Should We Be Concerned With Spam Emails? A Look at Its Impacts and Implications

Yanti Rosmunie Bujang and Husnayati Hussin

***Abstract*— As the most popular communication technology, email has been widely used by the Internet users. Most past researches on email has focused on major problems of email misuse such as spam emails and email overload. Technology-based papers focused on how to filter emails so that spam is minimized. In reality, however, most email users are not aware of the implications of spam problem because the impacts are not clearly visible to an individual. At the organizational level or higher, the impacts of spam emails are even more serious as it has financial implications. This paper aims to discuss the spam email problems from the social and behavioral perspective and highlight the impacts of the spam email on individuals, organization and the society in general. The understanding on how the email users' deal with the spam email currently has revealed their weaknesses when dealing with spam. Some recommendations are also proposed to encourage the good ethics in dealing with emails. It aims to instill the awareness and hope that email users can take proactive steps to protect their inbox.**

I. Introduction

The existence of email has transformed the traditional method of communication in a better way in term of cost, efficiency and usability of the email. However, in the last decade or so, as a popular communication tool, email has been misused by the irresponsible person. As a result junk email or best known as spam email has existed. Email is among the best type of application that support fast and reliable communication. In reality, most email users are not really aware the real consequences of spam emails [1]. Although the impact of spam email is real, it is still unknown to most email users. Most email users rely on other party to solve the problem and relatively unconcern about the issue [2]. It is unfortunate that most email users are not aware of the real impacts of the spam emails either at the individual level or the organizational level, and eventually affect the economy of the country.

Yanti Rosmunie Bujang is with the Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Malaysia. (phone: +601-3801-2717; fax: +603-6196-5179; e-mail: yrosmunie@yahoo.com.my).

Husnayati Hussin is an Associate Professor in Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Malaysia. (phone: +603-6196-5624; fax: +603-6196-5624; e-mail: husnayati@kict.iiu.edu.my).

Spam email is defined as Unsolicited Commercial Email (UCE)[3] and Unsolicited Bulk Email [4]. The similarity is the 'unsolicited characteristic' which means that the email was sent without the permission or in short, it is an unwanted email. From the definitions the three main characteristics of spam email are; (i) not requested by the recipients; (ii) has commercial value; and (iii) always sent in bulk. Unwanted is a problem because it wasted the email storage, email recipients time to open, read and delete the email. Initially the spam email is sent to commercialize the products, the problem with these is the spammer always destruct the dealing [2].

The purpose of this paper is to discuss the problem and impacts of the spam emails in a comprehensive manner, not just from the technological perspective. The issue of spam has expanded over the years, and evolved from just an 'unwanted email' into an activity that is motivated by financial gains and can cause major destruction to the network infrastructure. The following sections will present a review of relevant concepts and literature to the spam problem.

II. Email as a Marketing Tool

Email is mainly used as communication tools other than telephone and any other tools. In an organizational setting, employees are more alert on incoming emails rather than telephone calls. A majority of employees view the email within 6 seconds of its arrival which is faster than letting the telephone ring three times [7]. It happened more than a decade ago when the use of instant messaging and social network is not popular as today. Nowadays, email is more portable and email users can receive the email or instant messaging on their mobile phone personally which is always with them. Thus, the response on email notification is quicker than before.

In business, email marketing is among the best way of advertising the business products of services online [8]. The ability of email to reach the global customers as their target market with the cheapest method is the main reasons email is widely used in marketing. Comparing to other methods, email is also popular because of the usability where different files can be attached such as pictures, documents and videos. Recently, the use of video emails become more popular among the SMB internet marketers in promoting the products or services. According to the survey conducted by Get Response in 2010 Email Marketing Trends Survey [9]

almost 64% of them claim that it shows significant increment in sales. However, the use of video emails are most effective for training courses, followed by product demos (22%), product promotions (19.1%) and Customer Testimonial (17.8%). This feature make the email become more useful in promoting the products or services because it allows detail product description. Creating effective communication with the customers is the most important aspect in service marketing [10], therefore, it is up to the marketers' creativity to attract the interest of customers on their products or services.

III. Spam Email Problem

The existence of spam email in the email inbox is one of the threats [11-13] in email communication in the current society. The ease of spam entering email users' inbox is the main threat to the email users. Most of the email users do not know where the spammer get their email address and they have limited knowledge how to protect their email address from being attacked. Although there are many anti-spam technology in the market, however none of them are completely effective because of the false positive rate which is impossible to achieve zero and 100% capture rate [14]. This is because of the fast growth of spam technology to bypass the anti-spam technology within a few months [15]. This is called susceptibility perceiveness of the spam or also defined as an individual's subjective probability that a malicious IT will negatively affect him or her [12]. Therefore, obviously there is not much can be done to protect their email account besides installing the anti-spam filter. Even by doing this, some spam emails still can go through the filter. It is observed that although many technological solutions have been proposed, the spam problem is not solved completely.

