

## **A Critical Analysis of Financial Fraud Spam in English in Terms of Persuasive Strategies: Personalization, Presupposition, and Lexical Choices**

**Biook Behnam\***

Islamic Azad University, Tabriz Branch, Tabriz, Iran

**Behrooz Azabdaftari**

Islamic Azad University, Tabriz Branch, Tabriz, Iran

**Ali Hosseini**

Islamic Azad University, Tabriz Branch, Tabriz, Iran

**Received: December 19, 2012**

**Accepted: February 13, 2013**

---

**ABSTRACT:** The term ‘spam’ addresses unsolicited emails sent in bulk; therefore, the term ‘financial fraud spam’ refers to unwanted bulk emails in which different tricks and techniques are employed to swindle money from the recipients. Estimates show that more than 80% of worldwide email traffic in 2011 was spam. It should be noted that while the number of daily spam emails in 2002 was 2.4 billion, this number rose to 200 billion spam emails in 2011. Considering the incurred cost of spam emails, finding effective ways for identifying spam emails may help decrease the cost to a great extent. It must be borne in mind that the generators of the financial fraud spam emails employ intricate persuasive strategies that make their stories believable to the readers. In an attempt to unravel some of these persuasive strategies, the present paper focuses on the use of presupposition, personalization, and lexical choice that are frequently used by the generators of the financial fraud spam emails. The results of the analysis showed that the above mentioned persuasive strategies were widely used in the text of financial fraud spam emails. Furthermore, the study demonstrated that persuasive lexical devices were used throughout the spam emails, including the email addresses. In terms of personalization and presupposition, the study showed that all parts of the spam emails, except the address section, were subjected to the use of these persuasive strategies.

---

**Keywords:** financial spam, lexical choices, personalization, persuasive strategies, presupposition

---

The term *discourse* addresses the whole process of social interaction (Fairclough, 1989); therefore, discourse analysis is concerned with the analysis of language in its social context (Matthiessen, McCarthy & Slade, 2002). According to van Dijk (2001), the term *discourse* covers the broad meaning of communicative event, e.g. interaction, written texts, images, associated gestures, etc. Communication among individuals can be accomplished through different devices, and the development of new technologies has provided new ways for communication. It should be noted that the change of technology directly affects the discourse (Scollon & Wong, 2004). The popularity of the internet in recent decades has given rise to new communication devices like email. Sending email is an easy, cheap and widespread method for connecting people to the world. However, just like any other form of technology, email has its own problems. This paper focuses on one of these problems, which is generally known as the spam emails.

---

\* Corresponding author's email address: behnam\_biook@yahoo.com

The term ‘spam’ refers to unsolicited or unwanted emails sent in large quantity (Hoffman, 1997). Spam emails can be classified based on their characteristics, e.g. the level of danger, topic and content, and source country. Sometimes the categorization process is based on the aims and effects that spam emails carry (Sophos, 2005). Financial fraud spam is one of the main spam categories that deal with unwanted emails that are generated to persuade the recipients to behave in a certain way (Garcia-Molina & Gyöngyi, 2005). In these emails, the ultimate goal of the spammer is to swindle money from the recipients.

In this study, the researchers try to analyze spam emails to uncover persuasive strategies that spammers employ in their emails. To this end, 36 genuine financial spam emails are collected and analyzed based on the following persuasive strategies: *personalization*, *presupposition*, and *lexical choices*. In addition to frequency counts, the researchers also focus on the strategies that spammers employ to deceive the recipients of spam emails. The present research highlights the personalized items that spammers employ to create a sense of trust in their readers. It also unveils the presuppositions that spammers use to infuse a particular thought into the mind of the recipients.

In line with these purposes, the present study is designed to answer the following research question:

What is the occurrence rate of presupposition, personalization, and lexical choices in financial fraud spam emails and how are these persuasive strategies positioned and used within the spam emails?

This main research question can be broken down into three sub-questions:

1. Are presupposition, personalization and lexical choices used in the text of the financial fraud spam emails?
2. If the answer to the first question is positive, what is the occurrence rate of each persuasive strategy in the text of financial fraud spam emails?
3. How are these persuasive strategies positioned and used in the text of financial fraud spam emails?

