Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

Asian Journal of Scientific Research 8 (3): 403-412, 2015
ISSN 1992-1454 / DOI: 10.3923/ajsr.2015.403.412

Commercialization Strategy and Implementation Plans for the Proposed Vitual Anti-Spam System based on Feasibility Study

[1]A.A. Zaidan, [1]M.B. Lakulu, [1]M. Hashim, [1]Mussab Alaa, [2]B.B. Zaidan, [3]O.H. Salman, [1]Bahbibi Rahmatullah and [1]Nazre Abdul Rashid

[1]Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Tanjong Malim Perak, Malaysia

[2]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

[3]Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, Selangor, Malaysia

Corresponding Author: A.A. Zaidan, Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Tanjong Malim Perak, Malaysia

ABSTRACT

The aim of this feasibility study is to find out objectively, if the proposed vitual anti-spam system (BVAS) with document processing is a viable idea in terms of technology, market considerations and finance. This feasibility study further attempts to identify the potential problems that the proposed system would face and ensure, if it is a workable and profitable business enterprise. In this study, a market strategy of the proposed vitual anti-spam will be discuss on four parts namely, market feasibility study on the use of an effective vitual anti-spam system, market feasibility analysis, formation of anti-spam company and proposed commercialization strategy, strategy justification and implementation plans. The finding from this study has shown the proposed BVAS is cheap, the anti-spam catch rate is above 98% and more importantly the false positive rate is around 0.5%. This makes BVAS to be much desired and in demand among anti-spam users. This means if BVAS is developed commercially, it can compete successfully in the open market.

Key words: Feasibility study, vitual anti-spam system, market potential

INTRODUCTION

There has been a tremendous growth in spam messages over the last ten years so much so that companies have lost millions of dollars in terms of reduced productivity (Zhang, 2005; Potluri, 2008). Now, millions of dollars have been spent on installing anti-span products and even though, there are many valuable products available in combating spam, none has been fool proof yet. Unsolicited e-mails have in fact now become increasingly deceitful and felonious especially phishing emails that bait end users into giving up personal information and spam that covertly spread pornography (Wood *et al*., 2010).

Presently, the ten popular anti-spam products namely Symantec Brightmail Anti-Spam, Kaspersky Anti-Spam, Surf Control E-mail Filter for SMTP, Symantec Mail Security for SMTP, MX termed Mail Firewall, Bogofilter, MacAfee Spam Filter, OEM's Mail Guard, Barracuda's and Ikarus My Spam Wall are available in the market. Besides these two other open source anti-spam tools namely Spam Assassin and Bogofilter are currently available (Gansterer *et al*., 2005; Park *et al*., 2007). Most of these commercial anti-spam products claim that upon implementation, they can attain a spam recognition rate of more than 80% with essentially no false positives. This claim is questionable as companies, schools, institutions of higher learning and households are still not satisfied with existing filters as unsolicited e-mails in the form of advertisements and offensive pornography percolate through the existing spam filters. A fool proof anti-spam filter is therefore extremely essential to curb the influx of unsolicited messages (Subramaniam *et al*., 2010).

The aim of this feasibility study is to find out objectively, if the proposed vitual anti-spam system (BVAS) with document processing is a viable idea in terms of technology, market considerations and finance.

MATERIALS AND METHODS

Product description of the proposed anti-spam system: According to Zaidan *et al*. (2011), the proposed BVAS makes use of the Bayesian classifier to classify documents either spam or non-spam. The BVAS makes use of Bayes principles during the machine learning training process. As a result, during the document processing, word stemming, stop words and short words forms, HTML trices were effective used to combat spam. A comprehensive evaluation of the system by comparing it with the existing anti-spam products was done and the investigational results of BVAS appraisal disclose that the proposed system is both reliable and efficient.

Comparison of anti-spam products: In order to choose an appropriate anti-spam system, a number of anti-spam products were evaluated using certain common anti-spam criteria and techniques. The proposed BVAS was included in this evaluation. Table 1 depicts the common anti-spam methods against the quality criteria used in the anti-spam products.

