WILEY-
BLACKWELL
International Encyclopedia of Language and Social Interaction edited by Karen Tracy, Cornelia Ilie & Todd Sandel (*Wiley Blackwell & International Communication Association (ICA),*

Final Version accepted November 27, 2013

Email Fraud

Innocent E. Chiluwa
Covenant University, OTA Nigeria
Email: *innocent.chiluwa@covenantuniversity.edu.ng*

Abstract

Email fraud as is used in this context refers to different forms of deceptive email, particularly those motivated by the intention to defraud the addressee. This entry examines the common textual features of email fraud as well as their forms and discursive structures with reference to some specific samples. It also gives a detailed description of the approaches that have been adopted in the study of email fraud.

Main Text

Email fraud is differentiated from general spam mails or "email hoaxes" from the fact that it can result (or has actually resulted) in online scams, where a victim is swindled. Email fraud therefore, is not merely a *hoax* because it is false, "funny" or "a joke" (Heyd, 2008; Orasan & Krishnamurthy, 2002), but more importantly that it is criminally oriented and characteristically fraudulent. Hence, email fraud includes fake lottery winning announcement or false business invitation. The latter also referred to as "419 mail" or "yahoo-yahoo" in Nigeria, often comes in the form of a money transfer business invitation, investment opportunity, dormant account claim invitation or money inheritance information.

HISTORICAL OVERVIEW

Email fraud began in the late 1980s and early 90s mainly as hoax computer virus warnings and became common in the 2000s following the use of email technology to transmit internet business scams. Thus, 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.* The writers of this type of emails also referred to as "advance fee fraud" are generally unknown. Some scholars have however suggested that they come from Africa probably because most of the so-called dormant bank account claim/money transfer business invitations are presumably sent from the "African Development Bank, Ouagadougou, Burkina Faso." Some writers (e.g., Heyd, 2008) have claimed that "email hoaxes" are written by Nigerians, thus these kinds of messages are referred to as "Nigeria mails." Blommaert (2005) further opines that the writers come from the "periphery of the world" writing to addressees in the "core countries of the world system" (p.2). However, Chiluwa (2009) has argued that email fraud could have been written by anyone, just as the addresses shown on the mails are presumably those of Europe, Asia, Africa, and the Middle East.

TEXTUAL FEATURES OF EMAIL FRAUD

Some common features of these emails are that they are usually associated with money or "business," although they lack credibility and are usually unreliable. On the surface, many of them look genuine and business-like, often written with some degree of expertise in digital communication by the writers. Some of the emails have a veneer that sound very persuasive, but their arguments are usually not quite convincing. Generally, they sound too ambitious with a great deal of false promises and rewards. Very often, some bits of information in the messages are contradictory while some are outright nonsense. Due to their suspicious nature, most skeptical receivers of these deceptive mails immediately delete them from their inboxes as they come. Almost every internet user with an email account has received some forms of these hoax emails, and the fact that deceptive emails are encountered almost daily, suggests that there might still be people that patronize them. Samples of hoax "2009 e-lottery bonanza" and money transfer business invitation are reproduced here:

> ***(Ef1)***Your email address has brought you an unexpected luck, please read through this message. You have been approved to claim a total sum of 1,500,000.00 GBP (One million five Hundred Thousand Great Britain Pounds) in cash credited to file MSW/9080118308/02/LA.
> Contact Person: Name: Mr. Harris Howell.
> E-mail:harrishowell01@gmail.com
> Tel: +44–702–408–0951
>
> (**Ef2**)From: Jabolynne@aol.com from your e-mail list
> Sent: Sat, 28 Feb 2009 6:23 am
> Subject: Greeting
> I am Mr. Patrick Chan from hang seng Bank Hong Kong, there is the sum of $12,500,000.00 in my bank and i need you to work together with me to claim it, we shall then share in the ratio of 60% for me, 40% for you. Contact me for more details Email: patrickchan.12@hotmail.com. (Chiluwa, 2009)

DISCURSIVE STRUCTURE OF MESSAGES

The messages of email fraud are usually quite clear like those of the samples ***Ef1*** and ***Ef2*** above, i.e., someone with a particular email has won a lottery; some money in a dormant account in Hong Kong (or elsewhere) is ready to be shared or transferred; or someone had died in an air crash leaving his wealth for the addressee. In ***EF3*** below for example, the addressee is to act as an expert business entrepreneur on behalf of a four-year old child whose father (the writer) has been diagnosed with cancer and has but a few months to live. In all the described situations, the receiver is to contact a named person in the email, or is urged to treat the message in confidence and of course, to act fast. In most cases, the receiver is reassured of his/her personal safety and the genuineness of the business. In some of the mails, the writers come in the name of God, and tacitly appeal to the religious sentiments of the receivers (see Blommaert, 2005; Chiluwa 2009).

