, as well as my parents, my aunt Miruna Baban, and Kelly McCauley for always being there for me and supporting me throughout my university experience. Special thanks to Sara Kosman, Celine Moss and Tara Gaunt-Nelson for sticking with me throughout university, despite the ups and downs, and making it such a wonderful experience.

Abstract

Cybercrime has been named as one of the biggest threats globally and a national priority (Schreuders *et al.*, 2020). Departments such as the Office of National Statistics collecting statistics on fraud and computer misuse offences with the use of the Crime Survey for England and Wales, the National Fraud Intelligence Bureau, Action Fraud, Cifas and UK Finance, have been working together to tackle cybercrime and cyber fraud. However, the publication of the new fraud strategy will hopefully produce a shift in the existing approach in tacking fraud to achieve positive results.

This research project aimed to explore the public perception of cyber fraud in the United Kingdom, to gain a better understanding of the perceptions surrounding cyber fraud. The Home Office (2018) identified a perception gap and this research aimed to try and breach said gap. This research utilised an exploratory research design and collected primary data with the use of an anonymous survey distributed on the social media platforms, Facebook, X and Instagram. The survey collected both qualitative and quantitative data that was analysed using thematic analysis, descriptive statistics and inferential statistic using Statistical package for Social Science (SPSS) software.

The results found that overall people have heard of a variety of different types of cyber fraud, and that they believe cyber fraud to be a great issue. Research also showed that some preventative measures were taken, and that the majority would call the police and the bank in case of a cyber fraud incident. The results also concluded that the majority did not know what the police were doing to tackle, and deal with, cyber fraud. Results of the qualitative data analysed produce themes such as the belief that further education is needed for the public, greater involvement of organisations and government agencies, as well as the need for more resources and training for the police to be more prepared to tackle cyber fraud. Further studies would be preferred to strengthen the validity of these findings, along with the fact the cyber fraud will evolve alongside technology and therefore continuous research may be needed.

Contents

Introduction

This research aims to analyse and understand the public perception of cyber fraud in the United Kingdom (UK) population. This was done by identifying the different types of cyber fraud the public has knowledge about, what the public do in order to protect themselves from cyber fraud, and what they would do if they became a victim of cyber fraud. This research also looked at whether the public are aware of what the police are doing to tackle cyber fraud, as well as if they are satisfied with how they tackle and deal with cyber fraud.

Defining cyber fraud can be broken down into two parts. Firstly, by defining fraud, and secondly by defining cybercrime. In section 2(1) of the Act (Fraud Act 2006) it states that a person is guilty of fraud if they make a deceitful presentation that is false with the intention of gaining something or putting someone at risk of loss or cause loss. Action Fraud (2023a) describes cybercrimes as being any actions that involves computers and the internet for criminal deeds. Cybercrime is used as a broad term to cover all crimes that take place online, that are committed using computers or are facilitated by online technology (Gordon and Ford, 2006; Education & Skills Funding Agency, 2023). Cybercrime also known as cyber fraud (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014; Metropolitan Police, 2024), is a form of cyber enabled crime (Home Office, 2013), which are traditional crimes that with the addition of technology it can increase their scale and reach (Crown Prosecution Service, 2019). Alternately, the Council of Europe Recommendations of 1989 defined cyber fraud as "the input, altercation, erasure or suppression of computer data or...programs...that influences the result of data processing thereby causing economic or possessory loss of property..." (Schjolberg, 2014, pp. 38). For the purpose of this project cyber fraud will also be used in reference to computer fraud, cyber-related fraud, cyber-enabled fraud and online fraud.

The first record of cybercrime occurred in the 1960s and the offenders were often found to be the people that were on the inside that had easy access to the computer (Richards *et al*., 2010). Cybercrime legislation did not come into action in the UK until the 1990s (Yar, 2006) and prior to the introduction of the Act (Computer Misuse Act 1990), offenders were charged under traditional crimes as cybercrime was not acknowledged as an offence (Richards *et al*., 2010). Phone phreaking, that was at its peak in the 1960s and 1970s (Kumar, 2022), was the

manipulation of phone networks (Jordan, 2017). While phone phreaking had roughly stopped by the 1990s (Kumar, 2022), many of these offenders went on to become hackers (Richards *et al*., 2010). Cyber fraud has continued to increase at a rapid rate that shows no sign of decreasing (Gordon and Ford, 2006; Curtis and Oxburgh, 2023), while criminals initially started with basic scams and fraud it has grown to include targeting consumers and banks, stock manipulation, forming firms and legitimate businesses as a cover for their criminal activities (Howard, 2009). Police recorded crimes as well as sentencing data did not distinguish whether crimes were committed online in the past, instead recording it as the actual offence, such as recording the crime as fraud even though it was committed online (Home Office, 2013). Cybercrime is a significant facilitator of fraud (National Crime Agency, 2020), and it is estimated that the internet plays a role in at least 61% of all fraud (Office of National Statistics, 2022). Correia (2022) referenced the crime statistics from the year ending 2021, which corroborates with the reported by the Office of National Statistics (2022) who compared the crime statistics from the year ending 2021 and 2022.

The Home Office (2018) have identified a perception gap in between the UK public's perception and cybercrime, however there is little known if this perception gap can also be generalised across to the perception of cyber fraud. The Home Office is the head government branch for crime and their prime concerns were to decrease crime, minimise immigration, and prevent terrorism (National Audit Office, 2015). While there have been studies done into cyber fraud (Howard, 2009; Brooks and Button, 2011; Button, Lewis and Tapley, 2012; 2014; Drew and Cross, 2013; Cross, 2013; 2015; 2018; Cross and Blackshaw, 2015; Cross, Richards and Smith, 2016; Button and Cross, 2017; Levi *et al*., 2017; Correia, 2019; 2022; Akdemir, Sungur and Başaranel, 2020; Bossler, 2020; Ma and McKinnon, 2021), this research aims to achieve a better understanding of the publics' perception of cyber fraud and the policing side to gain a better grasp of the issues surrounding cyber fraud and how it is handled.

The types of cyber fraud identified in this research were botnet-related fraud, click fraud, call centre fraud, computer hacking, domain name scams, facility takeover, fraudulent takeover, internet dialler scams, invoice scams, identity theft, malware and computer virus, mailbox and

multiple post re-directions, phishing, proxy servers and remote access tool scams. Definitions of these types of frauds can be found in the glossary section.

Aims and Objectives

The aim of this research is to understand the public perception of cyber fraud.
The objectives are:

- To explore the government departments and police agencies on cyber fraud.
- To analyse the public knowledge and opinion of cyber fraud.
- Identify what, if any, steps the public take to protect themselves from cyber fraud.
- To assess the public knowledge on police handling of cyber fraud.

Hypotheses

These hypotheses were produced after research into; education (Bele *et al*., 2014; Cross, Richards and Smith, 2016; Button and Cross, 2017; Witsenboer, Sijtsma and Scheele, 2022), public perception (Bidgoli, Knijnenburg and Grossklags, 2016; Home Office, 2018), knowledge (Button and Cross, 2017; Akdemir, Sungur and Başaranel, 2020), and preventative measures (Higgins and Ricketts, 2010; Christin *et al*., 2012; Sağlam, Miller and Franqueira, 2023), regarding cyber fraud were conducted.

1. H0 – There will be no correlation between the participants education level and their opinion of how extensive cyber fraud is of an issue.
H1 – There will be a correlation between the participants education level and their opinion of how extensive cyber fraud is of an issue.

2. H0 – There will be no relationship between the participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud.
H1 – There will be a relationship between the participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud.

3. H0 – There will be no relationship between the participants opinion of how extensive cyber fraud is of an issue and how many steps they take to protect themself from cyber fraud.

H1 – There will be a relationship between the participants opinion of how extensive cyber fraud is of an issue and how many steps they take to protect themself from cyber fraud.

This project will first review existing literature into cyber fraud. It will then set out the methodology adopted for the purpose of this research project. After this the researcher will outline, analyse and discuss the results, findings and limitations from the study. Finally, with the use of the key findings, an overall conclusion will be drawn where recommendations may be given.

Literature Review

In this section the theme of cyber fraud will be explored. Firstly, the subtheme of government departments and police agencies will be explored, looking at reasons cyber fraud may not be reported. Next the public knowledge will be investigated, as well as looking at cyber fraud during coronavirus pandemic (COVID-19), prevention, and cyber fraud education. Lastly, the public perception and policing cyber fraud will be investigated, and the theoretical underpinning of this research will be described.

The earliest recorded occurrence of cybercrime was in the 1960s (Dupont and Whelan, 2021), however it mostly consisted of insiders abusing their powers due to their free access (Brenner, 2007). By the 1990s with the evolution of computers and the internet, criminals also became more sophisticated, with cyber fraud becoming the most common by the 2000s (Brenner, 2007). Nonetheless, cyber fraud was excluded from the main measures of crime as the criminal justice system focused on traditional crimes which meant that cyber fraud remained neglected (Button and Cross, 2017). More recently a significant shift in accepting the existence of cyber fraud took place, most notably by the Office of National Statistics (ONS) in its inclusion of fraud and computer misuse statistics in 2016 (Button and Cross, 2017). As well as this, the Crime Survey for England and Wales (CSEW) began recording figures on fraud and computer misuse in 2015 and while the CSEW collects information from the adult population it offers a more overall picture than the police recorded data that only gives a partial picture as most fraud offences are not reported (Office for National Statistics, 2016). During COVID-19 period, the Telephone-operated Crime Survey for England and Wales (TCSEW) identified a 25% increase of cyber fraud offences compared to the year ending March 2020 (Office of National Statistics, 2022). This data corroborates the National Fraud Intelligence Bureau (NFIB) data collected from Action Fraud, Cifas and UK Finance, however they also identified that offences referred by Action Fraud to have decreased while report to UK Finance increased (Office of National Statistics, 2022). Action Fraud remains a lead resource in generating crime trend analysis, managing threat assessments and appraising crime prevention campaigns (Correia, 2022, Curtis and Oxburgh, 2023). However, just as there are issues with police recorded crime due to relying on the victims to report the crime (Correia, 2019), there are still various challenges when using Action Fraud data in research (Correia, 2022). Office of National Statistics (2022) affirm that the percentage of

offences reported to Action Fraud are low and that long term trends for fraud and computer misuse are unavailable due to only having full year data from 2017 onwards. In a study by Correia (2022) into Action Fraud, under-reporting was found to have a substantial impact on the accuracy of knowledge about recorded crime. Furthermore, 66% of participants were found to have never even heard of Action Fraud and 10% assumed fraud was reported to a different authority (Correia, 2022). In addition, research found issues with Action Fraud data collection and recording procedures that seemed to worsen the issues pertaining reporting problems of cybercrimes (Akdemir, Sungur and Başaranel, 2020). Victims of fraud may report their incident straight to the bank and therefore this data may be lost to the overall statistics of cyber fraud (Wall, 2008).

The lack of reporting cyber fraud may be due to the embarrassment of becoming a victim, the chance the police may view fraud as low priority and victim blame, victims not knowing they are victims (Button and Cross, 2017), and confusion as to where it is best to report it to (Button and Cross, 2017, Curtis and Oxburgh, 2023). Despite that, Levi *et al*., (2017) found that victims of cyber fraud were instructed to contact Action Fraud, unless immediate response from the police was needed. However, not only were these victims blaming themselves (Bossler *et al*., 2020), but the police were also blaming them (Van de Weijer, Leukfeldt and Bernasco, 2019), and the victim's concerns were being trivialised (Cross, Richards and Smith, 2016). Victims may find themselves involved with cyber fraud not understanding the possible ramifications, not accepting that they were involved in such an incident or even find themselves unwilling to report such offences due to their embarrassment and the stigma surrounding being a victim of cyber fraud (Ma and McKinnon, 2021). This is supported by Wall (2007) who suggests that due to the victim feeling humiliation and shame, unknowing of what to do next, or simply because the want to move on from what has happened, they are hesitant to report the police. There are multiple debates that blame the victims of cyber fraud, relaying responsibility onto them to hold themselves amenable for their conduct (Cross, 2013). Including Wall (2008) who believes that the individual should take responsibility for their actions. To put simply, it is hypothesized that if an individual does not participate then there cannot be a victim of cyber fraud (Cross, 2015). Having said that, this argument fails to acknowledge how sophisticated these offenders are to be able to manipulate and exploit the victims, nor the difficulty of the amount of people targeted (Drew and Cross, 2013). Studies show that cyber fraud victims share the same outcomes as

victims of serious crimes (Cross, 2015), such as financial loss, psychological and emotional impact, relationship issues, mental and/or physical health issues (Button, Lewis and Tapley, 2009a). Research into cyber fraud victims shall hopefully succeed in eliminating the belief that only unintelligent individuals become victims, and that they will be treated akin to victims of serious crimes due to the similar effects on the victims (Button, Lewis and Tapley, 2009a).

The public lack of knowledge is one of the reasons such cybercrimes are not reported (Akdemir, Sungur and Başaranel, 2020). Button and Cross (2017) argue that the reason there is a lack of understanding is due to cyber fraud being excluded from the main measures of crime and therefore lacking an accurate record of the extent of these offences. Even though there are multiple agencies involved with cyber fraud (Cross, 2018), there are still victims that admit a lack of knowledge around online threats which can lead to lack of reporting cyber fraud offences (Akdemir, Sungur and Başaranel, 2020). The Home Office (2018) identified three key myths that explain the existence of the perception gap between the public's knowledge of cybercrimes and the reality of it. The three key myths are that cybercrimes are not something the public need to be worried about and that they are not real crimes, as well as that there is nothing the public can do to protect themselves against cybercrimes (Home Office, 2018). Another reason the public may lack understanding may be because of the complexities of the definitions. Beals, DeLiema and Deevy (2015) identified multiple terms and sub-categories of cyber fraud, with definitions differing as fraud covers a wide range of offences (Button and Cross, 2017; Bossler *et al.*, 2020). For example, Action Fraud (2023b) has a list of 165 types of fraud that include a cyber aspect. Due to the multiple characteristics of cyber fraud, there are multiple agencies a victim can report the incident to which may cause the victim to become overwhelmed especially if after going through all the trouble of choosing an agency that agency then goes to refer them to another (Cross, 2018). Grimes (2021) found that individuals may not be comfortable reporting cybercrimes due to experiencing emotions of uncertainty or scaredness as well as believing the process to be too difficult. Because of this the offence may go unreported and therefore unnoticed for a longer period (Grimes, 2021). Other research has also found victims to be reluctant to report incidents of cybercrimes (Grabosky and Smith, 2001; Button and Cross, 2017) and therefore concluded that the task fell to trying to handle the risk of becoming victims so that the best plausible outcomes are achieved (Grabosky and Smith, 2001).

The increase in cyber fraud incidents that were identified in the year ending March 2022, is suggested to be related to increased online activity and the behaviour changes due to COVID-19 (Office of National Statistics, 2022). Nikolovska, Johnson, and Ekblom (2020) state that multiple agencies and online platforms warned the public of the possibility of an increase in cyber fraud at the beginning of COVID-19. As with the increase of people shifting to additional online activities, the possibility of victimisation also increases (Ma and McKinnon, 2021). The spike in advance free fraud and consumer and retail fraud, refer to glossary section for definitions, suggests offenders are taking advantages of said behaviour changes in this period as online shopping increased (Office of National Statistics, 2022). However, Kemp *et al*., (2021) theorised that the increase in cyber fraud is only short term and that eventual the numbers will decrease back to the initial trend. Ma and McKinnon (2021) found that offenders utilise victim's psychological vulnerabilities and manipulate their emotional uncertainty from COVID-19 to facilitate cyber fraud. By utilizing the victim's weaknesses, the offender creates a situation where the probability of a positive reciprocation and complaisance by the victims heighten (Drew and Cross, 2013).

This further supports the need for educational programmes about online threats to improve public awareness (Akdemir, Sungar and Başaranel, 2020). It is important to increase the public knowledge and understanding of cybercrimes as attempts to measure cybercrimes have been varied and frequently generated unreliable results (Hernandez-Castro and Boiten, 2014). Research into cyber fraud has shown that there is a varied scope of frauds being perpetrated as well as diverse victims with their age, gender, education and socio-economic standing ranging, proving that many of us are prone to fall victim to fraud offences (Button, Lewis and Tapley, 2009a). Considerable importance has started being placed on the individual to become capable of protecting themselves from becoming victims of cyber fraud, such as encouraging them into employing their own preventative strategies, in hopes that cyber fraud offences will reduce with the help of a greater awareness of such crimes as well as with the use of education preventative strategies (Button, Lewis and Tapley, 2009a). Button and Cross (2017) advise that the use education and awareness are key components for victims regarding crime prevention. However, research into the victim's education levels have produced mixed results, producing negative and positive relationships with regards to the likelihood of reporting the offence (Van de Weijer, Leukfeldt and Bernasco, 2019). Bidgoli, Knijnenburg and Grossklags (2016) recommended that

more awareness on how to report cybercrimes as well as statistics on victims and prevention tips are necessary for reducing victims of cybercrimes.

Children and teenagers were identified as a vulnerable group of falling victim to cybercrimes as they spend a great deal of time on the internet and social platforms (Bele *et al*., 2014). This is supported by Oksanen and Keipi (2013) as they found 15- to 24-year-old to be the most targeted by offenders than any other target group. Research by Bidgoli, Knijnenburg and Grossklags (2016) established that undergraduates are at risk of cyber fraud as they have just started having greater financial responsibilities and are highly active on the internet during this period. This vulnerable target group are found to be exposed to the same threats as adults; however, the consequences may be even more catastrophic due to the seriousness of the consequences that can occur such as becoming victims of grooming (Bele *et al*., 2014). Bele *et al*., (2014) recognised a need for further education concerning the significance of information safety, the risks of cybercrimes and the implementation of preventative strategies in all target groups to be capable to effectively address the issue of cybercrimes. Concluding that constant recurring education is instrumental in promoting awareness and motivating the public to apply preventative procedures in daily life (Bele *et al*., 2014). For that reason, researchers suggest that strategies and education policies need to be developed for the younger generation (Sağlam, Miller and Franqueira, 2023). Witsenboer, Sijtsma and Scheele (2022) recommended that cyber security should be implemented as an integral part of basic school education, with significant scrutiny being placed on cyber fraud. Cybercrime experience and media awareness seemed to also increase the public's perception of cybercrime risk, which was found to increase the publics resolve to avoid online banking, online shopping and online socialisation (Riek, Böhme and Moore, 2015). The media also allow the police to gain an understanding of the publics perceptions which is crucial for the purpose of maintaining a positive relationship (Ralph *et al*., 2022).

