Persuasion Strategies: Use of Negative Forces in Scam E-mails

Chitchanok Naksawat
cnaksawat@yahoo.com
King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand

Songyut Akkakoson
songyutbee@gmail.com
King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand

Chek Kim Loi
lck734@yahoo.com
Universiti Malaysia Sabah

ABSTRACT

The 21st century globalisation strongly influences the world as a result of highly improved technology and communications which made it possible for everyone involved to have equal access to a global market and information exchange via English. As a result, electronic communication has become part of the present-day multinational professionals of all fields who work daily in front of their digital monitors. At times, these professionals may receive Nigerian 419 scam e-mails in which fraudsters target victims to make advance payments for financial gains that do not materialise. In these e-mails, situations in which persuasion techniques are intertwined are well crafted. As a result, the victim who is susceptible to the offer is more likely to respond and be lured into losing money eventually. The present study, consequently, analysed a corpus of 50 Nigerian 419 scam e-mails through a textual analysis to examine language aspects in terms of persuasion strategies fraudsters used as a compelling force to achieve their communicative purposes of lures and deceits. The study has revealed two major types of deceptive techniques which are used in combination, namely framing-rhetoric triggers, disguised as the traditional genre of electronic communications and human weakness-exploiting triggers, intended as incitement of recipients' emotions. Finally, the paper includes not only pedagogical suggestions for business English teachers when implementing classroom activities, but also warnings for either pre-experienced or experienced business professionals in relation to interpreting the unknown e-mails' messages they receive with great caution.

Keywords: spam; Nigerian 419 scam; e-mail; fraud; persuasion strategies

INTRODUCTION

At the start of the 21st century and globalisation, the role of English in international communication has rapidly risen. The language has been widely used in internet-based communication methods, especially in the form of electronic mail (e-mail) which has become an increasingly popular mode of interpersonal communication and intra-/inter-organisational communication. Not only does the language become a medium of communication for worldwide business professionals, it also catches swindlers' eyes. As a result, e-mail communication becomes an important tool in internet crimes. In 2011 and 2014, e-mail was the third frequent method of contact employed by fraudsters of internet fraud, accounting for 20.44% and 15.71% respectively (Fraud.org, n.d.a, b). In fact, the Internet does not create any new evil; it would only be a medium that could provide a new space for already undesirable behaviours (Cukier, Ngwenyama & Nesselroth-Woyzbun, 2008). One of these is the

phenomenon of advance-fee fraud, Nigerian 419 scam e-mails which were formerly "Nigerian letters", sent via regular mail or through fax (Fraug.org, n.d.c). The writers of these scams are real world hustlers who seem to be excellent psychologists, who know humans' weakness for avarice. According to Mason (2011), at the present moment, they are perhaps using the blanket targeting approach to grab as many victims as possible. They, moreover, go even further to convince the victims to be excited about a huge amount of hard-earned cash and finally losing their own money. Unbelievable situations have been created to lure the victims. The story may end with the scene that those who are more susceptible to the offer respond to the trap. At worst, they have to pay instead of receiving the expected money. The severity and consequences of this type of online frauds are a real shock. In 2011, 419 scam was ranked seventh among the top 10 internet scams, accounting for 1.60% of the total percentage according to the National Consumers League's Fraud Centre of the US (Fraud.org, n.d.b). During the period of June to December 2014, the Internet Crime Report revealed that there were 3,735 cases of 419 victims with the total victim loss of $6,619,195 (National White Collar Crime Center, 2014).

Realising this harm, the present researchers attempt to address what deceptive elements have been used in Nigerian 419 scam e-mails. In this paper, how persuasion strategies can drive victims to fall for 419 attackers has been investigated. We present an empirical analysis of these psychological attacks, a description of how these schemes operate as tools of deception and manipulation and how 419 scammers mask indiscriminate appeal to form a delusion of familiarity, sincerity and urgency. As unanimously agreed among previous researchers (Atkins & Huang, 2013; Dion, 2010; Dyrud, 2005; Manson, 2011; Stajano & Wilson, 2009), we conclude with an urge to tackle this socially-globalised problem by educating people on potential threats from these perpetrators.

LITERATURE REVIEW

In this section, a brief discussion of Nigerian 419 scam is described. Some theoretical premises which are proposed to explain scammers' online fraudulent activities (physical attacks) and their use of persuasion strategies (psychological attacks) have also been examined. Lastly, related studies have been reviewed.

NIGERIAN 419 SCAM E-MAILS

Nigerian 419 scam is one of the digital documents sent to a large number of recipients over the Internet as unsolicited or unwanted electronic messages, or the so-called "spam" (Viosca, Bergiel, & Balsmeier, 2004). This specific form of spam appears in the form of advance-fee fraud initiative, more commonly referred to as "Nigerian advance-fee frauds", "Nigerian letters", "Nigerian Money Offers", "Nigerian 419 scams", or just "419s". These scam messages used to be called "Nigerian letters" because they came by ordinary mail, but now these messages are also sent by phone, fax, or e-mail. The name "Nigerian" comes originally from the fact that this scam violates Section 419 of Nigeria's Criminal Code (Nigeria - The 419 Coalition Website, n.d.). Sandler (2010) defines Nigerian 419 scam as a fraudulent e-mail in which a stranger (often from Nigeria, and also from other places in Africa, Asia, or Europe) contacts you and asks for your permission to transfer a large amount of money obtained in any of a number of hard-to-believe situations to your account. But before that, you are convinced to advance money to the criminal first. As a result, you are led to expect that a much larger sum of money will be returned to your account soon. Of course, there has never been any amount of money returned. What is more, once becoming a victim, you are

likely to be persuaded to make additional payments, a second or third advance, before the promised money is received.

Nigerian 419 writers are scammers who cunningly use English through e-mails to swindle us by means of deception or fraud. At first glance, a Nigerian 419 e-mail seems to take the shape of a recognisable form of general business e-mails. Not only can business people be a target for tricking by writers of this kind of scams, general internet users do receive such an e-mail, from time to time as well. A number of recipients, more or less, might have taken the bait attracted in its fabulous promise and ended up with paying a number of fees in advance as a guarantee before the unreal grand sum would be transferred into their accounts.