## **Persuasive language**

Language is considered as a tool or medium through which different opinions, ideas, goals and purposes are expressed. In fact, language is a ubiquitous component of our personal, educational, and professional life (Woods, 2006). When someone tries to convince or persuade an individual or a group of individuals in daily life, he/she takes advantage of reasoning, instantiating, or even specific intonation and non-verbal techniques in order to affect the audience or make them believe a claim. Hence, persuasive language and persuasive techniques are used in almost any society and by almost all people in different contexts. For instance, political elites may exercise power through language (Behnam, 2008), and commercial advertisers may employ some persuasive language to encourage consumerism and create artificial needs (Koteyko & Nerlich, 2007).

Therefore, while employing persuasive techniques and strategies sometimes seems to be an immediate and spontaneous action or reaction, in some other cases, it is a skill which can be or even should be taught. According to Johnston (2008), when people think that it is necessary to persuade others to behave or act in a desired way, they may consciously employ a certain form of discourse. Critical discourse analysis is widely concerned with such types of discourse. The term “critical” here addresses the associations that are probably hidden from people (Fairclough, 1989). It also addresses the concentrations on social problems and issues in different domains of science (Wodak, 2002a). In this sense, critical discourse analysis may concentrate on the problems that a group or groups of people suffer from (Meyer, 2002). Critics in this regard may aim at finding and revealing injustice, paradox, and inconsistency in different types of discourse (Wodak, 2002b).

One important point in this regard is that persuasive language does not necessarily refer to employing positive, attractive, or deceptive words and ideas but sometimes warning, and threatening may also be used to persuade the audience (Behnam & Jabbarpour, 2012). A military recruitment advertisement, for instance, may emphasize an enemy and warn about a war in order to encourage the youth to join the army (Behnam & Kuhl, 2008).

### ***Lexical choices***

In order to persuade the addressee, discourse producers need to choose the right words in the related context. Persuasive words and terms refer to those words and terms which try to grab the attention of their audience in a particular context or persuade them to think or act in a certain way (Woods, 2006). For instance, when watching, reading or hearing a piece of advertisement about an arm chair, words such as “new”, “comfortable” and “beautiful” may be used widely. These descriptive words are used to demonstrate the product in a more attractive way. Different contexts may host different words for persuasive purposes. The point which has to be noticed here is that what makes a word to be considered persuasive in a given discourse is the context in which it is used. Hence, lexical choices are context-dependent. For instance, while the technical term “fuel-injector system” may play the role of a persuasive word in public newspapers, it is not probably regarded as such in a special and expert automobile magazine. That is because the readers of auto magazines are mostly familiar with technical terms.

Legitimization is another technique which is frequently employed in social and political contexts. This technique is mainly used by politicians who “legitimize their actions in front of their audience in the hope of gaining acceptance” (Behnam & Kheradmandi, 2009). Providing good reasons or acceptable motivations for a past or present action which is subject to criticism are among the techniques that are used for legitimization (van Dijk, 1998). In this case, words such as “legal”, “official” and “government” can be considered as legitimizing words.

### ***Presupposition***

In some cases the intended meaning of an utterance or a sentence is different from what it appears to be at first glance. In presupposition, an advertiser, politician, or manager tries to infuse a supposition into his audience’s mind to persuade him to act in a desired way. As an example, a spammer had included the following phrase in one of the spam emails that was used in the present research: *Send your e-mails to: smortgage@dhimail.com*

The above phrase is composed on the supposition that the recipient will certainly reply to the spammer’s message. In fact, soliciting for further communication in this example is not created forthrightly. Instead, the spammer provides his own email address. He never asks whether the recipient prefers to reply the message or not. This is a technique that is used to encourage the recipients to have further communication with the spam generator. This is a common strategy that spammers use in different types of spam emails (Barron, 2006). While presuppositions can be studied semantically and pragmatically (Spenader, 2002), in the present research the focus is on their representation in critical discourse analysis and their persuasive function in the discourse of financial spam emails.