A study by Cross, Richard and Smith (2016) found that participants had varied levels of knowledge of cyber fraud, and that many were unaware of what recovery fraud is, refer to glossary section for definition. Establishing that education and raising awareness was an important aspect of cyber fraud prevention (Cross, Richard and Smith, 2016). According to research many people believe that the law enforcement and other agencies are responsible in setting up educational sessions to prepare individuals to respond to all types of fraud they may

become susceptible to, which will potentially help repeat victims especially (Levi *et al*., 2017). It is implied that greater early education of risk management is needed and that it may be done better by third sectors, such as voluntary organisations, focusing on helping target groups to manage the risks of cyber fraud (Levi *et al*., 2017). This is supported by Akdemir, Sungar and Başaranel (2020) who also highlighted the need for more educational programmes for the improvement of awareness relating to online threats, such as cyber fraud.

Recent UK government reports show that victims are also unlikely to report offences because of the perception that the police are ill-equipped to deal with cybercrimes (Curtis and Oxburgh, 2023). Lee *et al*., (2021) conducted a survey with 155 inspectors working in cybercrime departments and found that they perceived cybercrimes to be just as severe as traditional crimes, however they were generally uninterested in responding to such offences viewing them as less significant in comparison to in life crimes. A study by Holt, Bossler and Fitzgerald (2010) concluded that the police officers acknowledge their lack of knowledge pertaining cybercrimes and that they need expert agencies to help in investigations, including restricted resources and capacity were also identified. A survey by Bossler and Holt (2012) established that local police officers had a limited understanding on how to respond to incidents of cybercrimes, finding that 80% of officers were reluctant to a degree to participate in cybercrime investigations and 63.5% of officers acknowledged that most cybercrime incidents are not reported to the police. However, in a more recent study a decrease was found. Bossler *et al.,* (2020) who collected data from over 1,200 officers across 34 police agencies in the UK, found that more than half (57%) of police officers felt neutral or unprepared to deal with cyber fraud. Additionally, fraud and cybercrimes are still found to be under-reported (Correia, 2022).

Policing cyber fraud is a complex problem, and as such a multi-agency approach is needed with international and national agencies working together more extensively (Brooks and Button, 2011; Akdemir, Sungar and Başaranel, 2020). Grabosky and Smith (2001) proposed that a substantial number of cybercrimes and security will be contingent on an extensive reach of agencies, with the responsibility falling on agencies, government agencies, informational security experts, and individuals. The magnitude of the internet permits offenders to remain under anonymity and therefore leads victims and the police to come to terms with the probability of identifying the offenders as low (Yar, 2006). In addition, the global side means that practical

police actions nay become problematic and time-consuming (Wall, 2001). Yar (2006) identified that due to the limited resources and expertise available it can result in the appropriate authorities regarding reporting to become unknown to the victim. Research shows that in case of the victim's money being sent offshore, recovery of said money becomes difficult and, in most cases, unlikely (Button, Lewis and Tapley, 2009b). Moreover, the transnational aspect of cyber fraud, the use of technology and identity fraud by the offenders to come these crimes, the lack of resources and training to respond to cyber fraud as well as inadequate legislation (Button, Lewis and Tapley, 2012; Cross and Blackshaw, 2015) means that it is incredibly difficult for the police to respond to cyber fraud in a way that satisfies the victims and the public (Cross, 2018). While agencies may have absences of authority, resources and capacity to help victims of cyber fraud, it is important that victims are treated without judgement and are given a realistic overview of what can be done for them in that situation (Cross, Richards and Smith, 2016). This can be done by following the victims' code for policing that also contains the right to offer victims support when they report a crime (College of Policing, 2021).

It is hard for law enforcement agencies to successfully tackle cybercrimes without understanding the perpetrators motives and due to the high-volume aspect of it, traditional ways of policing are not working effectively anymore despite the multitude of legislation (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014). This clearly demonstrates and strengthens the idea that prevention is key and that steps need to be taken to put a stop to or in the least case minimise the risk of victimisation of fraud (Drew and Cross, 2013). Levi *et al*., (2017) propose that the law enforcement response must be strategic, in order for the strategy to achieve the desired goals (College of Policing, 2018). The Home Office strategic new fraud strategy aims to put greater precedence on fraud by clarifying the roles and responsibilities of the police force and how to utilises the agencies available in addition to placing a focus on resources as well as maximising the current resources to tackle fraud (Secretary of State for the Home Office, 2023).

Social learning theory, proposed by Bandura (1977), can be used to explain people's behaviour as being influenced by inner forces such as their needs, drives, and impulses. Research implies that individuals will weigh up the level of protection they believe will be enough to keep them safe against the inconvenience of having to employ such actions, finding the more than not individual will discard the preventative action if they decide they are inconvenient (Home Office,

2018). Due to the public lack of knowledge of the risk of cybercrimes, they do not feel dissuaded from being online and are therefore incapable of making informed decisions concerning any risks, old and new, they may encounter (Wall, 2008). Victim typologies fortify the perception that if individuals change and regulate their actions, they will be able to avoid victimisation, maintaining the ideology that the guilt falls on the victim and that they should be held responsible (Cross, 2015). However, social learning theory also argues that new patterns of behaviour can be learned through observation of others behaviour or through direct experiences (Bandura, 1977), with recent studies showing that behaviours are mainly learned through experience (Witsenboer, Sijtsma and Scheele, 2022). Implying that once an individual becomes a victim of cyber fraud, they will change their behaviour to avoid becoming victims again in the future. This can also be used to explain why cybercrimes are such a huge issue, as it argues that individuals learn through observing behaviour how to engage in cybercrimes and that behaviour is then reinforced when they ascertain a profit and are not get caught by the police. The routine activities theory proposes that there are three variables that can explain crime: presence of motivated offenders, availability of targets and the absence of a capable guardian (Cohen and Felson, 1979). This also supported by Grabosky and Smith (2001) who found that most cybercrimes occurs when a suitable guardian is absent. Overall, while social learning theory can help explain how individuals may become victims and perpetrators, routine activity theory helps explain the conditions necessary for the crime to take place.

Methodology

This section explains the over overarching design for this research, as well as describing the methods used and the principles behind them.

Design

This project utilised an exploratory research design to discover the characteristics and interpretations of the participants (Holton and Burnett, 2005). An exploratory study was used to address certain topics where little information is known and to tests hypotheses (Swedberg, 2020). A mixed method research strategy was used, collecting both quantitative and qualitative data (Hurmerinta-Peltomäki and Nummela, 2006) to give statistical results as well as an in-depth understanding of the procedures and relationships (Birchall, Murphey and Milne, 2016). Quantitative data from open ended and multiple-choice questions were used as it eliminated random guessing so that the measurement error could be reduced (Bridgeman, 1992). Holton and Burnett (2005) found that this type of data is particularly good when studying a large population sample to make a generalisation from the results. Qualitative data was used to cast light on the quantitative data by granting a deeper insight of the participants perspectives and understandings (McKim, 2017). Mixed methods allow for a deeper and broader understanding of the results (Hurmerinta-Peltomäki and Nummela, 2006) even if it requires additional resources and time, it has been proved to add value to the research by increasing the validity of findings (McKim, 2017). Primary data was collected using a survey due to its low cost to be made and distributed, and its proficiency in collecting large amounts of information from the population sample (Fife-Schaw, 2020; Roopa and Roni, 2012). A survey was used due to its usefulness in gaining participant perceptions, especially in open ended responses in exploratory research (Fife-Schaw, 2020). While this method is time consuming, the data produced is current and of high accuracy (Ajayi, 2017). A deductive approach was taken to prove or disprove the hypotheses developed from the theories investigated (Barroga *et al.*, 2023).

Sample

The survey was distributed on social media, due to its inexpensiveness and rapid responses (Yun and Trumbo, 2000). Studies found that using social media runs the risks of unknowing if the target audience is being reached (Sims, 2019). However, this is in minimal risk as this research

only requires participants to be living in the UK and over the age of 18. Snowball sampling was used, which is a non-probability sampling method, were the initial participants are asked to identify other potential participants and so on, meaning the final participants are a sample made by referrals (Diamantopoulos and Schlegelmilch, 1997). This type of sampling has been criticised to depend on selection bias (Parker, Scott and Geddes, 2019), as the sample may be unrepresentative of the population (Krishna, Maithreyi, and Surapaneni, 2010) as participants may have similar perspectives to the researcher. To minimise this the researcher created new social media accounts and posted the survey in multiple different groups to achieve some variation.

In total there were 76 participants, most responders were female (67.1%, n=51) with only 23 male (30.3%), 1 non-binary/third gender (1.3%), and 1 participant preferring not to say (1.3%). The mean age of participants was 38.6 years, and the standard deviation was 14.031. The youngest participant was 18 and the oldest was 77, giving the range of 59 years. 17 participants had GCSE (Level 1&2) qualification or equivalent (22.4%), and 13 had A-level/B-tec (Level 3) qualifications or equivalent (17.1%). The majority had post-graduate Masters (Level 7) degree qualifications or equivalent (30.3%, n=23) and 20 participants had Undergraduate/Foundation (Level 4,5,6) qualifications or equivalent (26.3%). The minority of participant had Higher (PhD) level qualification or equivalent (3.9%, n=3).

Procedure

Participants were asked to answer fourteen questions that should take 5-10 minutes to complete. The survey was made using Qualtrics, as it is a fast and easy software to use (Boas, Christenson and Glick, 2018), and distributed on social media where it was available to complete for four months. At the end of the four months the data was saved in Excel format and sent to the supervisor, complying with General Data Protection Regulations 2016. Any responses where participants did not answer any questions or stopped responding after stating their age and gender were removed in the coding process in SPSS.

Materials and Equipment

The Qualtrics software was used to make the survey. Any questions that were not relevant for the participant were programmed to be skipped (Birchall, Murphey and Milne, 2016). Such as if participants answered they were satisfied with how the police dealt with cyber fraud they would not be asked the next question which is asking for their opinion on how the police could improve. Participants were also allowed to pick their level of satisfaction on certain questions with the use of Likert scales (Birchall, Murphey and Milne, 2016). There were three questions where participants could rate their level of satisfaction that focused on different aspects to do with cyber fraud and the police. In addition, using a Likert scale, participants were asked to rate their knowledge on cyber fraud and what the police are doing to tackle cyber fraud. Participants were also asked to answer how extensive of an issue they believed cyber fraud to be. While this could be seen as a leading question as it infers that cyber fraud is an issue to some extent, participants were given the option to pick not at all on the Likert scale.

Treatment of Data and Analysis

The data was saved from Qualtrics software to Excel format and imported to SPSS for analyses. Unanswered responses and any responses that stopped after providing age and gender were removed as it offered no value to the research. Descriptive statistics was conducted to describe the characteristics of the sample (Pallant, 2020). As there were 76 responses, the Kolmogorov-Smirnoff test was conducted to assess the normality of the distribution of data (Pallant, 2020). The non-parametric tests chosen were the Chi-square and the Kendall's Tau tests. Chi-square test was chosen to test the relationship between two categorical samples and the Kendall's Tau test was used as the test of association between ordinal variables (Diamantopoulos and Schlegelmilch, 1997). For the qualitative data analysis thematic analysis was used (McKim, 2017), due to its flexibility and usefulness as a research tool as it provides an ample and comprehensive explanation of the data (Braun and Clarke, 2006). Thematic analysis is used in deductive analysis to find direct and latent themes (Clarke and Braun, 2017). The open-ended questions were examined for semantic themes, after identifying the most evident themes the responses were re-examined for any underlying themes. Every re-examination investigated smaller samples which made it easier to find uncommon but likely significant themes and they were coded were necessary (Birchall, Murphey and Milne, 2016). The aim of the results along

with the social learning theory is to help identify if the public's perception of cyber fraud affects their behaviour and actions.

Ethics

Ethical research is important as research with participants cannot be conducted without the university ethics committee approval and so anything that may undermine the research such as any harm that can come to the participants need to be identified (Wright and O'Flynn, 2012). Bogdan and Biklen (1997) found that all researchers can suffer bias, and as it cannot be removed completely due to the possibility of it happening at any point of the research (Pannucci and Wilkins, 2010), acknowledging and taking them into account is one way to deal with it (Bogdan and Biklen, 1997). To reduce bias as much as possible as well as to avoid any risk to the researcher such as trolling, the survey was published on new social media accounts. Anonymity was given protect the privacy of the participants to maintain the integrity and precision of the collection and analysis of the data (Hoft, 2021). Any participant identifiers were avoided, and participants were numbered for use when referring to specific data. Participants were taken to an information sheet at the beginning of the survey. This was done with the aim of gaining informed consent, as participants need to understand the motive, procedure, risks and any benefits of taking part, before deciding whether to take part (Jefford and Moore, 2008). The participants were informed they did not have to participant if they did not want to and that they have the right to withdraw (Jefford and Moore, 2008), however withdrawal was only possible before submission at which after that point it was no longer possible. Ethical approval for this research was given by the Staffordshire University ethics sub-committee.

Results

To achieve the aims and objective this section will examine the primary qualitative and quantitative data collected from the survey.

This subsection will explore the themes and subthemes identified through qualitative data analysis by thematic analysis. An explanation of what each theme represents with supporting quotes for each will also be provided. Thematic analysis of the open ending question from the survey produced three common themes across the participants. These include: 1) a need for education; 2) police action and involvement; and 3) requiring additional resources and training for the police.

Theme 1: Education

This theme explores the participant's response on how they believe the public's knowledge of cyber fraud can be improved and their ability to protect themselves from it. This theme also consists of two subthemes that will be explored.

> "Teaching students when they are younger about it and making the subject more aware." *(P.2)*
>
> "We need more knowledge on this topic...Or being taught it in school… or even when you open a bank account and have access to money they teach you somethings at that point" *(P.5)*
>
> "Have more people come in to inform students about cyber fraud and have workshops on what to do and how to avoid those situations." *(P.7)*

A need for education surrounding the topic of cyber fraud was identified. Several participants touched upon the importance of more awareness, more education and more knowledge. As well as mentioning schools taking on the role of teaching people about cyber fraud, workshops, seminars, institutions and organisations were mentioned.

<u>Subtheme 1: Individual Actions</u>

Some participants expressed the belief that they should take on the responsibility of improving their ability to protect themselves from cyber fraud and their knowledge of cyber fraud themselves.

> "By informing myself of ways I can better protect my personal data and to put them in practice" *(P.21)*

> "I must study much more about it in order for me to be more carefull when I use my personal data, credit cards, etc." *(P.32)*

Some participants expressed a desire to attain knowledge about cyber fraud themselves by independent study, such as searching the internet for relevant sources of information to become more aware. On the topic of protection from cyber fraud some participants responded that they would inform themselves how they can protect their personal data and accounts better and implement those practices.

Subtheme 2: Organisations

Some participants mentioned other ways of spreading information and awareness as well as thoughts of what can be done to protect individuals from cyber fraud.

> "Adverts on the TV, posters around the country, posts on social media" *(P.8)*

> "Google could develop a software which could check if the sender is secure" *(P.18)*

Devices for spreading information and awareness consisted of radios, television programs, adverts, leaflets, social media, and technology for verification were mentioned. The use of television being the main one mentioned.

Theme 2: Police Action and Involvement

This theme explores the participants' response to their thoughts about how they believe the police can improve the way they deal with a cyber fraud incident and how they tackle cyber fraud as a whole.

> "A multiagency approach is needed." *(P.28)*

> "They don't really deal with them at all. Action Fraud take the reports and then very little seems to happen...there actually needs to be more effort to tackle it. Instead, the government choose to exclude online fraud crimes from national crime figures!" *(P.33)*

> "Police don't do much with it, not high on a long list of priorities. Action fraud triages it to collate and package actionable ones. More onus ought to be on financial institutions, requiring or requesting the police to do more is unrealistic and simplistic...it needs tackling at a National level with severed punishments coupled with financial institutions bearing the burden." *(P.67)*

A need for police action and involvement was identified. Some participants expressed their belief that the police do not do enough about cyber fraud. A recurring concept was that the police need to take more action and be more involved in cyber fraud offences. Multiple elements were identified that need to work together to tack cyber fraud, such as financial institutions, multi-agency approach, helplines to support victims, government and the police needing to improve the way they identify and punish offenders.

Theme 3: Resources and Training

This theme explores the participants' belief that the police are in need of more resources and training to deal with cyber fraud more effectively.

> "Become educated on technology and how to deal with these cases" *(P.12)*

> "There needs to be more police training and more resources available for the police to tackle the issue." *(P.28)*

> "More training and investment in resources is required." *(P.70)*

A need for the police to receive further resources and training was identified. Responses included suggestions such as a budget increase, more officers, learning further information about cyber fraud, and to improve how they investigate cyber fraud offences. Furthermore, better technology to deal with offences was proposed, and that police need to become more technologically aware.

This subsection will display the findings collected from the UK public. These findings have been analysed through SPSS using descriptive statistics and inferential statistics. Different variables were tested against each other to determine whether there is a relationship between the variables as well as how strong the relationship is.

Descriptive/Frequency Statistics

Of the 76 participants that answered, 51 were female (67.1%), 23 were male (30.3%), 1 non-binary/third gender (1.3%), and 1 participant preferred not to say (1.3%). The standard deviation was found to be 14.031 and the mean age of participants to be 38.6 years (see Table 1). The oldest participant was 77 and the youngest was 18, giving the range of participants age to be 59 (see Table 2). 17 of the participants had GCSE (Level 1&2) qualification or equivalent (22.4%), 13 had A-level/B-tec (Level 3) qualifications or equivalent (17.1%). The majority had post-graduate Masters (Level 7) qualifications or equivalent (30.3%, n=23) and 20 participants had Undergraduate/foundation (Level 4,5,6) qualifications or equivalent (26.3%). The minority of participant had Higher (PhD) level qualification or equivalent (3.9%, n=3). (See Table 4)

The majority of participants, 77.6% (n=59) were found to have had not been taught any cyber fraud topics in school. In contrast 21.1% (n=16) were taught some cyber fraud topics, and of those the majority had an A-level/Btec (Level 3) (31.3%, n=5) and Undergraduate/foundation (Level 4,5,6) qualifications or equivalent (37.5%, n=6) (see Table 5). Of those that have not been taught any cyber fraud topics, 35 participants (59.3%) believed cyber fraud to be an extensive issue a great deal, 16 participants (21.1%) a lot, 3 participants (5.1%) a little, and 1 participant (1.7%) not at all. In contrast, participants that have been taught cyber fraud topics 6 participants (37.5%) believed cyber fraud to be an extensive issue a great deal, 7 participants (43.75%) a lot, and 1 participant (6.25%) a little. This shows that regardless of participants being taught cyber fraud topics or not, over half of the participants (53.9%, n=41) believe cyber fraud to be an extensive issue a great deal. (See Table 7).