Because deceptive emails are letters written as narratives, they consist of greetings and introductory notes about the writer. Then there is the content - showing the subject matter and including some persuasive argument in the body of the message. The concluding part ends with a sign-off and short explanatory notes of reassurance. The tone and style of the emails generally resemble that of normal interpersonal email, which sometimes makes it difficult to distinguish them from the genuine (Orasan & Krishnamurthy, 2002). Language forms of the emails are unsophisticated, and according to Blommaert (2005) belong to the "grassroots," level of English, which unfortunately does not match the advanced digital performance of the writers. This is one of the main kinds of evidence that tend to prove that the writers of email fraud may have come from non-English speaking countries (e.g., Africa and Asia).

> ***(EF3)*** **Reply Soon!**
> Saturday, October 4, 2008 6:32 AM
> **From:** "David Ibrahim" <diddibrahim@gmail.com>
> **To:** undisclosed-recipients
>
> My name is David Ibrahim, a merchant in Oman. I have recently been diagnosed with esophageal cancer, which has defiled all medical treatment. Expert diagnosis has shown that I have few months to live. The intention of this email is to employ the expertise of a business entrepreneur, who can identify a viable investment and guarantee reasonable returns on my wealth. This is to secure a future for my 4 years old son who lost his mother during birth. I cannot rely on his closest relatives any more, as they did not show responsible behaviour two years ago when I entrusted half of my wealth to them to invest on his behalf. They thought I wouldn't survive the operation and then used the money for their personal needs. To prevent any more mishaps, my attorney will act as a check, monitoring every aspect of the

investment. Funds should be split in half and distributed to charity organisation and the other half, as investment for my son. If this interests you, please reach me on the email address: david.ibrahim@mcom.com to discuss terms and compensation.

Kind regard
David Ibrahim

APPROACHES TO THE STUDY OF EMAIL FRAUD

Studies in email fraud are not yet widespread probably due to the search for appropriate methodologies. The first studies of hoax emails focused on fake email virus warnings and "junk emails," which also included "hot" business opportunities. There are also studies of "web of deception," "email forwardables" and unsolicited mails. These unsolicited emails included virus warning and alerts, spam emails, and email hoaxes. For instance, Fernback (2003) studied traditional oral folklore among online discussion groups and examined how it blends with the literate textual online environment. She adopted a macro-textual or "formal" analytical approach in the investigation of features of "oral folklore-urban legends, among which are hoax emails, and the cultural significance of their existence" (p. 29) in online communication. The study concludes that the prevalence of urban legends on the web demonstrates that the cyberspace can serve as a platform for the practice and perpetuation of oral culture and "its attendant humanity and sociability in a simultaneously textual environment" (p. 29). Similarly Barron (2006) adopted a macro-textual approach in the genre analysis of spam emails in order to investigate the promotional function of spam emails about medical supplies. The study revealed that the emails are characterized by "obligatory moves" that consist of "persuasive communicative purpose in the specific rhetorical context in which spam mail functions" (p.100).

Orasan and Krishnamurthy (2002) applied a corpus linguistic methodology to investigate the linguistics features of junk mails. Their study identified some lexical and grammatical characteristics of the emails in order to decide whether junk emails constituted a distinct genre. The study argues that junk emails form a distinct genre of spam mails with a consistent distribution of words such as *free*, *money*, *investment*, *credit*, *sex*, *miracle* etc. across the corpora used for the study.

Kibby's (2005) study is a textual analysis of "forwardables" and she concludes that emails have enabled the birth of "new folklore" as well as an effective and rapid distribution medium for gossip, rumor, and urban legends. Anne Mintz's (2002) edited book, *Web of Deception: Misinformation on the Internet*, harvested several insightful expositions of web hoaxes and counterfeit sites, most of which offer spurious information, as well as "lies and damned lies." Most internet data (hoax emails inclusive) according to the authors are replete with untrustworthy materials that are intentionally erroneous and misleading. And these, the authors argued, are capable of affecting the reader's health, privacy, investment and business decisions.

