Investigating the relationship between consumers' style of thinking and online victimization in scamming

Francesco Sofo
University of Canberra
Australia
Francesco.sofo@canberra.edu.au

Michelle Berzins
University of Canberra
Australia
Michelle.berzins@canberra.edu.au

Salvatore Ammirato
University of Calabria, Italy
ammirato@deis.unical.it

Antonio P. Volpentesta
University of Calabria, Italy
volpentesta@deis.unical.it

doi: 10.4156/jdcta.vol4.issue7.4

Abstract

Unsolicited emails and online scams can erode both consumer confidence and consumer safety when interacting and transacting over the Internet. This paper uses content analysis to identify the most frequent psychological tricks used in scamming and the most frequent flags which alert consumers to the illegitimate and unsolicited nature of the contact. Findings are then explored in light of individual thinking styles to reveal how some consumers may be more vulnerable to online scams as a result of their own personal preference for thinking in a particular way. The rationale is to establish a foundation for the use of content analysis of unsolicited emails to offer insight into the possible relationship between a consumer's style of thinking and online victimization.

Keywords*: Thinking style, Scam, Spam, Online victimization, Consumer*

1. Introduction

Online interactions and online transactions are a factor of modern life. With even the most basic of internet connections, people are able to shop, date, gamble and chat online. There are countless benefits to Internet-based services including cost effectiveness, timeliness, accessibility, speed and convenience (Krone & Johnson, 2007). Despite these benefits, the presence of unsolicited emails and online scams [1] can erode both consumer confidence and consumer safety when interacting and transacting over the Internet.

Cyber-crime is said to be those criminal acts that are transformed by networked technologies (Wall, 2004), and crimes such as fraud that were traditionally executed in person or using paper are now being carried out over the seemingly anonymous environment of the Internet. A range of psychological and technological tricks are used to illegitimately gain the confidence and trust of individuals engaging in online interactions, thus consumer education regarding safe Internet use is essential to protect users while interacting and transacting online.

Globally, the war against online scams is not only an individual concern but also a social concern. People are not alone in their efforts to combat online scams, and both national governments and multinational organizations are trying to make online transactions more secure. Legislative acts such as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM act) are fundamental milestones to building a shared legal framework to combat spam. However, as Congress found when enacting CAN-SPAM, the spam problem cannot be solved by legislation alone, and technological approaches and international cooperation are key to enhancing the effectiveness of legislative approaches (Federal Trade Commission, 2005).

Using predetermined hypotheses, this study attempts to identify the most frequent psychological tricks used in scamming and the most frequent flags which alert consumers to the illegitimate and unsolicited nature of the contact. This paper explores the content of a sample of unsolicited email to

[1] Wikipedia.org defines scam as "an attempt to defraud a person or group by gaining their confidence".

ascertain some of the emerging trends in online interactions and transactions. These findings are then explored in light of individual thinking styles to reveal how some consumers may be more vulnerable to online scams as a result of their own personal (and sometimes subconscious) preference for thinking in a particular way. The paper commences with a review of the literature, including an overview of the effects of online scams, and a thinking style inventory (Sofo, 2008) that has face validity for further analysis of the data. By first exploring the relevant literature and defining the key terms, the context of the study is established and a foundation is laid for the use of content analysis to examine the unsolicited emails.

2. Literature review

Computer technology is used on a daily basis to facilitate the planning and implementation of criminal activity. Online scams are varied, and can include offers to purchase cheap products such as pharmaceuticals or replica goods, romance scams, requests to launder money under the guise of a legitimate offer of employment as well as get rich quick schemes.

Scams have existed for a long time, with some of the earliest scams being advance fee frauds where individuals pretended to sell something they did not have, while taking money in advance from their victims. While these types of scams were initially transmitted via post and facsimile, the early 1990s saw a proliferation of their circulation due to the speed and ease with which they could be transmitted via the Internet by individuals throughout the world (Holt & Graves, 2007). This proliferation has had two noticeable effects: first, a decline in consumer confidence levels, and second, increased reports of monetary loss as a result of scam activity.

In numerous parts of the world such as Australia, the United Kingdom, United States of America and the European Union, scams are causing substantial economic damage. Hannaford (2010) states that online interactions and online transactions cost Australian consumers at least AUS$69 million during 2009. Hannaford (2010) notes that the figures show a dramatic spike in both the amount of money being lost every year to fraud and the number of victims, with more than 20,000 people nationally reporting losses to consumer protection authorities. Fraudsters are also targeting the elderly, with victims in the United Kingdom losing a combined total of approximately £3million of life savings every six months (Ward, 2004). Indeed, the cost of identity theft to Australian businesses is over AUS$1 billion per year (Debus, 2008), with advance fee frauds alone costing Australian consumers between AUS$170 million and AUS$680 million per year (Bowen, 2008). By comparison, it has been estimated that around ten million Americans were victims of identity theft, with a total cost of approximately US$50 billion within a single year (Sarel & Marmorstein, 2006). A study of the European Union's Internal Market Commission estimated in 2001 that "junk e-mail" cost Internet users €10 billion per year worldwide (European Commission, 2001); furthermore the California legislature found that spam cost United States organizations alone more than $13 billion in 2007, including lost productivity and the additional equipment, software, and manpower needed to combat the problem (California Law, 2007).

