Cardiff Metropolitan University

Prifysgol Metropolitan Caerdydd

B.Sc. (Hons) Psychology

Final Year Project

Investigating factors that influence scamming vulnerability through an online money scamming scenario.

2018

Dissertation submitted in partial fulfilment of the Requirements of the Cardiff Metropolitan University for the Degree of Bachelor of Science.

Declaration

I hereby declare that this dissertation is the result of my own independent investigation under the supervision of my tutor. The various sources to which I am indebted are clearly indicated. This dissertation has not been accepted in substance for any other degree, and is not being submitted concurrently for any other degree.

Acknowledgments

Firstly, I would like to express an immense amount of appreciation and gratitude towards my parents and my brother for all the support they have given me throughout my time at university. Without all the motivation speeches, reminders that I can get through this and of course the endless amount of chocolate and sweets you gave me to get through those long library sessions, I would not have been able to achieve what I have so far. I am truly thankful for everything you have done for me.

I would also like to thank my dissertation supervisor, for all the support through-out my dissertation. Thank you for all the times you reassured me especially when I sent my endless panic emails doubting myself! I was truly lucky to be allocated you as a supervisor, your patience, enthusiasm, and support got me through this tough stage at university!

Finally, I would also like to thank my friends in university and outside of university for maintaining my sanity through the never-ending stressful deadlines! You have all made my time here beyond memorable and I am so lucky to of shared my university experience with you.

Abstract

Attempts to maliciously influence people in an online environment, irrespective of the consequences, is dramatically escalating due to the growth of the internet. Furthermore, the change and development of social rules and norms from an offline environment to an online environment cause feelings of uncertainty regarding the authenticity of online communications and transactions. Thus, this led to the investigation of what makes an individual more susceptible to online manipulation such as fraud. Current understandings reveal certain demographic and personality factors result in an individual being more scam vulnerable. However, due to some conflicting research within this field of research, the present paper aims to review the previous literature regarding scamming vulnerability and overcome these uncertainties through the analysis of certain demographic and personality factors. Data was collected using snowballing and opportunity sampling techniques from 109 participants. The present study involved completing an email scam scenario from a low or high visceral approach, then completing the Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014), the Gullibility Scale (Teunisse, 2016) and the Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001). Results demonstrated that there was a main effect between age and the likelihood of compliance, and visceral influence and the likelihood of compliance. However, there was no interaction between these factors, nor was a significant effect found between gender and the likelihood of compliance. Additional analyses revealed that online trust significantly predicted the likelihood of compliance; however, gullibility and social intelligence were not significant contributors to predict the likelihood of compliance. Henceforth, the findings from the present study are later discussed in relation to prior research within the field of scamming vulnerability.

Table of Contents

Declaration........1

Acknowledgments........2

Abstract........3

Table of Contents........4

List of Figures........6

List of Tables........7

Chapter 1- Introduction........8

1.1 - Information processing........8

1.2 - Visceral influence........9

1.3 - Risky behaviour........10

1.4 - Age........11

1.5 - Online trust........12

1.6 - Gullibility........14

1.7 - Social intelligence........14

1.8 - Aim, Rationale and Hypotheses........15

Chapter 2 - Method........17

2.1 - Participants........17

2.2 - Design........17

2.3 - Materials........17

2.4 - Procedure........20

2.5 - Method of Analysis........20

2.6 - Ethical consideration........21

Chapter 3 – Results........22

3.1 - Three way ANOVA........22

3.2 - Multiple regression........24

Chapter 4- Discussion........26

4.1 - Introduction........26

4.2 - Summary of findings........26

4.3 - Limitations and future research........29

4.4 - Conclusion........30

Chapter 5 - References........31

Chapter 6 - Appendices........39

6.1 - Low visceral scam email........39

6.2 - High visceral scam email 39
6.3 - Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014) 40

List of Figures

Figure 1 – Mean likelihood of compliance for younger and older participants.

Figure 2 – Mean likelihood of compliance for low and high visceral conditions.

List of Tables

Table 1 – Examples of items from The Gullibility Scale (Teunisse, 2016)

Table 2 – Examples of items from The Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001)

Table 3 – Descriptive statistics of gender, visceral influence and age with respect to the likelihood of compliance

Table 4 – Summary of models predicting the significance of variables predicting the likelihood of compliance.

Table 5 – Summary of backward stepwise regression for variables predicting likelihood of compliance.

Table 6 – Summary of significant predictors of the likelihood of compliance.

Chapter 1- Introduction

The evolution of the internet has generated a vast growth in computer-mediated communication allowing greater opportunities for social communication to occur on a global level (Williams, Beardmore & Joinson, 2017). Despite the countless benefits of the internet, it has also increased the opportunity for 'social engineering' (Anderson, 2010) whereby scammers employ methods to influence victims to "engage in particular behaviours online for financial or other malicious gains" (Williams, Beardmore & Joinson, 2017, p.412). In the UK alone, an estimated £308.8 million of e-commerce fraud occurred in 2016 (Worobec, 2017), with numerous types of fraudulent claims, including investment fraud, charity, and pension scams etc, 91% of scams are sent and received via phone or email (Australian Competition & Consumer Commission, 2014). The consequences of defrauding an individual can result in a maximum of ten years imprisonment (Campbell, 2007).

Unfortunately, victims of scams are frequently labelled as 'greedy' or 'gullible', even though, such labels are 'superficial generalisations that presume every person is a perfectly rational consumer and ignores the fact that every individual is vulnerable to a persuasive approach at any one time' (Lea, Fischer & Evans, 2009, p.5). Social vulnerability refers to the inability to detect or avoid potentially harmful social interactions (Pinsker, Stone, Pachana & Greenspan, 2006). Thus, the advancement of the internet in conjunction with the ever-increasing problem of online fraud, this project intends to identify which factors contribute to an increased vulnerability to online mass marketing fraud, which could be advantageous to the online safety of society.

1.1 - Information processing

A number of different theories regarding scamming vulnerability have determined why individuals engage in scams. Firstly, victims may carefully evaluate the scam offer yet fail to recognise the scam cues that would alert them of the malicious transaction (West, Kover & Caruana, 2008; Wright, 1985). For example, scammers often present information using an official format ostensibly from a position of authority or use well-known brand images thereby reinforcing perceived credibility (Lea, Fischer & Evans, 2009). This serves to induce compliance by reducing suspicion and cue scrutiny by distracting the target from attending to cues such as bad grammar etc. (Fischer, Lea, & Evans, 2013). Secondly, victims may not carefully evaluate the malicious offer due to suffering from cognitive impairment resulting in a lack of financial literacy skills and judgement to notice scam cues (Earl, Gerrans, Asher & Woodside, 2013; Pinsker et al., 2006). Thus, causing victims to proceed without considering the possibility of being defrauded (Langenderfer & Shimp, 2001).

Consequently, this promoted the possibility that the way in which an individual processes information impacts the outcome of whether a scammer is successful or not. More specifically, the heuristic model presented by Chaiken (1980) demonstrated two modes of information processing. Firstly 'systematic processing' which demonstrates the carefully and strategically well thought-out decisions based on the quality of arguments presented (Vishwanath, Harrison & Ng, 2016). On the other hand, 'heuristic processing' adopts heuristic shortcuts which enables recollection from past experiences and applies them to the current situation (Vishwanath, Harrison & Ng, 2016). Due to the efficiency of heuristic processing, the majority of the human population adopt a heuristic level of processing (Sundar, 2008), however, employing this level of processing often results in increased errors of judgment and thus, poor decision making (Tversky & Kahneman, 1974) and lower risk evaluations (Trumbo, 2002). Consequently, adopting a heuristic style of information processing increases the likelihood that an individual will be more susceptible to comply with a scam because they are expected to overlook scam cues that may arouse suspicion (Vishwanath, Harrison & Ng, 2016).