THE NOTION OF SOCIAL ENGINEERING

An explanation of online fraudulent activities is drawn from the established notion of social engineering developed by psychologists (Huang & Brockman, 2011; King & Thomas, 2009; Ross, 2009). According to Mann (2008, p. 3), the term "social engineering" is defined as an act "to manipulate people, by deception into giving out information, or performing an action". In other words, social engineering has centred on the exploitive nature of deceptive communications perpetrators employ in committing fraudulent crimes. Individuals who intentionally mislead and manipulate people for personal benefit are called social engineers (Huang & Brockman, 2011). In their commission of fraudulent acts, social engineers rely greatly on a human interaction and a trusting relationship with the target before tricking people into breaking normal security procedures (Thompson, 2006). They run a kind of "con" or "con game", also known as *a confidence trick, a short/small con, a scam, a grift, a hustle, a bunko (or bunco), a swindle, a flimflam, a gaffle or a bamboozle*. It is assumed that once people place trust in social engineers, they fall victim to them because of their ignorance, naivety, or greed (King & Thomas, 2009). Social engineers exploit every opportunity to influence the victim's emotional state, pushing for full disclosure of their confidential information (Workman, 2008).

Social engineering is one of the greatest threats the globalised world is now encountering.

Goals of a social engineering attack may vary, including obtaining personal information, committing fraud, gaining computer access, gaining money or other valuable items such as financial records (Thompson, 2006). Social engineering attacks can take place at both the corporate and individual level and at both the physical and psychological level. Workplaces, telephones, trash cans and the Internet are the most common physical locations for social engineers to do their fraudulent jobs, whereas persuasion, impersonation, ingratiation, conformity and friendliness are their psychological attacks (Workman, 2008). Among other things, cognitive bias and social error are psychologically utilised by social engineers in order to set up the best way of dealing with their target groups (Raman, 2008). By cognitive bias, social engineers understand that general people sometimes make an error in thinking when they are processing and interpreting information in the world around them, which unfortunately leads to poor decisions and bad judgements. By social error, social engineers are aware of the fact that general people normally ignore a bad or unfamiliar person whilst a nice or familiar person is typically welcomed. Thus, social engineers try to present themselves in a good manner and make a positive first impression. Social engineers are also good at fitting into people's surroundings, knowing that their gullible target is a person who does not stand out in a social group. Moreover, social engineers are able to foresee changed behaviours of humans when they are pressured into conformity, compliance and obedience.

PERSUASION STRATEGIES

As mentioned earlier, one of the psychological attacks social engineers use is persuasion, which is the focus of this study. Persuasion is a compelling force in daily life and has a powerful impact on society and a whole. Good illustrations are advertising messages which can push viewers to purchase a certain product and a political candidate who successfully persuades voters to lean towards his/her name on the ballot box. All quarters of the society (eg politicians, legal enforcers, mass media communicators, journalists, advertisers) execute the power of persuasion and their actions have an effect on general people in turn. Based on different major definitions given by previous communication scholars, Perloff (2010, p. 12) simplifies the main features of persuasion into one integrated standpoint as "a symbolic process in which communicators try to convince other people to change their attitudes or behavior regarding an issue through the transmission of a message, in an atmosphere of free choice". This characterisation contains five key components, namely 1) persuasion is a symbolic process, 2) persuasion involves an attempt to influence, 3) people persuade themselves, 4) persuasion involves the transmission of a message and 5) persuasion requires free choice.

Contemporary persuasion has emerged by the advent of the 21st century and globalisation and it has differentiated itself from what was used in the past in five ways (Perloff, 2010). According to Perloff (2010), the first difference lies in the number of persuasive messages which has grown immensely. For example, a large quantity of advertisements a person is exposed to each day via modern media (eg advertising, public service announcements, internet banner ads, telephone marketers) is quite considerable. Second, persuasive communications now travel far more quickly with the touch of a screen through television, radio, smartphone and the Internet. These help to spread persuasive messages very rapidly. Third, persuasion is big business. Apart from advertising agencies, marketing firms, or public relations companies, the business of which is solely for persuasive purposes, many other businesses (eg lobbying groups, social activists, pollsters, speech writers, image consultants) are dependent on various facets of persuasion to sell goods and services as well. Fourth, modern-day persuasion is now much more subtle and devious. Even though a plenty of ads use very obvious persuasive strategies, a lot of messages are far more delicate and complicated. For instance, businesses sometimes initially create very specific image designed to urge viewers to buy products or services in order to attain a proposed lifestyle. Deviousness can be found in the deceptiveness of persuasion in the news media. Finally, persuasion is now more complex and impersonal. Consumers who may come from different cultural groups are more different and have more options. As a result, marketers have to be sensible when it comes to creating and choosing their persuasive mediums and messages. What is more, with the assistance of present-day technologies, the content of persuasive messages can be changed, giving new meanings that were not originally embedded and that were not intended by the original sender.

Persuasion can be used as strategies for achieving something in both positive and negative ways. On the one hand, if persuasive communications have been used by good people as a positive force, they could implement change and help to improve people's lives. Public service campaigns that have tried to persuade people to recycle used rubbish like bottles, glass, or paper; or stop damaging the environment are great examples of utilising positive persuasion. Health communicators have started numerous campaigns to change people's bad behaviours such as smoking cigarettes, drinking alcohol, getting addicted to drugs, or having unsafe sex. On the other hand, there is the other side of the coin too. Negative examples call to mind images of those who use misguided persuasion, for example dishonest salespeople, devious manipulators, or unscrupulous bankers. The situation is

getting very worrying if persuasion strategies catch the eyes of those social engineers. They can apply these strategies to their persuasive writing to convince readers to agree with what they have deceitfully plotted. An example of this can be apparently seen in Nigerian money fraud cybercrime, which is the focus of this study.