A popular method by which scams are transmitted is via unsolicited bulk email or ‘spam’. Spam has been defined by the Australian Institute of Criminology (2005) as an electronic version of junk mail. These electronic mailouts are sent to a large number of people without their prior consent, and typically contain information about products or services in which the recipient may have no interest. An email message is therefore said to constitute spam when it has not been requested nor has it been sent by a sender who is known to the recipient (Holt & Graves, 2007).

A key characteristic of spam is that it is sent in high volumes during short periods of time (Calais et al., 2007). It was estimated that over time, spam would account for 60% of all emails received by companies (Gartner Inc, 2003), and Vaile (2004) found that 50% of all electronic mail is classified as ‘spam’. The scientific literature is lacking in quantitative studies concerning how successful spam campaigns are and to what degree they are profitable. According to Kanich et al. (2009), “spammers do not file quarterly financial reports, and the underground nature of their activities makes third-party data gathering a challenge at best”. Even if conducting quantitative studies in the sector is difficult, the increasing number of frauds due to spam activities raises an interesting question regarding the profitability of spam campaigns. Australian researchers estimate that between one and five percent of consumers in western countries are victimised by scams (Smith, 2007). Given that an estimated 1,000-

million scam emails are sent worldwide every year, the potential to extract enormous amounts of money is quite high – as shown by the losses reported above. Judge and Aplerovitch (2005) hypothesize that a response rate to spam emails equal to 0.000001% is enough for profitability of the mean. Kanich et al. (2009) experimented that on 350,000,000 spam emails sent, only 28 frauds resulted; but they proved that even the conversion rate is well under 0.000001%. Under determined conditions, this can still be profitable. This leads to the conclusion that sending as much spam as possible is likely to maximize profit (Goodman & Rounthwaite, 2004).

Few studies have examined the structure or content of spam messages to ascertain whether there are any specific patterns that might increase the likelihood of a victim responding to the sender (Holt & Graves, 2007). One recent study monitored the traffic data of incoming email for an eight week period finding that the first letter of the recipient's email address made a difference to the proportion of incoming spam (Clayton, 2008). Another study monitored the clustering behaviour of spammers in an effort to identify some anti-spam strategies (Li & Hsieh, 2006). Spam and scams are designed to be persuasive, and there is no current literature that theorises about the effect of thinking style on a consumer's response to unsolicited email. The links between spam and thinking style may be argued to be arbitrary and largely subjective, but it is possible to at least speculate about those links without the support of formal assessment.

A theory that links thinking style and online solicitations is therefore presented below in an effort to explore whether future work in this area may be warranted. To begin, it is necessary to define what is meant by 'thinking style'. Thinking style is an influential part of decision making and particular preferences for thinking and acting may lead to increased vulnerability and susceptibility to online scams. Thinking style is a unique human characteristic emerging as a distinctive construct which bridges intelligence and personality, and has been conceptualized as three broad categories which include cognition, personality and learning theories (Tang, 2003). Overall these approaches to thinking style represent an historical analysis of the field in its infancy and the theories are not clear on whether thinking style is a cognitive predisposition, a preferential personality trait or a bias for learning in a particular way.

Thinking style bridges many domains including cognitive, affective, psychomotor, physiological, psychological and sociological realms (Sofo, 2008). Style of thinking is said to be both cognitive and affective in essence. It is cognitive because information is processed, and it is affective because one's feelings are involved in using a preferred way of thinking (such as welcoming or avoiding various aspects including authority, conformity, structure, ambiguity, reflectivity and impulsivity). In a more integral sense, style of thinking is 'affective' since it refers to preferred thought processes and our most comfortable ways of thinking. Thinking style has psychomotor and physiological dimensions because one's nervous system and senses are involved in how information is preferred to be perceived and processed. It is psychological because the choice includes preferential interaction of one's personality with the context (Sofo, 2008). To the extent that the context is social, then style is also sociological because it is contingent on preferred crossing points with others. It is therefore evident that style of thinking is a social whole-person preference involving more than the brain alone but also involving one's creative sense of intuition and feeling.

