EZEKIEL OPEYEMI OLAJIMBITI
Elizade University, Nigeria

DOI: 10.15290/cr.2018.21.2.05

Discourse Pattern, Contexts and Pragmatic Strategies of Selected Fraud Spam

Abstract. The thrust of this paper is the pragmatic investigation of fraud spam, the unwanted emails containing the strategic use of language with the intention to swindle money from the recipients. Sixty (60) English medium email samples were collected from the author of the present paper's email spam between July 2017 and February 2018 in Nigeria. These were analysed using Halliday and Hasan's Generic Structure Potential and an aspect of Fetzer's cognitive context model. The study identified six discourse patterns: salutation, discourse initiation, enticing information, mild conscription into business, request and subscription; orienting to contexts of business and religion; manifesting pragmatic strategies of adversatives, evocation of business idea, evocation of religious affinity and evocation of messianic figure. The study, therefore, concludes that cyber-fraudsters deploy similarly familiar patterns and contexts evincing strategic persuasive language to defraud their prospective victims. Significantly, the study complements existing literature on fraud discourse in linguistic scholarship.

Keywords: Fraud spam, generic structure potential, mild conscription, messianic figure and cyber-fraudster.

1. Introduction

The ubiquitous nature of email fraud, the unwanted emails containing the strategic use of language with the intention to swindle money from the recipients, is a continuous social concern worthy of scholarly investigation. Studies have shown that millions of people, the world over, have become and still fall victims of this form of cybercrime because the fraudsters have not desisted from sending such emails. I was almost a victim a few years ago when I ignorantly responded to one of the emails in my spam account; at the verge of taking a loan in an attempt to raise the money requested by the fraudsters, but for the intervention of one of my acquaintances who divulged to me the secrete of cyber-fraudsters. The foregoing motivated this study, the pragmatic investigation of fraud spam, with a view to determining the discourse patterns, contexts and pragmatic strategies that are often evinced in the criminally oriented and fraudulently characterised emails allegedly sent to recipients to swindle money from them.

Hua, Abdollahi-Gullani and Zi (2017) aver that the issue of the victim's vulnerability has continued to be on the increase and the reasons behind it certainly deserve further linguistic and

Metalinguistic scrutiny. Studies in this direction have not been widespread due to the search for appropriate methodologies. Significantly, the existing studies have mostly covered linguistic discourse analytical approach (Chiluwa 2009, 2013; Barron 2006; Orasan and Krishnamithy 2002; Heyd 2008). The present study, therefore, complements these studies by its adoption of a discourse-pragmatic approach to email fraud (cyber fraud) in linguistic scholarship in Nigeria.

Email (electronic mail) is one of the most frequently used services in the net. Runkehl, Siever and Schlobinsk (1998) claim that email is quicker than ordinary post service, cheap, and can be sent to a lot of addresses simultaneously. This seemingly friendly phenomenon has been greatly abused for fraud purpose. Email fraud includes fake lottery winning announcement or fake business invitation, money transfer, investment opportunity, dormant account claim invitation, money inheritance information (Chiluwa 2013:1). According to him "in the last ten years, email as a form of computer-mediated communication (CMC) has increasingly become the main medium for perpetrating digital deceptions, email fraud or digital lies.

Fraud, according to Idowu (2009: 629), is the deliberate falsification, camouflage, or exclusion of the truth for dishonesty/ stage management to the financial damage of an individual or an organization. It is the dishonesty or an act of cheating someone or business to give up possession of some lawful right (Polick 2006). In their view, Fadipe-Joseph and Titiloye (2012: 215) refer to fraud as any actions by which one person intends to gain a deceitful advantage over another.

2. Related studies

The continuous rise of cyber fraud cases demands serious preventive actions that would emanate from scholarly investigations. Chiluwa (2009) investigates the pragmatics of hoax email business proposals; where he applies speech acts theory to the study of discourse strategies and functions of hoax email. He classifies this as "419 emails", being the Nigerian term form all forms of online fraudulent acts. His submission is that such practices have become a regular part of our internet social life since economic hardship being witnessed by the world today can force people to criminal activities.