1.2 - Visceral influence

Additional explanations as to why scam victims fail to analyse a scam are presented by Loewenstein (1996) who introduced the concept of 'visceral influence' and explained how it can affect an individual's motivation to engage in scams. The defining characteristics of visceral factors reflect an individual's wants and desires (Loewenstein, 1996) which scammers employ as a tool of manipulation to gain a quick and irrational response. Scammers exploit their victims through the use of visceral triggers which ultimately cause the victim to make decisions that lack cognitive deliberation causing the victim to shift their attention towards the reward (Langenderfer & Shimp, 2001). To do this, a scammer will present a reward (e.g money), which produces emotionally orientated triggers such as excitement thereby increasing physiological arousal (Whitty, 2013). Consequently, this technique is employed to motivate the individual to engage in the scam. As such, victims fail to notice the scam cues which would usually arouse suspicion and reveal the malicious intent of financial deception (Langenderfer & Shimp, 2001), thus emphasising the impact of rewards on motivation to participate in scams.

Within the role of visceral influence, there is two paths: high and low visceral influence. High visceral influence in a scamming situation would expect to cause an individual's cognitive resources to be directed towards the reward, rather than the scamming cues (Loewenstein, 1996). Consequently the loss of control results in victims engaging in activities which may not be in their best long-term interest (Strack & Neumann, 1996). On the other hand, low visceral influence typically involves a lack of interest in the proposed scam because the victims may not be motivated by their greed (Loewenstein, 1996). Hence, their attention would be directed towards the non-reward arguments of the scam such as trustworthiness and authority etc. Thus, low visceral influence is associated with low scamming vulnerability (Langenderfer & Shimp, 2001).

1.3 - Risky behaviour

In addition to that, scamming vulnerability can also be influenced by a process termed 'sensation seeking' (Zuckerman, 1994). Sensation seeking refers to the risky behaviour individuals pursue to elicit feelings of increased physiological and psychological arousal with the hope of benefitting from a reward (Lea, Fischer & Evans, 2009). Further to this, Lea, Fischer, and Evans (2009) also proposed the phenomenon 'long odds gamble' which demonstrates how despite the victim being aware of the scam cues, the potential gains from the pay-out involved from engaging in the scam outweigh the risk of taking part. Therefore, some individuals are motivated to engage in scamming behaviour because they are intrigued by the feelings of physiological and psychological arousal from participating in risky behaviour.

Regarding the issue of participating in risky behaviour, the term emerging adulthood also plays a key role in influencing the outcome. Emerging adulthood is a transition period 'distinguished by relative independence from social roles and normative expectations' where an individual between the ages of 18 to 25 years explores their life possibilities (Arnett, 2000, p.469). Consequently, due to the lack of responsibility placed on emerging adults, it enables them to pursue new experiences more freely than older adults (Arnett, 2000). Thus, the term risk is often associated with emerging adults because of their desire to gain more experiences and make the most of their time before the responsibilities of adulthood approach them (Arnett, 2000).

In addition to that, the term ‘online disinhibition effect’ describes how people may act differently in an online environment in comparison to the real world (Suler, 2004). This factor has resulted in younger individuals being more likely to engage in risk-taking behaviour online in comparison to an offline environment (CEOP, 2010). Although, despite young individuals being aware of the consequences of engaging in risk-taking behaviour, they still persist in taking part (Mishna, McLuckie & Saini, 2009).

Ultimately this demonstrates that younger individuals, particularly those aged 18-25 are more likely to participate in risky behaviour. Moreover, due to the relationship between risk and scamming vulnerability (Lea, Fischer & Evans, 2009), this would suggest that younger individuals may be more susceptible to fraud in comparison to later adulthood. In addition to this, research also highlights that males are more likely to engage in risky behaviour (Weber, 2003), hence the assumption that younger males may be the most vulnerable population to engage in scams can be made.

1.4 – Age

Although, previous literature has revealed that every individual is vulnerable to mass marketing fraud, although specific demographic and personality factors have been found to increase an individual’s scamming vulnerability. More specifically, research typically describes a scam victim as older, less educated and socially isolated (Fischer, Lea & Evans, 2013; Lea, Fischer & Evans, 2009). The assumption that older individuals are more vulnerable to fraud is firstly due to age-related health issues which impact the mobility of an individual, this often results in a reduced amount of physical social contact with friends and family, thus putting the elderly at a greater risk of social isolation (Holt-Lunstad, Smith, Baker, Harris & Stephenson, 2015; Olivier, Burls, Fenge & Brown, 2016). Another influencing factor describing why older individuals tend to be more scam vulnerable is because older people may have more savings, which is recognised as a more desirable trait from the perception of scammers (Age UK, 2015). Thus due to the following reasons, studies have shown that people over the age of 64, in particular, are the most vulnerable to fraud (Langenderfer & Shimp, 2001). Consequently, this has led to the development of campaigns which offer wise and informed financial decisions to the general population, for example, the Financial Conduct Authority (FDA, 2014) who developed guidelines which promote ways to become ‘scam smart’ (Olivier et al., 2016).

On the other hand, the notion that older people are more likely to be victims of fraud has been evaluated and reconsidered with time. More specifically, Modic and Lea (2013) discovered younger people were more sceptical of scams although, they are also just as likely to take part as older people. This was demonstrated in an internet fraud study that revealed 33% of students, aged 18 to 21, complied with internet fraud in comparison to 3% of the general population (Modic & Lea, 2013). However, this study may lack reliability because the student sample involved in the experiment were told the study incorporated a scamming scenario prior to participating. Consequently, the results may not be a true representation of the student's response because they may have responded to demand characteristics.

Similarly, research has shown that across all scam types, older consumers were three times less likely to be a victim of fraud in comparison to younger individuals who are disproportionately victimised (Shadel, & Pak 2007; Titus, Heinzelmann & Boyle, 1995). An explanation of this pattern of data may be due to the fact that students typically lack financial funds compared to the general population due to a deficiency of constant income (Norvilitis et al., 2006). Therefore, corresponding to Loewenstein's theory (1996), students would be more likely to comply with scamming because gaining money satisfies their visceral needs. In addition to that, the differing social norms and ethical judgments adopted in online interactions are also likely to influence the fact that younger individuals are more vulnerable in an online environment (Berson, 2000). More specifically, the increased levels of disclosure and lowered inhibition in an online environment contribute to an increased vulnerability in younger people which is less common in an offline setting (Suler, 2004; Webster et al., 2012). Thus, the research presented has revealed that there is contradictory research regarding how scamming vulnerability is influenced by the age of the individual.

1.5 - Online trust

In addition to that, another salient factor that impacts an individual's susceptibility to fraud is the power of online trust. Online trust is defined as a relationship between an online user and their informational or transactional use of the internet (Corritore, Kracher & Wiedenbeck, 2003). Notably, however, prior research on the topic of offline trust has revealed there are some similarities to online trust, although there are some significant distinctions. Within the online world, technology mediates the transaction between the trustor and the trustee, thus increasing its complexity for the trustor (Dutton, 2013, p.269). In addition to that, both a spatial and temporal separation exists between the individuals communicating online which is not the case in offline communication (Dutton, 2013). Thus, there is a greater risk of the individual they are communicating with behaving in an opportunistic manner in comparison to interactions in the offline world. Hence, the role of trust has been perceived to be increasingly important to the online world and is essential in facilitating online transactions and building online relationships (Ridings, Gefen & Arinze, 2002; Turilli, Vaccaro, & Taddeo, 2012).

More specifically, due to the absence of traditional social rules in an online environment, the schemas developed from face-to-face communication cannot be applied to the online world. The anonymity of computer-mediated communication enables scammers to manipulate and strategically edit the information they present, maximising the likelihood that their potential scam victims will view them positively and thus, be more likely to trust them (Joinson & Paine, 2007; Williams, Beardmore & Joinson, 2017, p.413). Consequently, the online world can increase the power of social influence in a negative manner by making individuals more susceptible and vulnerable to manipulation (Whittle, Hamilton-Giachritsis, Beech & Collings, 2013). Furthermore, Gronroos (1994) highlights that the greater uncertainty the customer feels towards the online world, the more influential the component of trust becomes. Thus, research has posed that trust is a significant predictor of whether a customer will be willing to engage in a transaction online (Jarvenpaa, Tractinsky & Vitale, 2000; Yoon, 2002) and it also predicts an individual's likelihood of detecting deception (McCornack & Levine, 1990). Further to this, individuals assume all the people with whom they communicate with are being truthful most of the time, thus they develop a truth bias (DePaulo, Charlton, Cooper, Lindsay, Muhlenbruck, & 1997; Levine, Park & McCornack, 1999). However, if the individual detects deception, the bias reduces considerably yet it increases detection accuracy, thus highlighting the relationship between trust and detecting deception (Blair, Levine & Shaw, 2010; McCornack & Levine, 1990).