Since style of thinking accounts for at least half of one's successful interactions and achievements, with IQ accounting for the other half (Sternberg, 1997), it can be inferred that preferences for ways of thinking impact on one's response to stimuli including unsolicited emails. Thinking style profiles constitute basic processes underlying problem-solving and decision-making and have a major impact on the outcomes (Zhang, 2004). Thinking style profiles can be measured through specific inventories designed to test the preferences of an individual. The theory of reality construction is a general theory that under-emphasizes the principles of societal or mental self-government and focuses on dimensions of dependence, inquiry, multiple perspectives, autonomy and imagery (Sofo, 2005). The validated Thinking Styles Inventory (TSI) emanates from a theory of how people create their reality through their thinking and measures reported preferences for stylistic aspects of intellectual functioning. The name of the theory of reality construction emanates from constructivist theory where exists the idea that people actively construct their reality from their social interactions which are based on personally preferred ways of thinking.

Interpersonal responses or interactions are based on how people like to think about problems. Sofo's (2005) theory of reality construction is a meta-cognitive perspective that underpins five styles of

thinking. The basic assumption inherent to the styles shown in Table 1 is that people have preferences and different degrees of confidence and control in how they use their knowledge, attitudes and mental skills in building their reality and in dealing with information, people, tasks and daily situations through their thought processes.

Table 1. Summary of the five thinking styles (Sofo, 2008).

1. Conditional	Accepting what others think and say without questioning them.
2. Inquiring	Asking questions to improve understanding of message or information.
3. Exploring	Looking for alternatives and difference.
4. Independent	Allocating priority to one's own thinking.
5. Creative	Thinking in pictures to get a sense of the whole.

In the conditional style of thinking, individuals are said to strongly rely on, and accept, what others think and say without questioning which creates a personal reality based on a predominantly convergent thinking. In terms of spam and online scams, conditional thinkers would be the most gullible and the most likely to respond to requests to send their personal details or to click on a link without questioning the safety or legitimacy of the site. Conditional thinkers are said to enjoy rules and to gain comfort from approval processes, but this in turn may lead them to respond to a stimulus without question. They would have a relatively high level of impulsivity towards obeying norms.

When people prefer to ask questions and inquire about feelings and solutions, they are said to be co-constructing their reality through preferring to use an inquiring style of thinking. Consumers possessing a preference for an inquiring style of thinking may be inquisitive and ask questions such as "What is this email?" and "Who is sending me this?" If the consumer's questions are answered within the email itself, and a source of legitimacy is found (such as a claimed affiliation with a known bank or other organization), then the consumer may feel satisfied with their level of inquiry and thus respond to the unsolicited email.

When people explore feelings and seek multiple perspectives they are constructing their reality through an exploring style of thinking. These consumers may be attracted to the idea or offer contained in the email, but they might take the time to explore all their options and seek different explanations to appreciate the unsolicited correspondence in a different way. For example, the exploring thinker may see that the email requires immediate reply via email, but the consumer may choose to seek out alternative methods of replying that do not involve online interaction. They would tend not to react impulsively but maintain a locus of control while options were identified.

Allocating priority to one's own thinking and relying on one's own feelings, solutions and opinions is said to be a preference for an independent style of thinking. When thinking about scams and spam, the independent thinker may stop to think about how they are feeling about this unsolicited contact and they may apply some meta-cognition to think about the thinking. Independent thinkers also look for alternatives and thus critical thinking may be applied whereby the individual views the correspondence from multiple perspectives prior to making a decision. Their response would tend to be impulsive, but anti-norm and non-conformist unless the norms suited their proclivity.

Individuals who have a preference for thinking in pictures, visualizing and imagining in order to obtain a sense of reality are said to have a creative style of thinking. These consumers would stop to imagine the scenario of winning the lottery, or of making a very cheap purchase online, but they may also stop to picture the consequences of responding hastily to an unsolicited email.

It is important to note that a person with a particular preference in one circumstance may have a different inclination in another situation which means that people may be flexible and adaptive in their thinking. Also, whilst individuals may show a preference for a particular style of thinking, it is their complete thinking style profile that will dictate the way in which decisions are made. The key assumption in Sofo's theory of reality construction is that people can be located within a mix of thinking preferences, ranging from conditional to creator, dependent on the characteristic mode in which they solve problems, create or make decisions. Without doubt, all thinking styles are potentially useful – the challenge is to utilize a style that works best for a person in each situation. A situation is dominated by the demands placed by outside influences such as the law, social expectation, issues of

safety and expediency. Other influences may include and demands of a profession, how those in charge of a situation expect subordinates to behave and pressures that individuals may impose on themselves.