Majority of the participants reported that they would go or call the police or the bank in case of a cyber fraud incident (78.9%, n=60) (see Table 9). When asked to rate their satisfaction with how police deal with cyber fraud incidents and tackle cyber fraud as a whole, the majority of

participants did not know how the police deal with (47.4%, n=27) or tackle cyber fraud (48.7%, n=27) (see Table 10 and 11).

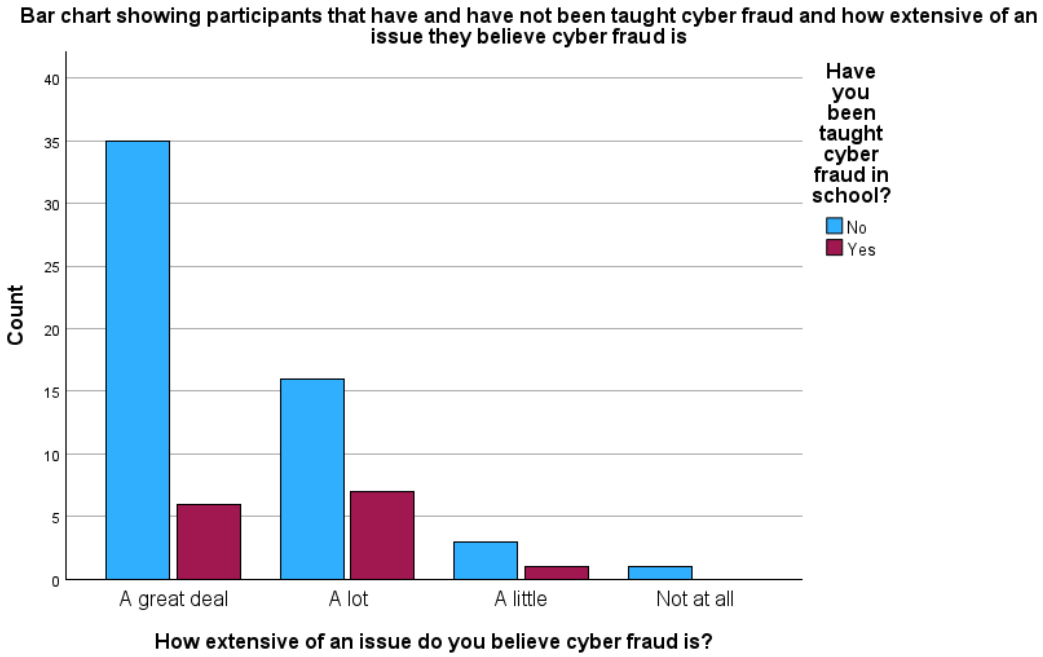


Figure 1. showing participants that have and have not been taught about cyber fraud in school, and how much of an issue they believe cyber fraud to be.

Within the survey participants were asked to select how extensive of an issue they believe cyber fraud to be, this was compared to what they believed their knowledge of cyber fraud to be. Of those that answered both questions (89.5%, n=68), most rated their knowledge as Average (42.6%, n=29). The second highest response was Good (32.4%, n=22), then Poor (17.6%, n=12), and lastly Excellent (7.4%, n=5). From the participants that believed cyber fraud to be an extensive issue a great deal, only 4.4% participants (n=3) rated their knowledge on cyber fraud as Excellent. The majority rated their knowledge as Good (23.5%, n=16), followed by Average knowledge (22.1%, n=15), and lastly Poor knowledge (10.3%, n=7). In contrast, the participants that believed cyber fraud to be an extensive issue a lot (32.4%, n=22), the majority rated their knowledge as Average (54.5%, n=12), then Good knowledge (22.7%, n=5), then Poor knowledge (18.2%, n=4), and lastly Excellent knowledge (4.5%, n=1). (See Table 12)

Inferential Statistics – Demographics

The Kolmogorov-Smirnov test of normality was used, as there were more than 50 responses, (n=76), to determine the normality of the data (Pallant, 2020). Result show significant value P>.001, which means the dataset was not normally distributed. (See Table 14)

1. H0 – There will be no correlation between the participants education level and their opinion of how extensive cyber fraud is of an issue.
H1 – There will be a correlation between the participants education level and their opinion of how extensive cyber fraud is of an issue.

Chi Square was used to test the association of two categorical variables (Pallant, 2020). The test showed a non-significant association was found when looking at the relationship between the participants education level and their opinion of how extensive of an issue cyber fraud is, X^2(16, n=76) = 14.175, p>.05 (see Table 15). Participants with a Masters (Level 7) degree qualifications or equivalent were more likely to believe cyber fraud to be an extensive issue of a great deal (36.6%, n=15) than participant that had A-level, Btec (Level 3) qualifications or equivalent (12.2%, n=5). However, GCSE (Level 1&2) qualification or equivalent were found to believe cyber fraud to be an extensive issue of a great deal (19.5%, n=8) more than then participants that had A-level, Btec (Level 3) qualifications or equivalent (12.2%, n=5) (see Table 16). The significance (2-tailed), p = 0.586, therefore, there is no significant association between the two categories and the null hypothesis that there will be no correlation between the participants education level and their opinion of how extensive cyber fraud is of an issue can be accepted while the alternative hypothesis is rejected.

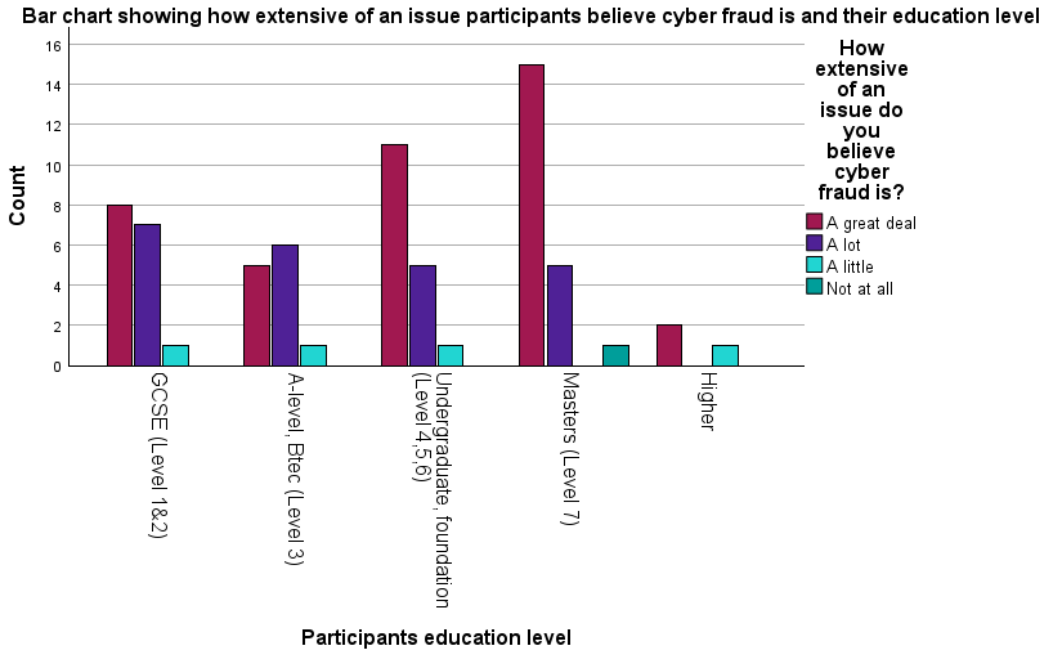


Figure 2. showing how extensive of an issue participant believe cyber fraud is and their education level.

2. H0 – There will be no relationship between the participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud.
H1 – There will be a relationship between the participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud.

Kendall's Tau test was used at the sample size <100 responses, as a measure of association between ordinal data (Diamantopoulos and Schlegelmilch, 1997). The test established there was no significant positive correlation between participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud, τ_b = -.094, p= >0.5 (see Table 17). Therefore, we can accept the null hypothesis as no relationship was identified between the participants opinion of how extensive of an issue cyber fraud is and their knowledge rating of cyber fraud and reject the alternate hypothesis.

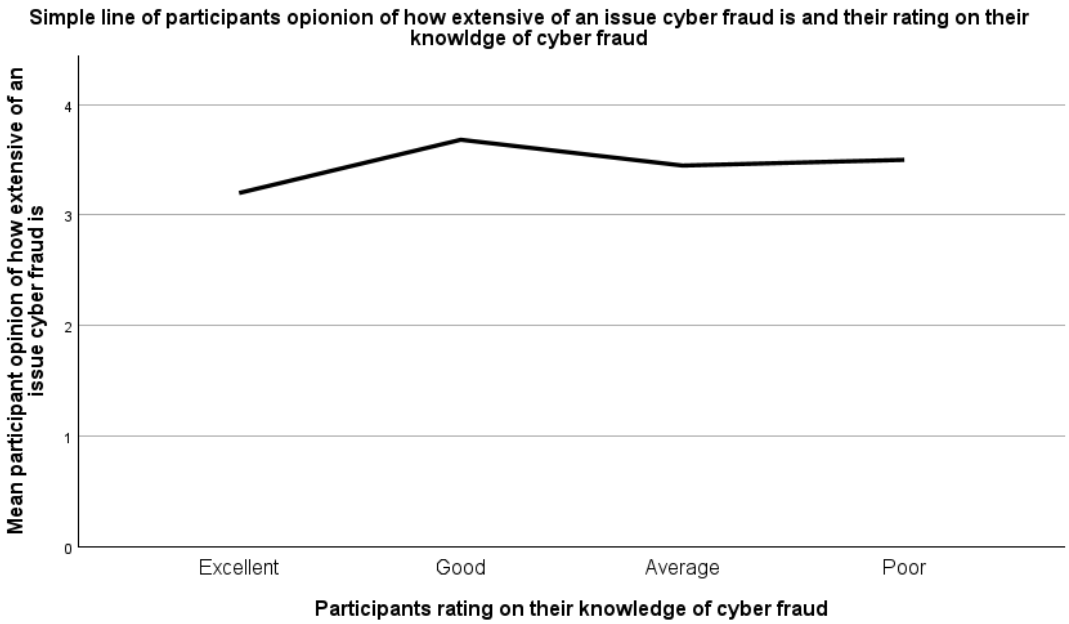


Figure 3. showing how extensive of an issue participants believe cyber fraud is in relation to their knowledge rating of cyber fraud.

3. H0 – There will be no relationship between the participants opinion of how extensive cyber fraud is of an issue and what steps they take to protect themself from cyber fraud.
H1 – There will be a relationship between the participants opinion of how extensive cyber fraud is of an issue and how many steps they take to protect themself from cyber fraud.

Chi Square was used to test the association of two independent categorical variables (Pallant, 2020). The test showed a significant association when looking at the relationship between the participants opinion of how extensive cyber fraud is of an issue, and how many steps they take to protect themself from cyber fraud, X^2(208, n=76) = 276.858, p<.001 (see Table 18). The significance (2-tailed), p = <.001, therefore, there is a significant association between the two categories and the alternative hypothesis, that there will be relationship between the participants opinion of how extensive cyber fraud is of an issue and how many steps they take to protect themself from cyber fraud, can be accepted. Participants were found to take more steps to protect themselves if they believed cyber fraud to be an extensive deal a great deal (59.4%, n=41) and a lot (31.9%, n=22), compared to participant who believed cyber fraud not only be a little (5.8%, n=4) or not at all (1.4%, n=1) an extensive issue (see Table 19).

Discussion

In this section the aim is to attempt to critically discuss the key results from this project, by comparing and analysing the results to the previous research explored in the literature review. Findings in this research found three main themes in the quantitative data collected from the survey. The hypotheses test in the results section will also be examined to decide whether previous research support the hypotheses or if further research is needed. Towards the end of this section, the limitations of this research will be included.

Interpretation of the results identified the overall perception of the participants was that more education to raise awareness of cyber fraud is needed in order to protect themselves from cyber fraud. This is supported by previous research that found that participants lack of knowledge and understanding was a cause for cybercrimes offences to not be reported (Button and Cross, 2017; Akdemir, Sungur and Başaranel, 2020), as well as leaving themselves at risk of becoming victims by failing to follow secure online behaviour (Home Office, 2018). Research into cyber security from other countries have also identified a need for education to improve cyber fraud awareness and therefore online safety (Bele *et al*., 2014; Cross, Richards and Smith, 2016; Button and Cross, 2017; Witsenboer, Sijtsma and Scheele, 2022). Preventive techniques that have been successfully implemented are important in order to be able to address the issue of cybercrimes (Bele *et al*., 2014). While this research focused on the UK public, global literature can also be taken into consideration as Grimes (2021) found that most people approach online security in similar ways, with a main difference being that culturally one country may put different levels of importance on online security compared to others. But as cybercrimes have become a greater threat, research has found that international and national bodies have increased their efforts in online security and cybercrimes (Akdemir, Sungur and Başaranel, 2020).

The majority of participants had not been taught any cyber fraud related topics and were identified to take precautions to keep themselves safe from cyber fraud. This implies that education into prevention is not necessary as participant are found to take preventative measures. This contradicts previous research, that has found that education is important in terms of prevention and reduction of cybercrimes (Bele *et al*., 2014; Cross, Richards and Smith, 2016; Button and Cross, 2017). A subtheme identified that some participants were willing to put in the

work themselves to improve their awareness and knowledge of cyber fraud which can be argued supports the findings that participants knew preventative steps to keep themselves safe from cyber fraud even though they have not been taught in school. Further, interpretation of the qualitative results implied that participants still believed that greater education into cyber fraud is important, whether it be given from schools, independent studies or by different organisations. These findings are supported by Witsenboer, Sijtsma and Scheele (2022) who recommend that elementary schools should start teaching students how to be safe on the internet with a focus on phishing. Sağlam, Miller and Franqueira (2023) believe that by providing education in cyber security, with the help of government resources, pupils will become aware and conscious of their safety online and will then pass on the teachings to the next generation. This is supported by Witsenboer, Sijtsma and Scheele (2022) who found that students learn online behaviour from their parents and siblings. In contrast Bidgoli, Knijnenburg and Grossklags (2016) found that undergraduate student's knowledge of cybercrimes came from social media and people that have been victims of cybercrimes instead.

Early education in managing risk of cyber fraud to help vulnerable groups, has been suggested to be done by associates and the third sector rather than the police and reading from websites (Levi *et al*., 2017). Illustrated by the results, subtheme of participants suggesting ways to spread information and awareness about cyber fraud was identified, with examples ranging from television programs to social media to leaflets. These findings are supported by Correia (2019) who also mentioned third sector organisations such as Victim Support to lead in helping reduce victims from being re-victimised and address the impact cyber fraud offences has had on victims. Ionescu, Mirea and Blăjan (2011) concluded that managing cyber fraud risk can only be done with the ongoing commitment of organisations being involved, collecting information and skills to deal with cyber fraud, which requires training.

Furthermore, participants conveyed their feelings regarding their perception of what the police can do to improve as many implied the police were not doing enough concerning cyber fraud and that more involvement is required. These findings contradict research by Brooks and Button (2011) who found that police officers are not entirely indifferent to cyber fraud, however it does need to be noted that this research was conducted thirteen years ago making it not as relevant now. More relevant, is research by Curtis and Oxburgh (2023) that supports these findings as it

affirms that the perception that police officers are not prepared to deal with cybercrimes as research has found that police officers that did not receive some cybercrime training felt less confident and prepared to deal with such offences (Bossler *et al.*, 2020).
This is visible by the findings as it was found that participants believe that for police to improve regarding cyber fraud, police should overall receive more resources and training. This is supported by previous research (Holt, Bossler and Fitzgerald, 2010; Brooks and Button, 2011; Cross and Blackshaw, 2015; Levi *et al.*, 2017) that found that police lack the resources and training to deal with cyber fraud incidents and due to this police struggle to meet the public expectations (Levi *et al.*, 2017). In addition, Levi *et al.*, (2017) found that the police perception that they lacked intelligence on rising cyber threats that they need so that they could act, also contributed to the matter.

Bidgoli, Knijnenburg and Grossklags (2016) also found limited literature on the relationship between education and perceptions. Nevertheless, quantitative results found that there was no correlation between the participants education level and their perception of how extensive of an issue cyber fraud is. In addition, over half of the participants reported that they would go or call the police, or the bank, or both in the case of a cyber fraud incident, with their education level and perception of cyber fraud seeming to have no effect on their decision. These findings are consistent with research by Van de Weijer, Leukfeldt and Bernasco (2019) that also found mixed results in terms of education level and reporting the offence, finding no significant association with various types of offences. Results showed the majority would report the cyber fraud incident, these findings contradict research by Van de Weijer, Leukfeldt and Bernasco (2019) who found that older victims were more likely to report incidents to the police. Previous research identified that cyber fraud victims will report the incident to their bank which means that the incident would not be recorded as a crime and therefore be omitted from the overall statistics of cyber fraud data (Wall, 2008; Correia, 2022). Bidgoli, Knijnenburg and Grossklags (2016) found that past victimizations seemed to decrease the likelihood of participants reporting offences of cybercrimes. Although, Correia (2019) identified that the introduction of Action Fraud made it easier for victims to report offences. However, despite this, Bidgoli, Knijnenburg and Grossklags, (2016) noted that the findings may be due to participants not knowing how to report cybercrime incidents and Correia (2019; 2022) proposed that a reason for not reporting incidents

to Action Fraud may have been due to lack of awareness of the organisation. In support of this quantitative results showed a very small minority of participants that mentioned they would report to Action Fraud in case of a cyber fraud incident.

No relationship was found between the participants perception of how extensive of an issue cyber fraud is and how they would rate their knowledge of cyber fraud as, implying that regardless of what their knowledge of cyber fraud is, they believe that cyber fraud is an extensive issue. This is supported by the fact that the majority of the participants believed cyber fraud to be an extensive issue a great deal or a lot. These findings contradict the myths identified by the Home Office (2018) where the public believe cybercrimes to not be real crimes and therefore, that they do not need to be worried about them. Additionally, previous research found that student's knowledge influenced their perceptions regarding cybercrimes which in turn affected their behaviour regarding reporting such offences and preventative steps (Bidgoli, Knijnenburg and Grossklags, 2016). The Home Office (2018) found that due to conflicting advice by experts on cyber security, participants do not take on any safety or preventative measures as they perceive it to be pointless if experts cannot come to a conclusion on how to keep safe online either.

Qualitative results identified a relationship between participants perception of how extensive cyber fraud is of an issue and how many steps they take to protect themselves from cyber fraud, showing that participant who perceived cyber fraud to be an extensive issue took more steps to protect themselves from cyber fraud. Previous research recognised a gap in literature regarding preventative measures (Bidgoli, Knijnenburg and Grossklags, 2016). A study by Marcum Higgins and Ricketts (2010) found that following preventative measure did not increase cyber security, as well as findings that suggest that those that implement cyber security measure are more susceptible to take part in risky behaviours (Christin *et al*., 2012). These findings are supported by the Home Office (2018) who identified that research suggests that people debate if the perceived risk of taking an action outweighs the risk of ignoring the protective measures, they abide by to take the action that achieves what they want.