RELATED STUDIES

Previous research has documented lessons and principles learnt from scams in order to raise the awareness of the dangers of currently operating scams as the main defence against the scammers is people education, leading to self-protection. Dyrud (2005) examined a corpus of 111 Nigerian 419 letters and revealed several deceptive but persuasive techniques that make the fraudulent plan successful, namely appealing to pity, trust and avarice. She proposed that these 419 messages can be used as fertile grounds for in-class activities related to persuasion in the business communication classroom, for instance asking students to carefully examine 419 letters, putting students in small group discussions, having students examine further some of the websites mentioned. This could facilitate students' mental ability for critical evaluation of online information and could be enjoyable classroom activities. Cukier, Nesselroth, and Cody (2007) have analysed a sample of 111 Nigerian letters received by e-mail to explore their key motifs including the use of form, purpose and tone. These researchers discovered that these letters use rich narrative appeals to strong emotions such as greed, guilt and lust in order to stimulate typical beliefs of windfall fortunes. The study suggested that the masked promise of enormous riches may impair the victims' rational judgement, resulting in believing that great prosperity has dropped into their e-mail inboxes. Cukier, Ngwenyama and Nesselroth-Woyzbun (2008) study focused on a detailed analysis of 111 Nigerian letters. According to these researchers, this genre of spam uses a lot of common devices in order to appeal to recipients' emotions. These letters also make reference to a tragedy, a charitable appeal or the large treasure. A warning is given that the Internet may transform the Nigerian letter which once was an insignificant source of fraud to a significant criminal threat. Stajano and Wilson (2009) analysed a variety of scams and short cons and documented and recreated them for educating viewers through the BBC TV documentary series *The Real Hustle*. These researchers extracted from the collected scams seven general principles about the recurring behavioural patterns of victims that hustlers learnt to exploit namely, the distraction principle, the social compliance principle, the herd principle, the dishonesty principle, the deception principle, the need and greed principle and the time principle. Dion (2010) explored a sample of 100 Nigerian scams, which can be classified into six categories: lottery scams, humanitarian gifts, abandoned money, business opportunities, deceased estate/last will, gold bars and diamonds. This researcher concluded that these scams are narratives that give us various perceptions about the present globalised era. To reduce the damages from cyber-criminals, educating people is quite effective in the long run. Tricks, traps and main defects of advance-fee fraud letters should be learnt so that no response to such letters will be made. Manson (2011) reported crimes of persuasion, concerning scams and their victims based on the evidence of Citizens Advice Bureau clients across Scotland. The report said that anyone can fall victim to a scam e-mail and some become repeat victims that are plagued by scammers. The scammer uses various types of scam e-mail such as debt advice firms, switching suppliers, prizes and lottery scams and loan offers. The techniques that scammers use to gain the victims' confidence are making the scam look legitimate, exploiting basic human desires and needs, personalising the scam, making scams look urgent and setting deadlines, and asking victims to comply in several steps. An important method of protecting consumers is to educate the public about the types of scams operating and the techniques and tricks that scammers use, which can lessen the number of victims. Atkins and Huang (2013)

examined the contents of 100 phishing e-mails and 100 advance-fee-scam e-mails and evaluated the persuasion tactics used by social engineers. These researchers identified seven types of persuasion used in their tested advance-fee fraud e-mails, including attraction/excitement, authority, politeness, urgency, pity, tradition and formality. Scammers use a threatening tone via urgency, potential monetary gain, business proposals and large unclaimed funds as the main persuasions to lure victims. Moreover, these social engineers use both positive and negative statements in combination with authoritative and urgent persuasions to persuade naive addressees on their decisions to respond. The researchers concluded that although technological defences and legislative efforts are being used to combat social engineering attacks, education is the most efficient way to prevent online frauds. In the classroom setting, Gillespie (2012) used genuine spam e-mails as teaching materials in his persuasive writing classes. His students are given a selection of these e-mails and asked to write down what their replies to these would be. He affirms that when our students become adults, they will make connections with the online world**.** Not only should they now be open to its potential, its pitfalls should also be well aware of. Gillespie further emphasises that:

> As an English teacher, it was important to zoom in on the persuasive language techniques used in spam emails. By the end of the unit pupils could tell you that spam emails use terms of endearment to hook in the recipient, include hyperlinks to news articles to make their stories more plausible, describe accidents or impending threats to generate sympathy, and specify tight deadlines to make the deal seem juicier.
>
> (para. 11)

Based on the results of previous studies on fraudulent communications and the background information on social engineers' behaviours and persuasion strategies reviewed, scam e-mails offer rich pedagogical possibilities to various social groups, including our future adults who are still in the classroom right now. Focusing on the deceptive techniques, the present study has the principal purpose to warn against trusting the information in this specific form of scam e-mails. Its results could be beneficial not only to the public, but also to those in the educational field, for example teachers with regard to syllabus development and production of teaching materials for business English courses and learners of business English both pre-experienced and experienced in relation to interpreting daily e-mails' messages with extreme caution. Moreover, the analysis of persuasion strategies exploited as negative forces in this study is hoped to illustrate "the value and efficacy of a multi-level of a genre specific corpus" (Upton & Connor, 2001, p. 5), which eventually adds to the growing body of genre knowledge. The following research question has been addressed:

- What are the significant language aspects that scammers apply in order to gain the addressee's confidence?

METHODOLOGY

CORPUS COLLECTION

Materials used in this study were authentic spam e-mails that the three researchers directly received in their e-mail inboxes and those given by their colleagues, friends and relatives during a 5-month period (June - December 2013), excluding duplicates. In total, 85 spam e-mails of various types (ie general merchandise sales (7, 9%), phishing (8, 10%), lottery scams (20, 23%) and Nigerian 419 scams (50, 58%)) were gathered. Since the largest number of spam e-mails received was the Nigerian 419 scam (50), it was selected as a corpus for

analysis in this study. An example is included in the appendix. The word length of each selected e-mail was not limited. Since this study focused only on the contents of the e-mails, other variables concerning the e-mail writers such as nationality, gender, age, status were not considered.

FRAMEWORK FOR DATA ANALYSIS

Deceptive operations and techniques identified by Dyrud (2005) and Manson (2011) were used as a framework for the analysis of persuasion strategies in the present study. Based on the definition of persuasion simplified by Perloff (2011), persuasion strategies in this study refer to acts or plans or methods of persuading people to do or believe something. Equivalent terms used hereinafter include *persuasions, techniques, tactics, triggers, persuasive elements, persuasive techniques, strategic technique*. Seven types of persuasive elements which were applied to the collected e-mails are listed below. Their definitions, as described by Dyrud (2005) and Manson (2011), are provided in brackets.