As noted by Sternberg (1997), thinking style is at least partly socialized because the environment can influence the style that a person prefers to use. This point is particularly important to this exploration, as the online environment presents the consumer with fewer stimuli through which informed decisions can be made. For example, when interacting and transacting online, there is an absence of face-to-face interaction between the scammer/spammer and the target (Cameron & Galloway, 2005). There are also a number of psychological traps which work to manipulate the recipient's belief as to the legitimacy of the unsolicited email, and it has been shown that legitimacy can erroneously be inferred through claimed credibility and assumed affiliation (UKOFT, 2009). Techniques include choosing legitimate-sounding names in order to improve credibility, or to adopt domain names that contain the names of local cities in order to improve the marketability and credibility of the contact with a person in another country. Email and internet addresses can therefore be manipulated to include information which helps mislead the recipient into thinking that the correspondence is legitimate (Berzins, 2010). It is therefore evident that the relationship between thinking styles and online consumer behavior is worthy of exploration, and there is potential for consumers' online behavior to become more informed and better understood if a relationship between the two can be shown.

3. Methodology

Documents and written communication are key ways in which reality is constructed. For this reason, documented communication constitutes a good starting point from which research and analysis can be conducted (Prior, 1997). This paper seeks to use aspects of three analytical frameworks as bases for interpreting the data:

- Cialdini's (2006) weapons of influence
- Sofo's (2008) thinking style inventory and theory of reality construction, and
- Holt and Graves' (2007) study into the characteristics of spam.

The sample

For conducting our study, three existing email accounts were used to capture unsolicited emails that were regarded as primary documents: two different accounts from the same Australian university and one account located within a private company. Each of these accounts had advanced firewalls and spam filters which attempt to reduce the number of spam emails reaching recipients. These filters work by blocking and quarantining emails that contain known viruses, images or key words. Despite these filters, unsolicited emails were still received into each of the three accounts.

Overall, 412 emails were received across the three accounts. When broken down by the location where the unsolicited emails were received, 99 were received through the university accounts and 313 emails were received at the private company. It should be noted that the 412 emails are the spam emails that managed to get through the extensive firewalls and filters installed at the two locations, thus this number does not represent the total number of spam emails that would have been received if the protective infrastructure was not in place.

Data

Pre-determined elements of each unsolicited email were recorded including the date, time of day, sender, type of product, sex of the sender, salutation, whether a website link was embedded within the email, preferred method of response and whether any claims were made regarding the credibility and/or legitimacy of the sender. All of the above elements were coded, and entered into Excel to facilitate quantitative analysis. Moreover, in order to perform minimal qualitative analysis each email was examined to check for spelling mistakes and/or grammatical errors, the presence or absence of pre-identified psychological tricks as well as the abovementioned elements.

Analysis

The present study was focused on objective measures that could be easily categorized and verified. As a result, this study is both explanatory and exploratory. It is explanatory as it seeks to identify and describe main types of psychological tricks in the content of emails received during a one month period. It is also exploratory as it is not known a priori what sort of themes or observations would arise as a result of the collection, collation and analysis of the spam mail and it is unclear what insights – if any – could be obtained through analyzing the email content and contemplating what styles of thinking may be in operation and thus may facilitate online victimization.

The measures devised for use in this study are based on frequency analyses of

1. psychological tricks used by email scammers featuring the work of Cialdini (2006), and Holt and Graves' (2007) model including the presence of a salutation, whether a website link was embedded within the email, preferred method of response and whether any claims were made regarding the credibility and/or legitimacy of the sender.
2. flags that may alert recipients to the illegitimate and unsolicited nature of the email contact.

Psychological tricks frequency analysis

Starting from the six "weapons of influence" defined by Cialdini (2006), we adopted the following classification of psychological tricks (PT):

- PT1: Emails that try to instil a sense of a "pre-existing relationship";
- PT2: Emails that try to "mislead the recipient" on the legitimacy of the correspondence;
- PT3: Emails containing "reciprocation" tricks whereby scam operators offer the recipient something, such as a 'free' gift or assistance, in an effort to get something in return.
- PT4: Emails containing "commitment and consistency" tricks whereby the scammer tries to obtain the recipient's commitment to something early in the piece, but the agreement is later recalled to get the recipient to agree to something different.
- PT5: Emails containing "social proof" tricks such as words to inspire confidence (for example "Everybody does it, so it must be alright".
- PT6: Emails containing "liking" tricks which may include good looks, similar interests or background, humour or other attractive characteristics which helps to generate a good rapport with a previously unknown individual.
- PT7: Emails containing "authority" tricks. Authority figures, either in or out of a uniform, can cause an automatic response in most people. In an unsolicited email, an authority figure may appear as a lawyer, a tax official or a law enforcement officer.
- PT8: Emails containing "scarcity" tricks such as the fear of missing out! Being told that this is the last chance or that there are only so few still available, leads most people to agree hastily before they have had the opportunity to think about what they're doing.

Each unsolicited email in the sample was classified according to the types of psychological tricks listed above (noting that an email may belong to one or more class) followed by a frequency analysis.