### ***Personalization***

When a person feels that an advertiser has exclusively devoted his time to him, he will be more encouraged to react by giving positive response. That is why in advertisements personal pronouns and direct phrases are frequently used. It should be pointed out that the present study focuses on ‘recipient-oriented’ and ‘recipient-and-sender-oriented’ personalization and disregards the ‘sender-oriented’ personalization. This is done due to the nature of spam emails. Discourse producers sometimes address themselves with personalized items such as the pronoun “we” (Woods, 2006); however, it seems that the case is justifiable only if the identity of discourse producer is clearly known. For instance, a famous company may address itself by the pronoun “we” to create a sense of intimacy with the audience to promote its products or services. But in the discourse of financial spam, spammers try to introduce themselves as creditable companies, organizations, and characters. Hence, they need to emphasize these fake personalities.

### ***Spam email***

The term *spam email* or *email spam* refers to ‘unsolicited’ emails sent in ‘bulk’ (Hoffman, 1997). In general, an email is considered spam when both of the above mentioned specifications exist. To clarify this point, these specifications are explained below:

- Unsolicited: this is one of the two obligatory specifications of spam emails. However, not all unsolicited emails can be considered as spam. For example, a surprise email from an old friend after some years is neither expected nor requested but it is not spam.
- Bulk: the word “bulk” is defined as size, mass, or volume, referring to a large quantity. Therefore, emails sent in bulk are numerous copies of a single email that are sent to many individuals. Again, not every email sent in bulk is spam. For example, a big company may send an email to thousands of its employees in order to inform them of its new strategies but obviously such a message should not be called spam.

## Methodology

### Materials

In order to conduct the research, 36 genuine instances of financial fraud spam emails were collected from the following online archive: [<http://www.419scam.org>]. The archive consists of thousands of financial spam emails which are arranged chronologically. A sample of a financial fraud spam is provided below:

From: "N Chan" <[sunchales@managerzone.com](mailto:sunchales@managerzone.com)>  
Reply-To: [vrteodoro2@gmail.com](mailto:vrteodoro2@gmail.com)  
Date: Thu, 8 Sep 2011 13:27:50 +0200  
Subject: hello

Hello, I'm Norman Chan, Tak-Lam, S.B.S., J.P, Chief Executive, Hong Kong Monetary Authority (HKMA). I have a Business worth \$47.1M USD for you to handle with me. I need you to assist me in executing this Project from Hong Kong to your country. After hearing from you, I shall provide you with detailed information regarding this Business.

Kind Regards,

N. Chan

Try the worlds greatest manager game online: <http://managerzone.com/>

### Procedures

In the above mentioned online archive, there are nine rows and twelve columns. It should be noted that the rows represent the years, which range from 2004 to 2012 and columns correspond to the 12 months of each year. In order to avoid time gaps for the selected samples, all the emails (total=36, 3 for each month) were selected from the 2011 archive. In order to make the selection process as random as possible, three samples were selected from the first day of January 2011; three from the second day of February 2011, three from the third day of March. This pattern was repeated for the other months.

### Labeling

One of the most important steps in this research was labeling the persuasive items. Labels are tags or categories which describe the characteristics of specific persuasive devices. Consequently, they clarify the reason for which an item is identified as persuasive. In the following section these labels are introduced:

#### Labels for lexical choices

- **Warn/Enc** (Warning / Encouraging): This label includes the words which try to push the recipient to act in a certain way. The words which urge the recipients or encourage them to act or react immediately are also included in this category. Furthermore, it is important to note that those words which warn the recipient about a threat or deadline fall within this category. Example: *immediately / be aware*.

- **Exp/Tec** (Expert / Technical): This label is used for expert and technical words, terms, names, or acronyms which augment the prestige or credit of an item or case. Example: *advanced ballot system*.
- **Legitimization**: This label includes judicial words or terms. Example: *legal / legitimate*.
- **Assuring**: Those words which try to ensure the recipient of the safety and security of any process or event. Example: *free of risk / secure*.
- **Accrediting**: This label includes those words, or terms that add to the validity of a phenomenon, proposition, person, or event. Example: *Ban Ki-Moon (the 8th Secretary-General of the United Nations) / World Bank / international*.
- **GPW** (General Persuasive Words): This label includes the words, mostly adjectives and adverbs, which try to strengthen the effect of another word, item, or case. Example: *never / soon / good / rich*.
- **Relig/Hmstic** (Religious/Humanistic): This label includes those words or terms which carry religious or humanistic senses. Example: *God Bless / true love*.