The first study of email fraud/online scam is that of Blommaert (2005) in which he studied "English, indexicality and fraud" in "email spam hoax messages." His study adopts a sociolinguistic approach to analyze the level of English competence of the writers. It is in this piece that he concludes that the writers demonstrate "grassroots" level of English, which do not march their advanced digital literacy. Blommaert's study further identifies generic features of email fraud with their varied indexical information and suggests that further linguistic, stylistic and generic studies of this genre of online communication are possible. In addition to the above study, Blommaert & Omoniyi (2006) argue that the authors of email fraud demonstrate technical competence to explore the opportunities that the global email systems offer them. However, they lack linguistic competence, which is the capacity of the writers to actually produce linguistic messages that are appropriate to the projected identities and relationships in the proposed transactions. The results are the kind of "rich indexical signals pointing towards fraud" (p.573) that are evident in the message. The study concludes that the genre of email fraud yields insights into the changing nature of communication in the era of globalization.

Perhaps, the most rigorous study of email hoaxes has been that of Heyd (2008). The term: "email hoaxes" is generally used to include "virus hoaxes, giveaway hoaxes, charity hoaxes, urban legends and hoaxed hoaxes" (pp.31-38). This research is described as a genre study that sets out to describe the various types of hoaxes, as well as their structural and discourse features. Analyses of data are based on a linguistic/discourse analytical approach, consisting of a qualitative methodology that requires the description of the forms of email hoaxes, their pragmatic contents and communicative purposes. Analyses also include an account of their textual patterns, persuasive strategies, narrative structures and sequences. An offshoot of this research is Chiluwa's (2009) study of "digital deceptions and 419 emails." The study analyzes the discourse structures and functions of email fraud and concludes that the writers of deceptive emails apply both discourse and pragmatic strategies to make their messages persuasive. As a follow-up on the above study, Chiluwa (2010) analyzes the pragmatics of hoax email business proposals using speech act theory. His study reveals that the fake business proposals actually perform "speech acts," the most frequent being the representative act. According to Paul Grice, the "representative act" is the act of describing, stating, asserting or claiming. This is possible in the emails since they are structured as narratives. The above studies of email fraud show that research is still evolving with a promise of greater research interest in this interesting aspect of Computer Mediated Communication.

CONCLUSION

Email fraud is recognizable not only by its suspicious content but also by its style. As many more people increasingly become aware of the fake promises, obvious lies, and

criminal intents of email fraud, it is to be expected that fewer people will be deceived by them. Email fraud is an interesting emerging genre of CMC, not only in linguistics but also in communication and cultural studies. However, although a new area of study, it is not a distinctive genre of asynchronous CMC of its own. It is therefore recommended that greater research focus be accorded this emerging area of new media communication. This will enhance greater research impetus and contribute in no little way to the development of wider approaches and methodologies from media studies, psychology, cultural studies and perhaps sociology to the study of email fraud.

SEE ALSO evasive or untruthful discourse → morality in discourse → strategic maneuvering → indexicality

References

Barron, A. (2006). Understanding spam: A macrotextual analysis. *Journal of Pragmatics 38*(6), 880–904.

Blommaert, J. (2005). Making millions: English, indexicality and fraud. *Working Papers in Urban Language & Literacies 29*, 1–24.

Blommaert, J. & Omoniyi, I. (2006). Email fraud: Language, technology and the indexicals of globalisation." *Social Semiotics 16*(4), 573–605.

Chiluwa, 1. (2010). The pragmatics of hoax email business proposals. *Linguistik Online 43*, 3.

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

Fernback, J. (2003). "Legends on the net: An examination of Computer-Mediated Communication as a locus of oral culture," *New Media and Society 5(1),* 29–45.

Heyd, T. (2008). *Email Hoaxes*. Amsterdam: John Benjamins.

Kibby, M. (2005). Email forwardables: Folklore in the age of the Internet," *New Media & Society 7*(6), 770–779.

Mintz, A. (Ed.). (2002). *Web of Deception: Misinformation on the Internet*. Medford, MA: CyberAge Books.

Orasan, C. & Krishnamurthy, R. (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.