The attention of researchers has continued to be drawn to the strategies deployed by these fraudsters to swindle money from their intending victims. For instance, Behman, Azabdaftari and Hosseini (2011) identify persuasive strategies of personalization, presupposition and lexical choices as frequently being used by fraudsters in financial fraud spam emails. In a similar vein, Hiss (2015) in his study on fraud and fairy tales: storytelling and linguistic indexicals in scam emails, opines that most of us receive numerous spam emails, text that in one way or another try to convince us to engage in transactions of enormous sums of money, promising unbelievable benefits. He argues further that in the fraudsters' attempts to get the recipients involved combining cultural indexicals, interactional roles and narrative strategies. Recently, Hua, Abdollahi-Gullani and Zi (2017), explore linguistic deception of Chinese cyber fraudsters. They argue that cybercrimes are on the increase in China, where fraudsters manipulate language to deceive users into revealing their bank account or depositing sums in the cheats' account. The study adopted speech acts and politeness theories to conversations of 50 interlocutors who had already chatted with different on-

line cheats in China. It submits that fraudsters manipulate language to present untruth as truth using online deceptions.

Proffering solution, Yoon et al. (2010:12) propose a hybrid spam filtering framework for email communication using a combination of contact-based filtering and challenge-response. The study performs some preliminary experiments to investigate whether plagiarism direction tools could be used as a filter form of spam emails. In a related view, Leap (2007:63-64) points out that email fraud may have either one of two objectives, first, fraudulent emails techniques may be used to cover up the misappropriation or misapplication of funds. Secondly, fraudulent financial statements may be issued by email writers to mislead the mail recipients. An overview of the literature, however, shows that the myriad of techniques can be broken down into four broad categories the first two are revenue based schemes and expense based schemes the two revenues are aimed at anticipating a firm current profitability as reported on the income statement. The third and fourth categories are asset-based schemes and liability-based schemes. Scholars like Young (2006) and Dechow et al., (2011) have, however, suggested that the primary motivation for email fraud is only a small subject of cases. Those fraudsters also use well-known business entities or organisations and charity instinct to deceive the recipients.

3. Theoretical perspectives: Generic Structure potential and cognitive context

3.1. Generic Structure potential

Generic Structure Potential directly derives from Contextual Configuration (CC). According to Odebunmi (2007: 88), "Generic Structure Potential (GSP) emerges from Halliday and Hasan's (1989) concept of contextual configuration, which has been added to the earlier Hallidayan context of situation dimensions". These functional linguists argue further that field is the social action or what is going on, and language is playing a significant role. It determines the register used. The tenor of discourse is the cluster of a meaningful relationship between relationships the participants in acts communication. CC gave prominence to the immediate constituents of a text, with no serious consideration to all the potentials of a genre. Therefore, GSP was developed to take into cognizance, all the possibilities that can occur in a text- obligatory, optional and recursive elements in possible orderings. It also refers to the staging of the genre at its attending sequencing and formalisation within the cultural experience. So it takes into cognizance all the features of texts possible by locating such within a specific genre if its structure is compatible with one of the possibilities specified by the GSP. The notations and their meanings are as follows: the dot (.) indicates more than one option in sequence, the round brackets ( ) represent optionality of enclosed elements, the square brackets [ ] show restraints of sequence, the braces with curved arrow { } indicate that the degree of interaction for elements in braces is equal, the caret sign ^ shows sequence. The choice of GSP to this study is significant in unpacking the discourse patterns of the

selected fraud emails. The structure of the theory allows for the sequences that characterise the content of email messages.

3.2. Cognitive context

Fetzer's contribution to cognitive context is adopted in this study. Cognitive context is a structured multilayered construct which is indispensable for language processing and inferencing. It is required for a cognitively based outlook on communication as it contains assumptions about mutual cognitive environments. According to Fetzer (2007: 12), "the nature of the connectedness between its constative layers and subsystems is meta-communicative and meta-systemic". Sperber and Wilson (1986: 95) stress that cognitive context refers to a set of premises, namely, true or possibly true mental representations. Deductive reasoning from the foregoing is that mental construct or representations on practical reasoning on language use are central to cognitive context. Fetzer identifies elements of this context as mental representations, propositions and contextual assumptions which may vary in strength and factual assumptions. Features of this context are deployed in accounting for the contexts the assumed cyber-fraudsters orient to by cognitively appealing to the psyche of the email recipients to defraud them.