Furthermore, demographic differences have been found to influence an individual's level of trust. In particular, research has revealed that men are more trusting of others than women (Riedl, Hubert & Kenning, 2010). Opposed to this view, however, is a study presented by Madathil, Greenstein, and Koikkara (2014) which revealed young, educated females were more likely to trust information online. Hence, demonstrating that there is contradictory research regarding whether there is a relationship between gender and the likelihood of compliance and whether a prediction can be made in relation to which gender is more scam vulnerable.

1.6– Gullibility

Additional arguments that confound the prediction of which gender is more likely to comply with a scam are related to the component ‘gullibility’. The term ‘gullibility’ is defined as the acceptance of a false premise in the presence of untrustworthy cues which demonstrates a sense of vulnerability to being manipulated (Greenspan, 2008; Teunisse, 2016). Yamagishi, Kikuchi, and Kosugi (1999) have established a clear distinction between the two components ‘trust’ and ‘gullibility’. They stated that an individual’s gullibility is dependent upon their insensitivity to information which indicates a sense of mistrust, whereas trust relates to the perceived trustworthiness of an individual (Yamagishi, Kikuchi & Kosugi, 1999). Whereas, Rotter (1980) argues that the level of expectation one has regarding the trustworthiness of others in the absence of evidence describes the term ‘trust’.

With regards to the topic of gullibility, research shows the degree of visceral influence and scamming vulnerability is moderated by gullibility (Langenderfer & Shimp, 2001; Teunisse, 2016). More specifically, low visceral influence combined with high levels of gullibility results in an individual being more vulnerable to scams (Langenderfer & Shimp, 2001). Thus, highlighting the role gullibility has on an individual’s scam vulnerability in combination with visceral influence. Whereas, the combination of high visceral influence and gullibility has minimal impact on scamming vulnerability (Langenderfer & Shimp, 2001).

Moreover, research referring to the component of gullibility has shown that females of all ages were more gullible than males (Preece, & Baxter, 2010). Thus, since studies have shown that gullibility plays an important role in victim behaviour (Garfield, 1994), the assumption that females may be more likely to comply with a scam could be made. As a result, the relationship between gullibility and scamming vulnerability conflicts with the relationship between trust, and risky behaviour with scamming vulnerability in terms of which gender is more likely to comply with the scam.

1.7- Social intelligence

A number of individual differences have also been found to influence an individual’s scamming vulnerability (Grimes, Hough & Signorella, 2007). More specifically, high trust is associated with a greater number of social interactions, consequently, this leads to greater social intelligence (Carter & Weber, 2010). Social intelligence refers to the ability to understand and predict the motives and intentions of others in from an interaction (Pinskar & Mcfarland, 2010). Thus, greater social intelligence improves an individual's ability to recognise scam cues which emphasise that the source is untrustworthy and decreases the likelihood of being scammed (Carter & Weber, 2010). Similarly, Pinsker and McFarland (2010) also agrees with this view and highlights that greater social intelligence is associated with less social vulnerability. Hence, the rise in online transactions has resulted in individuals adapting their offline social intelligence for use in an online environment (Turilli, Vaccaro & Taddeo, 2010).

Research has also demonstrated that high social uncertainty promotes commitment formation (Yamagishi, Cook & Watabe, 1998). Consequently, forming a relationship with an individual provides a person with security which ultimately reduces social uncertainty. However, if the individual continues to apply the positive cognitive bias of trust to all of their potential new relationships, it implies a level of gullibility. The emancipation theory (Yamagishi, 2011) argues that individuals need a good judge of character to determine the trustworthiness of their new potential relationships. Ultimately, this demonstrates that investing in cognitive resources that implement the ability to judge an individual's trustworthiness results in benefits such as the ability to detect deception. Therefore, this shows that there is an interaction between social intelligence and the level of trust and the ability to judge trustworthiness. Consequently, the assumption that high trusters who have a high level of social intelligence are less gullible than low trusters was determined (Yamagishi, Cook & Watabe, 1998). Thus, high trusters in combination with high social intelligence and low gullibility would be less likely to be deceived by scammers.

1.8- Aim, Rationale and Hypotheses

Hence, the present study aims to investigate factors such as age, gender, visceral influence, social intelligence, trust, and gullibility to see how they influence an individual's susceptibility to online fraud through the use of money scamming scenarios and personality tests. Due to the relative infancy of the research in this area, along with the conflicting research on which gender or age alongside the personality factors discussed would impact the likelihood of complying in a scam, it could be advantageous to investigate this topic area to overcome the issues of uncertainty.

To conclude, it is predicted:

(1) There will be a difference in the number of females and males that comply with the scam.

(2) Participants who complete the high visceral scam scenario will be more likely to comply with the scam than those who take part in the low visceral scam scenario.

(3) There will be a difference in the number of younger participants who comply with the scam in comparison to older participants.

(4) Likelihood of compliance will be predicted by:

  (a) Online Trust

  (b) Gullibility – The higher the gullibility score, the greater likelihood of compliance.

  (c) Social intelligence – The higher the social intelligence score, the lower the likelihood of compliance.

Chapter 2 - Method

2.1 – Participants

The sample consisted of 109 participants in total which was made up of students aged 18 to 24 years, and individuals who were 40 years old and older, who were recruited using opportunity and snowballing sampling techniques. The student population was made up of 59 participants with an average age of 20.00 years old (St Dev. = 1.20) and consisted of 35 females and 24 males, recruited from a university in South Wales using a university recruitment system that allowed students to participate in exchange for course credits. The remainder of the sample was made up of individuals over the age of 40 which included 50 participants with an average age of 52.72 years old (St Dev. = 9.93) and an equal number of males and females. The older population was recruited through social media and were personal contacts of the researcher however they did not gain any reward for participating.

2.2 – Design

A between measures design was adopted involving the following independent variables: age, gender, and low/high visceral influence. The dependent variable was the likelihood of compliance on a scale of 1-100%. Additionally, a multiple regression design was used to investigate the relationship between social intelligence, interpersonal trust and gullibility (predictor variables) with the likelihood of compliance (criterion variable).

2.3 - Materials

The present study required two scam emails which were developed from the office of UK Fair trading report on the psychology of scams (Fischer, Lea, & Evans, 2008). One scam email created for the present study obtained a low visceral influence format which included phrases such as "Would you like to become the next stock market millionaire" (Appendices). The second scam email that was developed from a high visceral influence format, for example, "Do **you** want to become the next stock market millionaire?" (Appendices).

Additionally, the program 'Qualtrics' was employed to present a response form which included a compliance scale (0% =strongly disagree, 100%= strongly agree) and questions requesting the participant number, age, and gender of the participant. The questionnaires involved in the present study were also distributed using ‘Qualtrics’, this included the following: the Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014), the Gullibility Scale (Teunisse, 2016) and the Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001).

The Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014)

The Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014) is made up of 28 statements that measure an individual’s online trust score. The questionnaire is scored using a five-point scale where one represents ‘never’ and five represents ‘always’. The scores can range from 28 to 140, the higher the score reveals a higher level of online trust. An example of a question included in the questionnaire is “I do not use social media to tell people where I am”.

With regards to the internal consistency of the Online Trust Behaviour Scale, the scale is still in process of being validated.

The Gullibility Scale (Teunisse, 2016)

The Gullibility Scale (Teunisse, 2016) contains 24 statements which measure multiple facets of gullibility broken down into three categories: persuadable, unsuspecting and unassertive (Table 1).

Table 1: Examples of items from The Gullibility Scale (Teunisse, 2016).

Facet	**Description of facet**	**Example item**
Persuadable	This subscale investigates an individual’s propensity to be manipulated.	“I guess I am more gullible than the average person.”
Unsuspecting	This subscale focuses on feelings of suspicion.	“I’m pretty good at working out when someone is trying to fool me.”
Unassertive	This subscale analyses the inability to assert oneself.	“I have been persuaded to make donations to charities when I couldn’t really afford it.”