1) Appealing to pity (*sympathy-generating messages*)
2) Trust (*a feeling of confidence in the victim and a reciprocal agreement*)
3) Avarice/exploiting basic human desires and needs (*provoking an intuitive desire for possessing a lot of money*)
4) Making the scam look legitimate (*creating legitimacy, trust and creditability*)
5) Personalising the scam (*using the little knowledge about the victim to great effect*)
6) Making the scams look urgent and setting deadlines (*setting artificial deadlines and stressing on the exigency of the situation*)
7) Asking victims to comply in several steps (*asking the victim to make small steps of compliance*).

CORPUS ANALYSIS

The researchers applied textual analysis manually to code emerging persuasion strategies in each e-mail in the present corpus according to the established framework. The persuasion strategies identified were first counted and grouped according to similarities. These strategies were then categorised according to the rate of recurrence. Finally, all strategies in each identified category were translated into percentages. Three weeks after the first analysis, all of the collected e-mails were re-analysed by the researchers once again for intra-rater reliability. In order to verify the content validity of the completed categorisation, the data from the second analysis was double-checked by three experts who have a PhD in Applied Linguistics (two of them are colleagues of the second author in Thailand and the other is a colleague of the third author in Malaysia), using the index of the Item-Objective Congruence measure (IOC) (Rovinelli & Hambleton, 1977). Discrepancies in the items noted by two out of three experts were rechecked and changed after the researchers had a discussion with the experts. As a result, all identified strategies in the categorisation scored greater than 0.50 on the IOC measure, which is acceptable due to the congruence between the strategies and their communicative purposes set for expert verification (Brown, 1996). Pearson product-moment correlation coefficient (r) was also deployed to find the relationships between the experts' opinions and the categorised strategies, which is based on the fact that the inter-rater reliability value of the completed categorisation which is larger than 0.7 is acceptable because it shows a high correlation of the experts' opinions. The results obtained are $r = 0.70$ (Expert 1 and Expert 2) and $r = 1$ (Expert 1 and Expert 3, and Expert 2 and Expert 3 respectively), which means that the inter-rater reliability of this categorisation is high.

RESULTS

The study seeks to reveal the significant language aspects in terms of persuasion techniques that are used to make the scam contents believable. Upon analysing the collected 50 Nigerian 419 scam e-mails, based on the established framework, the researchers found that personalising the scam was not used by the 419 scammers in the present corpus. This persuasive element was then removed. However, appealing to politeness and being genuine emerged and this element was included. In total, seven persuasion strategies were employed in the examined corpus. Details are presented in Table 1 below.

TABLE 1. Aspects of persuasion strategies and their recurrence in the Nigerian 419 scam e-mails

#	Persuasion Strategies	Frequency (*N* = 50)	Percentage (100%)
1.	Asking victims to comply in several steps	50	100%
2.	Avarice/exploiting basic human desires and needs	48	96%
3.	Making the scam look legitimate	39	78%
4.	Making the scam look urgent and setting deadlines	29	58%
5.	Appealing to politeness and being genuine	27	54%
6.	Trust	24	48%
7.	Appealing to pity	10	20%

As illustrated in Table 1, the second column ranks the identified persuasion strategies in ascending order of recurrence. The third and fourth columns show the frequency and percentage of the identified techniques respectively. Six strategies in the table (ie items 1-4 and items 6-7) are classified according to the strategies identified by Dyrud (2005) and Manson (2011) whilst the other one (ie item 5) emerged from the present corpus. The following descriptions exemplify the identified persuasion techniques.

STRATEGY 1: ASKING VICTIMS TO COMPLY IN SEVERAL STEPS

Asking victims to comply in several steps occurred in all of the Nigerian 419 scam e-mails corrected in this study, accounting for the biggest share of the corpus (100%). This trick can be measured by the fact that scammers plot various small steps to draw the victim into continuing to comply with their deceitful plans. The italics in the following excerpts illustrate how scammers use this strategy (original data kept intact):

Example 1: *You have to contact my Bank* directly as the real next of kin of this deceased account with next of kin application form. *You have to send me those your information below* to enable me use it and get you next of kin application form from bank, so that *you will contact Bank for the transfer of this money into your account*. (EM 11)

Example 2: If you are interested, *get back to me* with your following details below. As soon as I receive these data's, *I will forward to you the application form* which *you will send to the bank*. (EM 19)

Example 3: I will *require from the following details*:- Your name in full. Your residential Address in full, Your Mobile (Cell) telephone number, Tel/Fax Number, Brief information on your profile, this should include your age, marital status and nature of Job. (EM 34)

From the illustrated excerpts, the victim is likely to be asked to do a number of things such as contacting the bank, revealing his/her personal information (eg residential address in full, mobile phone number, Tel or Fax number, profile, age, marital status, nature of job), filling in

an application form, forwarding the filled-in form to the bank. Eventually, the victim ends up transferring an advance fee, waiting in vain for the promised sum to be paid into his/her bank account.

STRATEGY 2: AVARICE/EXPLOITING BASIC HUMAN DESIRES AND NEEDS

Avarice or exploiting basic human desires and needs represented 96% of the corpus. The italics in the following excerpts show the employment of this persuasive element (original data kept intact):

Example 1: I will be very glad if you do assist me to relocate a sum of (US 18.5 Million) to your personal bank account for the benefit of both of us. *You will be entitled to have 30% of this fund as a foreign partner*, since you will provide a bank account where this money will be transferred to, whilst 70% will be for me, by indicating your interest on assurance of trust, I will send you the full details and how this business will be executed. (EM 19)

Example 2: In my department we discovered an abandoned sum of ($50.500, 000.00) Fifth Million Five Hundred Thousand United States Dollars). If you accept my offer *I shall compensate you with 40% of the money*, 60% goes to me, after which we shall visit your country for disbursement according to the percentages indicated. (EM 22)

Example 3: I have an opportunity to transfer US$19.1 Million Dollars (Nineteen Million One Hundred Thousand United States Dollars) I'm Inviting you for a business deal where this money can be share between us, *I intend to offer to you 40% of the total sum* on a provision of a foreign account where this fund can be remitted immediately. (EM 44)

Avarice is another frequently-used strategic technique because scammers have learnt to predict human beings' natural feeling of wanting a lot of money and keeping it for themselves. By this trick, scammers have set some alluring conditions to stimulate human greed, or cause a sense of excitement to the recipient (Atkins & Huang, 2013), for example offering a large sum of money, presenting shared portions of the fund between the sender and the recipient by doing little or nothing in order to attain it, or proposing a better life from a huge cash prize. After taking the bait, the recipient will then be asked to reveal his/her personal information so as to receive the promised sum of money.