4. Methodology

Data for the study consist of sixty (60) English medium email samples collected from the author of the present paper's email spam between July 2017 and February 2018 in Nigeria. These emails were retrieved from the spam to show that they were sent from the unknown individuals. Their contents reflect that they are crime-related manifesting money transfer, lottery, business and charity engagements. These were analysed using Halliday and Hassan's Generic Structure Potential to unpack the discourse patterns of the data and an aspect of Fetzer's cognitive context model to track the context the cyber-fraudsters orient to in defrauding the email recipients and pragmatic strategies often deployed for such intention.

5. Data analysis and findings

The analysis is structured into discourse patterns, contexts and pragmatic strategies. These are analysed in turn.

5.1. Discourse patterns of fraud emails

Six discourse patterns characterise the selected fraud emails reflecting the language use of the cyber-fraudsters, namely, Salutation (ST), Discourse Initiation (DI), Enticing Information (EI), Mild Conscription into Business (MCB), Request (RQ) and Subscription (SB). These are catalogued thus:

[ST] ^ [DI] ^ [EI] ^ [MCB] ^ {RQ} ^ [SB]

The catalogue shows that all the elements are obligatory as one stage sequences to another in fixed positions representing the discourse patterns of email fraud. These are analysed in turn.

5.1.1. Salutation (ST)

Salutation describes phatic communication in routine greeting addressed to the email recipients. Four forms of salutation characterise selected data are polite concentration seeking method, pious greeting, polite routine observance and social tie marker. The polite concentration seeking method relates to a form of greeting addressed to the email recipients to get their attention by using honorific and polite terms like 'sir'. An example of this is "Attention Sir". Pious greeting explains a Christian way of showing affinity with a person. Salutation like "Dearest in Christ" is intended to appeal to the religious minds of the recipients. Polite routine observance connects to the ritual-like function of language but in this case, the cyber-fraudsters affiliate to social tie and romance markers like "friend", "dear", "love" to dress the positive face want of the recipients to defraud them.

5.1.2. Discourse initiation (DI)

This elucidates how the email writers introduce themselves to their recipients, entailing self-presentation reflecting identity terms of name, sex and one's occupation. Noticeable in the selected data are the uses of pronouns: personal and possessive pronouns and fictitious personal details of the email writers. These are exemplified below.

Example 1

'I am Dr Takashi Shimada, Japanese origin

'I am Mrs Mary Martins, an ageing widow'

'My wife and I won the euro millions lottery of J53 million'

'My name is Alice Joe from UK'

The foregoing indicates first person and possessive pronouns through which email writers get themselves introduced to the recipients. Such pronouns are immediately followed by fictitious names of the cyber-fraudsters, who also disclose their social identity reflecting social status and national identity. These implicate self-presentation through identity acknowledgement to authenticate the emails but such strategy constructs pragmatic nuances of deception.

5.1.3. Enticing information (EI)

Enticing information projects persuasive narratives by the email writers with the intention to convince the email recipients to be interested in the conversation and thereby swindle money from them. Such narratives revolve around business, charity, health, friendship money transfer and ATM card. The following samples exemplify this further.

Example 2

'I have some funds I inherited from my loving husband Mr Martins J martins the sum us &3.800.000.00. (Mail 2)

Example 3

'I am … a woman who was diagnosed for cancer about 4 years ago I have decided to donate my fund ($ 2,000,000.00) (Mail 6)

Example 4

We have voluntarily decided to donate $2,000,000.00 (Two Million Dollars) to 5 individuals randomly as part of our own charity project.

Example 5

Friendship is a gift. It is a blessing that only the fortunate have. I am lucky to have a friend like you…

Example 6

Right now we have finally succeeded in getting your ATM CARD worth of $1.5 million out of delivery your ATM CARD with the help of Adams Mole Attorney General of Federal High Court of Justice Benin Republic…

Example 7

I am here to search for a business partner or friend who will help me to invest my fund in his company or country.