Alert flag frequency analysis.

Based on the literature and past studies such as Holt and Graves (2007), the sampled emails were analysed for the presence of the following alert flags (AF):

- AF1: messages relating to fixed fee transfers;
- AF2: messages asking the recipient to reply via a website link;
- AF3: messages asking the recipient to reply via telephone or email;
- AF4: messages containing spelling mistakes or grammatical errors.

Each unsolicited email in the sample was classified according to the types of alert flags listed above (an email may belong to one or more class) followed by a frequency analysis.

Frequencies are of interest in terms of thinking style because the presence of certain requests, excessive spelling mistakes or poor grammar may work as a flag which alerts the recipient to the

illegitimate and unsolicited nature of the contact. It is not uncommon for scammers to hack into email accounts and send requests for money under the guise of being a 'friend' of the victim who is in desperate need of emergency funds due to an unexpected 'mugging', 'lost passport' or 'sickness' (ACCC, 2010). Thus the existence of these flags may serve as an important signal that alters the way in which the consumer thinks about a particular unsolicited communication, and hence may alter the way in which the individual thinks about the situation.

4. Results

Psychological tricks frequency analysis

After content analysis, it was found that the majority of unsolicited emails did not use tricks and were just "useless" emails full of garbage. The incidence of psychological tricks within the sampled emails was as follows (some emails contained more than one psychological trick):

- 9% tried to instill a sense of a pre-existing relationship (PT1);
- almost 6% tried to mislead the recipient on the legitimacy of the correspondence (PT2)
- 6% featured reciprocation tricks or sought the recipient's commitment (PT3 and PT4);
- no emails were found to contain tricks relating to social proof (PT5);
- 10% of emails sought to establish a good rapport with the recipient (PT6);
- 6% contained authority-type figures in the form of lawyers, tax officials or law enforcement officers (PT7).
- more than 3% contained scarcity tricks (PT8).

The type of salutation used within the email was examined. As noted in the literature review, it is not uncommon for spammers or scammers to try and instill confidence in their victim, and this can be facilitated through the use of a personally addressed salutation or other technique to make it appear as though the sender is known to the recipient (PT6). It was found that 90% of all emails did not contain any form of salutation, and thus the content of the spam commenced at the top of the email body. Of the remaining emails that did contain a solicitation, it was found to be in a form that is non-specific and gender neutral:

- 6.8% of the emails started with "Hello!"
- 2.2% started with "Dear [email address]"
- 1% started with "Welcome"
- one email started with "Attention,"

Another way to instill confidence in a recipient is for the sender to state credentials which claim affiliation with a particular company, role, financial institution or law firm, or to appear as an authority figure (PT7). To test the prevalence of this technique, the data analysis included an examination of any claims about such affiliations. It was found that in 94% of the emails, no such claims were made. Of the 24 emails containing such a claim:

- 14 contained the logo and similar (not exact) contact details of a major Australian bank
- five claimed to be from a "renowned car sales company"
- two claimed there was a "history of major contracts" between the recipient and the sender's company
- two claimed the recipients contact details had been obtained through either the Ivory Chamber of Commerce or a dating agency, and
- one claimed to be from a "renowned Lithuanian company located in Lithuania".

It was found that 94% of emails did not attempt to obtain something from the recipient (PT3 and PT4). This element was tested through examination of the content of the emails, and a positive was recorded if the email contained a phrase such as "please send through your curriculum vitae/bank account details/passport number" or something similar. In 2% of emails, recipients were offered money

in the form of lottery winnings and/or inheritances, but to claim the money, it was necessary for the recipient to act quickly and send via return email or website link their personal details including specific banking information (PT8).

Alert flag frequency analysis:

Table 2 presents a frequency analysis results in terms of percent of sampled emails containing the considered alert flag.

Table 2: Summary of Alert Flag frequencies

	Emails containing the AF
AF1 messages relating to fixed fee transfers	3%
AF2 messages asking the recipient to reply via a website link	82%
AF3 messages asking the recipient to reply via telephone or email	14%
AF4 messages containing spelling mistakes or grammatical errors	22%

Three percent of emails related to fixed fee transfers or requests to move a specific amount of money. Sometimes the provision of some detailed information – such as a physical address or telephone number – may be enough to instill confidence and faith as to the legitimacy of the contact. No emails received in this study contained a physical business address. Indeed, the preferred method for the recipient to get in contact with the sender was via a website link (82%), with 13% requesting contact be made via return email and 1% requesting a telephone call. No method of reply was specified in 4% of the unsolicited emails received during this study. Almost one quarter (22%) of unsolicited emails contained either spelling mistakes or grammatical errors.