### **Labels for personalization**

Labels of personalization in the present research are of two types and they focus on the recipient or the recipient and the sender.

- Recipient: Items such as pronouns, names, which address only the recipient. Example: *you, your, yourself*.
- Recipient and Sender: Items such as pronouns, names, which address the recipient and the sender at the same time. Example: *we, us, ourselves*.

### **Labels for presupposition**

Persuasive presupposition is essentially aimed at infusing a pre-defined assumption into the mind of audience to make them behave or think in a particular way. In this regard, three labels were designated as follows.

- Past-Infusion: a presupposition which refers back to an event, act, request, etc. in the past. Example: [*Once Again, Thanks For Contributing To Our Financial Success!!!*] This statement claims that another (appreciation) message has been sent before.
- Present-Infusion: a presupposition which refers to an event, act, request, etc. in the present time. Example: [*All confirmable documents to back up the claims will be made available to you prior to your acceptance.*] This statement presupposes that the message-sender already has *confirmable document* and the suggested plan is legal.
- Future-Infusion: a presupposition which refers to an event, act, request in the future. Example: [*we have authorized Robert Calvin to assist you in getting your compensation check across to you*]. This statement presupposes that the recipient will receive a particular amount of money in the near future.

It is important to note that recording the total number of occurrences for each persuasive strategy was not enough and it was necessary to record and show the exact items too. If, for example, there were five presuppositions in a given spam email, it was necessary to show what those five items were and where they occurred in the text. The ‘Content Table’ was designed for this purpose. For each spam email there were three Content Tables, one for each of the three persuasive strategies. Since the data collection contained 36 spam emails, 108 Content Tables were needed. The tables below are sample Content Tables and the data inside them are derived from our selected corpus.

**Table 1. A Sample Content Table for Lexical Choices**

Persuasive Lexical Choices	Exact Item	Label
We will advise and <b>urge</b> you	urge	Warn/Enc

**Table 2.** *A Sample Content Table for Personalization*

Personalization	Exact Item	Label
Were <b>you</b> scammed	you	Recipient

**Table 3.** *A Sample Content Table for Presupposition*

Presupposition	Exact Item	Label
<u>Thanks for your</u> understanding and <u>co-operation</u> in this matter	Certainly you will co-operate with us	Future-Infusion

### ***Calculating the mean and percentage***

Counting the total occurrences of the persuasive strategies was not adequate because tallies won't lead to a systematic mechanism for comparing the outcomes. Therefore, it was necessary to calculate the percentage of occurrences for all the three persuasive strategies.

## **Results and discussion**

### ***Percentage and total mean***

After analyzing all 36 spam emails, the researchers calculated the percentage of persuasive strategies. One reason for calculating the percentage value rather than the frequency count was the length of the texts. When the lengths of the texts vary, the frequency counts of the strategies cannot be compared. To solve this problem, the total words of each spam email were counted by Microsoft Word 2003 software. Then, the percentage value was calculated using the following formula:

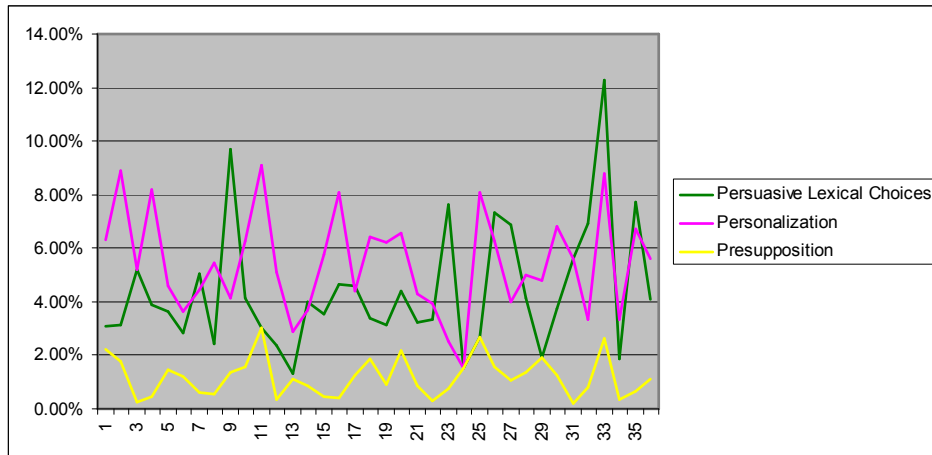
$$\text{Occurrence rate percentage} = (\text{Total words of spam} \times \text{occurrence rate of strategy}) / 100$$