The foregoing evinces different narratives ranging from business, charity, ATM card, friendship related matters. These, though, look ordinarily convincing to engage the email recipients to initiate the process of defrauding them. Expectedly, this stage of the email arouses and activates the interest of the recipients as it creates psychological prominence in their thinking faculties.

5.1.4. Mild conscription into business (MCB)

The mild conscription into business stage describes amiably gentle encouragement and provocation of an invitation to lure an individual into business. Business in this context extends beyond buying and selling to any engagement of human beings. Therefore, MCB characteristically explains an allurement, enticement, or attraction of a written request for someone's presence or participation. Its manifestation in the selected data reflects assistance often solicited from email recipients in terms of fund management, business establishment and friendship engagement.

Example 8

We need your assistance by representing my company in Nigeria

Example 9

I need a very honest and God fearing person that can use these funds for God's work and 15% out of the total funds will be for your compensation…

Example 10

Beloved let us join hands together to help our fellow brothers and sisters who are poor, sick and homeless so that blessings will be ours while glory goes to the Lord our creator.

Example 11

Although, I just want us to become friends maybe something more if you wish, and I want you to write me back for more discussion with you as soon as you receive this email.

This trend is obviously noticeable in the sampled data. The email recipients are mildly lured into company representation, fund management and friendship as traps to engage them in further discussions that would lead to syphoning money from them. Importantly, these narratives are intended to active attitudinal disposition in the recipients.

5.1.5. Request (RQ)

This obligatory element captures the act of asking or employing email recipients to do something by responding to emails received to indicate interest or give more information on personal details with the intention to facilitate further discussions. This has been classified into two, namely, information request and inherent request. Information request describes the method the cyber-fraudsters deploy to know the identity and other personal details of the email recipients. Examples of such include: "reply us with your resume/CV", "reply back the message he will respond to you immediately", "please reply me back". These convey strategic means of getting the email recipients engaged to aid their dubious intention. Interest request in the same vein shows how fraudsters want the email recipients to be committed by positively responding to the enticing information already given. This is captured in the following: "I will give you more details if you show more interest", "Please kindly get back to me as soon as possible if you are interested", "Please if you would be able to use the funds for the charity works, kindly let me know immediately". These are politely constructed to appeal to the positive face want of the email recipients, especially with the frequent use of "please".

5.1.6. Subscription (SB)

Subscription signals the closure of an email as a similitude of formal correspondence. Usually, it entails closing remarks and marker of authorship of the emails. Three forms of subscriptions identified in this study are formal closure ("Yours sincerely, Dr Takashi Shimada, Executive Director"), pious closure ("Your sister in the Lord Mrs Martins"), informal closure ("Best regards, Alice"). One noticeable trend is that the salutation and subscription follow similar narrative features.

5.2. Contexts and pragmatic strategies

Two contexts namely, business and religion, configure the selected data. These heavily manifest in all the stages presented in the discourse pattern section. Of significance is the fact that the cyber-fraudsters orient the recipients of the emails to these contexts to trigger a positive response from them. These are analysed along with the following pragmatic strategies: adversatives, evocation of business idea, evocation of religious affinity and evocation of messianic figure.

5.2.1. Context of business

This context indexes linguistic features pointing to commercial engagement involving the production, buying and selling of goods and services and other monetary matters. Fraud emails writers often orient their intending victims to fictitious economic activities like investments, company representation, lottery related matters and so on with the intention to activate psychological relevance in them. This is exemplified in the following:

Example 12

I am the executive director American Devices and Diagnostics Manufacturers Association (AMDD), we specialize in the production of interventional cardiology product and other devices… we need your assistance by representing the company in Nigeria.

Example 13

I am here to search for a business partner or friend who will help me to invest my fund in his company or country.

Example 14

..will you like to come and work and live in the USA?