Interpretations of the results highlights the overall participant perception of cyber fraud to be that it is a great issue, and findings identified that preventative measures are being taken. Similarly linking to the research question, results show that overall participant still believe that further education and involvement by the police, agencies, and other organisations are required concerning cyber fraud.

Limitations

During the research, some limitations were identified that could have affected the study. Firstly, a limitation was of this research was that although it used mixed methods and there were sections where participants could make comments, four of the qualitative questions relied on the answer to the previous question meaning that the questions would only appeared if participants answered that they have been taught cyber fraud topics or if they were dissatisfied or extremely dissatisfied, in order for them to expand on their answers. This meant that some participants did not give as detailed responses as others. For the interpretation of the results to be relevant and beneficial it is essential that participants give enough information (Bachiochi and Weiner, 2004). Another limitation identified is that there were more qualitative questions that might have been beneficial to ask, such as what their beliefs are regarding why cyber fraud may not be reported, to get a deeper understanding of participant perceptions.

Another limitation could have been the non-probability sampling method, as this method has been found to have the possibility of limiting the generalisability of the data (Gobo, 2008). The sample size was smaller than what was wanted, as research found that the size of the sample must be a representative of the population under consideration (Boddy, 2016), which in this case is the UK population. This may have been due to the short time the survey was available, due to the time frame for the research, to the public which could have affected the size of the sample as Patton (2002) found that sample size depends on time and resources.

Conclusion

The overall aim of this research was to get an understanding of the UK public perceptions of cyber fraud. This was done through the collection of primary data with the use of a survey posted on social media platforms. The data collected helped give an overview of what the public perception and knowledge of cyber fraud is, if they take any measures against cyber fraud, and what they believe the police are doing to deal with and tackle cyber fraud. This research aimed to add to previous literature regarding cyber fraud, while there is research done into police officers' perception of cyber fraud and victims of cyber fraud. A limited amount of literature was identified to focus on the general UK public and due to this, this research included global literature and research to compare against the findings of this research.

This research has contributed to the existing literature of cyber fraud by exploring in more depth the public perceptions regarding cyber fraud. It has investigated education levels, knowledge and opinions on how the police deal with and tackle cyber fraud. This research uncovered the perception of the public to be that further education of cyber fraud is desired and that more involvement by police, agencies and other organisations are required. Findings were in line with previous literature that also identified a need for more education involving cyber fraud and that the police need more resources and training to better respond to cyber fraud and cybercrimes in general. However, results recognised that most people would report a cyber fraud incident to the police. This differs from other studies that identified issues of under-reporting (Correia, 2019; 2022; Ma and McKinnon, 2021); however, this may be due to the small sample analysed in this research, as well as the fact that people's actions and answers may differ from a hypothetical situation and if they are in such a situation or were in the past. These findings imply the relevancy of social learning and routine activities theories to cyber fraud as it may explain why people are at risk of becoming victims of cyber fraud and what factors affect the likelihood of falling victim to cyber fraud.

In practice, findings indicate the need for multiple agencies and organisations to work together to tackle the issue of cyber fraud and cybercrimes overall. Research proposes a need for government agencies to produce educational curriculums or workshops as an early intervention strategy to improve the public's knowledge of cybercrimes in hopes that the learned behaviour

results in avoidance in partaking in risky behaviour online (Sağlam, Miller and Franqueira, 2023). Increased engagement between the police agencies, public, and victims may help improve the current negativity surrounding victimisation and the unrealistic expectations that are placed on the police (Cross, 2018).

Overall, the primary aim of the research was to determine the UK public perception of cyber fraud, and this was achieved. Based on the results, the research found that the public believed cyber fraud to be a vast issue that requires a multi-agency approach with involvement of organisation to attempt to tackle cyber fraud and minimise the risks. The research also highlighted police involvement in cyber fraud investigations. Enforcing the importance of the police following the national fraud strategy, which can be summed up to; pursuing the offenders by prosecution and interference, preparing to reduce the impact of the offence, be prepared to protect individuals and groups from being victimised and prevent individuals from participating in crime (Correia, 2019; Secretary of State for the Home Department, 2023). The main issue identified was that the public lacked enough knowledge and awareness of cyber fraud and the risks associated, which may be due to its absence in education, main figures of crime, as well as any misinformation in the media that can wrongly influence the public perceptions. Overall concluding that the UK public perception is that cyber fraud is an extensive issue, and that agencies and organisations need to take more action regarding cyber fraud.

Recommendations

As a result of the findings, the researcher suggests the following recommendations.
This research identified that the public do not know much about how the police deal with and tackle cyber fraud, which may impact the likelihood of victims reporting to the police especially if they believe there is no point as it will not be taken seriously due to it being a cyber fraud offence. While it may be argued it is understandable if individuals that were never victims of cyber fraud do not know police procedures, it can be argued that it is an important factor as it can influence the decisions of people when and if they become victims of cyber fraud. In terms of victims, this can be addressed by police officers following the victims' code for policing that covers how victims should be treated and the responsibility of making sure victims understand what is happening and what will happen next, as well as being kept up to date with the

investigation (College of Policing, 2021). In terms of the public, it may be useful to have seminars with experts or influential people raising awareness of cyber fraud in a way that is easy for the public to understand. Regarding this aspect, further research needs to be conducted to conclude on how to keep safe online as the Home Office (2018) identified that people get confused due to the conflicting advice online and not knowing which are credible sources.

References

Action Fraud (2023a) *What is fraud and cyber crime?* Available at: https://www.actionfraud.police.uk/what-is-fraud (Accessed: 17 June 2023)

Action Fraud (2023b) *A-Z Fraud.* Available at: https://www.actionfraud.police.uk/a-z-of-fraud-category/ (Accessed: 17 June 2023)

Action Fraud (2023c) *Call centre fraud*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/call-centre-fraud (Accessed: 10 October 2023)

Action Fraud (2023d) *Domain name scams*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/domain-name-scams (Accessed: 10 October 2023)

Action Fraud (2023e) *Facility takeover*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/facility-takeover (Accessed: 10 October 2023)

Action Fraud (2023f) *Account takeover*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/account-takeover (Accessed: 10 October 2023)

Action Fraud (2023g) *Internet dialler scams*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/internet-dialler-scam (Accessed: 10 October 2023)

Action Fraud (2023h) *Invoice scams*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/invoice-scams (Accessed: 10 October 2023)

Action Fraud (2023i) *Malware and computer virus*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/malware (Accessed: 10 October 2023)

Action Fraud (2023j) *Mailbox and multiple post re-directions*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/mail-boxes-and-multiple-post-redirections (Accessed: 10 October 2023

Action Fraud (2023k) *Remote access tool scams*. Available at: https://www.actionfraud.police.uk/a-z-of-fraud/remoteaccesstoolscams (Accessed: 10 October 2023)

Ajayi, V.O. (2017) *Primary sources of data and secondary sources of data*. PhD thesis. Benue State University. Available at: https://www.researchgate.net/publication/320010397_Primary_Sources_of_Data_and_Secondary_Sources_of_Data (Accessed: 14 December 2023)

Akdemir, N., Sungur, B. and Başaranel, B. (2020) 'Examining the Challenges of Policing Economic Cybercrime in the UK', *Güvenlik Bilimleri Dergisi,* International Security Congress Special Issue, pp. 113-134. Available at: https://doi.org/10.28956/gbd.695956

Bachiochi, P.D. and Weiner, S.P. (2004) 'Qualitative data collection and analysis', in S.G. Rogelberg (eds) *Handbook of research methods in industrial and organizational psychology*. Oxford: Blackwell Publishing, pp. 161-183.

Bandura, A. (1977) *Social learning theory*. New York City, NY: General Learning Press.

Barroga, E. *et al.* (2023) 'Conducting and Writing Quantitative and Qualitative Research', *Journal of Korean medical science,* 38(37), pp. e291–e291. Available at: https://doi.org/10.3346/jkms.2023.38.e291.

Beals, M., DeLiema, M. and Deevy, M. (2015) *Framework for a taxonomy of fraud.* Stanford Center on Longevity, Financial Fraud Research Center. Available at: https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf (Accessed: 16 September 2023)

Bele, J.L. *et al.* (2014) 'Blended Learning as a Strategic Method Against the Illegal Use of Internet' *10th International conference: mobile learning*, Madrid (Spain), 28 February - 2 March, pp. 281-284. Available at: https://files.eric.ed.gov/fulltext/ED557171.pdf#page=304 (Accessed: 2 October 2023)

Bidgoli, M., Knijnenburg, B.P. and Grossklags, J. (2016) 'When cybercrimes strike undergraduates.' *APWG Symposium on Electronic Crime Research (eCrime),* Toronto (Canada): IEEE, 1-3 June, pp. 1-10. Available at: https://doi.org/10.1109/ECRIME.2016.7487948

Birchall, S., Murphy, M. and Milne, M. (2016) "Mixed Methods Research: A Comprehensive Approach for Study into the New Zealand Voluntary Carbon Market," *Qualitative report*, pp. 1351-1365. Available at: https://doi.org/10.46743/2160-3715/2016.2398

Boas, T.C, Christenson, D.P., and Glick, D.M. (2018) 'Recruiting large online samples in the United States and India: Facebook, Mechanical Turk, and Qualtrics', *Political Science Research and Methods,* 8(2), pp. 232-250. Available at: https://doi.org/10.1017/psrm.2018.28

Boddy, C.R. (2016) 'Sample size for qualitative research', *Qualitative market research: An international journal,* 19(4), pp. 426-432. Available at: https://doi.org/10.1108/QMR-06-2016-0053

Bogdan, R. and Biklen, S.K. (1997) *Qualitative research for education*. Boston, MA: Allyn & Bacon.

Bossler, A.M. *et al*. (2020) 'Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness', *Security journal,* 33(2), pp. 311–328. Available at: https://doi.org/10.1057/s41284-019-00187-5

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative research in psychology,* 3(2), pp.77-101. Available at: https://doi.org/10.1191/1478088706qp063oa

Brenner, S.W. (2007) 'History of computer crime', in K.D. Leeuw and J. Bergstra (eds) *The History of Information Security: A Comprehensive Handbook.* Elsevier Science BV, pp. 705-721. Available at: https://doi.org/10.1016/B978-0444451608-4/50026-2

Bridgeman, B. (1992) 'A Comparison of Quantitative Questions in Open-Ended and Multiple-Choice Formats', *Journal of Education Measurements,* 29(3), pp. 253-271. Available at: https://doi.org/10.1111/j.1745-3984.1992.tb00377.x.

Brooks, G. and Button, M. (2011) 'The police and fraud investigation and the case for a nationalised solution in the United Kingdom', *The Police Journal*, 84(4), pp. 305-319. Available at: https://www.doi.org/10.1358/pojo.2011.84.4.559

Button, M., Lewis, C., Tapley, J. (2009a) *A better deal for fraud victims: research into victims' needs and experiences*. London: National Fraud Authority. Available at: https://pure.port.ac.uk/ws/portalfiles/portal/1924328/NFA_Report_1_15.12.09.pdf (Accessed: 23 September 2023)

Button, M., Lewis, C. and Tapley, J. (2009b) *Fraud typologies and the victims of fraud: Literature review.* London: National Fraud Authority. Available at:

https://pure.port.ac.uk/ws/portalfiles/portal/1926122/NFA_report3_16.12.09.pdf (Accessed: 23 September 2023)

Button, M., Lewis, C., Tapley, J. (2012) 'The 'fraud justice network' and the infrastructure of support for the individual fraud victims in England and Wales', *Criminology and Criminal Justice*, 13, pp. 37-61. Available at: https://doi.org/10.1177/1748895812448085

Button, M., Lewis, C. and Tapley, J. (2014) 'Not a victimless crime: The impact of fraud on individual victims and their families.', *Security Journal*, 27, pp. 36–54. Available at: https://doi.org/10.1057/sj.2012.11

Button, M. and Cross, C. (2017) *Cyber Frauds, Scams, and their Victims*. Oxford: Routledge.

Christin, N. *et al.* (2012) 'It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice', (from 15th International Conference on Financial Cryptography and Data Security, Gros Islet, St. Lucia, 28 February - 4 March 2011), *Financial Cryptography and Data Security*, Revised Selected Papers 15, pp. 16-30. Available at: https://doi.org/10.1007/978-3-642-27576-0_2

Clarke, V. and Braun, V. (2017) 'Thematic analysis', *The journal of positive psychology*, 12(3), pp. 297-298. Available at: https://doi.org/10.1080/17439760.2016.1262613

Cohen, L.E. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', *American Sociological Review, 44(4),* pp. 588-608. Available at: https://doi.org/10.2307/2094589

College of Policing (2018) *Strategic Planning.* Available at: https://www.college.police.uk/app/operations/operational-planning/strategic-planning (Accessed: 6 March 2024)

College of Policing (2021) *Victims' Code of Practice*. Available at: https://www.college.police.uk/guidance/victims-code/victims-rights-policing (Accessed: 6 March 2024)

Computer Misuse Act 1990, c. 18. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed: 8 January 2024)

Correia, S.G. (2019) ‘Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales’, *Crime Science*, 8, pp. 1-12. Available at: https://doi.org/10.1186/s40163-019-0099-7

Correia, S.G. (2022) ‘Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud’, *International journal of population data science*, 7, pp. 1721–1721. Available at: https://doi.org/10.23889/ijpds.v7i1.1721

Cross, C. (2013) 'Nobody's holding a gun to your head...': Examining current discourses surrounding victims of online fraud’, in J. Tauri and K. Richards (eds) *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*. Crime and Justice Research Centre: Queensland University of Technology, pp. 25-32.

Cross, C. (2015) ‘No laughing matter: Blaming the victim of online fraud’, *International Review of Victimology*, 21(2), pp. 187-204. Available at: https://doi.org/10.1177/0269758015571471

Cross, C. and Blackshaw, D. (2015) ‘Improving the police response to online fraud’, *Policing: A Journal of Policy and Practice*, 9(2), pp. 119-128. Available at: https://doi.org/10.1093/police/pau044

Cross, C., Richards, K. and Smith, R. (2016) *Improving responses to online fraud victims: An examination of reporting and support*. Final report for Criminology Research Grant, 29/13-14. Available at: https://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf (Accessed: 22 January 2024)

Cross, C. (2018) ‘Expectations vs reality: Responding to online fraud across the fraud justice network’, *International Journal of Law, Crime and Justice*, 55, pp. 1-12. Available at: https://doi.org/10.1016/j.ijlcj.2018.08.001

Crown Prosecution Service (2019) *Cybercrime – prosecution guidance.* Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (Accessed: 8 November 2023)

Curtis, J. and Oxburgh, G. (2023) ‘Understanding cybercrime in ‘real world’ policing and law enforcement’, *The Police Journal: Theory, Practice and Principles*, 96(4), pp. 1-20. Available at: https://doi.org/10.1177/0032258X221107584

Diamantopoulos, A. and Schlegelmilch, B.B. (1997) *Taking the Fear Out of Data Analysis.* London: The Dryden Press

Drew, J. and Cross, C. (2013) 'Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes', *Journal of Financial Services Marketing,* 18(3), pp. 188-198. Available at: https://eprints.qut.edu.au/220321/8/66444.pdf (Accessed: 22 January 2024)

Dupont, B. and Whelan, C. (2021) 'Enhancing relationships between criminology and cybersecurity', *Journal of criminology*, 54, pp.76-92. Available at: https://doi.org/10.1177/00048658211003925

Education & Skills Funding Agency (2023) *Cyber crime and cyber security: a guide for education providers.* Available at: https://www.gov.uk/government/publications/indicators-of-potential-fraud-learning-institutions/guide-on-cyber-crime-and-cyber-security-for-education-providers (Accessed: 7 November 2023)

Fife-Schaw, C. (2020) 'Questionnaire Design', in G.M. Breakwell, D.B Wright and J. Barnett (eds) *Research Methods in Psychology.* London: Sage Publications, pp. 344-365

Fraud Act 2006, c. 35. Available at: https://www.legislation.gov.uk/ukpga/2006/35/section/2 (Accessed: 28 January 2024)

Gobo, G. (2008) 'Re-conceptualizing generalization: Old issues in a new frame', in P. Alasuutari, L. Bickman and J. Brannen (eds) *The Sage handbook of social research methods*. London: Sage Publications, pp. 193-213.

Goodman, M. (2015) *Future Crimes.* New York: Doubleday

Gordon, S. and Ford, R. (2006) 'On the definition and classification of cybercrime', *Journal in computer virology*, 2, pp. 13-20. Available at: https://www.doi.org/10.1007/hofts11416-006-0015-z

Grabosky, P and Smith, R. (2001) 'Telecommunication fraud in the digital age', in D. Wall (eds) *Crime and the Internet.* London: Routledge, pp. 29-43.

Grimes, R.A. (2021) *Security Approaches Around the Globe.* Available at: https://www.knowbe4.com/hubfs/Security-Habits-2021.pdf (Accessed: 16 November 2023)

Hernandez-Castro, J. and Boiten, E. (2014) 'Cybercrime prevalence and impact in the UK', *Computer fraud & security*, 2014(2), pp. 5–8. Available at: https://doi.org/10.1016/S1361-3723(14)70461-0.

Hoft, J. (2021) 'Anonymity and confidentiality', in J.C. Barnes and D.R. Forde (eds) *The Encyclopedia of Research Methods in Criminology and Criminal Justice*. Hoboken, NJ: John Wiley & Sons, pp. 223-227.

Holt, T.J., Bossler, A.M. and Fitzgerald, S. (2010) 'Examining state and local law enforcement perceptions of computer crime', in T. Holt (eds) *Crime on-line: Correlates, causes, and context.* Raleigh, NC: Carolina Academic, pp. 221-246.

Holton, E.F. and Burnett, M.F. (2005) 'The basics of quantitative research', in R.A. Swanson and E.F. Holton (eds) *Research in organizations: Foundations and methods of inquiry*. Oakland, CA: Berrett Koehler Publishers, pp. 29-44.