STRATEGY 3: MAKING THE SCAM LOOK LEGITIMATE

78% of the present corpus contained making the scam look legitimate. The italics in the following excerpts confirm the utilisation of this persuasion (original data kept intact):

Example 1: My Name is Mr. …… *the Bill and Exchange (assistant) Manager of the BANK OF AFRICA (B.O.A)*, Ouagadougou Burkina Faso. (EM 22)

Example 2: "I am Mr. ……. from Burkina Faso. I want to seek your assistance after my discovery during auditing in my bank *as am the manager of Bill and Exchange at the Foreign Remittance Department of BANK OF AFRICA, (B.O.A.)* (EM 39)

Example 3: I Am A Banker By Profession From Burkina Faso In West Africa And *Currently Holding The Post Of Manager Of Bill And Exchange At The Foreign Remittance Department; Central Bank Of Burkina-Faso (BCEAO)*. (EM 49)

The scammer takes the role of an authority and tries to inform the reader of the nature and source of the funds in detail in order to give the impression that the e-mail has been sent from an official institution or a reliable business organisation. This fake authority could be a representative from a Nigerian or South African companies (eg Nigerian National Petroleum, Central Bank of Nigeria, Anglogold Corporation, Apex Paying Bank, Liquefied Natural Gas, Petro Ivoire) (Dyrud, 2005), or someone like an executive of a corporation, an attorney, a retired FBI official or a doctor (Atkins & Huang, 2013). This strategy will convince the reader whereby the reader will be asked to act as a beneficiary or an overseas agent and permit the scammer to put millions of dollars in his/her bank account.

STRATEGY 4: MAKING THE SCAM LOOK URGENT AND SETTING DEADLINES

58% of the collected e-mails included making the scam look urgent and setting deadlines. The excerpts below show how scammers employ this technique (original data kept intact):

Example 1: *I am waiting for your urgent respond* to enable us proceed further for the transfer. (EM 11)

Example 2: *Return back to me immediately* if you can handle this transfer project on my behalf before death cross my way. (EM 13)

Example 3: *Await your urgent response* to enable me give you more details. (EM 39)

To successfully commit their fraudulent tasks, 419 scammers need prompt responses from their recipients. If not, their plans may be caught and their attempts may fail. Therefore, scammers set a limited time or deadline to make their e-mails look urgent and to reduce the addressee's time to realise their tricky plans. The addressee will have to process the scam content as soon as possible and finally make a decision to follow the tricks. Statements like "please...quickly help me", "waiting with thanks" pressured the recipient into answering the e-mail.

STRATEGY 5: APPEALING TO POLITENESS AND BEING GENUINE

Appealing to politeness and being genuine appeared as a tactic in 54% of the collected e-mails. The use of this strategy is italicised in the following excerpts (original data kept intact):

Example 1: *Sorry if you received this letter in your spam*, Due to recent connection error here in the country. (EM 1)

Example 2: *I must apologize for barging this message into your mail box without any formal introduction due to the urgency and confidential of this issue* and I know that this message will come to you as a surprise. (EM 11)

Example 3: This message may Surprise you. *Please accept my apology if it does embarrass you*. However, it's my urgent need for a foreign partner that made me to contact you." (EM 44)

Scammers try their best to create a friendly communication in the hope of making the recipient fall victim to their lures. They typically begin their e-mails with friendly salutations and end them with polite closings. The body part is full of polite sentences to convince the

addressee to believe that their e-mails are not a deceit. They try to behave towards the addressee in such a pleasant way, following the usual rules of business English writing.

STRATEGY 6: TRUST

Trust, another persuasive element employed by 419 scammers, accounted for 48% of the present corpus. Illustrated below is how scammers use this persuasion (original data kept intact):

Example 1: I sourced your e-mail contact through the Internet *in search of trusted person who can assist me*…….However, he advised me to provide a trustee who will stand on my behalf. (EM 1)

Example 2: Though I have not met with you before but I believe one has to risk confidence to succeed sometimes in life. And *I hoped that you will not expose or betray this trust and confident that I am about to repose on you for the mutual benefit of our both families*. (EM 6)

Example 3: This project is based on trust, confidentiality and sincerity of purpose in order to have an acceptable meeting of the minds. However, before further details of this laudable transaction will be revealed to you. *I must be convinced of your integrity, transparency and honest*. (EM 34)

Scammers try to impress the recipient or make the addressee feel proud of being trusted and selected to do an important task. Moreover, making the addressee trust everything the e-mail says and giving the impression that the given information is for the purpose of this contact are also what scammers do (Atkins & Huang, 2013). The addressee is finally convinced and becomes confident in the sender, believing he/she is honest, fair and reliable.

STRATEGY 7: APPEALING TO PITY

Appealing to pity only accounted for 20% of the corpus in the present study. Examples of this tactic are shown in the excerpts (original data kept intact):

Example 1: I am constrained to contact you because of *the maltreatment which I am receiving from my stepmother*. She planned to take away all my late father's treasury and properties from me since the unexpected death of my beloved father. (EM 1)

Example 2: I am Mrs. …….. , *and I have been suffering from ovarian cancer disease and the doctor says that I have just two days to leave*. Now that I am about to end the race like this, without any family members and no child, But my mind is not at rest because I am writing this letter now through the help of my computer beside my sick bed. (EM 13)

Scammers use this trick as a tool for making up hard-to-believe situations or tragic stories that can impact on the addressee's sympathised feelings. Stories such as the death of loved ones or concerns of someone's safety or health are typically dramatised. Cukier, Ngwenyama, and Nesselroth-Woyzbun (2008) provided some more examples, such as a war; a political event; a tsunami or a plane crash; dying of some diseases like esophageal, breast, or unspecified cancer. Once the addressee believes that the fake character in such stories is

really unhappy or in a bad situation, he/she is then persuaded to transfer the money and fall victim to the lured conditions.