The scores of each category are added up to produce an overall gullibility score in which a high score demonstrates a higher level of gullibility. The questionnaire requires the respondent to read each statement, and score on a seven-point scale to indicate how true the statement applies to that particular individual (1= strongly disagree, 7=strongly disagree). The scores can range from 39-273. The internal consistency analysis revealed a Cronbach's alpha score of α = .91 which demonstrates extremely high internal consistency (Teunisse, 2016).

The Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001)

The Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001) presents a 21-item scale that measures multiple facets of social intelligence broken down into three sub-scales: social information processing, social skills and social awareness (Table 2).

Table 2: Examples of items from the Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001).

Facet	**Description of facet**	**Example item**
Social information processing	This subscale measures the ability of understanding verbal and nonverbal messages in regards to human relations.	"I can predict other peoples' behaviour."
Social Skills	This subscale measures the basic communication skills such as active listening, acting boldly, establishing, maintain and breaking up a relationship.	"I often feel uncertain around new people who I don't know."
Social awareness	This subscale measures the ability of active behaving in accordance with the situation, place and time.	"I often feel that it is difficult to understand others' choices."

Each question involves reading a statement regarding areas within social intelligence and answering using a seven point scale (1= extremely poorly and 7= extremely well) based on how well the statement describes the respondent. The scores can range from 21 to 147, the outcome reveals that if the respondent has a high score, they demonstrate high levels of social intelligence and vice versa.

The analysis of the internal consistency for the following subscales: social information processing, social skills, and social awareness revealed that the Cronbach's alpha scores are as follows .80, .79 and .75 respectively (Grieve & Mahar, 2013). Thus highlighting that each subscale holds a satisfactory level of reliability. Lastly, the reliability score for the whole scale revealed .83 Cronbach's alpha score demonstrating that the Tromso Social intelligence scale is a highly reliable source of analysing social intelligence.

2.4 – Procedure

Participants were first introduced to an information sheet and consent form by the researcher. Directing the participants to log onto the email address provided, and completing the study in an isolated room aimed to increase ecological validity by recreating a naturalistic environment for the individual. After giving consent, participants were given the email address and password set up for this experiment to enable them to access the email scenario and told their participant number Participants were then told to log into the email address and read the unread email in the inbox (low or high visceral influence) then click on the Qualtrics link containing the survey questions. Following this, each participant was presented with a scale of 0% to 100% and asked to state on the scale how likely they would be to comply with the scam. Questions regarding participant number, age, and gender of the individual were also requested. In addition, the Gullibility Scale (Teunisse, 2016), the Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014) and the Tromso Social Intelligence Scale (Silvera, Martinussen & Dahl, 2001) were presented in this survey using Qualtrics on the computer. Once the participants had completed the survey, the participants were debriefed.

2.5 - Method of Analysis

The appropriate method of analysis consisted of a three-way ANOVA because the present study aimed to test for a significant difference in data involving three forms of categorical independent groups (age, gender, and low/high visceral influence) and a dependent variable consisting of interval data (likelihood of compliance). Additionally, a multiple regression was used to see if the following variables: social intelligence, interpersonal trust and gullibility (predictor variables) can significantly predict the likelihood of compliance (criterion variable).

Within the process of the multiple regression, the backward stepwise method was selected which allows the assessment of how each predictor variable contributes to the model (Field, 2009).

2.6 - Ethical consideration

Prior to the start of data collection, the present study gained ethical approval from Cardiff Metropolitan University School of Health Science’s ethical committee. Each participant was made aware of their right to withdraw whilst the study took place and they were also reminded that their data would be stored securely and anonymously. The researcher also reassured the participants that the data would only be accessed by the researcher and the research supervisor. There were no major ethical concerns expected with regards to the present study however, contact details were presented on the debrief sheet regarding the appropriate support for any concerns related to fraud.

Chapter 3 – Results

3.1 - Three way ANOVA

A three-way analysis of variance was conducted to analyse the impact gullibility, social intelligence and online trust (independent variables) had on the likelihood of compliance (dependent variable).

Table 3: Descriptive statistics of gender, visceral influence and age with respect to the likelihood of compliance.

	Mean likelihood of compliance	**Standard deviation**	**N**
Female	12.22	17.62	60
Male	10.72	16.57	49
Low visceral influence	7.44	9.17	57
High visceral influence	15.11	17.90	52
18-24 years old (Young)	17.45	19.99	59
40+ year olds (Old)	4.64	13.18	50

During the analysis, the Levene's test for the independent variables age, gender, and visceral influence was significant, therefore this suggests the homogeneity of variance was violated and a transformation was necessary. After the transformation was completed, the outcome revealed the following statistical statement: (F(7,45)=1.602 p=.159).

The main effect for gender yielded an F ratio of F(1,45)= 2.89, p=.096 indicating that there was no main effect between gender and likelihood of compliance (Table 3). This demonstrates that gender does not predict whether an individual would be more or less likely to comply with a scam.

The main effect for age yielded an F ratio of F(1,45)= 7.99 p=.007 indicating a highly significant difference between young participants and older participants in the likelihood of compliance (Table 3). This suggests that younger individuals are more likely to comply with a scam in comparison to older individuals (Figure 1).

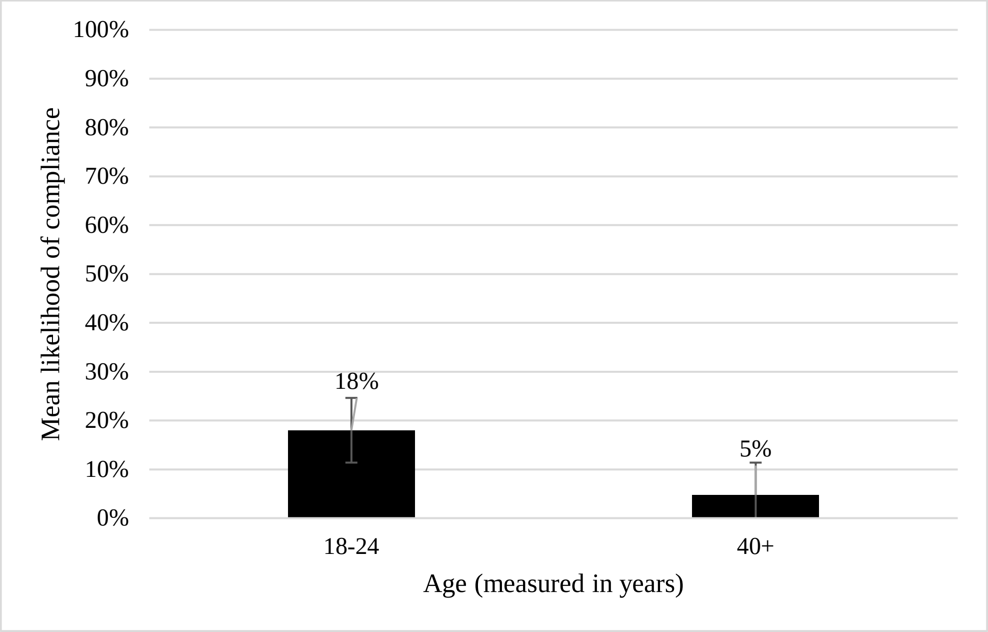


Figure 1: Mean likelihood of compliance for younger (18-24 years) and older participants (40 years and older).

The main effect for visceral influence yielded an F ratio of F(1,45)= 6.36 p=0.013 indicating there was a significant difference between low visceral influence and high visceral influence (Table 2). Consequently, this shows that when scammers manipulate their victims by responding to their visceral needs (high visceral influence), victims are more likely to fall for the scam (Figure 2).