The following table and figures show the obtained results of the analysis.

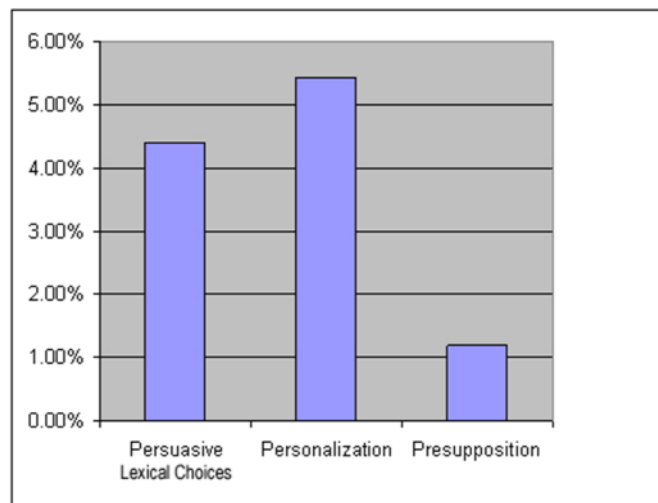
**Table 4.** *The Percentage of Persuasive Strategies in the Selected Spam Emails*

Spam NO.	Persuasive words	Personalization	Presupposition
1	3.06%	6.33%	2.24%
2	3.11%	8.89%	1.78%
3	5.20%	5.20%	0.25%
4	3.87%	8.20%	0.46%
5	3.63%	4.60%	1.45%
6	2.82%	3.63%	1.21%
7	5.06%	4.46%	0.60%
8	2.45%	5.43%	0.54%
9	9.72%	4.17%	1.39%
10	4.17%	6.25%	1.56%
11	3.03%	9.09%	3.03%
12	2.37%	5.08%	0.34%
13	1.32%	2.86%	1.10%
14	3.99%	3.70%	0.85%
15	3.54%	5.75%	0.44%
16	4.67%	8.07%	0.42%
17	4.58%	4.40%	1.28%
18	3.40%	6.42%	1.89%
19	3.11%	6.22%	0.89%
20	4.38%	6.57%	2.19%
21	3.24%	4.32%	0.86%

22	3.33%	3.94%	0.30%
23	7.61%	2.54%	0.76%
24	1.49%	1.49%	1.49%
25	2.70%	8.11%	2.70%
26	7.33%	6.28%	1.57%
27	6.86%	3.97%	1.08%
28	4.17%	5.00%	1.39%
29	1.92%	4.81%	1.92%
30	3.73%	6.83%	1.24%
31	5.62%	5.62%	0.22%
32	6.91%	3.31%	0.83%
33	12.28%	8.77%	2.63%
34	1.85%	3.33%	0.37%
35	7.74%	6.73%	0.67%
36	4.10%	5.60%	1.12%



**Figure 1.** This diagram represents the occurrence rates of each persuasive strategy for the spam emails.



**Figure 2.** Total arithmetic mean.

### Results in terms of lexical choices

As noted above, lexical choices should be defined and identified according to the context in which they occur because a word which is considered persuasive in one context does not necessarily play the same role in another context. Although all 36 spam emails in this research had the same ultimate goal, the stories behind them were more or less different.