The severe impact of the spam to the email users is another threat of spam email. Some literatures have mentioned that spam is a potential threat to the credibility of email as a reliable and efficient means of Internet communications [11, 13]. False positive is the main problem with the anti-spam technologies. This situation could not be stopped because email also has its own revolution. The spammer always aims to create the contents of spam email more advance than the filtering technologies to ensure the message will go through and can reach the email users successfully. The effect of spam on the Internet infrastructure and conveniences has augmented privacy concerns among email users and has served to reduce users' welfare. In addition, majority of the spam receivers has responded that spam compromises their privacy [16].

It seems the spam war is never ended and as far as today none can be done to stop it totally. However the efforts of technology experts are highly appreciated because they do not give up tho find the appropriate method to control the spam outbreak. If there is no contribution from the technological experts, probably our inbox are polluted with spam email and none of legitimate email is able to enter the mailbox.

IV. The Impacts of Spam Email

In general, the impact of spam email is affecting the email users and organizations alike. The following sections describe each impact in more detail.

A. Productivity

Productivity is the major drawback of the spam email. Spam email has caused loss of productivity [11]. A decade ago, as stated by Rebbeca Wettemann in New York Times, dated 28 July 2003 spam could cause a severe impact on productivity. The workers receive 13.3 spam messages per day and had spent six and a half minutes on them. Thus they have loss 1.4 percent of their productive time in managing spam email [17]. According to MacAfee survey, spam email is the main technology time waste which is 49% as compared to other technology related annoyances such as automated voice response systems and slow internet connections [11]. The survey also exposed that 49% of American spend at least 40 min per week deleting spam [13].

Other than individual, businesses also face the loss of productivity because of spam [18]. One of the major problems of spam email is the waste of time and human resources [19]. The employees spend their valuable time to scan manually between spam email and legitimate mail. Furthermore, anti-spam technology itself requires time and resources because it requires updating regularly. Thus, it is widely known that spam email costs businesses large amount of money in terms of workforce productivity [20, 21]. As happened in Japan, the GDP (Gross Domestic Product) has been decreased by spam email about 464 billion yen (0.1%) of the Japanese GDP [20]. In addition at the same time, the effect also reduces labor productivity. This is important because productivity of the country depends on the productivity of the employees. From the organizational perspective, the way how employees manage spam emails is very important to ensure that it would not affect their productivity. The duration of time they spent in isolating the spam emails from legitimate emails is very important.

B. Infrastructure

In 2007, a study estimated spam has accounted for 85% of email traffic and the number would increase to 90% by year end if the prevailing trends continued [22]. The increase causes bad storage capacity, like the unexpected overload of email systems bandwidth. To overcome this, more network bandwidth is added to process a large volume of emails including the spam. Besides, every year, the Internet Service Providers (ISP) and Email Service Provider (ESP) install more servers to process and filter spam. Additionally, cost is also involved in maintaining and to updating the anti-spam technology [19, 23]. At the same time, the ISP also need to provide more helpdesk service due to the complaint of spam from their customers [18]. All these effort have been made to

ensure the internet users get the best services from ISP and ESP. However, the spammers take this advantage to send more advance type of spam emails such as email with interesting graphic attachments. One of the characteristics of spam is it always send in bulk [4]. The sheer volumes of spam once the spammer hit send button has slowed down the email traffic and eventually cause DDoS (Distributed Denial of Services). To avoid this from happening, normally the ESP or ESP will upgrade the network infrastructure by providing more network bandwidth and email storage to the Internet users.

C. Internet User Trust

The email users' trust can be categorized into two types, namely, trust on internet marketing and trust on the anti-spam technologies. In internet marketing, trust for web merchant is defined as the belief that the marketers will not behave opportunistically by taking advantage of the situation [24]. From a different perspective, consumers expect the ability, benevolence and integrity of the merchant [25-27]. Malhotra et al., [28] has found that both users' trust toward a web merchant affect directly and positively on users' willingness to use the Internet in order to buy products or services or to retrieve information. In addition, collection of personal information affect directly and negatively on users' trust toward a web merchant. The findings also highlighted that both users' concerns for information privacy and users' perceived privacy control have direct impact not only to users' trust toward the web site as expected but also the willingness to transact online when personal information needs to be disclosed.