Home Office (2013) *Cyber crime: A review of the evidence.* 75. Available at: https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf (Accessed: 8 November 2023)

Home Office (2018) *A call to action: the cyber aware perception gap*. Available at: https://www.gov.uk/government/publications/cyber-aware-perception-gap-report (Accessed: 15 May 2023)

Howard, R. (2009) *Cyber Fraud: Tactics, Techniques and Procedures.* London: CRC Press Taylor & Francis Group

Hurmerinta-Peltomäki, L. and Nummela, N. (2006) 'Mixed methods in international business research: A value-added perspective', *Management International Review*, 46(4), pp. 439-459. Available at: https://doi.org/10.1007/s11575-006-0100-z

Ionescu, L., Mirea, V. and Blăjan, A. (2011) 'Fraud, corruption and cyber crime in a global digital network', *Economics, Management and Financial Markets*, 6(2), p. 373-380. Available

at: https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=e02ca6a4-d4c8-4b03-b0b7-6557c0ccc393%40redis (Accessed: 27 November 2023)

Jahankhani, H., Al-Nemrat, A. and Hosseinian-Far, A. (2014) 'Cybercrime classification and characteristics', in A. Staniforth, B. Akhgar an F. Bosco (eds) *Cyber crime and cyber terrorism investigator's handbook.* Waltham, MA: Elsevier Science, pp. 149-164.

Jefford, M. and Moore, R. (2008) 'Improvement of informed consent and the quality of consent documents', *The lancet oncology*, *9*(5), pp. 485-493. Available at: https://doi.org/10.1016/S1470-2045(08)70128-1

Jordan, T. (2017) 'A genealogy of hacking', *Convergence: The International Journal of Research into New Media Technologies*, 23(5), pp. 528-544. Available at: https://doi.org/10.1177/1354856516640710

Kemp *et al*. (2021) 'Empty Streets, Busy Internet: A Time-series Analysis of Cybercrime and Fraud Trends During COVID-19', *Journal of Contemporary Criminal Justice,* 37(4), pp. 480-501. Available at: https://doi.org/10.1177/10439862211027986

Krishna, R., Maithreyi, R. and Surapaneni, K.M. (2010) 'Research bias: a review for medical students', *Journal of Clinical Diagnostic Research*, 4(2), pp.2320-2324. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cda74cab25cfb58b0927ee926afc25997c4519a7 (Accessed: 12 February 2024)

Kumar, S. (2022) 'AN ANALYSIS OF PHREAKING AS A SIGHT OF CYBERCRIME', *International Research Journal of Modernization in Engineering Technology and Science*, 4(5), pp. 2472-2477. Available at: https://www.irjmets.com/uploadedfiles/paper/issue_5_may_2022/22616/final/fin_irjmets1652855937.pdf (Accessed: 1 February 2023)

Lee, J.R. *et al*. (2021) 'Examining English and Welsh detectives' views of online crime', *International Criminal Justice Review*, 31(1), pp. 20-39. Available at: https://doi.org/10.1177/1057567719846224

Levi, M. *et al*. (2017) 'Cyberfraud and the implications for effective risk-based responses: themes from UK research'. *Crime, Law and Social Change*, 67, pp. 77-96. Available at: https://doi.org/10.1007/s10611-016-9648-0

Ma, K.W.F. and McKinnon, T. (2021) 'COVID-19 and cyber fraud: Emerging threats during the pandemic', *Journal of Financial Crime*, 29(2), pp. 433-446. Available at: https://doi.org/10.1108/JFC-01-2021-0016

Marcum, C.D., Higgins, G.E. and Ricketts, M.L. (2010) 'Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory', *Deviant Behavior*, 31(5), pp.381-410. Available at: https://doi.org/10.1080/01639620903004903

Metropolitan Police (2024) *Cyber Crime.* Available at: https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/ (Accessed: 25 February 2024)

McKim, C.A. (2017) 'The value of mixed methods research: A mixed methods study', *Journal of mixed methods research*, 11(2), pp. 202-222. Available at: https://doi.org/10.1177/1558689815607096

National Audit Office (2015) *A Short Guide to the Home Office*. Available at: https://www.nao.org.uk/wp-content/uploads/2015/07/Home-Office-Short-Guide1.pdf (Accessed: 8 March 2024)

National Crime Agency (2020) *National Strategic Assessment of Serious and Organised Crime.* Available at: https://nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file (Accessed: 8 November 2023)

McKim, C.A. (2017) 'The value of mixed methods research: A mixed methods study', *Journal of mixed methods research*, 11(2), pp. 202-222. Available at: https://doi.org/10.1177/1558689815607096

Nikolovska, M., Johnson, S. D. and Ekblom, P. (2020) '"Show this thread": Policing, disruption and mobilisation through Twitter. An analysis of UK law enforcement tweeting practices during the Covid-19 pandemic', *Crime Science*, 9, pp. 1-16. Available at: https://doi.org/10.1186/s40163-020-00129-2

Office for National Statistics (2016) *Overview of fraud statistics: year ending Mar 2016.* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016 (Accessed 2 February 2024).

Office for National Statistics (2022) *Nature of fraud and computer misuse in England and Wales: year ending March 2022*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 (Accessed: 1 February 2024).

Oksanen, A. and Keipi, T. (2013) 'Young people as victims of crime on the internet: A population-based study in Finland', *Vulnerable children and youth studies, 8*(4), pp. 298-309. Available at: https://doi.org/10.1080/17450128.2012.752119

Pallant, J. (2020) *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. London: Routledge.

Pannucci, C.J. and Wilkins, E.G. (2010) 'Identifying and avoiding bias in research.', *Plastic and reconstructive surgery,* 126(2), pp. 619-625. Available at: https://doi.org/10.1097/PRS.0b013e3181de24bc

Pannu, M. *et al.* (2016) 'Exploring proxy detection methodology', *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. Conference in Vancouver (Canada), 12-14 June. New Jersey: Institute of Electrical and Electronics Engineers, pp. 1-6. Available at: https://doi.org/10.1109/ICCCF.2016.7740438

Parker, C., Scott, S. and Geddes, A. (2019) 'Snowball sampling', in P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug and R.A Williams (ed) *SAGE Research Methods Foundations*. London: SAGE Publications Ltd. Available at: https://doi.org/10.4135/9781526421036831710

Patton, M.Q. (2002) *Qualitative research & evaluation methods*. London: Sage publications.

Pettit, J. (2023) 'Social Engineering: Definition & 6 Attack Types', *Tripwire blog*, 1 March. Available at: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-

for#:~:text=CEO%20fraud%20is%20also%20known,type%20of%20spear%2Dphishing%20attack (Accessed: 10 October 2023)

Ralph, L. *et al*. (2022) 'Maintaining police-citizen relations on social media during the COVID-19 pandemic', *Policing and Society*, 32(6), pp. 764-777. Available at: https://doi.org/10.1080/10439463.2022.2091565

Richards, D. *et al.* (2010) 'What is CyberCrime?', *Dan Richards*, 21 May. Available at: https://www.danmrichards.com/blog/2010/05/21/what-is-cybercrime/ (Accessed: 1 February 2024).

Riek, M., Böhme, R. and Moore, T. (2015) 'Measuring the influence of perceived cybercrime risk on online service avoidance', *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261-273. Available at: https://doi.org/10.1109/TDSC.20152410795

Roopa, S. and Rani, M.S. (2012) 'Questionnaire designing for a survey', *Journal of Indian Orthodontic Society*, 46(4), pp. 273-277. Available at: https://doi.org/10.5005/jp-journals-10021-1104.

Sağlam, R.B., Miller, V. and Franqueira, V.N. (2023) 'A Systematic Literature Review on Cyber Security Education for Children', *IEEE Transactions on Education*, 66(3), pp. 274-286. Available at: https://doi.org/10.1109/TE.2022.3231019

Schjolberg, S. (2014) *The History of Cybercrime: 1976-2014.* Norderstedt: BoD – Books on Demand.

Schreuders, C.Z. *et al.* (2020) 'Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force', *International journal of cyber criminology*, 14(1), pp. 316-340. Available at: https://doi.org/10.5281/zenodo.3757271.

Secretary of State for the Home Department (2023) *Fraud Strategy: Stopping Scams and Protecting the Public* (Cmnd. 839). Available at: https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf (Accessed: 6 March 2024)

Sims, C. M. (2019) *Survey Distribution Methods—The Pros and Cons of Using Social Media, Professional Organizations, and Email Distribution List: A Case Study of Leadership Research*

on Small Business Owners and Their Direct Reports. London: Sage Publications, Inc. Available at: https://doi.org/10.4135/9781526478702

Swedberg, R. (2020) 'Exploratory Research', in C. Elman, J. Gerring and J. Mahoney (eds) *The Production of Knowledge: Enhancing Progress in Social Science*. United Kingdom: Cambridge University Press, pp. 17-41.

Tyagi, A.K. and Aghila, G. (2011) 'A wide scale survey on botnet', *International Journal of Computer Applications*, 34(9), pp. 9-22. Available at: DOI:10.5120/4126-5948

Van de Weijer, S.G., Leukfeldt, R. and Bernasco, W. (2019) 'Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking', *European Journal of Criminology*, 16(4), pp.486-508. Available at: https://doi.org/10.1177/1477370818773610

Wall, D. (2001) 'Maintaining Order and Law on the Internet', in D. Wall (eds), *Crime and the Internet.* London: Routledge, pp. 167-183.

Wall, D. (2007) *Cybercrime: The transformation of crime in the information age*. Vol 4. Cambridge: Polity Press.

Wall, D.S. (2008) 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime', *International Review of Law, Computers & Technology*, 22(1-2), pp. 45-63. Available at: https://doi.org/10.1080/13600860801924907

Wilbur, K.C. and Zhu, Y., 2009. Click fraud. *Marketing Science*, 28(2), pp. 293-308. Available at: https://jstor.org/stable/23884264 (Accessed: 10 October 2023)

Witsenboer, J.W.A., Sijtsma, K. and Scheele, F. (2022) 'Measuring cyber secure behavior of elementary and high school students in the Netherlands', *Computers & Education*, 186, p.104536. Available at: https://doi.org/10.1016/j.compedu.2022.104536

Wright, J. and O'Flynn, G. (2012) 'Conducting ethical research', in K. Amour and D. Macdonald (eds) *Research methods in physical education and youth sport*. London: Routledge, pp. 66-78.

Yar, M. (2006) *Cybercrime and society.* London: SAGE.

Yun, G.W. and Trumbo, C.W. (2000) 'Comparative response to a survey executed by post, e-mail, & web form', *Journal of computer-mediated communication*, 6, p. JCMC613. Available at: https://doi.org/10.1111/j.1083-6101.2000.tb00112.x

Appendices

Appendix A

Glossary

Advance free fraud	Advance free fraud is when payments are made, on the promise of employment, wealth or gifts, to fraudsters that claim to a high authority figure (Office of National Statistics, 2022).
Botnet-related fraud	Botnet fraud is using robots that are designed to perform specific functions automatically. These actions can range from illegally searching of online data, accessing lists, to phishing and click fraud (Tyagi and Aghila, 2011).
CEO fraud	CEO Fraud where criminals imitate company email accounts and impersonate executives to try to fool employee into making unauthorized transfers, or provide sensitive information (Pettit, 2023).
Call centre fraud	Call centre fraud involves making fake call centres, or infiltrating genuine call centres, to gain peoples sensitive information (Action Fraud, 2023c).
Click fraud	Click fraud is deceitfully clicking on search advertisements with the intention of growing a third-party website income or depleting the advertiser's budget (Wilbur and Zhu, 2009)
Computer hacking	Hacking is the unauthorised access to a computer system. It can include the hacking

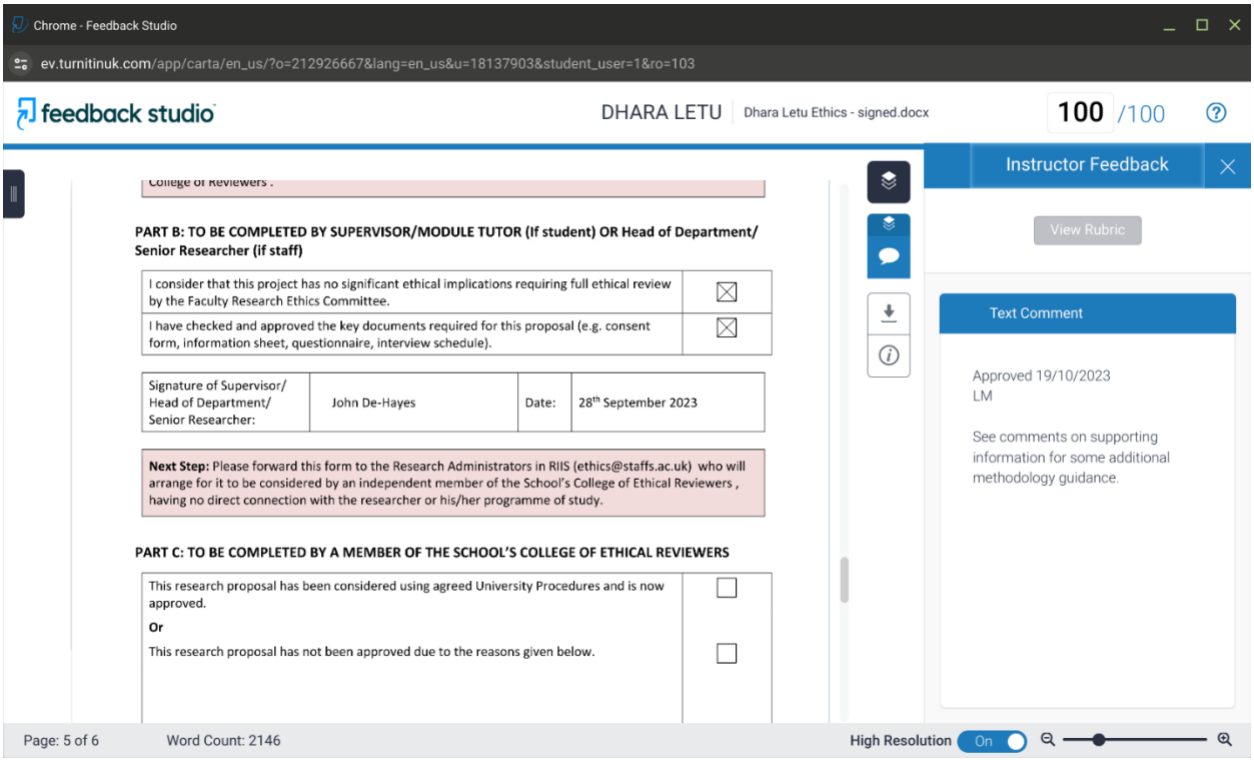
	into computers, servers, telephone systems, social media and email accounts, and can be done with and without blackmail (Correia, 2022).
Consumer Fraud and Retail Fraud	Consumer and retail fraud happens when a person pays for goods or a service, but those things do not appear, were falsely described, faulty or stolen (Office of National Statistics, 2022).
Domain name scams	Domain name scams are when fraudsters offer businesses first refusal on a domain name, stating that they have little time left to buy it as someone else is also about to buy it (Action Fraud, 2023d).
Facility takeover	A facility takeover happens when a fraudster pretends to be a real customer to obtain access and control of the account to illegally carry out transactions (Action Fraud, 2023e).
Fraudulent takeover	Fraudulent takeover is when a fraudster conducts an account takeover, of any type of account, by pretending to be a real customer, to make illegal transactions (Action Fraud, 2023f)
Internet dialler scams	Internet dialler scams are where settings on a computer are changed so that the internet connection re-routs. This can happen when a person opens a spam email, clicks pop-ups, or downloads software that makes changes on their computer (Action Fraud, 2023g).
Invoice scams	Invoice scams happen when fraudsters send invoices to a company asking for payment for goods or a service (Action Fraud, 2023h).
Identity theft	Identity theft is where a criminal illegally gains sensitive information about an individual and uses that information to commit fraud or theft (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014).

Malware and computer virus	Malware and computer viruses are software that has been produced so that your devices do not work how it is meant to. Sometime the software can also collect information or data from the devices, that the offender can pass on (Action Fraud, 2023i).
Mailbox and multiple post re-directions	Mailbox and multiple post re-directions fraud is where legitimate mail services are used by fraudsters to enable fraud (Action Fraud, 2023j).
Phishing	Phishing is where the offenders fraudulently communicate to trick someone into giving personal information or to leave software that is malicious (Office of National Statistics, 2022).
Proxy servers	Proxy servers can be used by fraudsters to commit illegal transactions, as it can hide their real IP address and location, meaning that they can avoid being tracked prosecuted by law enforcement agencies (Pannu *et al.*, 2016).
Remote access tool scams	Remote access tool scams involve fraudsters exploiting remote access software and using the internet to connect to a victim's device with the goal of stealing money or gaining access to financial information, which can be done by deceiving the individual into allowing them to remotely access their device (Action Fraud, 2023k).
Recovery fraud	Recovery fraud is where fraudsters share information about their victimised to other offenders who will then try and further victimise the individuals, this may be done by using a new scheme or the same one (Cross, Richard and Smith, 2016).
Romance Scam/Fraud	Romance scam/fraud is where fraudsters use the cover of a relationship to gain benefits

	such as money from the victim (Button and Cross, 2017)

Appendix B

Ethical approval



RESEARCH ETHICS

Proportionate Review Form

The Proportionate Review process may be used where the proposed research raises only minimal ethical risk. This research must: focus on minimally sensitive topics; entail minimal intrusion or disruption to others; and involve participants who would not be considered vulnerable in the context of the research.