Header based anti-spam products like Surf Control E-mail Filter for SMTP and Symantec Mail Security for SMTP have certain limitations. The information of the sender in the e-mail header can be forged during the transmission process. Scampers sometimes forge header entries and therefore, these two anti-spam products are not reliable. In the Bayesian classifier, there is a period of training where mail messages and content of the internet websites or URLs are fed into the classifier for training and subsequently to identify correctly the spam and non-spam messages. Another advantage of the Bayesian classifier is that it is able to update the ‘Short Word Forms’ and it has a very low rate of false positives. Whitelist and Blacklist have been good methods in the past to stop spam messages but the problem is that the e-mail protocol used lack strict security features. This means anybody can use anything in the sender’s address.

Though Kaspersky Anti-spam, McAfee Spam Guard and Sam Assassin are quite popular installed anti-spam software, they have weaknesses too. They do not make use of any kind of classifier. Therefore, they still allow spam to secretly enter the inboxes of clients. The rest of the anti-spam software’s are not in demand.

In most of the anti-spam products mentioned, except for Kaspersky Anti-Spam, McAfee Spam Killer, Barracuda Spam Firewall and BVAS during the testing stage, the false positive rate is 10% and this implies that quite a large number of e-mail messages which are legitimate but are falsely identified as spam. BVAS is able to attain a false positive rate of less than 2% and this feature makes BVAS as a desirable anti-spam product. It should be noted that BVAS fulfils all the quality criteria that are commonly used.

Market feasibility analysis: A market feasibility study was undertaken by the researchers to identify the market potential for spam products and further to identify potential customers and their dominant characteristics. Another aim of this study was to find out other competitors, potential sales volume, price product desirability, product demand and other issues related to

Table 1: Anti-spam product comparison

Quality criteria used	Symantec brightmail anti-spam	Kaspersky anti-spam	Surf control e-mail filter for SMTP	Symantec mail security for SMTP	Mxtreme mail firewall	Ikarus my spam wall	Spam assassin	Bogofilter	McAfee spam killer	OEM's mail guard	Barracuda spam firewall	Bayesian anti-spam system with document processing (BASS)
Whitelist	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Blacklist	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Has tokenizing process	✓	✓	✓	×	✓	✓	✓	✓	✓	✓		✓
Detects inappropriate short word forms	✓	✓	×	×	✓	✓	✓	×	✓	✓	✓	✓
Has stop word removal	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
Has word stemming	✓	✓		×	×	✓	✓	✓	✓	✓	✓	✓
Bayes classifier	×	×	×	×	×	×	×	×	×	×	×	✓
Document processing	✓	✓	×	×	×	×	×	×	✓	×	×	✓
Uses static techniques like keywords	×	×	✓	✓	×	×	×	✓	✓	✓	✓	✓

market analysis. A survey questionnaire was therefore designed and administered to 55 selected respondents. The respondents were carefully selected to include spam administrators, school principals, software designers, college principles, company proprietors, government officers and ordinary users. In other words, the questionnaire sets were distributed to people from different walks of life. The researchers found difficulty in implementing this questionnaire as they had to install the proposed system in the respondents' PCs. It meant that the researchers had to visit each respondent's home, school or institution. The questionnaire was framed using simple English and the respondents were ensured of the confidentiality of the information given. Out of the 55 questionnaires given out, the researcher managed to collect 50 questionnaires that were completed fully. Five questionnaires were incomplete and were therefore rejected.

Data analysis: In part 1 of the questionnaire survey, three demographic questions were given. Based on the data analysis of question 1, it was found that the majority comprising 40% of the respondents were from the 40-49 years age groups and this is depicted in Fig. 1. This indicates that the bulk of the respondents are mature and there are in a managerial position. It further shows that they are able to make a decision on choosing an effective anti-spam software. As regards gender, 40 out of a total of 50 respondents were men indicating that more men than women are in the computer sector.

In question 3, the data analysis showed that 16 out of a total of 50 respondents are spam administrators followed by 7 parents and 6 college principals. This is depicted in Fig. 2. This finding reflects that quite a number of respondents involved in the survey have a good understanding of different types of spam software and know how to evaluate the effectiveness of a particular spam software. It further shows that people in the education sector know the value and importance of installing an efficient anti-spam tool.

On income distribution, as depicted in Fig. 3, it is obvious that the higher income group show more concern in installing anti-spam software.