In order to gain consumers online trust, the third party approval and endorsement such as Verisign, Truste, WebTrust, Trusted Site Seal has reducing the consumer risk perception [29]. But how much the consumer can trust on these is questionable. According to the local newspaper, The Star dated 29th March 2012, online shopping scams has risen in Selangor, Malaysia from 247 to 445 cases last year [30]. This incident showed that, online shopping is not as easy as we heard because it has it owns risks. In another local newspaper in Malaysia, a teacher has lost some amount of money because of spam email [31].

Secondly, according to the recent survey, most people avoid email-marketing because sometime legitimate emails are classified as spam emails and will be directed to the spam box or folder [8]. The spam email has caused the loss of trust among the email users [19]. The true meaning of email has lost due to the legitimate messages need to be restored from the spam folder and for the worst case it could not be saved because have been deleted automatically if no actions within certain period of time. This situation indirectly showed that the email user does not trust the anti-spam technologies as well. That is the reason why email users prefer to delete the spam email manually rather than depend on the filtering method only [1]. Most organizations have started using security technologies but it is not sufficient [32]. Thus, recently practitioners and academics have recognized that information security cannot be achieved through technological tools only. In fact, the security of information in organization depends on three main components that are people, process and technology [32].

Besides that, other problem with spam email is the threat spreading through it. The concern is it may contain viruses, or URL link in the messages that might point to the website containing viruses. Obviously this will damage the computer and cause a problem to the company [19]. Apparently, these problems have reduced the trust of Internet users while using email technologies.

D. Internet Marketing

Email is a medium of communication in internet transaction either from selling or buying side. In internet marketing, email is known as a vital tool for building rapport relationship between seller and buyer. However, it has caused a high volume of spam nowadays. According to Herardian [33], economic is the fundamental factor that triggers the increasing number of spam and not technology. The reason is spam email is the least expensive method to advertise the product, although the response rate is very low but there it still profitable [33].

Prior to the spam existence, banner advertisement is a medium for advertisement in internet marketing. Unfortunately it can be easily ignored by most of the internet users and makes it as a passive advertisement. In contrast, with advertisement using email, the recipient has to take some action in order to respond with it either read or delete. Since using email the customers is not well targeted, it makes the marketing process ineffective [34].

The number of consumers avoiding Internet-based advertising and promotion campaigns has increased [Cho and Cheon, 2004; Dreze and Hussherr, 2003 as cited by 18, 35] which indicated the level of trust has decreased. They have negative perception on the truth of the advertisement and have difficulties to differentiate whether it is spam or not. Moreover, as found by Rose [35] most of the consumers recently avoid internet–based advertising because of the loss of control over consumer personal information. Recent survey has revealed that most people avoid email-marketing because the email always classified as spam email and will be directed to the spam box or folder [8].

V. Anti-Spam Measures

From the past literature, some researchers have concluded that email users are not concern with the spam emails. In line with this, the impact of spam email is also ignored by them [1, 36]. According to the study, most email users are not really sure on the negative impacts of spam emails. They claimed they are aware but action-wise, they still do not trust the filtering technology [1]. Furthermore they do not have knowledge to avoid spam email and protect their email

account. There is a research which study the behavior of email users when they receive the spam email [13]. From the study, it was found that the spam experience has a limited impact on user's protection behavior but has affects the usage-oriented behavior. In the study, the protection-oriented is a proactive behavior while usage-oriented is passive behavior. Therefore, it seems that the email user tend to perform passive behavior which is more easy because it does not require any physical efforts [13]. It showed that individually email users not taking spam email problem seriously.

Many countries has adopted legal action to control spam email, however it is not really effective because the spammer can move their location. Furthermore, very few of them report the spam cases to the respective agencies because of the limited information on how and to whom they should go [1]. Furthermore, the legislation alone is not sufficient to control the spam because spammer can move to another country to avoid the legislation action.

In technological aspect, many technology experts have proposed various method of anti-spam technology; unfortunately the false positive issues still exist. Thus, it causes loss of trust towards the anti-spam technology. Many legitimate emails have been classified as spam email therefore, most email users prefer to delete manually either in the inbox and spam box. This happens because the spammers always change their techniques according to the recent anti-spam technology. The spammer will ensure that they will be winners even for a very short time before new anti-spam technologies introduced. Thus, the battle with spam email will never end until each one respect each other's privacy. So far, as email users, what can be done is to make an effort to protect our email address and take precaution steps while on the Internet.