Based on the findings, the study has proposed the types of strategies scammers employ for the communicative purposes of lures and deceits. Figure 1 diagrammatically illustrates these persuasion strategies.

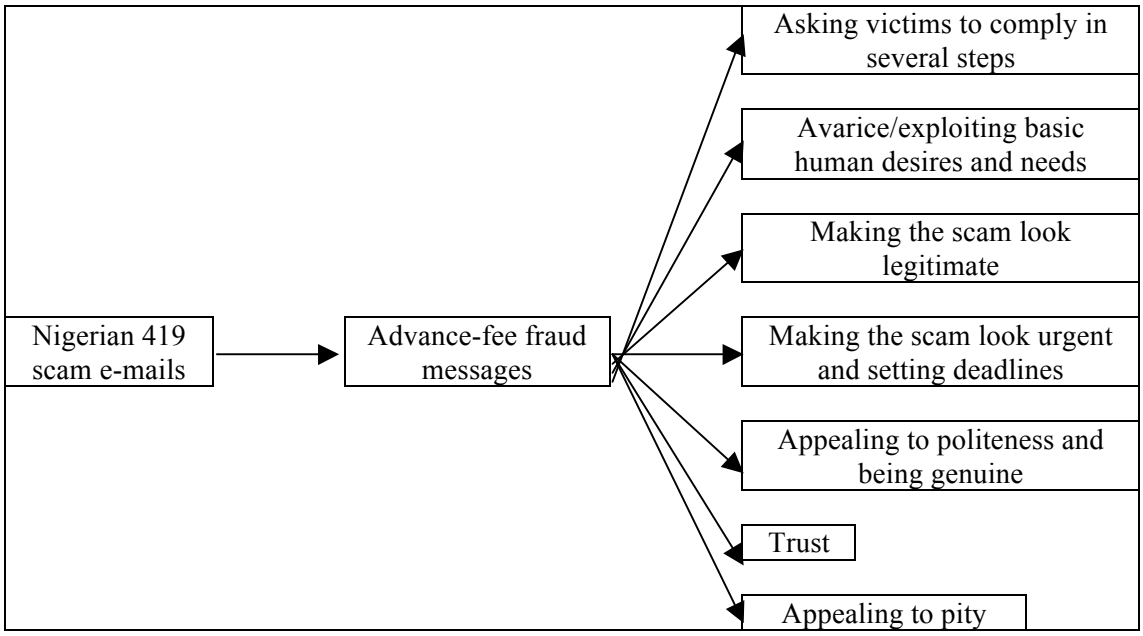

FIGURE 1. Diagram of persuasion strategies employed in Nigerian 419 scam e-mail messages

DISCUSSION

The analysis and results revealed in the present study draw attention to the significance of how persuasion strategies are exploited in Nigerian 419 scam attacks. The findings indicate that persuasive techniques are a must for 419 scammers when writing their scam e-mails. Moreover, two perspectives of examining these persuasive elements have been observed, frequency-based and characteristic-based. Viewed from the frequency of use, two types of persuasions (ie asking victims to comply in several steps and avarice/exploiting basic human desires and needs) are considered primary strategies, which are utilised to increase the attention of e-mail readers. The first strategy was found to be deployed in all e-mails in the present corpus (100%) and the second in almost all of the collected e-mails (96%). It is apparent that 419 scammers want to deploy these two tactics in combination in order to disguise their deceptive intentions as ordinary business contents in which a series of compliance may be requested and simultaneously try to provoke intuitive reactions by exploiting basic human desires and needs. The fact that the recipient is requested to perform tasks in sequence is corroborated by the notions of conformity, compliance and obedience (Huang & Brockman, 2011) which cause changes in people's behaviours (Raman, 2008). Avarice here can be compared to attraction/excitement which is the most frequently used strategy (94%) in the advance-fee fraud e-mails corpus as reported by Atkins and Huang (2013). Persuasions of lesser importance lie in making the scam look legitimate (78%), making the scam look urgent and setting deadlines (58%), appealing to politeness and being genuine (54%), trust (48%) and appealing to pity (20%). The use of legitimacy, urgency, politeness and pity in Atkins and Huang's (2013) corpus accounted for a bigger share, 84%, 70%, 78% and 31% respectively, whereas trust which bears comparison with formality in these researchers' corpus represented a lesser recurrence (24%).

When viewed based on their characteristics, persuasive techniques like asking victims to comply in several steps, making the scam look legitimate, making the scam look urgent and setting deadlines as well as appealing to politeness and being genuine can be grouped as "framing-rhetoric triggers" because they contribute to the layout of the business English e-mail genre and rhetorical devices commonly seen in everyday business e-mails. The three remaining techniques (ie avarice/exploiting basic human desires and needs, trust and appealing to pity) can be categorised as "human weakness-exploiting triggers" as they focus on the human factors and tap into human emotions. By taking advantage of the rhetorical structure of the ordinary e-mails, 419 scammers employ a range of its common devices. The subject line of their e-mails may include words like alert, warning, attention, update followed by exclamation points. Formal salutations (eg Dear Sir/Madam, Dear Partner, Dear Beneficiary) or informal ones (eg Dear Friend, Hello, My Dear friend, Dearest, Dearly Beloved) are employed for saying hello to the addressee. 419 scammers may first introduce themselves and/or indicate the source or how the addressee's e-mail address has been obtained. Next, making up a fake story, asking for help and offering benefits are included in the e-mail body, followed by phishing (providing a fake form to fill in, luring into contacting a fake banking officer or introducing a new contact person and/or giving new contact details). Before ending their e-mails, 419 scammers never forget to prompt their recipients for further contact and close with polite phrases or motivate the addressee to do the desired action. Formal closures (eg Yours sincerely, Best regards, Yours Faithfully, Sincerely) or informal ones (eg Thanks, Goodbye, Thanks and regards, Yours in Christ) are used. Finally, their e-mails end with a mimic signature block. By exploiting human weaknesses as scam triggers, 419 scammers as skilful manipulators are able to successfully strategise and complete their emotional attacks on people through their psychologically-constructed communications. They know that generally, a strong desire for more wealth exists in human beings, hence, making it more prone for an individual to be easily attracted by a fabulous opportunity. What is more, once a person is given the impression that someone has a feeling of confidence in him/her and offered a win-win proposition for consideration, he/she has a tendency to comply. Since humans generally have a natural feeling of kindness and understanding for someone who is experiencing something very unpleasant, they are always willing to lend a hand. Psychologically, these 419 scammers are not attempting to steal the victim's money, they are in fact exploiting moral principles and values so as to gain power over their victims (Dion, 2010).