The results show that accreditation with names such as “*Economic and Financial Crimes Commission*” and accrediting adjectives and adverbs like “*international*” and “*global*” have been widely used within the financial spam emails. The results also show that when the spammers want to discourage the recipients from talking to others about the email, they warn that because of security reasons the email content should remain confidential. In such cases, warning words and items such as “*be aware*”, “*security*”, and “*confidential*” are employed to show the urgency of the situation. Additionally, when spammers try to encourage the recipients to respond to the emails, they warn that if the message-receiver does not respond to the email in a particular period of time, the lottery prize for example, will not be delivered. In this regard, adjectives such as “*immediate*” and adverbs like “*immediately*” are used as “Warning/Encouraging” words. This technique is widely used in different types of spam including the medical spam (Barron, 2006).

The results also showed that the frequency of persuasive strategies in all emails was rather consistent. Figure 1 confirms this point by showing that there is not any grand peak in the data. The minimum and maximum rates of occurrence in terms of “lexical choices” are respectively 1.32% and 12.28%. The average rate is 4.38%. The results are as follows:

- The maximum rate of ‘persuasive words’ is 12.28% in spam NO.33.
- The minimum rate of ‘persuasive words’ is 1.32% in spam NO.13.
- The average rate of ‘persuasive words’ is 4.40%.

Based on the data recorded in the Content Tables, persuasive words were distributed in all parts of the texts even within the email address and in the subject line. Therefore, it can be argued that persuasive words were observed in all parts of the spam body. Figure 3 represents the areas in which persuasive words were used.

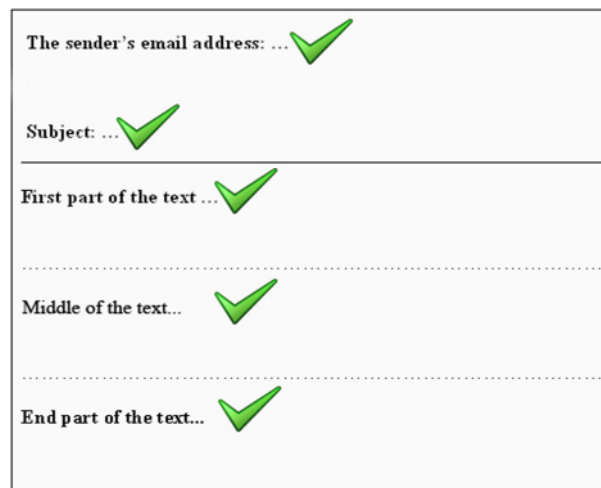


Figure 3. The distribution of persuasive words

### Results in terms of personalization

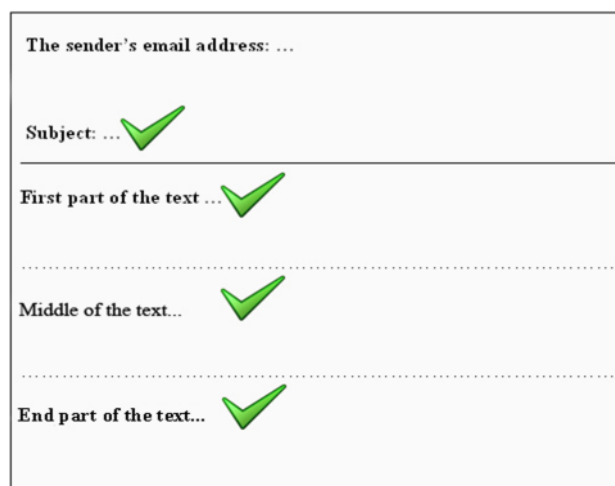
The analysis showed that the anticipated audiences were addressed personally by their names, or by pronouns or adjectives referring to them, e.g. *you*, *your*, *yours*. Personalization can be used as a persuasive technique to pretend that the audience is the only one with whom the writer/speaker is communicating (Woods, 2006). This technique may create a good sense in the addressee because most of the people prefer and like to be in the center of attention. When spamming, spammers do not know the exact name and email address of their addressees because spam emails are sent in bulk and in very large quantities (Hoffman, 1997). Therefore, it is impossible for the spammers to check and know all



the emails one by one. For this reason, they compose just one text for the entire recipients. That is why in none of the emails we find any reference to the name or even to the exact email address of the recipient and instead, only pronouns and adjectives are used, and in this situation personalization comes into play. The statistics for personalization are as follows:

- The maximum rate of ‘personalization’ is 9.09% in spam NO.11.
- The minimum rate of ‘personalization’ is 1.49% in spam NO.24.
- The average rate of ‘personalization’ is 5.44%.