VI. RECOMMENDATIONS

To improve the current situation of spam email, some recommendations are proposed. The spam email problem could not be solved successfully unless email users individually practice good ethics while using the email. Although various methods have been introduced in the form of technology and legislation, the spam email is still increasing. Technology and legislation itself could not eliminate the spam because it needs the cooperation from the email users or the spam email victim. The weakness of the society today is too much depending on the technology to solve the problem. Technology itself is created or developed by human, definitely email users involvement are required to solve the spam problem and not just leave it to the experts.

The simple example is how many of them report the spam cases or move the spam email into spam folder. Although anti-spam technology able to detect automatically, however the rapid growth of spam evolution make the accurate detection is impossible and sometimes it causes false positive situation which make the email user do not trust the anti-spam technologies [1]. As a result, email users prefer to scan their inbox and delete the spam email manually. Therefore email user cooperation is needed to ensure anti-spam database are up to date to enable it blocks most of the spam email.

From the past literature [1, 13] most email users do not have determination or spirit to fight spam. It could be because of lack of knowledge which has caused low awareness on spam email [1]. Ethics is a set of moral principles that govern a person's behavior or the conducting of an activity [37]. Thus, ethics of the email users need to be improved. Gaining knowledge alone is insufficient; actions are needed to stop the spam problem. Ethics of email users while using email is very important to complement other method to reduce spam email [38] . Technology and legislation method needs email users involvement to ensure the success of these methods. In technology, email users involvement is needed to categorize between legitimate email and spam email so that the database is up to date. To enforce legislation, email users are highly encouraged to report any spam cases to the related agencies for further action. As a result, the action taken towards the spammer will make others aware on the existence of the legislation. However all of these are out of individual's control because it is managed by the ISP or ESP (technological) or organization or government (legislation). In contrast, ethics is within oneself and all human are bestowed with the universal values such as honesty, willingness to help, and not to do injustice to other people. However, it is easily influenced by a negative environment. As an individual, good ethics is the best way to fight the spam. Spam email exists because of the unethical use of email for personal interest by the spammers.

By enforcing the legislation of spam, without further explanations of the issue, it makes the law as a tool to punish for their wrong doing only but not as a guard to avoid them doing the wrong things. The weakness here is that such law is not known to the email user and consequently they would not know whether their email use is ethical or not. An email user who simply forward the message would not know that he or she might invade the privacy of the email recipients although the intention just want to share the information. Due to the low awareness on the spam problem, thus relevant agencies should initiate an effort how to educate the email users. Some recommendation suggested here for those agencies.

For ESP they could make a compulsory for their registered user to read and understand the spam email issue and report spam cases or else the account will be blocked for a while, or they can provide incentives such as the email user who actively report spam cases will get more storage for their email account. Although the spammers can pretend to be a good email users unless the other email users can gain experience and knowledge on how to protect their email

account. Besides, showing a video to visualize how spam email could threat their email account is other method to educate the email users on the negative impacts of spam email towards their privacy life. The video should explain do and don't while using email. Other than that email user interface should shows spam folder clearly to ensure the email users realize the existing of spam folder as a solution for false positive cases. This is important because 45% of the email users in Malaysia experienced this problem[1]. Spam folder also very important to store the suspected spam email to ensure the legitimate email can be restore in the mailbox safely.

For anti-spam technology company, they should focus more on the effectiveness of their anti-spam technology and keep updating their anti-spam software. The software developer should be aware of the requirements from email users in order to develop usable anti-spam software. As happened in Malaysia, only 50% used anti-spam technology and approximately 25% of them willing to install their own security software by purchasing licensed software or free software [1]. It shows that email users are not interested to use the security software most probably because of the cost. In addition, their low awareness on the spam issue makes the impact of the spam email invisible to them. Furthermore, the existing of social network such as Facebook and Twitter which is more 'live' to them makes them forget about their data security and privacy. Therefore the software developer must find a way to develop high quality security software which can attract the email users to use it.

For the government, other than legislation, probably they can hold an awareness campaign on the spam issues. This should involve all levels of society from the top, such as technology experts; to the bottom level that is, active Internet users. The society is very excited to use the new technology but unfortunately they do not have enough knowledge and skills to protect themselves. The ethics on how to use Internet should be in the education syllabus not only in tertiary level but also should start in primary and secondary level. It is because nowadays, students also involve actively in social network with the latest gadgets which can connect to the Internet easily. Education in primary level has introduced the computing subject in Science subject. Therefore it is the best time to inform them the advantages and disadvantages of the Internet in general as an introduction. Besides, the parents also should promote and encourage their children to use Internet ethically. The parents must filter the Internet contents and must monitor their online activity closely to ensure the children are safe while on the Internet. If possible ask them to add their parents as friends in social network such as Facebook.