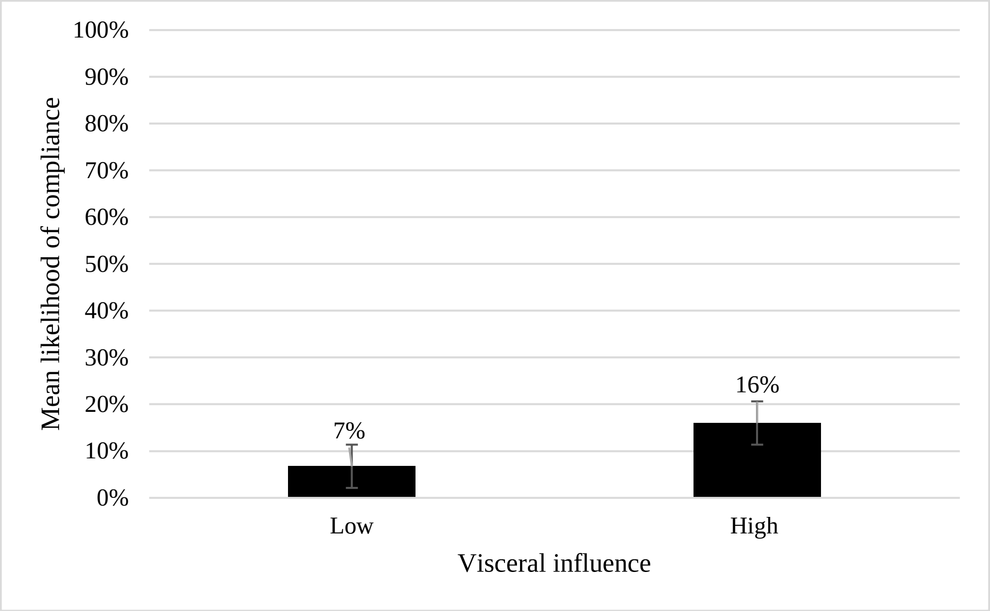


Figure 2: Mean likelihood of compliance for low and high visceral conditions.

The interaction effect, however, was not significant between age, gender, and visceral influence with the mean likelihood of compliance as it yielded an F ratio of F(1,45)= 2.32, p=.135 There was also no significant interaction between age and visceral influence which demonstrated an F ratio of F(1,45)= 0.04 p=.839.

3.2 - Multiple regression

A backwards multiple regression was conducted to see if gullibility, social intelligence and online trust predicted an individual’s likelihood of compliance. The underlying assumptions of the model in relation to residual statistics (Std.Residual Min = -1.38, Std. Residual Max = 3.28), multicollinearity (gullibility: Tolerance = .81, VIF: 1.24; social intelligence: Tolerance = .91, VIF = 1.10; online trust: Tolerance = .87, VIF = 1.15), independent errors (Durbin-Watson value = 1.93) and non-zero variance (gullibility: variance = 516.54, social intelligence: variance = 147.71, online trust: variance = 216.67, compliance: variance = 233.34) were checked and confirmed to be met.

Using the backward stepwise method the analysis found that gullibility, online trust, and social intelligence were significant predictors of the likelihood of compliance (Table 4).

Table 4: Summary of models predicting the significance of variables predicting the likelihood of compliance.

Model	Predictors	F	sig
1	Gullibility, Online Trust, Social Intelligence	3.47	**.019**
2	Gullibility, Online Trust	5.22	**.007**
3	Online Trust	9.70	**.002**

The resultant model however only identified online trust as having a significant impact on compliance as it contributes 8% (Table 5) to the variance ($F_{(1,\ 105)}$ = 9.7, p = .007, R^2 = .09, R^2_{Adusted} = .08).

Table 5: Summary of backward stepwise regression for variables predicting likelihood of compliance.

Variable	**Model 1**			**Model 2**			**Model 3**		
	B	*SE B*	*β*	*B*	*SE B*	*β*	*B*	*SE B*	*β*
Gullibility	.23	.09	.26	.23	.09	.25	.23	.08	.26
Social Intelligence	.07	.23	.03	.06	.22				
Online Trust	.04	.19	.02						
R^2		0.9			.09			.09	
R$^2_{\text{adusted}}$		.07			.07			.08	
F for change in R^2		3.47*			5.22*			9.70*	
*p < .05									

In addition, online trust was also found to be the only variable to significantly predict likelihood of compliance ($t_{(105)} = 3.12$, $p = .002$).

Table 6: Summary of significant predictors of the likelihood of compliance.

Model	**Predictors**	**Beta**	**t**	**Sig.**
1	Online Trust	.26	2.58	**.011**
	Social Intelligence	-.03	-.27	.790
	Gullibility	.08	.76	.448
2	Online Trust	.26	2.60	**.011**
	Gullibility	.09	.87	.386
3	Online Trust	.29	.002	**.002**

Chapter 4- Discussion

4.1- Introduction

The purpose of the present study was to investigate factors including gender, visceral influence, age, online trust, gullibility and social intelligence to see how they can influence or predict an individual's scamming vulnerability through an online money scamming scenario. A key aim of the study was to resolve conflicting research regarding which age group or gender would be more likely to comply with a scam. The present study successfully resolved the issues regarding the relationship between age and the likelihood of compliance as a main effect was significantly determined. However, additional results from the three-way analysis revealed there was no significant effect found between gender and the likelihood of compliance. Further to this, the results also demonstrated a significant difference between visceral influence and the likelihood of compliance. Although, despite the significant difference between age and the likelihood of compliance and visceral influence with the likelihood of compliance, there was no interaction between the two independent variables, age, and visceral influence. Furthermore, the current study also discovered that gullibility, online trust, and social intelligence were significant predictors of the likelihood of compliance. However, using a backwards multiple regression analysis, online trust was the only component analysed that significantly impacted and predicted the likelihood of compliance.

4.2- Summary of findings

The current study presented two forms of investment scams, taking either a low or high visceral approach. Literature within this topic area highlighted that scammers who deliver a scam from a high visceral approach with regards to their victim's visceral needs were more likely to successfully trick their victim (Loewenstein, 1996). Similarly, as predicted the present study found that participants who completed the task involving the high visceral email scam were more likely to comply with a scam in comparison to those who completed the low visceral email scam. This suggests that scammers who employ a high visceral approach to scamming, are more likely to gain an irrational response from their victims that lacks cognitive deliberation, a persuasive technique that increases the success rate for scammers and increases scamming vulnerability of the victims.

Previous findings have demonstrated conflicting research regarding the age of an individual and how this can impact one's likelihood of compliance with a scam. Research relating to health and mobility issues (Age UK, 2015; Holt-Lunstad et al., 2015), predicted older individuals, particularly those over the age of 64 were the most vulnerable age group to fraud (Langenderfer & Shimp, 2001; Lead Fischer & Evans, 2009). Whereas, alternative studies argue younger individuals are more scam vulnerable (Modic & Lea, 2013) due to the impact of one's visceral needs (Loewenstein, 1996) , differing social norms and ethical judgments (Berson, 2000) in an online environment and increased levels of disclosure (Suler, 2004; Webster et al., 2012). Congruous with the results demonstrated by Modic and Lea (2013), the present study also found a significant difference with regards to age and the likelihood of compliance. More specifically, it was found that the individuals aged 18-24 were more vulnerable than the comparison group aged 40 and over. Thus, coinciding with previous research regarding the 'emerging adulthood' theory (Arnett, 2000), the present study demonstrates additional supportive evidence with the prediction that younger individuals in the emerging adulthood stage are more likely to engage in risky behaviour.

Former research has highlighted gender differences within the components of online trust (Madathil, Greenstein & Koikkara, 2010; Riedl, Hubert & Kenning, 2010), risk-taking behaviour (Weber, 2003) and gullibility (Preece, & Baxter, 2010). Hence, due to the relationship between the following factors and scamming vulnerability, it has resulted in an unclear prediction as to which gender is more likely to comply with a scam. However, the present study did not resolve any uncertainty with regards to gender and the likelihood of compliance. This led to the conclusion that gender does not influence scamming vulnerability.

Nonetheless, the components of online trust (Jarvenpaa, Tractinsky & Vitale, 2000; Yoon, 2002), risk-taking behaviour (Weber, Blais & Betz, 2003) and gullibility (Garfield, 1994) have been heavily researched with regards to impacting an individual's likelihood of complying. However, despite the importance of gullibility in the role of victim behaviour (Garfield, 1994), the outcome of the present study did not agree with this statement. More specifically, the results did demonstrate how the combination of gullibility and online trust score impacted the likelihood of compliance, although, analysing the factor alone demonstrated it did not hold enough significant value to impact the outcome of compliance. The present study did, however, demonstrate that online trust alone significantly predicted the likelihood of compliance, thus agreeing with prior research highlighting the importance of online trust in an online environment (Ridings, Gefen & Arinze, 2002; Turilli, Vaccaro, & Taddeo, 2012). Although, this variable only predicted 8% of an individual's likelihood of compliance, which reveals other factors need to be taken into consideration which could hold greater influential value to predicting the likelihood of compliance.