The following figure shows the location of personalized items in the spam structure.



**Figure 4.** *The location of personalized items in spam emails*

### ***Results in terms of presupposition***

It should be pointed out that most of the persuasive presuppositions occurred either in the middle or at the end of the emails. One of the common presupposition strategies that spammers used was the request for help and assistance. Soliciting for assistance mostly appeared in the middle of the text because the first part of the message is usually allocated to introduction. Spammers usually invent jobs and/or qualities for themselves. They sometimes provide a short (though fake) biography of their family. Then they state the problem and the reason why they have sent the email. After stating the problem, they express their need for assistance. This is the point at which they take advantage of presupposition by using phrases and sentence like: “*I need your assistance...*” or “*I need you to assist me in...*” By declaring such sentences they infuse this presupposition into the mind of the recipient that he is able to assist the spammer. Another widely-used presupposition is soliciting for further communication. That is, spammers may say: *send your replies to this address...*” or “*send your reply immediately...*” These phrases are composed in a way that they presuppose that the recipient will certainly respond to the email. In the above example, the spammers do not ask whether the recipient likes to reply the email or not. Instead, they hypothesize that the messages will be responded. The summary of presuppositions in this study is presented below:

- The maximum rate of ‘presupposition’ is 3.03% in spam NO.11.
- The minimum rate of ‘presupposition’ is 0.22% in spam NO.31.
- The average rate of ‘presupposition’ is 1.20%.

Figure 5 shows the location of presuppositions in the spam emails.



**Figure 5.** *The location of presuppositions in spam emails*

## Conclusion

The purpose of the present research was to find out whether persuasive strategies were used in the texts of financial fraud spam emails. In this regard, the results of the study confirmed that all the three persuasive strategies were widely used in different parts of the financial fraud spam emails. The results also suggested that although presupposition was used less than other strategies, it was present in all spam emails. These results can be summarized in the following order:

1. Persuasive words appeared in all parts of the financial fraud spam emails. Furthermore, the study revealed that persuasive words were distributed consistently throughout the main text.
2. The research revealed that personalization is widely used in financial fraud spam especially in the body of the emails and sometimes in the subject field. However, no personalized item was identified within the email address.
3. Presupposition occurred less frequently in the spam texts. One remarkable point about presupposition is that it mostly occurs either at the beginning or at the end of the financial fraud spam emails. When it occurs at the beginning, the spammer usually presupposes the ability of the recipient in assisting the email sender. And when presupposition occurs at the end of the spam emails, it is mostly concerned with encouraging the recipient for further communications.

## References

- Barron, A. (2006). Understanding spam: A macro-textual analysis. *Journal of Pragmatics*, 38 (6), 880–904.
- Behnam, B. (2008). A critical study of selected political elites' discourse in English. *The Journal of Applied Linguistics*, 1(1) 14-33.
- Behnam, B. & Jabbarpour, N. (2012). Discourse of intimidation: Analyzing some selected institutional public notices in Persian context. Paper presented to the 1<sup>st</sup> Conference on English Language Studies. Azarbaijan: Shahid Madani University.
- Behnam, B. & Kheradmandi, M. (2009). Language and legitimization: A critical analysis of US political discourse prior to the Iraq war. Paper presented to the 7<sup>th</sup> International TELLSI Conference: *New Horizons in Language education*. Yazd.