In Example 12, the following co-texts lexicalise business orientations: "Diagnostics", "Manufacturers", "production", "cardiology product", "representing" and "company" which also capture company representation. The co-tests in Example 13, are "business", "invest", "fund" and "company" all pointing to the idea of investment. These are put together to appeal to the cognitive minds of the recipients who could relate easily to the mental representations of a business idea. Mental representation is a key term in the cognitive context that explains a presentation to the mind in the form of an idea or image that can be perceived. These cyber-fraudsters conjure mental representation of huge monetary opportunity to their recipients whom they have seen indirectly as lower socioeconomic status people.

Two pragmatic strategies associated with this context are evocation of business idea and adversative. The former relates to creating an image of the fantastic business idea with huge monetary opportunity. Significantly, the strategy configures mental representations of an ideal business world, while the recipients are expected to infer this by contextual assumptions from the contents of the emails. Contextual assumptions as used in cognitive context framework refer to

meaning inferred from the stated utterances. The latter entails information packaging act for a business purpose which in most cases is to win more "customers" in a competitive business world. Ong (1981: 51) argues that "'adversatives' is universal, but 'conspicuous or expressed adversatives is a larger element in the business world". This is illustrated in this example: "I would like you to handle the contract of supplying a product to my company". In this case, the fraudsters deploy this strategy to deceive their intending victims who may want to assume that such adverts are real.

5.2.2 Context of religion

The context of religion relates to linguistic configuration characterised by a system of belief in a being and the activities that are connected with this belief system. In the context of this study, the Christian religion is portrayed. This is evidenced by the linguistic elements in the contents of some of the selected emails. Of significance in fraud discourse, is the context of religion; because it appeals more to the religious inclination of the intending victims to defraud them. All the emails with religious contents manifest charity services. The email writers deploy in this cognitively based communication religion and its associated activity of charity to seek mutual cognitive environment to perpetrate their dubious act. The following examples further illustrate this.

Example 15

I need a very honest and God-fearing person that can use these funds for God's work (charity) and 15% out of the total funds will be for your compensation for doing this work of God.

Example 16

…I have decided to donate my fund ($2,000,000.00) to you for charitable goals…I want you to use this fund to help the orphanage homes, poor, sick ones in the hospital…Proverbs 19:17: he who gives to the poor lends to the Lord and the Lord will reward such a person for good work.

The co-texts lexicalizing the context of religion and charity services from the foregoing are: "God-fearing", "God's work", "charity", "work of God". "donate", "charitable goals", "fund", "orphanage homes", "Proverbs 19:17", "Lord", "good work". These items are capable of mentally constructing celestial idea within Christian religion from these propositions in the minds of the email recipients, especially those who believe in this system.

Also, two pragmatic strategies related to this context are evocation of religious affinity and evocation of messianic figure. Evocation in this situation implies that the email writers cognitively create these pictures in the emails through their use of language. The evocation of religious affinity relates to the assumption of shared religious belief through which cyber-fraudsters disguise with the intention to defraud the email recipients. This strategy is deployed by using Christianity terms like "God's work", 'charity work", "Your sister in the Lord" and so on. They do this to orient to the religious beliefs of the recipients.

The evocation of messianic figure describes how the email writers project themselves as messiahs, philanthropists to their recipients. They deploy this strategy by mentally creating the figure of generosity to the people they want to defraud. Lexical items depicting this are: "compensation", "reward", "beneficiary", "you will receive 30%" just to mention a few.

6. Conclusion

It has been shown in the analysis and findings that six stages characterise the discourse pattern of email fraud, namely, salutation, discourse initiation, enticing information, mild conscription into business, request and subscription. Through these the email writers (cyber-fraudsters) orient to the context of business and context of religion; thereby hiding under these guises to defraud the email recipients. Through mental representations and propositions evidenced in the contents of the emails, recipients are expected to inferentially process the meanings via contextual assumptions. Meanwhile, pragmatic strategies of adversative and evocation of business idea distinguish context of business, while those of evocations of religious affinity and messianic figure manifest in the context of religion. The preponderance configurations of business and charity instincts in the selected emails align with Young's (2006) findings. This study has also shown that there is a heavy use of polite expressions; importantly deployed to appeal to the positive face want of the recipients to yield easily to their tact. The choice of GSP and cognitive context has significantly made the study to unpack the linguistic configuration of email fraud and track the cognitive undertone of such discourse. The study, therefore, concludes that cyber-fraudsters deploy similarly familiar patterns and contexts evincing strategic persuasive language to defraud their prospective victims. The study complements existing literature on fraud discourse in linguistic scholarship.