Further to this, research has also highlighted that there are cross-cultural differences within the component of trust and perceived risk (Chong, Yang & Wong., 2003; Park, Gunn & Han, 2012) which may have an impact on scamming vulnerability. More specifically, eastern cultures adopt collectivist values who aim to avoid unpleasant emotions which promote anxiety and fear by avoiding risk, which is contrary to westernised individualistic behaviour (Schimmack, Oishi, & Diener, 2012). An example of this was demonstrated in a study which revealed that Koreans demonstrate a lower tendency to trust (Jarvenpaa, Tractinsky & Saarinen, 1999; Park, Gunn & Han, 2012) and perceive higher levels of risk (Mayer, Davis & Schoorman, 1995). Further to this, collectivist cultures tend to put greater emphasis on trust with regards to shipping and payment in comparison to individualistic cultures (Park, Gunn & Han, 2012). Thus, it could be suggested that the results gathered from the present study represent a westernised, individualistic response to scams; hence it may be beneficial to complete this experiment on a wider range of cultures to obtain a more representative sample.

Although, despite the concept of trust being a widely recognised term, there is also a large amount of disagreement regarding the definition, characteristics, antecedents and the outcomes of trust (Taddeo, 2009). Further to this, the analyses of trust have consistently agreed that it is essential for the development of a social system, however, there has been no explanation regarding why trust plays such a vital role in society (Taddeo, 2009). Consequently, the internet supplies a new dimension of trust to distinguish and define. Thus, due to the complexity and diversity in defining the concept 'trust', it may be beneficial to establish a culturally agreed upon definition, and determine why trust plays a key role in online and offline environments to gather a more comprehensive understanding of how it can impact scamming vulnerability.

Lastly, regarding the findings related to social intelligence, past research demonstrated that social intelligence predicted an individual's ability to detect scam cues (Carter & Weber, 2010). However, the present study demonstrated that social intelligence was not a significant predictor of the likelihood of compliance and it was also the weakest variable to have an effect on the likelihood of compliance. Thus, disagreeing with the present study's prediction that the higher level of social intelligence, the lower the likelihood of compliance. Consequently, the present study clearly demonstrated there was no significant link between social intelligence and scamming vulnerability which, therefore, disagrees with the assumption that social intelligence improves an individual's ability to detect cues (Carter & Weber, 2010).

4.3 – Limitations and future research

However, the magnitude of the effects of these different factors and how they interact with the other factors has not been explored. More specifically, the present study tested the relationship between the three personality factors analysed and how they predicted the likelihood of compliance in conjunction with one another, however, they were not compared to the demographic factors researched. For example, there may be a relationship between age and a personality trait which may or may not have a greater impact on an individual's scamming vulnerability in comparison to solely looking at the influence of age alone on scamming vulnerability. Thus, additional research could be conducted to analyse the interactions between all of the factors for a better knowledge and understanding on how the factors can influence scamming vulnerability.

The outcome of the present study could have beneficial implications regarding the study of persuasion in an online environment, specifically towards the topic of internet fraud. With the knowledge gained from the present study, in conjunction with prior investigations related to online fraud, it may benefit the media in producing more effective and targeted mitigations on the topic of online financial safety. Consequently, if this step towards reducing the issues relating to financial decisions is successful, it will hopefully improve society's financial awareness and decision making in an online environment. Hence, examining the most effective method of distributing information concerning online fraud with the expanding knowledge within this area, may also help reduce the issue of consumer fraud.

In relation to this point, the analysis of previous literature has revealed that to raise awareness about a risk-related product or situation, the media needs cater their advertisements to elicit increased motivation activation, which promotes resources to be automatically stored, hence the information is more likely to be internalised (Lang, Chung, Lee & Zhao, 2005). Further to this, research has also suggested that high-sensation seekers are motivated by novel and arousing content (Aluja-Fabregat & Torrubia-Beltri, 1998; Krcmar & Greene, 1999). Hence, due to the fact that younger people are higher sensation seekers (Arnett, 2000; CEOP, 2010) in comparison to older individuals, as well as being more scam vulnerable according to results from the present study, it is suggested that the media could target the issue of younger individuals being more scam vulnerable by presenting messages holding high sensation value (Lang, 2006).

4.4 – Conclusion

To summarise, through the investigation of which factors influence scamming vulnerability using an online money scamming scenario, results revealed that younger individuals, as well as the participants who completed the high visceral formatted scam, were more likely to comply with a scam. Although, it should be noted that there was no interaction between age and visceral influence with respect to the likelihood of compliance. In addition to that, the component 'online trust' was also the most significant variable in predicting the likelihood of compliance.

Chapter 5 - References

Age, U. K. (2015). Later life in the United Kingdom. London: Age UK.

Aluja-Fabregat, A., & Torrubia-Beltri, R. (1998). Viewing of mass media violence, perception of violence, personality and academic achievement. *Personality and Individual Differences*, *25*(5), 973-989.

Anderson, R. J. (2010). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.

Arnett, J. J. (2000). Emerging adulthood: A theory of development from the late teens through the twenties. American psychologist, 55(5), 469.

Australian Competition., & Consumer Commission. (2012). *Targeting Scams: Report of the ACCC on Scam Activity 2011*. The Commission.

Berson, M. J. (2000). The computer can't see you blush. Kappa Delta Pi Record, 36(4), 158-162.

Blair, J. P., Levine, T. R., & Shaw, A. S. (2010). Content in context improves deception detection accuracy. Human Communication Research, 36(3), 423-442.

Campbell, K. (2007). The Fraud Act 2006. King's Law Journal, 18(2), 337-347.

Carter, N. L., & Mark Weber, J. (2010). Not Pollyannas: Higher generalized trust predicts lie detection ability. Social Psychological and Personality Science, 1(3), 274-279.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of personality and social psychology, 39*(5), 752.

Child Exploitation and Online Protection Centre [CEOP] (2010). Strategic overview 2009–2010. Retrieved February 22, 2011

Chong, B., Yang, Z., & Wong, M. (2003). Asymmetrical impact of trustworthiness attributes on trust, perceived value and purchase intention: a conceptual framework for cross-cultural study on consumer perception of online auction. In *Proceedings of the 5th international conference on Electronic commerce* (pp. 213-219). ACM.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. International journal of human-computer studies, 58(6), 737-758.

Danner, P. (2000). Old fraud, new medium. Broward Daily Business Review, 9.

DePaulo, B. M., Charlton, K., Cooper, H., Lindsay, J. J., & Muhlenbruck, L. (1997). The accuracy-confidence correlation in the detection of deception. Personality and Social Psychology Review, 1(4), 346-357.

Dutton, W. H. (Ed.). (2013). The Oxford handbook of internet studies. Oxford University Press.

Earl, J. K., Gerrans, P., Asher, A., & Woodside, J. (2013). Investigating the influence of cognitive decline on the quality of financial decision-making in older adults: The case of self-managed superannuation funds.

Fischer, P., Lea, S., & Evans, K. (2008). The Psychology of Scams: Provoking and Commiting Errors of Judgement. Research for the Office of Fair Trading. In (draft 2 ed., pp. 56). Exeter, UK: University of Exeter.

Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060-2072.

Fletcher, E., & Pessanha, R. (2016). Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education. Houston: Page Publishing, Inc

Garfield, B. (1994). Ghetto of gadgets, get-rich schemes. Advertising Age,8-16.

Greenspan, S. (2008). *Annals of Gullibility: Why We Get Duped and How to Avoid It: Why We Get Duped and How to Avoid It*. ABC-CLIO.

Grimes, G. A., Hough, M. G., & Signorella, M. L. (2007). Email end users and spam: relations of gender and age group to attitudes and actions. Computers in Human Behavior, 23(1), 318-332.

Gronroos, C. (1994). From marketing mix to relationship marketing: Towards a paradigm shift in marketing. Asia-Australia Marketing Journal, 2(1), 9-29.