In part 2 of the questionnaire, respondents were asked in question 5, if they daily receive spam or unsolicited e-mails. All the 50 respondents acknowledged that they receive unsolicited e-mails daily and this reflects the magnitude of the spam problem. Analysis on the responses regarding respondents' feelings towards unsolicited e-mails in question 6 as depicted in Fig. 4, 70% of the respondents said that spam is a nuisance and annoying and another 26% said that they waste much time in deleting spam e-mails and hence, it affects productivity.

In question 7, respondents were asked if there is a dire need to install an effective anti-spam system or anti-spam tool in individual households, schools, institutions of higher learning and in

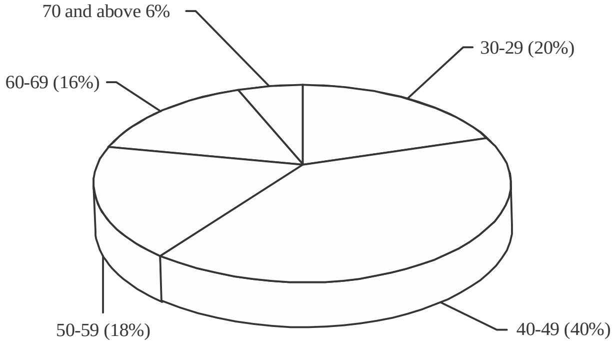

Fig. 1: Different age category

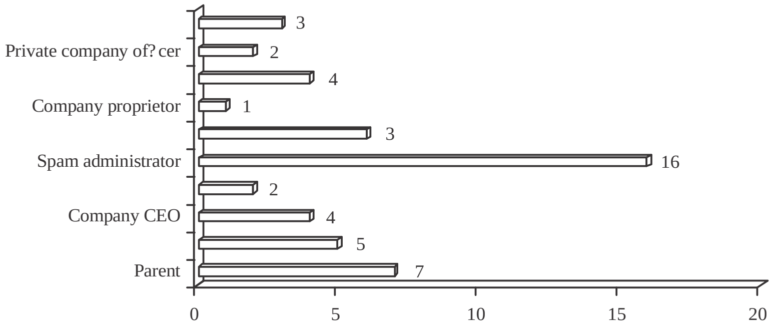

Fig. 2: Respondent’s occupations

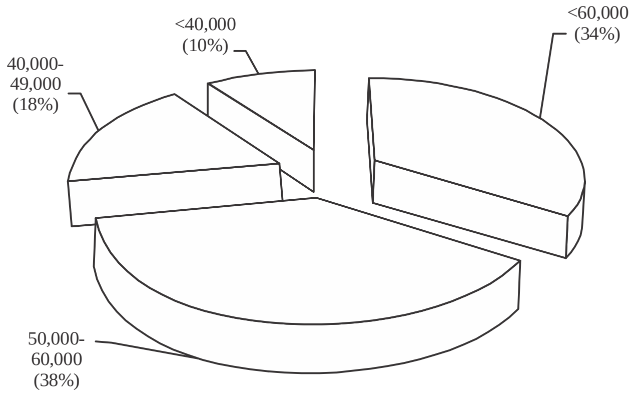

Fig. 3: Income distribution

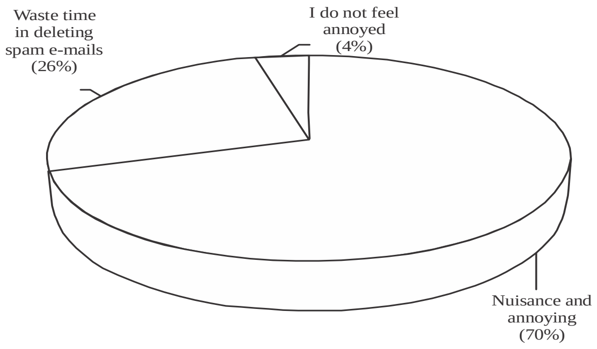

Fig. 4: Feelings towards spam

industry. Once again, all the 50 respondents affirmed that there is indeed an urgent need to stop all spam e-mails from entering the inbox. The researchers interviewed 3 of the respondents and asked the reasons for the response to this question. They explained that unwanted advertisements cause nuisance and the influx of covert pornography affects the morality of the younger generation. In relation to question 8, about 60% of the respondents affirmed that they have installed anti-virus software but no specific anti-spam software was installed. This is cause for concern as only 20% of the respondents had installed licensed anti-spam software while 80% had installed unlicensed