CONCLUSION AND IMPLICATIONS

The present study posits that in the ever-evolving world of technology and communications, there is a massive array of fraudulent scams spreading over the Internet in various forms, one of which is Nigerian 419 scam e-mails. The writers use persuasion techniques as cunning luring strategies or a tool for their deception. Based on a textual analysis for examining language characteristics of 50 e-mails of this particular type, the study revealed two major types of persuasive techniques which are used in combination, namely framing-rhetoric triggers, which are disguised as the traditional genre of electronic communications and human weakness-exploiting triggers, which are intended as incitement of recipients' emotions. These results lend support to the idea that the best strategy to tackle this socially-globalised problem is "to educate the public on potential threats from perpetrators" (Atkins & Huang, 2013, p. 23). This is because online fraud seems to be ineradicable since globalisation has progressed constantly.

On this basis, two implications have been drawn. First, for general internet users, the realisation that "...the Internet, with its potential for mass mailings, for anonymity and global

reach, has transformed what was a minor source of fraud to a significant criminal threat" (Cukier, Ngwenyama & Nesselroth-Woyzbun, 2008, p. 87) is really worth noting. They should keep it in mind that scammers are successful persuaders who receive considerable, albeit disreputable, rewards for their endeavours. Sensible people are prone to succumb to the allure of instant fortune scammers are luring. Developing their decisive faculties for examining Web information is definitely worth a try. For prevention and protection, Manson (2011) suggests that one important way to protect ourselves and others from scams is to report them to the authorities in order that enforcers can take action to stop scams not to cause widespread harm. Another way is to increase awareness of scams and educate consumers on how to avoid scam e-mails. Extravagant promises may successfully lure those who are not sceptical about the trick scammers play. Stories with the fabulous condition may be created to trap the recipient. It is likely that stories that sound too good to be true are of the scam type. In addition, since the scammer always rushes the recipient into making a prompt decision, it is recommended that the recipient take time to read any suspicious e-mail carefully. Personal information such as bank details, e-mail password or any personal data should be strictly protected. To protect your personal computer, a number of unsolicited e-mails should be regularly deleted. Anti-spam software and a firewall should also be installed in your computer.

Second, awareness of scams should be raised among those involved in the educational field. According to Kiang (2003), students are likely to use e-mails for their future occupational communication. Therefore, teachers should first understand the nature of e-mail communication in order to enlighten their students about e-mails' characteristics. As a teacher of English, the authors of this article posit that a negative mode of electronic communication, especially scam e-mails is also worthy of students' attention before they enter the working world. If they happen to receive such e-mails, they will not become victims of those scammers. The language features of Nigerian 419 scam e-mails containing psychological attacks should thus be brought to the students' attention as a warning of scam hazards. Nigerian 419 scam e-mails and business English e-mails look somewhat alike. Both genres share certain features of the e-mail genre layout. Business English students or pre-business professionals should be advised that the messages in the Nigerian 419 spam genre are usually crafted to resemble the traditional genre in their manifest form in order to enhance the possibility of bringing out certain behaviours. But the actual intent of this kind of spam is in fact dissimilar to what the messages appear. In-class group discussions can be assigned for students to analyse such issues as persuasion strategies, audience, language usage, or format of this kind of e-mails. Hard-to-believe stories described in the scam e-mails can serve as entertaining classroom activities. More in-depth research exercises can also be carried out in terms of researching some of the names mentioned in the factual content of 419 e-mails to see whether these people are really identifiable. In the same way, having students examine some of the websites mentioned in 419 e-mails can be another interesting assignment. Gillespie (2012) has also proposed the practice of cross-curricular lessons, which may bring about possibilities for interdisciplinarity knowledge. For example, computing teachers can provide lessons about anti-virus software, IP addresses, Trojan horses and other forms of hacking whilst the geography department could lecture on why most scam e-mails originate in poor African countries.

The present study also provides a few research agendas for future studies. Due to a small sample size used in the analysis, this research is the only a starting point for further work investigating scams and how they work in a corpus of a larger number of sampled e-mails. Moreover, further work should include persuasive techniques employed in other kinds of spam, for example finance (mortgage, loans); business opportunity (investment, money making); adult-orientated products/services (entertainment, male enhancement, singles);

health (prescriptions); computer hard/software; sales; others (recruiting, gaming, miscellaneous, news, sports, politics). Needless to say, new electronic forms are emerging with hidden agendas as the globalised world progresses continually. Thus, it would be worthy to investigate how spam genres are adapting. Lastly, examining the behavioural characteristics of consumers (eg spam addressees, scam recipients) is also of interest.

ACKNOWLEDGEMENT

The authors would like to acknowledge the constructive comments and suggestions of the reviewers, which have improved the quality of this paper. Our heartfelt thanks also go to the editor-in-chief for her invaluable advice for the well-formedness of language used in this article.

REFERENCES

Atkins, B. & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences. 1*(3), 23-32.

Brown, J. D. (1996). *Testing in Language Programs*. New Jersey, NJ: Prentice Hall Regents.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, narrative and the "Nigerian Letter" in electronic mail. HICSS 2007 Conference Proceedings, 3-6 January, Hawaii doi: 10.1109/HICSS.2007.238

Cukier, W. L., Ngwenyama, O. & Nesselroth-Woyzbun, E. J. (2008). Genres of Spam: Expectations and Deceptions. *Scandinavian Journal of Information Systems. 20*(1), 69-92.

Dion, M. (2010). Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives. *International Journal of Cyber Criminology. 4*(1&2), 630-642.