- Behnam, B., & Kuhi, D. (2008). Veiled trails of threat in the language of advertisements: A discourse analysis of a military job advertisement. *Samara AltLinguo E-Journal*, 3. Retrieved August 18, 2012, from [http://samaraaltlinguo.narod.ru/ejournal/308\\_behnam.pdf](http://samaraaltlinguo.narod.ru/ejournal/308_behnam.pdf)
- Fairclough, N. (1989). *Language and power*. New York: Longman.
- Garcia-Molina, H., & Gyöngyi, Z. (2005). Web spam taxonomy. Retrieved April 10, 2012, from <http://airweb.cse.lehigh.edu/2005/gyongyi.pdf>
- Hoffman, P. (1997). Unsolicited bulk email: Definitions and problems. Retrieved April 10, 2012, from <http://www.imc.org/ube-def.html>
- Johnston, B. (2008). *Discourse analysis*. Malden: Blackwell Publishing.
- Koteyko, N., & Nerlich, B. (2007). Multimodal discourse analysis of probiotic web advertising. *The International Journal of Language, Society and Culture*, 23, 20-31.
- Matthiessen, C., & McCarthy, M., & Slade, D. (2002). Discourse analysis. In N. Schmitt (Ed.), *An introduction to applied linguistics* (pp. 55-73). London: Arnold.
- Meyer, M. (2002). Between theory, method, and politics: Positioning of the approaches to CDA. In M. Meyer & R. Wodak (Eds.), *Methods of critical discourse analysis* (pp. 14-31). London: SAGE Publications.
- Scollon, R., & Wong, S. (2004). *Nexus analysis: Discourse and the emerging internet*. New York: Routledge.
- Sophos, P. (2005). Sophos identifies the most prevalent spam categories of 2005 [Press Release]. Retrieved April 11, 2012, from [http://www.sophos.com/en-us/press-office/press-releases/2005/08/pr\\_uk\\_20050803topfive-cats.aspx](http://www.sophos.com/en-us/press-office/press-releases/2005/08/pr_uk_20050803topfive-cats.aspx)
- Spenader, J. (2002). *Presuppositions in spoken discourse*. Stockholm: Akademitryck.
- Van Dijk, T.A. (1998). *Ideology: A multidisciplinary approach*. London: SAGE Publications.
- Van Dijk, T.A. (2001). Multidisciplinary CDA: A plea for diversity. In M. Meyer & R. Wodak (Eds.), *Methods of critical discourse analysis* (pp. 95-120). London: SAGE Publications.
- Wodak, R. (2002a). What CDA is about - a summary of its history, important concepts and its development. In M. Meyer & R. Wodak (Eds.), *Methods of critical discourse analysis* (pp. 1-13). London: SAGE Publications.
- Wodak, R. (2002b). The discourse-historical approach. In M. Meyer & R. Wodak (Eds.), *Methods of critical discourse analysis* (pp. 63-94). London: SAGE.
- Woods, N. (2006). *Describing discourse: A practical guide to discourse analysis*. London: Arnold.

## Authors:

**Biok Behnam** is Associate Professor in Applied Linguistics in Islamic Azad University, Tabriz Branch, Iran. His current research interests cover Discourse Analysis, ELT and Translation Studies. He has been involved in a wide range of projects in the area of Applied Linguistics and Discourse Analysis as a project director, consultant and researcher. He has widely presented papers to national and international conferences in North America, Australia, Europe, China, India and South East Asia. Relevant publication includes *Discourse of Advertising: A comparative study* (2006), with H. Piadeh, *A Critical Study of Selected Political Elites in English*, with L. Moghtadi and a sociolinguistic study of SMS Exchanges of Iranian Festive/Mourning Occasions, with M.R. Khodadust.

**Behrooz Azabdaftari** is Professor in Islamic Azad University, Tabriz Branch (IAUT). He received the bachelor's degree in English Language and Literature from Supreme Training College (Tehran), Diploma in English Language Teaching from Georgetown University, M.A in English Language Teaching from the American University of Beirut, and PhD in English Language Teaching from the University of Illinois, United States. Prof. Azabdaftari, who was the faculty member of the University of Tabriz, retired in 2000 and a year later joined IAUT faculty. He has written and translated numerous academic books. Also, tens of his papers have been widely presented in national and international seminars and conferences.

**Ali Hosseini** attended the Islamic Azad University, Tabriz Branch, in 2009 to receive his M.A. in English Language Teaching. Considering his bachelor's degree in computer software engineering, he

chose “Analyzing financial email spam in English in terms of persuasive strategies: Personalization, presupposition, and persuasive words” as his M.A. thesis topic. The supervisor and advisor of his thesis were Dr. Biok Behnam and Prof. Behrooz Azabdaftari, respectively. He received his M.A. degree in 2012. At the present time, he works for the Information Technology Magazine and Shabakeh, as writer and translator.