References

Barron, Anne. 2006. Understanding spam: a macro-textual analysis. *Journal of Pragmatics* 38(6), 880-904.

Behnam, Biook, Azabdaftari, Behrooz, Hosseini, Ali. 2011. A critical analysis of financial fraud spam in English in terms of persuasive strategies: personalization, presupposition, and lexical choices. *Journal of English Studies: Islamic Azad University, Science & Research Branch* 1(4), 15-26.

Blommaert, Janson. 2005. Making millions. English, indexicality and fraud. *Working Papers in Urban Language & Literacies* 29, 1-24.

Chiluwa, Innocent. 2009. The discourse of digital deceptions and "419" emails. *Discourse Studies* 11 (6), 635-660.

Chiluwa, Innocent. 2010. The pragmatics of hoax email business proposals. *Linguistik Online* 43(3), 32-48.

Chiluwa, Innocent. 2013. Email fraud. *International Encyclopedia of Language and Social Interaction*. Wiley Blackwell & International Communication Association (ICA).

Dechow, Patricia, M. 2011. Predicting material accounting misstatements. In: *Contemporary Accounting Research* 28, 17–82.

Fadipe-Joseph, Olubunmi, A., Titiloye, Emmanuel, O. 2012. Application of continued fractions in controlling bank fraud, *International Journal of Business and Social Science* 3(9), 210-213.

Fetzer, Anita. 2007. *Recontextualising Context*. Amsterdam/Philadelphia: John Benjamins.

Halliday, Michael,.A.K., Hasan, Ruqaiya. 1985. *Language, Context and Text: Aspects of Language in Social-semiotic Perspective*. Oxford: OUP.

Heyd, Theresa. 2008. *Email Hoaxes*. Amsterdam: John Benjamins.

Hua, Tan, K., Abdollahi-Guilani, Mohammad, Zi, Chen, C. 2017. Linguistic deception of Chinese cyber fraudsters. *The Southeast Asian Journal of English Language Studies* 23 (3), 108-122.

Idowu, Abiola. 2009. An assessment of fraud and its management in Nigeria commercial banks. *European Journal of Social Sciences* 10(4), 628-640.

Kerremans, Koen, K., Tang, Yan, Temmenman, Rita, Zhao, Gang. 2005. Towards ontology-based e-mail fraud detection (August, 2005). http://antiplushing.org/APWGplushingactivityReport August2005pdf.

Lan, Li. 2002. Email – a challenge to standard English? *English Today* 16 (4), 23-29.

Leap, Terry. 2007. *The Dynamics of White-collar Crime Ithaca*. NY: Cornell University press.

Odebunmi, Akinola. 2007. Explicatures and implicatures in News magazine editorials: the case of the Nigerian Tell. *Perspective on media discourse.* Rotimi. Taiwo, Akinola. Odebunmi and Akin. Adetunji. (eds.), 84-99.

Orasan, Constantin, Krishnamurthy, Ramesh. 2002. A corpus-based investigation of junk mails. *Proceedings of the 3rd International Conference on Language Resources and Evaluation*, 29–31 May, Las Palmas, Spain, Retrieved from: http://clg.wlv.ac.uk/papers/orasan-02b.

Ong, Walter, J. 1981. *Fighting for life: contest, sexuality, and consciousness.* Ithaca: Cornell University Press; Amherst: University of Massachusetts Press.

Polick M.Y. 2006. What is fraud? available at http://www.wisegeek.com.

Runkehl, Jens, Siever, Torsten and Schlobinsk, Peter. 1998. *Sprache+und+KomW munikation+im+ Internet:+Uberblick+und+Analysen*.! Opladen: Westdeutscher! Verlag.

Sperber, Dan, Wilson, Deirdre. 1986. *Relevance Communication and Cognition*. Oxford: Blackwell.

Young, Michael, R. 2006. *Accounting Irregularities and Financial Fraud: A Corporate Governance Guide*. 3rd edition. Chicago: CCH.