Dyrud, M. A. (2005). "I bought you a good news": An analysis of Nigerian 419 letters. ABC 70th Annual Conference Proceedings, 20-22 October, Irvine. Retrieved from http://www.businesscommunication.org/conventions/Proceedings/2005/PDFs/07ABC05.pdf

Fraud.org. (n.d.a). Top Scam of 2014. Retrieved from http://www.fraud.org/images/PDF/2014_fraud_report.pdf

Fraud.org. (n.d.b). Top Scam of 2011. Retrieved from http://fraudresearchcenter.org/wp-content/uploads/2012/02/National-Consumers-League-2011-Top-Scams-of-2011.pdf

Fraud.org. (n.d.c). Nigerian Money Offers. Retrieved from http://www.fraud.org/scams/direct-marketing/nigerian-money-offers

Gillespie, A. (2012, July 16). Using Spam Emails in your Classroom [Weblog post]. Retrieved from http://www.theguardian.com/teacher-network/2012/jul/16/spam-emails-classroom

Huang, W., & Brockman, A. (2011). Social Engineering Exploitations in Online Communications: Examining Persuasions Used in Fraudulent E-mails. In T. Holt (Ed.). *Crime Online: Correlates, Causes, and Context* (pp. 87-111). Durham, NC: Carolina Academic Press.

Kiang, N. Y. (2003). A Discourse Analysis of E-mail Messages in a Malaysian Business Community. *GEMA Online® Journal of Language Studies*. *3*(1), 1-12.

King, A., & Thomas, J. (2009). You can't Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian E-mail Scams. In F. Schmallegar, & M. Pittaro (Eds.). *Crimes of the Internet* (pp. 206-224). Saddle River, NJ: Pearson Education.

Mann, I. (2008). *Hacking the Human: Social Engineering Techniques and Security Measures*. Burlington, VT: Gower Publishing Company.

Manson, L. (2011). Crimes of persuasion: Scams and their victims. Edinburgh: The Scottish Association of Citizens Advice Bureaux - Citizens Advice Scotland. Retrieved from http://www.cas.org.uk/system/files/publications/crimes-of-persuasion.pdf

National White Collar Crime Center (2014). Internet crime report. Washington, DC: Bureau of Justice Assistance. Retrieved from https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

Nigeria - The 419 Coalition Website. (n.d.). The Nigerian Scam (419 Advance Fee Fraud) Defined. Retrieved March 28, 2015 from http://home.rica.net/alphae/419coal/

Perloff, R. M. (2010). *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century* (4th ed.). New York, NY: Routledge.

Raman, K. (2008). Ask and You Will Receive. *McAfee Security Journal*, *Fall*, 9-12.

Ross, D. (2009). ARS Dictaminis Perverted: The Personal Solicitation E-mail as a Genre. *Journal of Technical Writing and Communication, 39*(1), 25-41.

Rovinelli, R. J., & Hambleton, R. K. (1977). On the Use of Content Specialists in the Assessment of Criterion-referenced Test Item Validity. *Dutch Journal of Educational Research. 2*, 49-60.

Sandler, C. (2010). *Teen's Guides: Living with the Internet and Online Dangers*. New York: Facts on File.

Stajano, F., & Wilson, P. (2009). *Understanding Scam Victims: Seven Principles for Systems Security* (Report No. 754). Cambridge: University of Cambridge Computer Laboratory.

Thompson, S. (2006). Helping the Hacker? Library Information, Security, and Social Engineering. *Information Technology and Libraries. 25*(4), 222-225.

Upton, T. A. & Connor, U. (2001). Using Computerised Corpus Analysis to Investigate the Textlinguistic Discourse Moves of a Genre. *English for Specific Purposes. 20*, 313-319.

Viosca, R.C., Bergiel, B.J. & Balsmeier, P. (2004). Effects of the Electronic Nigerian Money Fraud on the Brand Equity of Nigeria and Africa. *Management Research News*. *27*(6), 11-20.

Workman, M. (2008). Wisecracker: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of Personality and Social Psychology. 9*(2), 1-27.

APPENDIX

AN EXAMPLE OF NEGERIAN 419 SCAM E-MAIL

Dear Friend.

My name is Mr. Zango Mbaka, an Accountant with a bank in West Africa. I will like you to indicate your interest to receive the transfer of US$8.5 Million. I got your contact from the Internet on my search for Honest/ Reliable person or company to execute this business together.

SUBJECT: After due consideration, I have fully agreed to privately invest extensively in a very business venture. I am intending to retire from government services to private business I decided to contact you for an urgent business proposal. I have decided to deal with a neutral person like you because of the nature of the transaction as I will equally be happy to arrange with you on terms of trade and possible transfer of the funds needed for the investment into your company's account or personal account.

To enable me start the process and remittance of the fund into your bank account successfully within 14 banking days, I need the following information from you by e-mail:
1.Full name:
2.Full Address:
3.Country:
4.Private cell phone:
5.Occupation:
6.Age.

Note that as soon as I receive this information forwarded it the appropriate departments for final processing and approvals. With the modalities I have worked out to makes it possible for you to act as the next of kin to my late customer whose account is presently dormant for claims who died 10 years ago with his family in a car accident.

This transfer is 100% risk free having done all the underground works locally for the smooth transfer of the fund into your bank account within the shortest period. I advised that you should keep this transaction a top secret and rest all correspondence to e-mail or phone only, because I am occupying a sensitive position in the government circle and also this is once in a lifetime opportunity.

Finally I want you to assure me that you will work on my instruction and my own share of the money will be safe. You will be rewarded with (40% which is $3.4 million) of the total sum for your honest assistance and co-operation, (60% which is $5.1 Million) remain for me.

Contact me by return mail for any question and further discussion on EMAIL: zangombaka2009@sify.com

Awaiting your urgent response.

ABOUT THE AUTHORS

Chitchanok Naksawat has an MA in English for Business and Industry Communication from the Faculty of Applied Arts, King Mongkut's University of Technology North Bangkok, Thailand.

Songyut Akkakoson is an assistant professor of English at King Mongkut's University of Technology North Bangkok, Thailand. He obtained his PhD in Applied Linguistics from University of Otago, New Zealand. His research interests include learning styles/strategies, EFL reading, English for business communication, English speaking anxiety, language identity and World Englishes.

Chek Kim Loi is a senior lecturer at Universiti Malaysia Sabah. After obtaining her PhD in Linguistics from University of Otago, New Zealand, she conducted her postdoctoral research in England. She has published papers in various international journals. Her research interests cover genre analysis, intercultural communication, bilingualism and discourse analysis.