Holt-Lunstad, J., Smith, T. B., Baker, M., Harris, T., & Stephenson, D. (2015). Loneliness and social isolation as risk factors for mortality: a meta-analytic review. Perspectives on Psychological Science, 10(2), 227-237.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, *5*(2), JCMC526.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. Information technology and management, 1(1-2), 45-71.

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. Handbook of personality: Theory and research, 2(1999), 102-138.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. Oxford handbook of Internet psychology, 237-252.

Kremar, M., & Greene, K. (1999). Predicting exposure to and uses of television violence. *Journal of communication*, *49*(3), 24-45.

Lang, A. (2006). Using the limited capacity model of motivated mediated message processing to design effective cancer communication messages. *Journal of communication*, *56*(s1).

Lang, A., Chung, Y., Lee, S., & Zhao, X. (2005). It's the product: Do risky products compel attention and elicit arousal in media users?. *Health Communication*, *17*(3), 283-300.

Langenderfer, J., & Shimp, T. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. Psychology And Marketing, 18(7), 763-783.

Lea, S. E., Fischer, P., & Evans, K. M. (2009). The psychology of scams: Provoking and committing errors of judgement.

Levine, T. R., Park, H. S., & McCornack, S. A. (1999). Accuracy in detecting truths and lies: Documenting the “veracity effect”. Communications Monographs, 66(2), 125-144.

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. Organizational behavior and human decision processes, 65(3), 272-292.

Madathil, K. C., Greenstein, J. S., & Koikkara, R. (2014, September). An Investigation of the Factors that Predict a Healthcare Consumer’s Use of Anecdotal Healthcare Information Available on the Internet. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 604-608). Sage CA: Los Angeles, CA: SAGE Publications.

Marcella, A. J. (1999). Establishing trust in virtual markets. Institute of Internal Auditors.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

McCornack, S. A., & Levine, T. R. (1990). When lies are uncovered: Emotional and relational outcomes of discovered deception. Communications Monographs, 57(2), 119-138.

Miller, M. J., &Weitman, C. J. (1992). The relationship between dogmatism and gullibility among counselors-in-training: An exploratory study. College Student Journal, 26, 205–208.

Mishna, F., McLuckie, A., & Saini, M. (2009). Real-world dangers in an online reality: A qualitative study examining online relationships and cyber abuse. Social Work Research, 33(2), 107-118.

Modic, D., & Lea, S. (2013). Scam Compliance and the Psychology of Persuasion. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.2364464

Norvilitis, J. M., Merwin, M. M., Osberg, T. M., Roehling, P. V., Young, P., & Kamas, M. M. (2006). Personality factors, money attitudes, financial knowledge, and credit-card debt in college students. Journal of Applied Social Psychology, 36(6), 1395-1413.

Office of Fair Trading (2006) Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers, Office of Fair Trading, London

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2016). Safeguarding adults and mass marketing fraud–Perspectives from the police, trading standards and the voluntary sector. *Journal of Social Welfare and Family Law*, *38*(2), 140-151.

Park, J., Gunn, F., & Han, S. L. (2012). Multidimensional trust building in e-retailing: Cross-cultural differences in trust formation and implications for perceived risk. *Journal of Retailing and Consumer Services*, *19*(3), 304-312.

Pinsker, D. M., & McFarland, K. (2010). Exploitation in older adults: Personal competence correlates of social vulnerability. *Aging, Neuropsychology, and Cognition*, *17*(6), 673-708.

Pinsker, D. M., Stone, V., Pachana, N., & Greenspan, S. (2006). Social Vulnerability Scale for older adults: Validation study. *Clinical Psychologist*, *10*(3), 109-119.

Preece, P. F., & Baxter, J. H. (2000). Scepticism and gullibility: The superstitious and pseudo-scientific beliefs of secondary school students. International Journal of Science Education, 22(11), 1147-1156.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. The Journal of Strategic Information Systems, 11(3-4), 271-295.

Riedl, R., Hubert, M., & Kenning, P. (2010). Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. Mis Quarterly, 34(2), 397-428.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American psychologist*, *35*(1), 1.

Schimmack, U., Oishi, S., & Diener, E. (2002). Cultural influences on the relation between pleasant emotions and unpleasant emotions: Asian dialectic philosophies or individualism-collectivism?. *Cognition & Emotion*, *16*(6), 705-719.

Shadel, D. P., & Pak, K. B. S. (2007). The psychology of consumer fraud. Unpublished PhD dissertation, Tilburg University..

Silvera, D., Martinussen, M., & Dahl, T. I. (2001). The Tromsø Social Intelligence Scale, a self-report measure of social intelligence. Scandinavian journal of psychology, 42(4), 313-319.

Strack, F., & Neumann, R. (1996). "The Spirit Is Willing, but the Flesh Is Weak": Beyond Mind–Body Interactions in Human Decision-Making. Organizational Behavior and Human Decision Processes, 65(3), 300-304.

Suler, J. (2004). The online disinhibition effect. Cyberpsychology & behavior, 7(3), 321-326.

Taddeo, M. (2009). Defining trust and e-trust: from old theories to new problems. *International Journal of Technology and Human Interaction*, *5*(2), 23.

Taylor-Jones, S. & Graff, M. (2014). The development and validation of an online interpersonal trust scale. Unpublished manuscript, Department of Psychology, Early Years and Therapeutic Studies, University of South Wales, Pontypridd, UK

Teunisse, A. (2016). Gullibility: a review of the literature and devising a self-report measure.

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. Crime & Delinquency, 41(1), 54-72.

Trumbo, C. W. (2002). Information processing and risk perception: An adaptation of the heuristic-systematic model. *Journal of Communication*, *52*(2), 367-382.

Turilli, M., Vaccaro, A., & Taddeo, M. (2010). The case of online trust. *Knowledge, Technology & Policy*, *23*(3-4), 333-345.

Turilli, M., Vaccaro, A., & Taddeo, M. (2012). Internet neutrality: Ethical issues in the internet environment. Philosophy & Technology, 25(2), 133-151.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *science*, *185*(4157), 1124-1131.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 0093650215627483.

Weber, E. U. (2003). Domain-Specific Risk Taking. Updated version of Weber, Blais, Betz (2002). Journal of Behavioral Decision Making.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T.,& Milazzo, V. (2012). European online grooming project (Final report). Retrieved from the European Online Grooming Program

West, D. C., Kover, A. J., & Caruana, A. (2008). Practitioner and customer views of advertising creativity: Same concept, different meaning?. *Journal of Advertising*, *37*(4), 35-46.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. Aggression and violent behavior, 18(1), 135-146.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology, 53(4), 665-684.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. Computers in Human Behavior, 72, 412-421.

Worobec. K. (2017). Fraud the facts 2017 (p. 24). London: Financial Fraud Action UK.

Wright, P. L. (1985). Schemer schema: Consumers' intuitive theories about marketers' influence tactics. In R. J. Lutz (Ed.), Advances in consumer research (Vol. 6, p. 1 – 3). Association for Consumer Research

Yamagishi, T. (2011). *Trust: The evolutionary game of mind and society*. Springer Science & Business Media.

Yamagishi, T., Cook, K. S., & Watabe, M. (1998). Uncertainty, trust, and commitment formation in the United States and Japan. *American Journal of Sociology*, *104*(1), AJSv104p165-194.