PART A: TO BE COMPLETED BY RESEARCHER

Name of Researcher:	Dhara Letu
School	Justice, Security and Sustainability

Student/Course Details (If Applicable)			
Student ID Number:			21012489
Name of Supervisor(s)/Module Tutor:			John De-Hayes
PhD/MPhil project:	☐		
Taught Postgraduate Project/Assignment:	☐	Award Title:	BSc Policing and Criminal Investigation
Undergraduate Project/Assignment:	☒	Module Title:	Project in Policing and Crimianl Investigation

Project Title:	Cyber Fraud
Project Outline:	This project will examine cyber fraud and the public knowledge on cyber fraud. I am interested in finding out if people know how to protect themselves from cyber fraud as schools do not tend to teach people about cyber fraud and as technology has continuously evolved, cyber-crime has also increased, increasing the chances of people being put at risk and the way police handle cyber-crime has had to change as well. Therefore, the aims of the research are to understand: the public's knowledge on cyber fraud, how they protect themselves from it, their belief of whether the Police tackle cyber fraud effectively, and if they know where they can go to ask for information and help to do with cyber fraud. The objective is to find out what the public's knowledge of cyber fraud and what steps they take to protect themselves, if they know where to go to get information to ask for help to do with cyber fraud, and if they know how the Police deal with cyber fraud. As well as this I will be looking into what the Police are doing to tackle these types of crimes, and why cyber fraud is still increasing.
Give a brief description of participants and procedure (methods, tests etc.)	Primary data gathered through on online questionnaire will be used, with quantitative and qualitative data being collected. The target audience are individuals 18 and over as I am interested in understanding if the public know how to protect themselves from cyber fraud without having been taught how to. There is a risk that individuals may lie about their age, which I will keep in mind. The questionnaire will be made on Qualtrics software and will be distributed on social media, such as Facebook and Twitter. I do not know who will

	answer the questionnaire so I will try my best that vulnerable people are not targeted. By sharing the questionnaire on social media, I am aware there may be a risk to me being targeted by the public for trolling and will be put at risk of researcher bias. To decrease these risks as much as possible, I will be opening new social media accounts and share the questionnaire to as many Facebook groups as possible. I will not be able to get back to participants that may have been affected by the nature of the questions, but I can signpost them at the end of the questionnaire to victim support, helplines and centres (e.g., Action Fraud) that they can go to ask or help. Snowball sampling will be used as it can reach a wider target audience as the primary participants pass on the questionnaire further by referrals. Snowball sampling is a non-probability sampling technique that can go on for a long time, generating a large sample that can be analysed to draw conclusive results so that the aim of the research can be reached. It will include both open and closed questions as well as Likert scale questions. Basic demographic information such as age and gender will be asked as well as what their educational level is, to be able to fully analyse the data. Questions on the participants knowledge of cyber fraud will be asked, as well as their belief on the police efficiency in handling cyber fraud. At the end participant will be given the option to add any further details on what they have been asked, if they wish to expand on their answers. This is not necessary but, if answered it will allow us to obtain an even greater understanding of the public knowledge as they may give us more information on anything we may have missed to ask. Once the questionnaire is public it will be open for two months to ensure enough data has been collected, the aim being 250 responses. Participants will be informed of their right to withdraw at any time during the completion of the questionnaire, however, to keep the participants anonymous withdrawal will not be possible after submission. The data will be collected through Qualtrics software and then saved in the university system where the access will be limited to the researcher to analyse and the supervisor for supervision. The data will be destroyed after 10 years. For descriptive statistics a test of normality will be done on the data to identify if the data is normally distributed or not. The test of normality will depend on how many responses there will be. If there are more than 50 responses, then the Kolmogorov-Smirnov test will be used and if there are less than 50 responses then the Shapiro-wilk test will be used. Parametric and non-parametric tests will be conducted on the data to achieve the research aims. Analysis such as cross-tabulation of nominal data and Spearman's rank order correlation will also be conducted.		
Expected Start Date:	23rd October 2023	Expected End Date:	15th June 2024

Relevant professional body ethical guidelines should be consulted when completing this form.

Please seek guidance from the School Ethics Coordinator if you are uncertain about any ethical issues arising from this application.

There is an obligation on the researcher and supervisor (where applicable) to bring to the attention of the School Ethics Coordinator any issues with ethical implications not identified by this form.

Researcher Declaration

I consider that this project has no significant ethical implications requiring full ethical review.	☒

University Research Ethics Committee (February 2018)

I confirm that:		
1.	The research will **NOT** involve members of vulnerable groups. Vulnerable groups include but are not limited to: children and young people (under 18 years of age), those with a learning disability or cognitive impairment, patients, people in custody, people engaged in illegal activities (e.g. drug taking), or individuals in a dependent or unequal relationship.	☒
2.	The research will **NOT** involve sensitive topics. Sensitive topics include, but are not limited to: participants' sexual behaviour, their illegal or political behaviour, their experience of violence, their abuse or exploitation, their mental health, their gender or ethnic status. The research must not involve groups where permission of a gatekeeper is normally required for initial access to members, for example, ethnic or cultural groups, native peoples or indigenous communities.	☒
3.	The research will **NOT** deliberately mislead participants in any way.	☒
4.	The research will **NOT** involve access to records of personal or confidential information, including genetic or other biological information, concerning identifiable individuals.	☒
5.	The research will **NOT** induce psychological stress, anxiety or humiliation, cause more than minimal pain, or involve intrusive interventions. This includes, but is not limited to: the administration of drugs or other substances, vigorous physical exercise, or techniques such as hypnotherapy which may cause participants to reveal information which could cause concern, in the course of their everyday life.	☒
6.	The research **WILL** be conducted with participants' full and informed consent at the time the study is carried out: • The main procedure will be explained to participants in advance, so that they are informed about what to expect. ☒ • Participants will be told their involvement in the research is voluntary. ☒ • Written consent will be obtained from participants. *(This is not required for self-completion questionnaires as submission of the completed questionnaire implies consent to participate)*. ☒ • Participants will be informed about how they may withdraw from the research at any time and for any reason. ☒ • For questionnaires and interviews: Participants will be given the option of omitting questions they do not want to answer. ☒ • Participants will be told that their data will be treated with full confidentiality and that, if published, every effort will be made to ensure it will not be identifiable as theirs. ☒ • Participants will be given the opportunity to be debriefed i.e. to find out more about the study and its results. ☒	YES ☒ N/A ☐
7.	A risk assessment has been completed for this research project	YES ☐ N/A ☒

If you are unable to confirm any of the above statements, please complete a **Full Ethical Review Form**. If the University Research Ethics Committee (February 2018)

research will include participants that are **patients,** please complete the Independent Peer Review process.

8. Information and Data Please provide answers to the following questions regarding the handling and storage of information and data:
a) How will research data be stored (manually or electronically)? It will be stored electonically in Staffordshire University's secure OneDrive system.
b) How is protection given to the participants (e.g. by being made anonymous through coding and with a participant identifier code being kept separately and securely)? Survey participants will not be asked to provide any personal information that might identify them. Any data gathered as a by-product of the use of Qualtrics will not be used in the final report. If any participant provides information that might lead to them being identified, it will either be anonymised or redacted in the final report.
c) What assurance will be given to the participant about the confidentiality of this data and the security of its storage? Participants will be assured in the participant information sheet that the data will be kept confidential in the university's secure storage which only the researcher and the supervisor will have access to, and that the data will be handled in accordance with university policies, Data Protection legislation and the GDPR.
d) Is assurance given to the participant that they cannot be identified from any publication or dissemination of the results of the project? Participants will be assured in the participant information sheet that they are completely anonymous, and that no personally identifiable information will be needed for the participation of the questionnaire.
e) Who will have access to this data, and for what purposes? The researcher, Dhara Letu, for analysis of the data and the supervisor, John De-Hayes, for supervision over the research.
f) How will the data be stored, for how long, and how will it be discarded? Data will be stored in folders on Staffordshire University's secure OneDrive system, accessible only by the researcher and project supervisor. The data will be retained for 10 years in compliance with the University Guidelines and GDPR Principles. After this time, the data will be destroyed simply by deleting the folders and material contained within them. .

Supporting Documentation

All key documents e.g. consent form, information sheet, questionnaire/interview schedule are appended to this application.	☒

Signature of Researcher:	Dhara Letu	Date:	28th September 2023

NB: If the research departs from the protocol which provides the basis for this proportionate review, then further review will be required and the applicant and supervisor(s) should consider whether or not the proportionate review remains appropriate. If it is no longer appropriate a full ethical review form **MUST** be submitted for consideration by the School Ethics Coordinator.

Next Step:

University Research Ethics Committee (February 2018)

STUDENTS: Please submit this form (and supporting documentation) for consideration by your Supervisor/ Module Tutor.

STAFF: Please submit this form to your Head of Department or a Senior Researcher in your School. Once they have reviewed the form, this should be forwarded to the Research Administrators in RIIS (ethics@staffs.ac.uk) who will arrange for it to be considered by an independent member of the School's College of Reviewers .

PART B: TO BE COMPLETED BY SUPERVISOR/MODULE TUTOR (If student) OR Head of Department/ Senior Researcher (if staff)

I consider that this project has no significant ethical implications requiring full ethical review by the Faculty Research Ethics Committee.	☒
I have checked and approved the key documents required for this proposal (e.g. consent form, information sheet, questionnaire, interview schedule).	☒

Signature of Supervisor/ Head of Department/ Senior Researcher:	John De-Hayes	Date:	28th September 2023

Next Step: Please forward this form to the Research Administrators in RIIS (ethics@staffs.ac.uk) who will arrange for it to be considered by an independent member of the School's College of Ethical Reviewers , having no direct connection with the researcher or his/her programme of study.

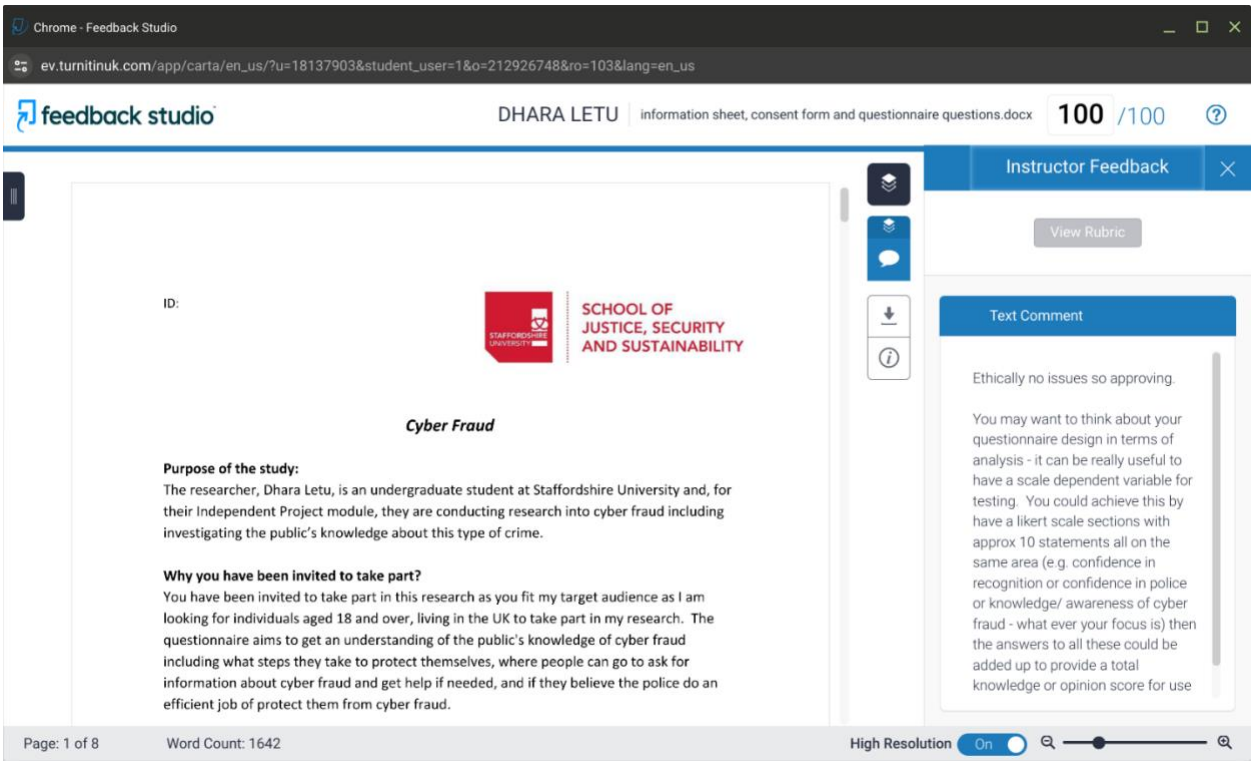
PART C: TO BE COMPLETED BY A MEMBER OF THE SCHOOL'S COLLEGE OF ETHICAL REVIEWERS

This research proposal has been considered using agreed University Procedures and is now approved.	☐
Or	
This research proposal has not been approved due to the reasons given below.	☐
Recommendation (delete as appropriate): Approve/ Amendments required/ Reject	

Name of Reviewer:		Date:	
Signature:			

Signed (School Ethical Coordinator)		Date:	

Participant Information Sheet



ID:

SCHOOL OF JUSTICE, SECURITY AND SUSTAINABILITY

Cyber Fraud

Purpose of the study:
The researcher, Dhara Letu, is an undergraduate student at Staffordshire University and, for their Independent Project module, they are conducting research into cyber fraud including investigating the public's knowledge about this type of crime.

Why you have been invited to take part?
You have been invited to take part in this research as you fit my target audience as I am looking for individuals aged 18 and over, living in the UK to take part in my research. The questionnaire aims to get an understanding of the public's knowledge of cyber fraud including what steps they take to protect themselves, where people can go to ask for information about cyber fraud and get help if needed, and if they believe the police do an efficient job of protect them from cyber fraud.

What does participation entail?
Participation in this research will involve filing out a questionnaire regarding your perception of cyber fraud and if the Police are tackling this type of crime efficiently. The questionnaire will take approximately 5-10 minutes and will be captured using Qualtrics software.

What are the risks associated with taking part in the research?
There are no risks associated with taking part in this study. Any information collected within the study remains anonymous.

What are the benefits of taking part in the research?
There are no direct benefits to you from taking part in this study. You are being asked to help in order to better understand the public's perception of cyber fraud and if the police are doing an efficient job and tackling this type of crime. As reiterated previously, you will not be mentioned in any reports as the data collected is anonymous.

Are there any reasons why I might not be eligible to take part in the research?
We require participants over the age of 18 years, with a variety of levels of education, and living in the UK.

How will any personal information used during the research be kept confidential?
All information collected from the questionnaire will be kept strictly confidential. No personally identifiable information will be needed to complete the questionnaire, and your answers will be anonymous. You will be asked for basic demographic information such as age, gender and ethnicity to allow us to fully analyse the data. All data collected, as part of this study, will be kept securely in electronic form for 10 years, and will then be destroyed.

Right to decline or withdraw
You are reminded that you are not under any obligation to take part in this study and hold the right to decline participation. You also hold the right to withdraw from the survey at any point before the final submission, however after you submit your responses it will no longer be possible to withdraw, as your submission will be anonymous.

GDPR Statement
Your data will be processed in accordance with the General Data Protection Regulation 2016 (GDPR).
The data controller for this project will be Staffordshire University. The university will process your personal data for the purpose of the research outlined above. The legal basis for processing your personal data for research purposes under the GDPR is a 'task in the public interest'. You can provide your consent for the use of your personal data in this study by completing the consent form that has been provided to you.
You have the right to access information held about you. Your right of access can be exercised in accordance with the GDPR. You also have other rights including rights of correction, erasure, objection, and data portability. Questions, comments and requests about your personal data can also be sent to the Staffordshire University Data Protection Officer. If you wish to lodge a complaint with the Information Commissioner's Office, please visit www.ico.org.uk.

Contact
If any questions or concerns should arise from this research, if you wish to raise a concern about the study, and in particular about the conduct of the study or the individuals involved or you require further information about the study, please do not hesitate to contact the researcher's supervisor, John De-Hayes on john.de-hayes@staffs.ac.uk or 01782 294371

Complaints:
We hope you take part and find our study interesting. However, we realise problems may arise. If you have any concerns, please contact the supervisor listed above. We will do our best to answer any problems.

ID:

Participant copy

Consent Form

By taking part in the study, you are agreeing that you understand the information provided and agree to the following:

- ☐ I confirm that I have read and have understood the information sheet dated for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.
- ☐ I understand that my involvement in the study will remain anonymous and once my responses have been submitted any identifiable information will be replaced with a code.
- ☐ I understand that my participation will be anonymous and any details that might identify me will not be included in any reports or publications produced from the study.
- ☐ I understand that I am free to not answer any questions and end the questionnaire at any point.
- ☐ I agree to anonymised quotes being used within reports/other publications produced from the study.
- ☐ I understand that any data I provide will be used to provide an overview of purpose of study.

By taking part in the interview after reading this information you are agreeing that you understand the information provided and agree to us analysing the answers you give.

Thank you for taking the time to read this information.

Participant:

Signed: ..... **Date: .....**

Researcher:

Signed: ..... **Date: .....**

Survey Questions

Q. After reading the information above, do you still wish to continue?

- Yes
- No

Q. are you aged 18 or over?

- Yes
- No

Q1. Can you please select your age?

Q2. Can you please describe your gender?

- Male
- Female
- Transgender female
- Transgender male
- Non-binary / third gender
- Prefer not to say
- Other

Q3. What is the highest level of education, or equivalent, that you have?

- GCSE (Level 1&2)
- A-level, Btec (Level 3)
- Undergraduate, foundation (Level 4,5,6)
- Masters (Level 7)
- Higher

Q4. Can you please state what you do for a living.

Q5. Have you been taught about cyber fraud in school?

- Yes
- No

Q5b. What cyber fraud topics have you been taught?

- Identifying cyber fraud
- Consequences of cyber fraud
- How to protect yourself from cyber fraud
- How to evaluate the reliability of online content
- Other

Q6. What types of cyber fraud are you familiar with? Tick all that apply.

- Botnet-related crime
- Click fraud
- Call centre fraud
- Computer hacking
- Domain name scams
- Facility takeover
- Fraudulent takeover
- Internet dialler scams
- Invoice scams
- Identity theft
- Malware and computer virus
- Mailbox and multiple post re-directions
- Phishing
- Proxy servers
- Remote access tool scams
- Tab-napping
- Website domain name scams
- None of the above
- Other

Q7. How extensive of an issue do you believe cyber fraud is?

- Not at all

- A little
- A lot
- A great deal

Q8. Can you please select what you would do in case of a cyber fraud incident. Tick all that apply.

- You wouldn't do anything
- Tell your friends and/or family
- Call or go to the Police
- Call your bank
- Search for advice online
- Other

Q9. Can you please select what steps you take to protect yourself from cyber fraud? Tick all the apply.

- Do not take any
- Do not provide personal information
- Verify organisations or people's credentials
- Computer has up to date anti-virus software
- Computer has a firewall installed
- Use strong passwords
- Check with banks about any suspicious emails
- Think before you click
- Signed up to Verified by Visa or Mastercard Secure Code for online shopping
- Regularly check your credit file to check for anything that you don't recognise
- Destroy receipts that contain card details
- Other

Q10. How would you rate your knowledge on:

- Cyber Fraud
    - Excellent

    - Good
    - Average
    - Poor
    - Terrible
- What the police are doing to tackle cyber fraud
    - Excellent
    - Good
    - Average
    - Poor
    - Terrible
- Cyber fraud websites that inform and help
    - Excellent
    - Good
    - Average
    - Poor
    - Terrible

Q11. Are you satisfied with:

- Your ability to protect yourself from cyber fraud
    - Extremely satisfied
    - Satisfied
    - Dissatisfied
    - Extremely dissatisfied
- Your knowledge on cyber fraud
    - Extremely satisfied
    - Satisfied
    - Dissatisfied
    - Extremely dissatisfied

Q11a. How do you think this can be improved?

Q12. Are you satisfied with how the police deal with a cyber fraud incident?

- Extremely satisfied
- Satisfied
- Dissatisfied
- Extremely dissatisfied
- Do not know how the police deal with a cyber fraud incident

Q12a. How do you think the police can improve the way they deal with a cyber fraud incident?

Q13. Are you satisfied with what the police are doing to tackle cyber fraud?