5. Discussion

Online scams are typically aimed at defrauding a person or group by gaining their confidence. Scams can be difficult to classify because they keep changing and often contain elements of more than one type. Types of online scams include phishing, advance-fee fraud, bidding fee schemes, click fraud, domain slamming, spoofing attacks, web-cramming, and online versions of employment scams and romance scams (Plazak, 2010). In this analysis, no attempt was made to classify the unsolicited emails on the types of scam involved; instead we concentrated on the psychological tricks contained in the sampled unsolicited emails.

Software and hardware filters may help distinguish spam from genuine emails, yet they do little to protect the average computer user from predators who might be using a range of psychological traps to build the confidence and trust of their victims. Software and hardware also does not protect against a consumer's own preferred way of thinking. For example, in the 9% of cases where a pre-existing relationship was feigned (PT1), a consumer with a preference for conditional thinking may simply think "How exciting! Someone knows me personally and is offering me a product" whereas the inquiring thinker would start to ask questions such as "Who is this person? What is the product?" Consumers with a preference for an exploring style of thinking may ask a range of higher order questions including "Who else knows me? Where did I meet this person? Where did this person obtain my email address?" whilst the creative thinkers would attempt to see the big picture by asking "What is going on? What is the whole picture? Who is this person and how does he/she fit into my life?"

There is also a high potential for both financial and identity theft when recipients are fooled into thinking that they will obtain some benefit (such as paid employment) through the provision of their personal details (PT3 and PT4). Six percent of emails requested recipients to send through their personal information such as curriculum vitae or bank account details, with potentially irreversible consequences. Again, consumers who may demonstrate a preference for conditional thinking would be most susceptible to providing their personal details. As shown by the ABC (2008), if only a few of

those 1,000-million unsolicited scam emails are responded to by unsuspecting recipients, the potential for both economic and identity theft is staggering.

As stated previously, email and internet addresses can be manipulated to include information which helps mislead the recipient into thinking that the correspondence is legitimate. This study found that the use of misleading information to instill credibility and confidence applied to 5.8% of emails containing such information. Of those that did claim existing credibility, it is those purporting to be from renowned banks that are particularly concerning given the likelihood that recipients might believe it is legitimate correspondence from their banking institution (PT7). The potential for both identity theft and financial theft is therefore unacceptably high, and to avoid this psychological trap, consumers would need to possess a preference for creative thinking and an ability to see the big picture. The fact that scammers hide their identity and develop an image to enhance their credibility creates an opening for the independent thinker to be less susceptible to online victimization, perhaps due to the independent thinker's ability to be headstrong and sceptical about unsolicited contact.

A further psychological trick can be the creation of a sense of urgency (PT8) for example, "To claim this lottery win, you must reply as soon as possible…". The inclusion of such sentences in an unsolicited email may result in individuals making hasty – and often ill-informed – decisions regarding their purchases or online communications. Again, the consumer with a preference for a conditional or inquiring thinking style would be most susceptible to online victimization. The conditional thinker would focus on compliance perhaps by thinking "That is a very tight timeframe, I had better respond quickly" or "I have won the lottery. I don't want them to give it to someone else because of my tardy reply" whilst the independent thinker might think "This person can't tell me what to do. I'll reply when I am ready". A failure for consumers to be operating in the higher order thinking styles (such as independent or creative) may leave them susceptible to falling for the psychological tricks contained within unsolicited emails, and for them to subsequently fall victim to online scams.

Those emails that did not seek a reply from the recipient and which did not contain a web link (AF2) or other form of future interaction appear to be the ultimate example of spam – that is, an email that is totally unsolicited and serves no other purpose than to simply fill up a person's in-box. Even though the theft of money or personal identity may not occur, the price of such unsolicited contact is staggering. For example, it has been estimated that if a company has 500 employees who each take 40 seconds to deal with four unsolicited emails per day, then approximately 166 working days are lost per year (Blackspider Technologies, 2004). These calculations therefore have the potential to impact greatly upon an organization's productivity, and it is assumed that the loss may be further exacerbated by the employee's thinking style and the amount of time the individual spends in engaging and contemplating the spam communication.

6. Conclusion

The aim of the present analysis was to draw insight into possible relationships between styles of thinking and the identification of flags that could alert a consumer to a possible unsolicited email. Throughout this paper we have suggested links between various thinking styles and potential response types to various categories of psychological tricks. Such exploration raises some important issues worthy of consideration. Some of the literature shows that thinking styles are situational thus the styles may change depending on whether the individual interprets the situation as an opportunity or a threat. Unsolicited email may be perceived by recipients as either an opportunity or a threat. For some recipients, it may be viewed as an opportunity to enter or win a lottery, to purchase some pharmaceuticals without a prescription or to receive an inheritance from a long-lost relative. This interpretation may give the recipient a sense of excitement or accomplishment. For other recipients, the situation is threatening and perceived to be what it is: a risky interaction that may result in identity theft, credit card fraud or the installation of unauthorized malware on their computer. It would therefore be important to see if consumers view unsolicited email as an opportunity or a threat, and depending on their interpretation, to measure the incidence of particular thinking styles.