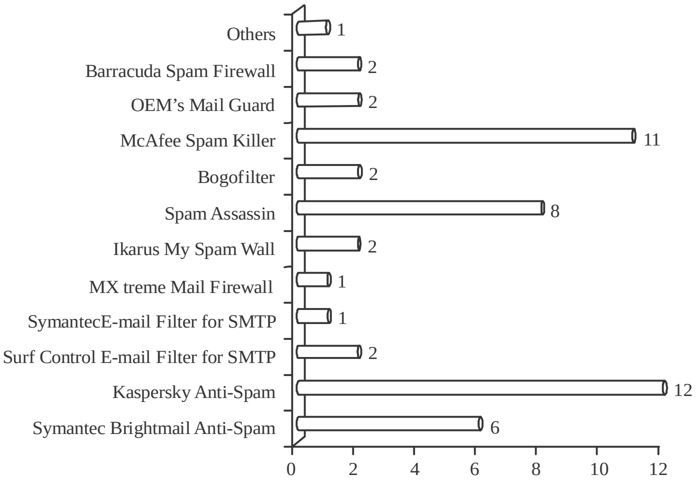

Fig. 5: Types of anti-spam software installed

Table 2: False positive rate

Percentage	Number of respondents
5<	4
10	31
15	9
20	6

anti-spam software even though they preferred to install unlicensed anti-spam software. In relation to question 10, as depicted in Fig. 5, Kaspersky Anti-spam, McAfee Spam Guard and Sam Assassin are the popular installed anti-spam software and they accounted for 24, 22 and 16%, respectively of the total share of installed anti-spam software. The rest of the anti-spam software are not in demand.

In question 11, respondents were asked for the average license price of anti-spam software for a single user per year. The majority of the respondents (i.e., 80%) affirmed the price to be RM140.00. The analysis pertaining to question 12 showed once again the majority of the respondents (i.e., 80%) affirmed that they are not fully satisfied with the usage of the existing installed anti-spam software. Question 13 was based on the false positive rate and this is the number of e-mail messages blocked by the installed anti-spam system that are legitimate but falsely identified as spam. Respondents were asked the false positive rate under the existing installed anti-spam system. Thirty-one out of the total of 50 respondents mentioned that their false positive rate is 10% and this indicates that quite a large number of e-mail messages which are legitimate but are falsely identified as spam. This means the installed anti-spam system is not efficient and reliable. Only 4 respondents as shown in Table 2 mentioned that their false positive rate is below 5%. A reliable anti-spam system ought to have a false positive rate of less than 1%.

In part 3 of the questionnaire in relation to question 14, all the 50 respondents unanimously agreed that the proposed BVAS is easy to install and further affirmed that the user license fee is the cheapest compared to other existing anti-spam systems. Data analysis based on the responses in relation to question 16 found an interesting finding. It showed that the catch rate of the installed BVAS is more than 98%. No other anti-spam software was able to achieve this feat. In addition, as regards question 17 another notable finding is that the false positive rate under the present installed BASS is only 0.5%.

More than 90% of the respondents affirmed that even with the installation of BVAS, the system's performance and the load of messages transiting through the system are still sustained. Data analysis based on the responses in relation to question 19 reflected that BVAS has both the blacklisting and white listing features making it robust and resilient to span attacks. As regards question 20 and 21, more than 95% of the respondents are convinced that BVAS would have a great demand in the anti-spam software market and they themselves would like to purchase a user license when it is commercially produced and recommend it to their friends.

Discussion of the findings: The survey findings revealed that spam is a nuisance and annoying and they waste much time in deleting spam e-mails and hence it affects productivity. A survey done by Park *et al.* (2007) affirms this finding that spam is a time waster. Further studies done by Uys (2009) affirm the finding that it costs businesses large amount of money in terms of workforce productivity. The survey analysis shows that there is a great demand for an anti-spam system that is fool proof especially among educationists as revealed by the questionnaire analysis. In relation to question 6, eight of the respondents gave elaboration on their feelings towards these unsolicited e-mails. They explained that junk e-mails have become a powerful armament in stealing consumers' money by using their private contacts and this finding was affirmed by studies done by Hinde (2002). Another respondent explained that malware and viruses are covertly embedded in spasm and thereby attack network security. This pertinent finding had been confirmed by studies made by Raad *et al.* (2010).