- Extremely satisfied
- Satisfied
- Dissatisfied
- Extremely dissatisfied
- Do not know how the police deal with a cyber fraud incident

Q13a. How do you think the police can improve the way they tackle cyber fraud?

Q14. Is there anything else you would like to add or expand on?

Appendix C

Thematic anaylsis

Q8. Can you please select what you would do in case of a cyber fraud incident.

'Report e-mail scams by the in-built reporting option in the e-mail app; forward scam texts to the text fraud number; report to Action Fraud' (P.33)

'Log with Action Fraud' (P.61)

'Action Fraud' (P.67)

Q9. Can you please select what steps you take to protect yourself from cyber fraud?

'Shred or block out address details on mail' (P.12)

'Confirm with business apartment payment details' (P.46)

‘Keep on checking online bank payments etc’ (P.61)

‘Check bank using online apps’ (P.67)

Q11a. How do you think this can be improved?

‘Teaching students when they are younger about it and making the subject more aware.’ (P.2)

‘We need more knowledge on this topic, wether that’s adverts on tvs/ radios/ social media Or being taught it in school… or even when you open a bank account and have access to money they teach you somethings at that point’ (P.5)

‘Schools should teach their students about the subject and how to avoid getting scammed! :)' (P.6)

Have more people come in to inform students about cyber fraud and have workshops on what to do and how to avoid those situations. (P.7)

‘Adverts on the TV, posters around the country, posts on social media’ (P.8)

‘protective my accounts more and banks’ (P.9)

‘I think it be a good idea that the banks teach you about this stuff when you sign up for cards as that’s one way it can happen. I know work places do E-Learnings about it but it’s not very extensive. Also if your in the job I am, it be good if the police go through it with you in depth to help victims of it if we get called to the job’ (P.17)

‘More awareness, seminars at schools, Google could develop a software which could check if the sender is secure’ (P.18)

‘By informing myself of ways I can better protect my personal data and to put them in practice’ (P.21)

‘TV programmes that provide information’ (P.23)

‘I must study much more about it in order for me to be more carefull when I use my personal data, credit cards, etc.’ (P.32)

‘more information’ (P.45)

‘taking classes’ (P.48)

‘Mass education’ (P.56)

‘More information be made available to educate us. But there is the chance that whoever provides advice is also a scammer so trusting people/companies can be difficult ‘(P.64)

‘More knowledge’ (P.65)

‘Regular msm updates Leaflets’ (P.66)

‘Searching online and being more aware of relevant sources of information’ (P.71)

‘There needs to be more information given to those who are most vulnerable. Offer them free workshops to attend, send warnings to them. In fact the whole population needs more information on how to protect themselves and how these organisations drag you in.’ (P.72)

‘Learn more’ (P.75)

Q12a. How do you think the police can improve the way they deal with a cyber fraud incident?

‘Better at punishing those who have commited cyber fraud’ (P.3)

‘Not dismiss people when they go with an issue and become more technologically aware so they can deal with the issues instead of ignoring people’ (P.12)

‘Better training’ (P.18)

‘Police need more resources to tackle the rise in cyber fraud’ (P.28)

‘They don't really deal with them at all. Action Fraud take the reports and then very little seems to happen’ (P.33)

‘Study more on the subject, train continuously, risk awareness campaigns and direct communications with public and relevant institutions (Banks, payment provideri, it companies)’ (P.46)

‘Be more involved, proper checks.’ (P.47)

‘More staff’ (P.51)

‘Investigate the small cases too’ (P.53)

‘Increase in force numbers and budget to have the resources required to deal with this growing threat’ (P.54)

‘Take more action against fraudsters’ (P.62)

‘Invest in bigger team with better tech to be more efficient’ (P.63)

‘Police don’t do much with it, not high on a long list of priorities. Action fraud triages it to collate and package actionable ones. More onus ought to be on financial institutions, requiring or requesting the police to do more is unrealistic and simplistic’ (P.67)

‘More training and investment in resources is required. A lot of police officers and staff who work in the sector are also tempted away by higher earnings in the private sector. Given the rigid structure of pay scales in policing, it is unlikely that additional payments could be made to retain staff, so perhaps the answer is for the police to "contract out" some of their investigations to those best trained and equipped to deal with them.’ (P.70)

‘By finding out who they are and arresting them.’ (P.72)

Q13a. How do you think the police can improve the way they tackle cyber fraud?

‘Improve methods of being able to identify perpetrators and punish them accordingly’ (P.3)

‘Become educated on technology and how to deal with these cases’ (P.12)

‘There needs to be more police training and more resources available for the police to tackle the issue. A multiagency approach is needed.’ (P.28)

‘As before - there actually needs to be more effort to tackle it. Instead, the government choose to exclude online fraud crimes from national crime figures!’ (P.33)

‘Answer provided at previous question.’ (P.46)

‘To be more involved and do proper checks.’ (P.47)

‘More staff’ (P.51)

‘By getting involved’ (P.53)

‘More officers need it, better training, bigger budget’ (P.54)

‘Take more action’ (P.62)

‘It needs tackling at a National level with severed punishments coupled with financial institutions bearing the burden.’ (P.67)

‘Needs more resources in a growing area of criminality’ (P.71)

‘More helplines for information and support to tackle what has happened to them. Be good to know issues are followed up to catching them.’ (P.72)

Q14. Is there anything else you would like to add or expand on?

‘I understand most people contact their banks and go through them if this issues occurs so the police don’t have a lot of data on the subject so there’s not much they can do … but if it happened to them (the police officers) I’m sure they’d take it more seriously than someone off of the street complaining about it … if that makes sense. Doesn’t feel like something they take seriously.’ (P.5)

‘I don't think many people know that cyber fraud is a police matter, so they are limited on what they can do. There needs to be more awareness for us to know what to do when it happens to us and that it is in fact a police matter’ (P.8)

‘I served 18 years in the police so do have a higher level of knowledge’ (P.43)

‘Through work we use Cyber Essentials and this information assists in how I can protect myself personally’ (P.60)

‘Think that frontline police do not have adequate knowledge of cyber and cyber-enabled Crime. Good knowledge from Specialist officers’ (P.61)

‘When someone’s identity is used on a social media platform, have the ability to work more efficiently with the platform to disable the account’ (P.63)

‘More resources required’ (P.66)

‘We now rely on too much electronic systems and are always aware there are far too many people out there just waiting for an opportunity to scam the public. Its a very scary world now.’ (P.76)

Theme 1: Education

- ‘Teaching students when they are younger about it and making the subject more aware.’ (P.2)
- ‘We need more knowledge on this topic...Or being taught it in school… or even when you open a bank account and have access to money they teach you somethings at that point’ (P.5)
- ‘Have more people come in to inform students about cyber fraud and have workshops on what to do and how to avoid those situations.’ (P.7)
- ‘I think it be a good idea that the banks teach you about this stuff when you sign up for cards as that’s one way it can happen. I know work places do E-Learnings about it but it’s not very extensive.’ (P.17)
- ‘More awareness, seminars at schools’ (P.18)
- ‘More information be made available to educate us.’ (P.64)
- ‘There needs to be more information given to those who are most vulnerable. Offer them free workshops to attend, send warnings to them. In fact the whole population needs more information on how to protect themselves and how these organisations drag you in.’ (P.72)

Subtheme 1: Individual Actions

- ‘protective my accounts more and banks’ (P.9)
- ‘By informing myself of ways I can better protect my personal data and to put them in practice’ (P.21)
- ‘I must study much more about it in order for me to be more carefull when I use my personal data, credit cards, etc.’ (P.32)
- ‘Searching online and being more aware of relevant sources of information’ (P.71)
- ‘Learn more’ (P.75)

Subthemes 2: Organizations

- ‘Adverts on the TV, posters around the country, posts on social media’ (P.8)

- ‘Also if your in the job I am, it be good if the police go through it with you in depth to help victims of it if we get called to the job’ (P.17)
- ‘Google could develop a software which could check if the sender is secure’ (P.18)
- ‘TV programmes that provide information’ (P.23)
- ‘Regular msm updates Leaflets’ (P.66)

Theme 2: Police Action and Involvement

- ‘Improve methods of being able to identify perpetrators and punish them accordingly’

  ‘Better at punishing those who have commited cyber fraud’ (P.3)
- ‘Not dismiss people when they go with an issue’ (P.12)
- ‘A multiagency approach is needed.’ (P.28)
- ‘They don't really deal with them at all. Action Fraud take the reports and then very little seems to happen’ ‘As before - there actually needs to be more effort to tackle it. Instead, the government choose to exclude online fraud crimes from national crime figures!’ (P.33)
- ‘risk awareness campaigns and direct communications with public and relevant institutions (Banks, companies)’ (P.46)
- ‘Be more involved, proper checks.’ ‘To be more involved and do proper checks.’ (P.47)
- ‘Investigate the small cases too’ ‘By getting involved’ (P.53)
- ‘Take more action against fraudsters’ (P.62)
- ‘Police don’t do much with it, not high on a long list of priorities. Action fraud triages it to collate and package actionable ones. More onus ought to be on financial institutions, requiring or requesting the police to do more is unrealistic and simplistic’ ‘It needs tackling at a National level with severed punishments coupled with financial institutions bearing the burden.’ (P.67)
- ‘perhaps the answer is for the police to "contract out" some of their investigations to those best trained and equipped to deal with them.’ (P.70)
- ‘By finding out who they are and arresting them.’‘More helplines for information and support to tackle what has happened to them. Be good to know issues are followed up to catching them.’ (P.72)

Theme 3: Resources and Training

- ‘Police need more resources to tackle the rise in cyber fraud’ (P.28)
- ‘More staff’ (P.51)
- ‘Increase in force numbers and budget to have the resources required to deal with this growing threat’ (P.54)
- ‘Invest in bigger team with better tech to be more efficient’ (P.63)
- ‘More training and investment in resources is required.’ (P.70)

- ‘become more technologically aware so they can deal with the issues’ (P.12)
- ‘Better training’ (P.18)
- ‘Study more on the subject, train continuously’ (P.46)
- ‘Become educated on technology and how to deal with these cases’ (P.12)
- ‘There needs to be more police training and more resources available for the police to tackle the issue.’ (P.28)
- ‘Study more on the subject, train continuously’ (P.46)
- ‘More staff’ (P.51)
- ‘More officers need it, better training, bigger budget’ (P.54)
- ‘Needs more resources in a growing area of criminality’ (P.71)

SPSS output

Descriptive Statistics

	N	Minimum	Maximum	Sum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Age	76	18	77	2932	38.58	14.031	.260	.276	-.488	.545
Gender	76	1	4	104	1.37	.585	1.764	.276	4.222	.545
Education	76	1	5	210	2.76	1.221	-.163	.276	-1.187	.545
Valid N (listwise)	76									

Table 1. Descriptive statistics on participant’s age, gender, and education level.

Descriptives

			Statistic	Std. Error
Age	Mean		38.58	1.609
	95% Confidence Interval for Mean	Lower Bound	35.37	
		Upper Bound	41.79	
	5% Trimmed Mean		37.99	
	Median		40.00	
	Variance		196.860	
	Std. Deviation		14.031	
	Minimum		18	
	Maximum		77	
	Range		59	
	Interquartile Range		26	
	Skewness		.260	.276
	Kurtosis		-.488	.545
Gender	Mean		1.37	.067
	95% Confidence Interval for Mean	Lower Bound	1.23	
		Upper Bound	1.50	
	5% Trimmed Mean		1.31	
	Median		1.00	
	Variance		.342	
	Std. Deviation		.585	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		1	
	Skewness		1.764	.276
	Kurtosis		4.222	.545
Education	Mean		2.76	.140
	95% Confidence Interval for Mean	Lower Bound	2.48	
		Upper Bound	3.04	
	5% Trimmed Mean		2.75	
	Median		3.00	
	Variance		1.490	
	Std. Deviation		1.221	
	Minimum		1	
	Maximum		5	
	Range		4	
	Interquartile Range		2	
	Skewness		-.163	.276
	Kurtosis		-1.187	.545

Table 2. Descriptives on participant's age, gender, and education level.

Q2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	51	67.1	67.1	67.1
	Male	23	30.3	30.3	97.4
	Non-binary / third gender	1	1.3	1.3	98.7
	Prefer not to say	1	1.3	1.3	100.0
	Total	76	100.0	100.0	

Table 3. Frequencies on participant's gender.

Q3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	GCSE (Level 1&2)	17	22.4	22.4	39.5
	A-level, Btec (Level 3)	13	17.1	17.1	17.1
	Undergraduate, foundation (Level 4,5,6)	20	26.3	26.3	100.0
	Masters (Level 7)	23	30.3	30.3	73.7
	Higher	3	3.9	3.9	43.4
	Total	76	100.0	100.0	

Table 4. Frequencies on participant's education level.

Q3 * Q5 Crosstabulation

			Q5 No	Q5 Yes	Total
Q3	GCSE (Level 1&2)	Count	0	14	3	17
		Expected Count	.2	13.2	3.6	17.0
		% within Q3	0.0%	82.4%	17.6%	100.0%
		% within Q5	0.0%	23.7%	18.8%	22.4%
		% of Total	0.0%	18.4%	3.9%	22.4%
	A-level, Btec (Level 3)	Count	0	8	5	13
		Expected Count	.2	10.1	2.7	13.0
		% within Q3	0.0%	61.5%	38.5%	100.0%
		% within Q5	0.0%	13.6%	31.3%	17.1%
		% of Total	0.0%	10.5%	6.6%	17.1%
	Undergraduate, foundation (Level 4,5,6)	Count	1	13	6	20
		Expected Count	.3	15.5	4.2	20.0
		% within Q3	5.0%	65.0%	30.0%	100.0%
		% within Q5	100.0%	22.0%	37.5%	26.3%
		% of Total	1.3%	17.1%	7.9%	26.3%
	Masters (Level 7)	Count	0	21	2	23
		Expected Count	.3	17.9	4.8	23.0
		% within Q3	0.0%	91.3%	8.7%	100.0%
		% within Q5	0.0%	35.6%	12.5%	30.3%
		% of Total	0.0%	27.6%	2.6%	30.3%
	Higher	Count	0	3	0	3
		Expected Count	.0	2.3	.6	3.0
		% within Q3	0.0%	100.0%	0.0%	100.0%
		% within Q5	0.0%	5.1%	0.0%	3.9%
		% of Total	0.0%	3.9%	0.0%	3.9%
Total		Count	1	59	16	76
		Expected Count	1.0	59.0	16.0	76.0
		% within Q3	1.3%	77.6%	21.1%	100.0%
		% within Q5	100.0%	100.0%	100.0%	100.0%
		% of Total	1.3%	77.6%	21.1%	100.0%

Table 5. Crosstabulation on whether participants were taught cyber fraud related topics in school and their education level.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.466[a]	8	.305
Likelihood Ratio	10.002	8	.265
N of Valid Cases	76		

a. 11 cells (73.3%) have expected count less than 5. The minimum expected count is .04.

Table 6. Chi-Square tests on whether participants were taught cyber fraud related topics in school and their education level.

Q7 * Q5 Crosstabulation

			Q5 No	Q5 Yes	Total
Q7		Count	1	4	2	7
		Expected Count	.1	5.4	1.5	7.0
		% within Q7	14.3%	57.1%	28.6%	100.0%
		% within Q5	100.0%	6.8%	12.5%	9.2%
		% of Total	1.3%	5.3%	2.6%	9.2%
	A great deal	Count	0	35	6	41
		Expected Count	.5	31.8	8.6	41.0
		% within Q7	0.0%	85.4%	14.6%	100.0%
		% within Q5	0.0%	59.3%	37.5%	53.9%
		% of Total	0.0%	46.1%	7.9%	53.9%
	A lot	Count	0	16	7	23
		Expected Count	.3	17.9	4.8	23.0
		% within Q7	0.0%	69.6%	30.4%	100.0%
		% within Q5	0.0%	27.1%	43.8%	30.3%
		% of Total	0.0%	21.1%	9.2%	30.3%
	A little	Count	0	3	1	4
		Expected Count	.1	3.1	.8	4.0
		% within Q7	0.0%	75.0%	25.0%	100.0%
		% within Q5	0.0%	5.1%	6.3%	5.3%
		% of Total	0.0%	3.9%	1.3%	5.3%
	Not at all	Count	0	1	0	1
		Expected Count	.0	.8	.2	1.0
		% within Q7	0.0%	100.0%	0.0%	100.0%
		% within Q5	0.0%	1.7%	0.0%	1.3%
		% of Total	0.0%	1.3%	0.0%	1.3%
Total		Count	1	59	16	76
		Expected Count	1.0	59.0	16.0	76.0
		% within Q7	1.3%	77.6%	21.1%	100.0%
		% within Q5	100.0%	100.0%	100.0%	100.0%
		% of Total	1.3%	77.6%	21.1%	100.0%

Table 7. Crosstabulation on participant's opinion on how extensive of an issue cyber fraud is and whether they were taught cyber fraud related topics in school.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.004[a]	8	.112
Likelihood Ratio	8.116	8	.422
N of Valid Cases	76		

a. 11 cells (73.3%) have expected count less than 5. The minimum expected count is .01.

Table 8. Chi-Square tests on participant's opinion on how extensive of an issue cyber fraud is and whether they were taught cyber fraud related topics in school.

Q8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		6	7.9	7.9	7.9
	Call or go to the Police	9	11.8	11.8	19.7
	Call or go to the Police,Call your bank	3	3.9	3.9	23.7
	Call or go to the Police,Call your bank,Other	1	1.3	1.3	25.0
	Call or go to the Police,Call your bank,Search for advice online	5	6.6	6.6	31.6
	Call your bank	7	9.2	9.2	40.8
	Other	2	2.6	2.6	43.4
	Search for advice online	2	2.6	2.6	46.1
	Tell your friends and/or family	1	1.3	1.3	47.4
	Tell your friends and/or family,Call or go to the Police,Call your bank	19	25.0	25.0	72.4
	Tell your friends and/or family,Call or go to the Police,Call your bank, Search for advice online	10	13.2	13.2	85.5
	Tell your friends and/or family,Call your bank	1	1.3	1.3	86.8
	Tell your friends and/or family,Call your bank, Search for advice online	5	6.6	6.6	93.4
	Tell your friends and/or family,Search for advice online	5	6.6	6.6	100.0
	Total	76	100.0	100.0	

Table 9.

Q12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		9	11.8	11.8	11.8
	Do not know how the police deal with a cyber fraud incident	27	35.5	35.5	47.4
	Extremely dissatisfied	5	6.6	6.6	53.9
	Extremely satisfied	1	1.3	1.3	55.3
	Somewhat dissatisfied	15	19.7	19.7	75.0
	Somewhat satisfied	19	25.0	25.0	100.0
	Total	76	100.0	100.0	

Table 10.