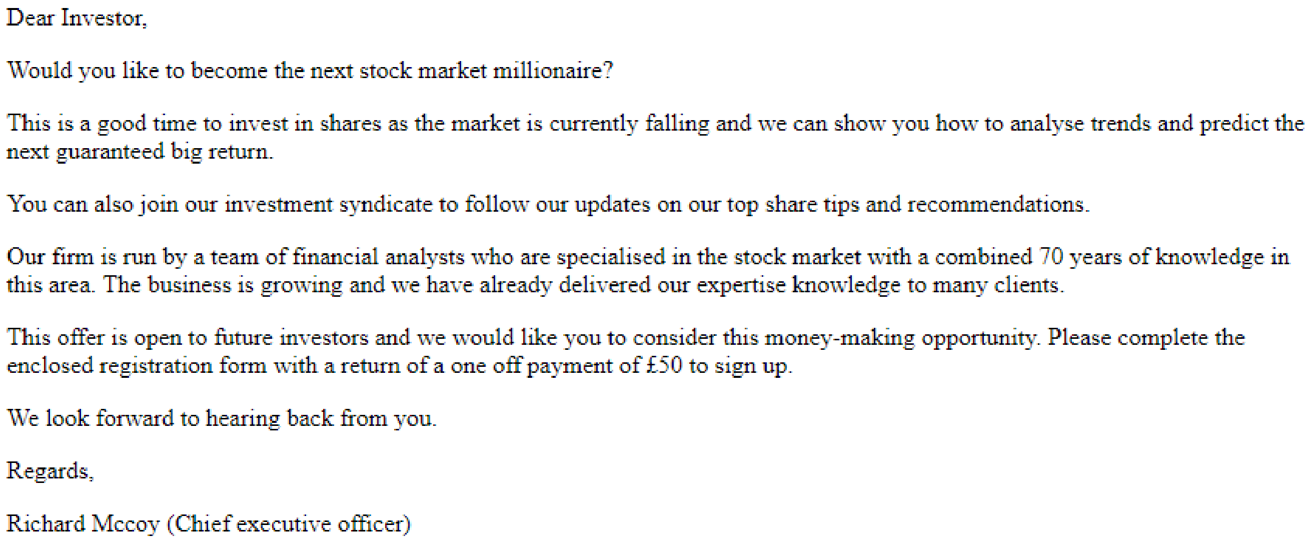
Yamagishi, T., Kikuchi, M., & Kosugi, M. (1999). Trust, gullibility, and social intelligence. Asian Journal of Social Psychology, 2(1), 145-161.

Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of interactive marketing*, *16*(2), 47-63.

Zuckerman, M. (1994). Behavioral expressions and biosocial bases of sensation seeking. Cambridge university press.

Chapter 6 – Appendices

6.1 – Low visceral scam email



Dear Investor,

Would you like to become the next stock market millionaire?

This is a good time to invest in shares as the market is currently falling and we can show you how to analyse trends and predict the next guaranteed big return.

You can also join our investment syndicate to follow our updates on our top share tips and recommendations.

Our firm is run by a team of financial analysts who are specialised in the stock market with a combined 70 years of knowledge in this area. The business is growing and we have already delivered our expertise knowledge to many clients.

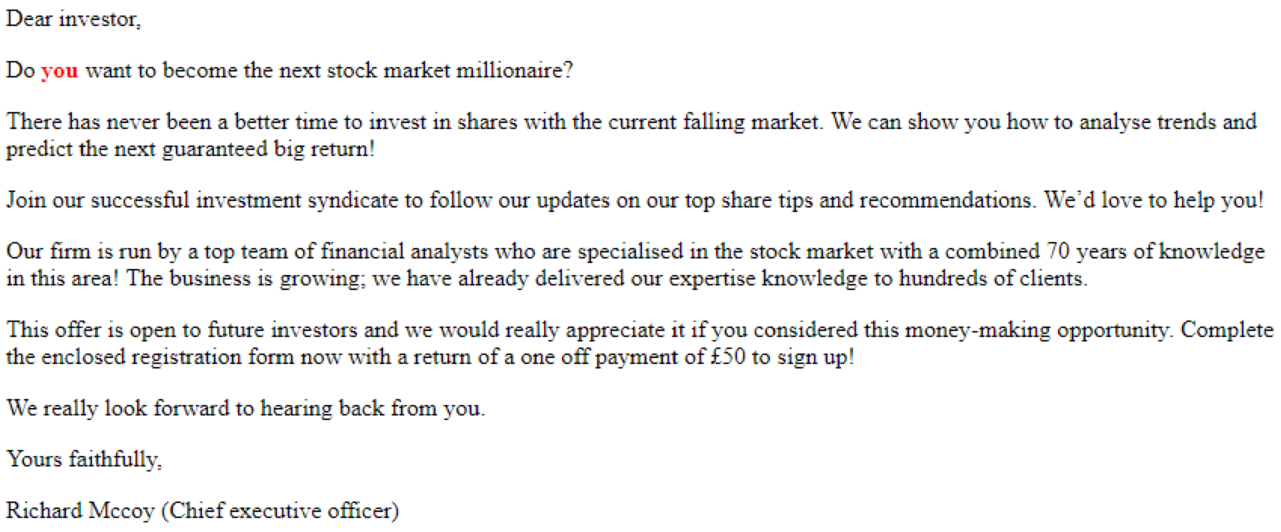
This offer is open to future investors and we would like you to consider this money-making opportunity. Please complete the enclosed registration form with a return of a one off payment of £50 to sign up.

We look forward to hearing back from you.

Regards,

Richard Mccoy (Chief executive officer)

6.2 – High visceral scam email



Dear investor,

Do **you** want to become the next stock market millionaire?

There has never been a better time to invest in shares with the current falling market. We can show you how to analyse trends and predict the next guaranteed big return!

Join our successful investment syndicate to follow our updates on our top share tips and recommendations. We'd love to help you!

Our firm is run by a top team of financial analysts who are specialised in the stock market with a combined 70 years of knowledge in this area! The business is growing; we have already delivered our expertise knowledge to hundreds of clients.

This offer is open to future investors and we would really appreciate it if you considered this money-making opportunity. Complete the enclosed registration form now with a return of a one off payment of £50 to sign up!

We really look forward to hearing back from you.

Yours faithfully,

Richard Mccoy (Chief executive officer)

6.3 – Online Trust Behaviour Scale (Taylor-Jones & Graff, 2014)

Please indicate, on the scale provided, how often you do the following when using the internet:

		Never	Rarely	Sometimes	Frequently	Always
1	I do not use social media to tell people where I am	1	2	3	4	5
2	I update my status and post photos using social media when I am on holiday	1	2	3	4	5
3	I keep the location services on my mobile phone activated	1	2	3	4	5
4	I take websites at “face value” when I browse/shop online	1	2	3	4	5
5	I keep a record of the IMEI (International Mobile Equipment Identity) number of any mobile phone I own so I can prove my ownership if it is stolen	1	2	3	4	5
6	I am cautious when prompted to save my details on websites	1	2	3	4	5
7	I am totally honest about myself when using online instant messaging facilities to talk to other people	1	2	3	4	5
8	I avoid clicking on “pop ups” regardless of the product/service being advertised	1	2	3	4	5
9	I password protect my mobile phone to keep it secure	1	2	3	4	5
10	I save my details on websites when prompted	1	2	3	4	5
11	I keep people I have met online at a distance and avoid giving them many personal details	1	2	3	4	5
12	I provide contact details when prompted on the internet	1	2	3	4	5
13	I only download information onto my mobile phone from trusted websites	1	2	3	4	5
14	I only upload holiday photos when I have returned home	1	2	3	4	5

15	I check the security of a website that I am buying products/services from before providing my details	1	2	3	4	5
16	I am careful with how much I tell people about myself even though online instant messaging facilities are anonymous	1	2	3	4	5
17	I check the credibility of a website before using it for the first time	1	2	3	4	5
18	I only buy products/services online from well-known reputable suppliers	1	2	3	4	5
19	I assume the websites I use to buy products/services from are secure	1	2	3	4	5
20	I read the terms and conditions before agreeing to buy/download something on the internet	1	2	3	4	5
21	I am careful with what I say when chatting with others online	1	2	3	4	5
22	I trust the person I am talking to when using online instant messaging facilities	1	2	3	4	5
23	I save passwords when prompted to do so by Internet Explorer	1	2	3	4	5
24	I ensure that the location services on my mobile are turned off when I don’t need them	1	2	3	4	5
25	I avoid using social media to tell people when I won’t be home	1	2	3	4	5
26	I keep the passwords I use private and avoid saving them online	1	2	3	4	5
27	I ensure that the photos I upload to mobile social networking sites remain private	1	2	3	4	5
28	I choose how I want to present myself to others when using online instant messaging facilities	1	2	3	4	5

Word Count:

Abstract:	271
Introduction:	3223
Method:	1393
Results:	723
Discussion:	1724
Total:	7063

Signed: ___________

Date: 20/04/18