Awareness of consumer thinking style can increase our understanding of online safety as well as our understanding of scam-related victimization. As this has been an exploratory study, inferences have been drawn without the benefit of surveys or interviews, thus any conclusions need to be viewed tentatively. This paper has shown that consumers' thinking styles may impact upon their decision

making, and may also inhibit their ability to recognize alert flags or interpret psychological tricks. Further investigations should be conducted to confirm the inferences drawn in this paper. It may be interesting to survey victims of scams to ascertain their thinking styles via completion of the Sofo (2008) Thinking Style Inventory, and to draw actual links between online behavior and victimization.

Beyond thinking style, it is evident that scams are carefully constructed products that are created by computer-savvy individuals who know how to instill confidence in consumers by manipulating an online situation to produce the type of behavior that they desire. Even people who are confident that they would not fall victim to a scam may be at risk, particularly given the seemingly legitimate appearance of many scams and the unknown influence of thinking style.

Legislation and cooperation at global level, need to be joined with "safe" behaviors of Internet users. When using a computer, there are many additions which can enhance a user's safety whilst simultaneously protecting his or her identity. Common enhancements include hardware, protected software, security processes, and the use of strong firewalls. Consumer education is another weapon against the growing threat of online scams. It is therefore essential for consumer education to be used as a means of developing the skills of users to detect and avoid fraudulent transactions and dishonest interactions. By adopting infrastructural measures in conjunction with education and awareness strategies, internet users may feel empowered by their ability to safely enjoy the many benefits afforded by emerging technology. A combination of technical solutions and behavior management (whereby consumers take responsibility to detect and avoid fraud, as well as being willing to modify their online behavior) is therefore necessary to establish consumer trust in the safety of online interactions and transactions (Sarel & Marmorstein, 2006).

7. Further research

Beyond these suggestions listed above, it has been demonstrated in this paper that the experimental exploration and statistical correlation between thinking style and consumers' online behavior may be a worthwhile future project in order to establish what other educational or behavioral interventions may assist in decreasing the incidence of scamming, spamming and online victimization. In this sense, researchers are undertaking further studies including experimenting with the effect of exposing a selected group of Internet users, each of them characterized by different thinking style profiles, to "aggressive" spam campaigns.

This study had a number of limitations including the restricted number and type of data collection points (3 email accounts featuring high-security firewalls). A consequence of these limitations could have made it unlikely for us to discover a high number of incidences of all the psychological tricks and alert flags given the presence of the firewall. This may have skewed the results. For further research, it is therefore suggested that the data collection occurs from sources with a range of security protection and from a wider range of locations. For a deeper understanding of the studied phenomenon, it would also be useful to measure relationships via statistical analysis and actual application of the Sofo (2008) Thinking Styles in light of consumer responses to unsolicited email. To do this, it would be necessary to recruit a sample of either past victims of online scams or a random sample of consumers taken from the general population.

It would also be useful to ascertain which types of thinking style lead to financial loss. As noted by Hannaford (2010), online scams cost Australian consumers at least $69 million during 2009, but for every dollar lost by Australian consumers, there would be an equal and if not bigger pool of consumers who did not fall victim to an online scam – despite receiving unsolicited emails inviting them to interact or transact online. It is therefore considered important to see if thinking style has any influence on the types of online victimization that occurs.

8. References

[1] ACCC (Australian Competition and Consumer Commission), Targeting scams: Report of the ACCC on scam activity 2009, ACCC: Canberra, 2010.
[2] Australian Institute of Criminology, Preventing spam, Retrieved 10 January 2010, from http://www.aic.gov.au/publications/crm/crm035.pdf, 2005.