Q13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		10	13.2	13.2	13.2
	Do not know what the police are doing to tack cyber fraud	27	35.5	35.5	48.7
	Extremely dissatisfied	3	3.9	3.9	52.6
	Extremely satisfied	2	2.6	2.6	55.3
	Somewhat dissatisfied	13	17.1	17.1	72.4
	Somewhat satisfied	21	27.6	27.6	100.0
	Total	76	100.0	100.0	

Table 11.

Q7 * Q10_1 Crosstabulation

			Q10_1				
			Excellent	Average	Good	Poor	Total
Q7		Count	6	0	0	0	1	7
		Expected Count	.6	.5	2.7	2.0	1.2	7.0
		% within Q7	85.7%	0.0%	0.0%	0.0%	14.3%	100.0%
		% within Q10_1	85.7%	0.0%	0.0%	0.0%	7.7%	9.2%
		% of Total	7.9%	0.0%	0.0%	0.0%	1.3%	9.2%
	A great deal	Count	0	3	15	16	7	41
		Expected Count	3.8	2.7	15.6	11.9	7.0	41.0
		% within Q7	0.0%	7.3%	36.6%	39.0%	17.1%	100.0%
		% within Q10_1	0.0%	60.0%	51.7%	72.7%	53.8%	53.9%
		% of Total	0.0%	3.9%	19.7%	21.1%	9.2%	53.9%
	A lot	Count	1	1	12	5	4	23
		Expected Count	2.1	1.5	8.8	6.7	3.9	23.0
		% within Q7	4.3%	4.3%	52.2%	21.7%	17.4%	100.0%
		% within Q10_1	14.3%	20.0%	41.4%	22.7%	30.8%	30.3%
		% of Total	1.3%	1.3%	15.8%	6.6%	5.3%	30.3%
	A little	Count	0	0	2	1	1	4
		Expected Count	.4	.3	1.5	1.2	.7	4.0
		% within Q7	0.0%	0.0%	50.0%	25.0%	25.0%	100.0%
		% within Q10_1	0.0%	0.0%	6.9%	4.5%	7.7%	5.3%
		% of Total	0.0%	0.0%	2.6%	1.3%	1.3%	5.3%
	Not at all	Count	0	1	0	0	0	1
		Expected Count	.1	.1	.4	.3	.2	1.0
		% within Q7	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%
		% within Q10_1	0.0%	20.0%	0.0%	0.0%	0.0%	1.3%
		% of Total	0.0%	1.3%	0.0%	0.0%	0.0%	1.3%
Total		Count	7	5	29	22	13	76
		Expected Count	7.0	5.0	29.0	22.0	13.0	76.0
		% within Q7	9.2%	6.6%	38.2%	28.9%	17.1%	100.0%
		% within Q10_1	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	9.2%	6.6%	38.2%	28.9%	17.1%	100.0%

Table 12. Crosstabulation on participant's opinion on how extensive of an issue cyber fraud is and how they rate their knowledge on cyber fraud.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	72.455[a]	16	<.001
Likelihood Ratio	44.753	16	<.001
N of Valid Cases	76		

a. 20 cells (80.0%) have expected count less than 5. The minimum expected count is .07.

Table 13. Chi-Square tests on participant's opinion on how extensive of an issue cyber fraud is and how they rate their knowledge on cyber fraud.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Age	.169	76	<.001	.931	76	<.001
Gender	.407	76	<.001	.621	76	<.001
Education	.187	76	<.001	.879	76	<.001

a. Lilliefors Significance Correction

Table 14. Test of normality on participants' age, gender. And education level.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.175[a]	16	.586
Likelihood Ratio	13.951	16	.602
N of Valid Cases	76		

a. 18 cells (72.0%) have expected count less than 5. The minimum expected count is .04.

Table 15. Chi-Square tests on what the participant's opinion on how extensive of an issue cyber fraud is and their education level.

Q3 * Q7 Crosstabulation

			Q7				
			A great deal	A lot	A little	Not at all	Total
Q3	GCSE (Level 1&2)	Count	1	8	7	1	0	17
		Expected Count	1.6	9.2	5.1	.9	.2	17.0
		% within Q3	5.9%	47.1%	41.2%	5.9%	0.0%	100.0%
		% within Q7	14.3%	19.5%	30.4%	25.0%	0.0%	22.4%
		% of Total	1.3%	10.5%	9.2%	1.3%	0.0%	22.4%
	A-level, Btec (Level 3)	Count	1	5	6	1	0	13
		Expected Count	1.2	7.0	3.9	.7	.2	13.0
		% within Q3	7.7%	38.5%	46.2%	7.7%	0.0%	100.0%
		% within Q7	14.3%	12.2%	26.1%	25.0%	0.0%	17.1%
		% of Total	1.3%	6.6%	7.9%	1.3%	0.0%	17.1%
	Undergraduate, foundation (Level 4,5,6)	Count	3	11	5	1	0	20
		Expected Count	1.8	10.8	6.1	1.1	.3	20.0
		% within Q3	15.0%	55.0%	25.0%	5.0%	0.0%	100.0%
		% within Q7	42.9%	26.8%	21.7%	25.0%	0.0%	26.3%
		% of Total	3.9%	14.5%	6.6%	1.3%	0.0%	26.3%
	Masters (Level 7)	Count	2	15	5	0	1	23
		Expected Count	2.1	12.4	7.0	1.2	.3	23.0
		% within Q3	8.7%	65.2%	21.7%	0.0%	4.3%	100.0%
		% within Q7	28.6%	36.6%	21.7%	0.0%	100.0%	30.3%
		% of Total	2.6%	19.7%	6.6%	0.0%	1.3%	30.3%
	Higher	Count	0	2	0	1	0	3
		Expected Count	.3	1.6	.9	.2	.0	3.0
		% within Q3	0.0%	66.7%	0.0%	33.3%	0.0%	100.0%
		% within Q7	0.0%	4.9%	0.0%	25.0%	0.0%	3.9%
		% of Total	0.0%	2.6%	0.0%	1.3%	0.0%	3.9%
Total		Count	7	41	23	4	1	76
		Expected Count	7.0	41.0	23.0	4.0	1.0	76.0
		% within Q3	9.2%	53.9%	30.3%	5.3%	1.3%	100.0%
		% within Q7	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	9.2%	53.9%	30.3%	5.3%	1.3%	100.0%

Table 16. Crosstabulation on what the participant's opinion on how extensive of an issue cyber fraud is and their education level.

Correlations

			Opinion	Knowledge
Kendall's tau_b	Opinion	Correlation Coefficient	1.000	-.094
		Sig. (2-tailed)	.	.395
		N	69	68
	Knowledge	Correlation Coefficient	-.094	1.000
		Sig. (2-tailed)	.395	.
		N	68	69

Table 17. Kendall's Tau test showing correlation between participants opinion on how extensive of an issue cyber fraud is and how they rate their knowledge on cyber fraud.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	78.333[a]	40	<.001
Likelihood Ratio	41.637	40	.399
N of Valid Cases	69		

a. 52 cells (94.5%) have expected count less than 5. The minimum expected count is .03.

Table 18. Chi-Square tests on what the participant's opinion on how extensive of an issue cyber fraud is and how many steps they take to protect themselves from cyber fraud.

steps * Q7 Crosstabulation

			Q7				
			A great deal	A lot	A little	Not at all	Total
steps	1	Count	0	0	2	0	2
		Expected Count	.0	1.2	.6	.1	.0	2.0
		% within steps	0.0%	0.0%	0.0%	100.0%	0.0%	100.0%
		% within Q7	0.0%	0.0%	0.0%	50.0%	0.0%	2.9%
		% of Total	0.0%	0.0%	0.0%	2.9%	0.0%	2.9%
	2	Count	1	1	2	0	0	4
		Expected Count	.1	2.4	1.3	.2	.1	4.0
		% within steps	25.0%	25.0%	50.0%	0.0%	0.0%	100.0%
		% within Q7	100.0%	2.4%	9.1%	0.0%	0.0%	5.8%
		% of Total	1.4%	1.4%	2.9%	0.0%	0.0%	5.8%
	3	Count	0	1	3	0	0	4
		Expected Count	.1	2.4	1.3	.2	.1	4.0
		% within steps	0.0%	25.0%	75.0%	0.0%	0.0%	100.0%
		% within Q7	0.0%	2.4%	13.6%	0.0%	0.0%	5.8%
		% of Total	0.0%	1.4%	4.3%	0.0%	0.0%	5.8%
	4	Count	0	3	5	0	0	8
		Expected Count	.1	4.8	2.6	.5	.1	8.0
		% within steps	0.0%	37.5%	62.5%	0.0%	0.0%	100.0%
		% within Q7	0.0%	7.3%	22.7%	0.0%	0.0%	11.6%
		% of Total	0.0%	4.3%	7.2%	0.0%	0.0%	11.6%
	5	Count	0	7	4	0	0	11
		Expected Count	.2	6.5	3.5	.6	.2	11.0
		% within steps	0.0%	63.6%	36.4%	0.0%	0.0%	100.0%
		% within Q7	0.0%	17.1%	18.2%	0.0%	0.0%	15.9%
		% of Total	0.0%	10.1%	5.8%	0.0%	0.0%	15.9%
	6	Count	0	7	1	0	0	8
		Expected Count	.1	4.8	2.6	.5	.1	8.0
		% within steps	0.0%	87.5%	12.5%	0.0%	0.0%	100.0%
		% within Q7	0.0%	17.1%	4.5%	0.0%	0.0%	11.6%
		% of Total	0.0%	10.1%	1.4%	0.0%	0.0%	11.6%
	7	Count	0	3	1	0	1	5
		Expected Count	.1	3.0	1.6	.3	.1	5.0
		% within steps	0.0%	60.0%	20.0%	0.0%	20.0%	100.0%
		% within Q7	0.0%	7.3%	4.5%	0.0%	100.0%	7.2%
		% of Total	0.0%	4.3%	1.4%	0.0%	1.4%	7.2%
	8	Count	0	3	2	1	0	6
		Expected Count	.1	3.6	1.9	.3	.1	6.0
		% within steps	0.0%	50.0%	33.3%	16.7%	0.0%	100.0%
		% within Q7	0.0%	7.3%	9.1%	25.0%	0.0%	8.7%
		% of Total	0.0%	4.3%	2.9%	1.4%	0.0%	8.7%
	9	Count	0	7	2	1	0	10
		Expected Count	.1	5.9	3.2	.6	.1	10.0
		% within steps	0.0%	70.0%	20.0%	10.0%	0.0%	100.0%
		% within Q7	0.0%	17.1%	9.1%	25.0%	0.0%	14.5%
		% of Total	0.0%	10.1%	2.9%	1.4%	0.0%	14.5%
	10	Count	0	7	2	0	0	9
		Expected Count	.1	5.3	2.9	.5	.1	9.0
		% within steps	0.0%	77.8%	22.2%	0.0%	0.0%	100.0%
		% within Q7	0.0%	17.1%	9.1%	0.0%	0.0%	13.0%
		% of Total	0.0%	10.1%	2.9%	0.0%	0.0%	13.0%
	11	Count	0	2	0	0	0	2
		Expected Count	.0	1.2	.6	.1	.0	2.0
		% within steps	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%
		% within Q7	0.0%	4.9%	0.0%	0.0%	0.0%	2.9%
		% of Total	0.0%	2.9%	0.0%	0.0%	0.0%	2.9%
Total		Count	1	41	22	4	1	69
		Expected Count	1.0	41.0	22.0	4.0	1.0	69.0
		% within steps	1.4%	59.4%	31.9%	5.8%	1.4%	100.0%
		% within Q7	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	1.4%	59.4%	31.9%	5.8%	1.4%	100.0%

Table 19. Crosstabulation on what the participant's opinion on how extensive of an issue cyber fraud is and how many steps they take to protect themselves from cyber fraud.

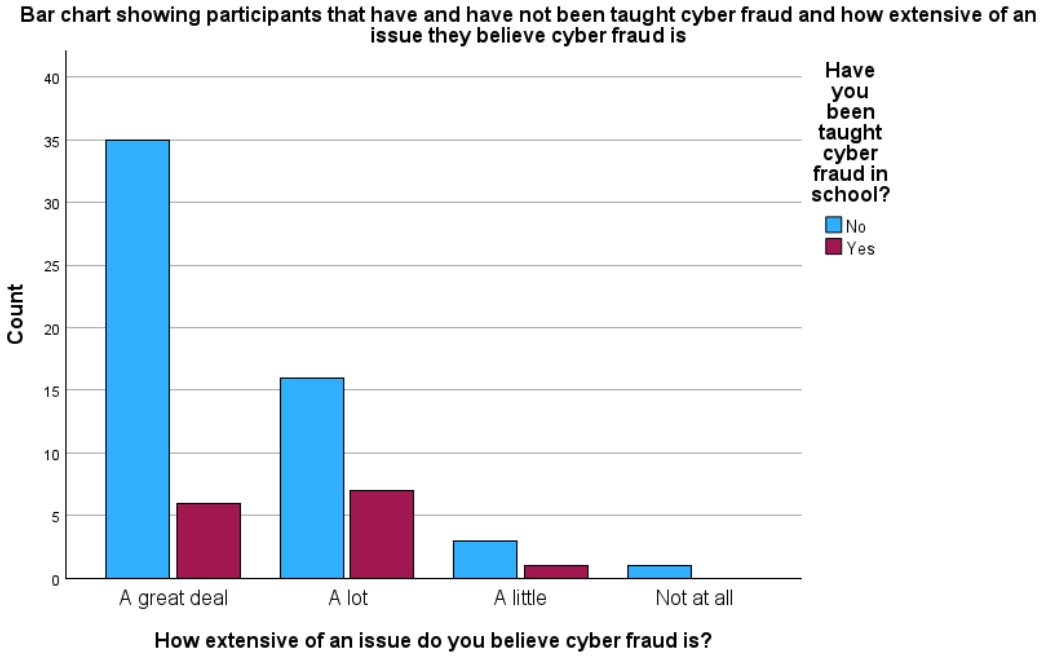


Figure 1 showing participants that have and have not been taught about cyber fraud in school, and how much of an issue they believe cyber fraud to be.

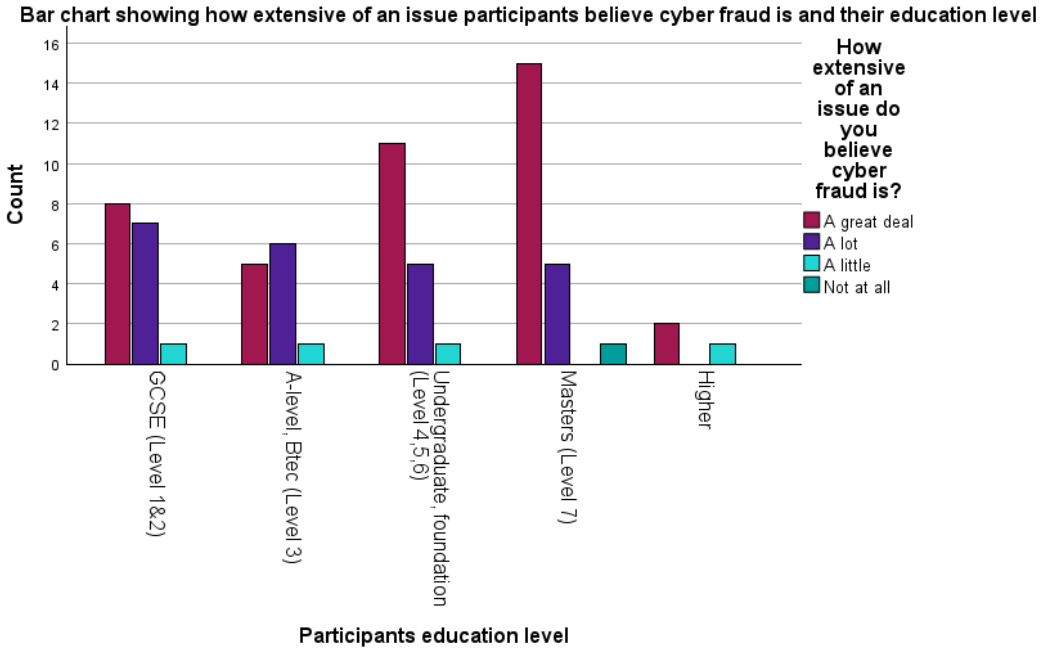


Figure 2 showing how extensive of an issue participant believe cyber fraud is and their education level.

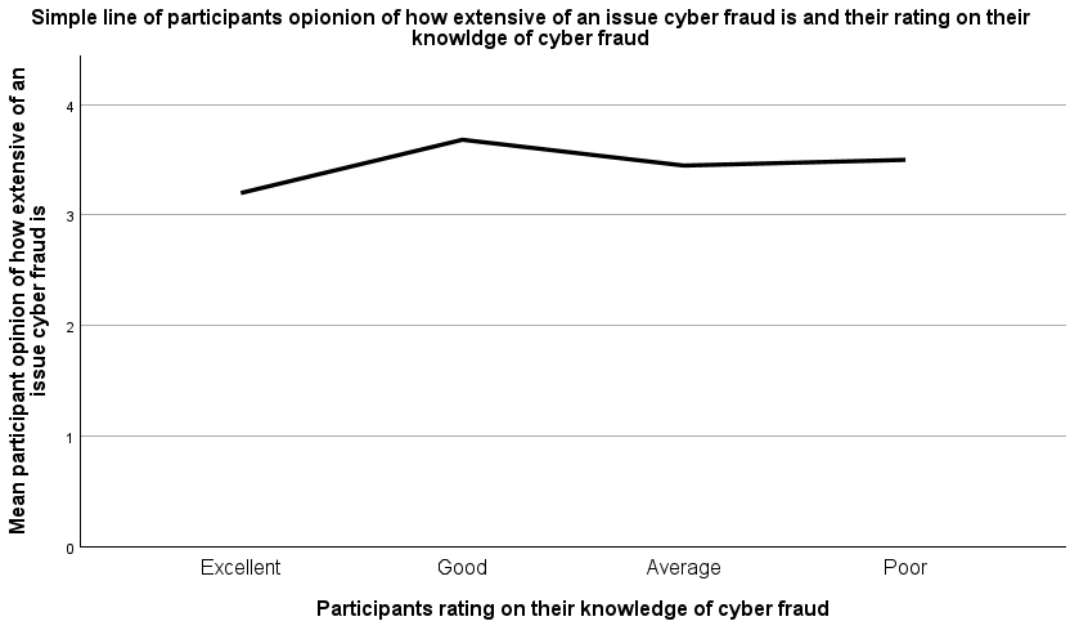


Figure 3 showing how extensive of an issue participants believe cyber fraud is in relation to their knowledge rating of cyber fraud.