The three interviewed respondents in relation to question 7 elaborated that spam carry pornography and this leads to moral decadence of the younger generation. This finding again was affirmed by studies undertaken by Wood *et al.* (2010). Findings from the analysis in Part 3, reflect that the proposed BVAS is cheap, the anti-spam catch rate is above 98% and more importantly the false positive rate is around 0.5%. This makes BVAS to be much desired and in demand among anti-spam users. This means if BVAS is developed commercially, it can compete successfully in the open market.

Formation of visual anti-spam company: The formation of Visual Anti-spam Company is governed by the Companies Commission of Malaysia (SSM). The formation of a new company has to follow the rules and regulations set by SSM (Suruhanjaya Syarikat Malaysia). This statutory body which is a merger between the Registrar of Companies (ROC) and the Registrar of Businesses (ROB) in Malaysia came into operation. Visual Anti-spam Company is a partnership company co-owned by UPSI.

The registration of Visual Anti-spam Company must be done within 30 days from the date of commencement of the business and this registration can be done at any SSM counter. In order to register the company, the UPSI have to complete the Business Registration Form (i.e., Form A) using guidelines for new business registration. Before the trade name of the company can be registered, the co-owners have to complete the business name approval form (i.e. Form PNA.42) using guidelines for business name application. The business name approval will be granted according to Rules 15, Rules of Business Registration 1957. Furthermore, business registration can be made for a period of 1 year and not more than 5 years. Once the approval for the trade name of the company is obtained, the owners have to pay a fee of RM60.00 per year for registration of the company called Visual Anti-spam Company. The procedure and projected plan for the formation of Visual Anti-spam Company is depicted in the flow chart in Fig. 6.

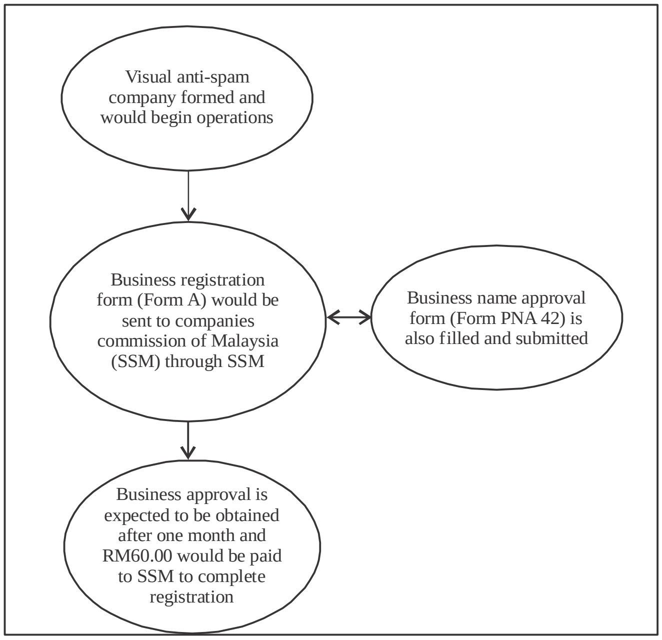
Visual anti-spam company formed and would begin operations
Business registration form (Form A) would be sent to companies commission of Malaysia (SSM) through SSM
Business name approval form (Form PNA 42) is also filled and submitted
Business approval is expected to be obtained after one month and RM60.00 would be paid to SSM to complete registration

Fig. 6: Projected plan on the formation of visual anti-spam company

Proposed commercialization strategy, strategy justification and implementation plans: It is proposed that there is a need to strategize further so that BVAS can compete successfully in the open anti-spam market. The following strategies are suggested:

- The user licence sale price of BVAS is maintained at RM100/ as suggested in the questionnaire
- The BASS would be tested and implemented on a small scale first. Once this initial implementation and sale is successful, then BVAS would be produces on a commercial basis
- At least one expert software developer is employed so that all glitches and bugs in the coding are resolved before BVAS is marketed and implemented on a commercial scale. There is a need now to form a company. The proposed company would be called Visual Anti-spam Company. An initial working capital of RM300000.00 is necessary to start this company. This initial capital would be used to employ staff, rent an office, obtain approval from government authorities and pay license fees. The staff would consists of an operations manager, administrative clerk to track in-coming orders and complaints, a financial clerk to keep track of the income and expenditure of the company, a webmaster to create, update and maintain the company website and finally a security guard to ensure that copyrighted CDs are not stolen but kept in a safe place. A salaried research officer needs to be employed so that there is continuous improvement to BVAS to face new challenges and attacks in the spam world
- In order to market this product, there is a need to advertise extensively in the Internet and in security magazines. This means a special BVAS website ought to be created by a qualified webmaster. This website should explain clearly the strength of the software in almost completely blocking unsolicited e-mails. The created portal should allow potential customers to pay through credit card and further allow download from the official website and hence, there is no need for a mass storage facility. However, individuals can purchase the anti-spam

software from the company either directly or through post. Therefore, a small storage facility would be sufficient. This means the manner of marketing is through CD packaging and through direct download from BVAS website

- A special brand ought to be created for BVAS so that potential users can easily recognize this renowned anti-spam software. The anti-spam software should be patented and the necessary approval obtained from SIRIM Malaysia
- The proposed BVAS should be marketed locally first and once it is successful, only then it should be marketed internationally

If the above steps are strictly adhered, then the production and commercialization of BVAS is justified.

CONCLUSION

Anti-spam has become a real challenge for this kind of marketing. There is no study before this provide a feasibility study to find out objectively, if the proposed BVAS is a viable idea in terms of technology, market considerations and finance a market strategy of the anti-spam proposed. Accordingly, a market strategy of the proposed vitual anti-spam has been presented in details. A survey questionnaire was designed and administered on the area of the marketing. Data collecting, gathering, summarizing and analyze the result has been obtained. As conclusion, there is a great demand for an anti-spam system that is fool proof especially among educationists as revealed by the questionnaire analysis.

ACKNOWLEDGMENTS

This research was funded by the research management and innovation center of the Universiti Pendidkan Sultan Idris, under grant number 2014-00084-109-01. We would like to express our very great appreciation to all of author for their valuable comments and constructive suggestions during the planning and development of this research. Their generosity with their time is very much appreciated.

REFERENCES

Gansterer, W., M. Ilger, P. Lechner, R. Neumayer and J. Strau, 2005. Anti-spam methods-state-of-art. Faculty of Computer Science, University of Vienna, Austria, pp: 1-93.

Hinde, S., 2002. Spam, scams, chains, hoaxes and other junk mail. Comput. Secur., 21: 592-606.

Park, I., R. Sharman, H.R. Rao and S. Upadhyaya, 2007. The effect of spam and privacy concerns on e-mail users' behavior. J. Inform. Syst. Secur., 3: 39-62.

Potluri, R.M., 2008. Assessment of effectiveness of marketing communication mix elements in Ethiopian service sector. Afr. J. Bus. Manage., 2: 59-64.

Raad, M., N.M. Yeassen, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010. Impact of spam advertisement through e-mail: A study to assess the influence of the anti-spam on the e-mail marketing. Afr. J. Bus. Manage., 4: 2362-2367.

Subramaniam, T., H.A. Jalab and A.Y. Taqa, 2010. Overview of textual anti-spam filtering techniques. Int. J. Phys. Sci., 5: 1869-1882.

Uys, L., 2009. Voice over internet protocol (VoIP) as a communications tool in South African business. Afr. J. Bus. Manage., 3: 89-94.

Wood, P., D. Bleaken, M. Nisbet, J. Zhang, N. Johnston, M. Lee and D. Lewis, 2010. The messagelabs intelligence annual security report: 2009 security year in review. http://www.symantec.com/connect/blogs/messagelabs-intelligence- annual-security-report-2009-security-year-review.

Zaidan, A.A., N.N. Ahmed, H. Abdul Karim, G.M. Alam and B.B. Zaidan, 2011. Spam influence on business and economy: theoretical and experimental studies for textual anti-spam filtering using mature document processing and naive Bayesian classifier. Afr. J. Bus. Manage., 5: 596-607.

Zhang, L., 2005. The CAN-SPAM act: An insufficient response to the growing spam problem. Berkeley Technol. Law J., 20: 301-325.