[3] Berzins M, "Online scams: case studies from Australia", In T. Dumova and R. Fiordo (Eds.), Handbook of Research on Social Interaction Technologies and Collaboration Software: Concepts and Trends, Pennsylvania: IGI Global, 2010.
[4] Blackspider Technologies, Spam: now a corporate concern, Reading: Blackspider Technologies, Retrieved 10 February 2008, from http://www.blackspider.com/services/spam_whitepaper.pdf, 2004.
[5] Bowen C, Shining the light on scams and fraud, Retrieved January 2010, from http://www.chrisbowen.net/pages/ministry.do?newsId=587, 2008.
[6] Calais P, Pires D, Guedes D, Meira W, Hoepers C, Steding-Jessen K, "A campaign-based characterization of spamming strategies", In Proceedings of Fourth Conference on Email and Anti-Spam, August 2-3, Mountain View, California USA., 2007.
[7] California Law, California Business And Professions Code - Division 7, Part 3, Chapter 1 Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers, Retrieved February 2010, from http://www.spamlaws.com/state/ca.shtml on, 2007.
[8] Cameron D, Galloway A, "Consumer motivations and concerns in online auctions: an exploratory study", International Journal of Consumer Studies, vol. 29, no. 3, pp.181-192, 2005.
[9] Cialdini RB, Influence: The Psychology of Persuasion. Harper Paperbacks, Revised edition, 2006.
[10] Clayton R, "Do zebras get more spam than aardvarks?", In proceedings of the Fifth Conference on Email and Anti-Spam, Mountain View, California USA, 2008.
[11] Debus B, New identity crime offences proposed [Press Release], Retrieved January 2010, from http://www.ministerhomeaffairs.gov.au/www/ministers/ministerdebus.nsf/Page/MediaReleases_2008_Firstquarter_27March2008-Newidentitycrimeoffencesproposed, 2008.
[12] European Commission, Data protection: "Junk" email costs internet users 10 billion a year worldwide – Commission study. Retrieved February 2010 from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en on 8, 2001.
[13] Federal Trade Commission, Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress. December 2005. Retrieved February 2010 from http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf, 2005.
[14] Gartner Inc., Gartner says marketers must differentiate e-mail marketing from spam, Retrieved January 2010 from http://www.gartner.com/5_about/press_releases/pr29sept2003a.jsp, 2003.
[15] Goodman J, Rounthwaite R, "Stopping outgoing spam", In Proceedings of the 5th ACM Conference on Electronic Commerce, pp. 30–39, 2004.
[16] Hannaford S, "Nation fleeced for $70m in 2009", The Canberra Times, p.1 [12 January 2010], 2010.
[17] Holt T, Graves D, "A qualitative analysis of advance fee fraud e-mail schemes", International Journal of Cyber Criminology, Vol. 1, no. 1, pp. 137-154, 2007.
[18] Kanich C, Kreibich C, Levchenko K., Enright B, Voelker GM, Paxson V, Savage S, "Spamalytics: An Empirical Analysis of Spam Marketing Conversion", Communications of the ACM, Vol. 59, no. 9, pp. 99-107, 2009.
[19] Krone T, Johnson H, "Internet purchasing: perceptions and experience of Australian households", Trends and Issues in Crime and Criminal Justice, Vol. 330, no. 1-6., 2007.
[20] Judge WYP, Alperovitch D, "Understanding and Reversing the Profit Model of Spam", In Proceedings of Workshop on Economics of Information Security 2005 (WEIS 2005) (Boston, MA, USA), 2005.
[21] Li F, Hsieh M-H, "An empirical study of clustering behaviour of spammers and group-based anti-spam strategies", In Proceedings of the Third Conference on Email and Anti-Spam, July 27-28, Mountain View, California USA, 2006.
[22] Plazak D, A Hole in the Ground with a Liar at the Top: Fraud and Deceit in the Golden Age of American Mining. University of Utah Press, 2010.
[23] Prior L, Following in Foucault's footsteps: text and context in qualitative research, In D. Silverman (Ed.), Qualitative research: theory, method and practice, London: Sage, pp. 63-79, 1997.
[24] Sarel D, Marmorstein H, "Addressing consumers' concerns about online security: a conceptual and empirical analysis of banks' actions", Journal of Financial Services Marketing, Vol. 11, no. 2, pp. 99-111, 2006.

[25] Sofo F, "Thinking styles of modern Chinese leaders: independence and exploration in an historically conditional China", Australian Journal of Adult Learning, Vol. 45, no. 3, pp. 304-330, 2005.
[26] Sofo F, "Differences of degree or differences in kind? A comparative analysis of thinking styles", International Journal of Interdisciplinary Social Sciences, Vol. 3, no. 1, pp. 293-301, 2008.
[27] Sternberg R, Thinking styles, Cambridge: Cambridge University Press, 1997.
[28] Tang J, "Are Asian thinking styles different? Acculturation and thinking styles in a Chinese Canadian population", Dissertation Abstract International, Section B: The Science and Engineering, Vol. 65, no.3-B, 1573, 2003.
[29] UKOFT, Psychology of scams, United Kingdom Office of Fair Trading, London, 2009.
[30] Vaile D, "Spam canned – new laws for Australia", Internet Law Bulletin, Vol. 6, no. 9, pp. 113-115, 2004.
[31] Wall D, "Digital realism and the governance of spam as cybercrime", European Journal on Criminal Policy and Research, Vol. 10, pp. 309-335, 2004.
[32] Zhang L, "Revisiting the predictive power of thinking styles for academic performance", The Journal of Psychology, Vol. 138, no. 4, pp. 351-370, 2004.