VII. CONCLUSION

The impact of spam email has been explored in many studies, however the information still could not reach the public user and only known to the researchers, academician, and technology security person. Apparently, the impact of spam email is less serious from an individual perception but more serious from organization perception. Moreover, most of email users believe it is ISP, ESP and relevant organizations responsibility to fight the spam email not them personally. They must realize that the spam email is initiated by email-user who has misused the email services and send the message to the other group of email users. Therefore only email users can control the situation because they are the user of the email services, anti-spam technologies and the person that legislation want to protect. Understanding the individual's perception towards spam is very important in order to find better solution to this problem. By identifying the weaknesses in current efforts in combating spam emails will lead to improvements needed. Obviously, ethics of email users while they deal with the spam email is very important to reduce the number of spam email. Latest guidelines are needed to overcome the latest techniques of spam. The guidelines should move together with the spam evolution.

Whatever the reasons of the spammers, sending spam threatens email recipients in terms of their trust, reputation, productivity and privacy. It could be considered as a mischief to the internet infrastructure. From the Islamic point of view, although it is hard to curb this problem, Allah has promised that those who do wrong will be punished in the Hereafter, as stated in the Qur'an [5]:

"And if any do evil, their faces will be thrown headlong into the Fire: Do ye receive a reward other than that which ye have earned by your deeds?" (27:90)

"If any does good, the reward to him is better than his deed; but if any does evil, the doers of evil are only punished (to the extent) of their deeds." (28:84).

The Qur'an also stated clearly that those who uphold falsehood and lie, they are not considered as following the Right path[5]:

"It is only those who believe not in the Ayat (proofs, evidences, verses, lessons, sigh, revelation, etc) of Allah, who fabricate falsehood, and it is they who are liars". (16:105)

REFERENCES

[1] Y.R. Bujang, and H. Hussin, "Spam E-mail: How Malaysian E-mail Users Deal With It?," *Online Special International Journal Issues*, vol. 2010, no. 43, 2010, pp. 1007-1013.

[2] J. Durgin, and J.S. Sherif, "Effects of unsolicited email on the virtual business world," *Emerald Group Publishing Limited*, vol. 35, no. 5, 2006, pp. 668-679.

[3] "Report on the Spam Act 2003 Review," *Book Report on the Spam Act 2003 Review*, Series Report on the Spam Act 2003 Review, 2006, pp.

[4] G. Schryen, *Anti-Spam Measures Analysis and Design*, Springer-Verlag Berlin Heidelberg 2007, 2007.

[5] A.Y. Ali, *An English interpretation of the Holy Quran*, Lushena Boook, 2001.

[6] M. Ciampa, "Security Awareness Applying Practical Security in your world.," 3rd Edition ed., Course Technology, Cengage Learning, 2010, pp. 114.

[7] T. Jackson, R. Dawson, and D. Wilson, "The Cost of Email Interruption," *Journal of Systems & Information Technology*, vol. 5, no. 1, 2001, pp. 81-92.

[8] M. Raad, N.M. Yeassen, G.M. Alam, B.B. Zaidan, and A.A. Zaidan, "Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing.," *African Journal of Business Management*, vol. 4, no. 11, 2010, pp. 2362-2367.

[9] "Get Response Email Marketing Solved," *2010 Email Marketing Trends Survey*2010.

[10] R. Potluri, "Assessment of effectiveness of marketing commuunication mix elements in Ethiopian service sector.," *African Journal of Business Management*, vol. 2, no. 3, 2008, pp. 59-64.

[11] A.A. Zaidan, N.N. Ahmed, H. Abdul Karim, G.M. Alam, and B.B. Zaidan, "Spam influence on business and economy: Theoretical and experimental studies for textual anti-spam filtering using mature document processing and naive Bayesian classifier," *African Journal of Business Management*, vol. 5, no. 2, 2011, pp. 596-607.

[12] H. Liang, and Y. Xue, "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly*, vol. 33, no. 1, 2009, pp. 71-90.

[13] I. Park, R. Sharman, R.H. Rao, and S. Upadhyaya, "The Effects of Spam and Privacy Concerns on Email Users' Behavior," *Journal of Information System Security*, vol. 3, no. 1, 2007, pp. 24.

[14] Malaysian Communications and Multimedia Commission, "Anti-Spam Toolkit " *Book Anti-Spam Toolkit* Series Anti-Spam Toolkit version 1 ed., Malaysian Communications and Multimedia Commission, 2006.

[15] C. Dhinakaran, C.J. Chae, and J.K. Lee, "An Empirical Study of Spam and Spam Vulnerable email Accounts," *Book An Empirical Study of Spam and Spam Vulnerable email Accounts*, Series An Empirical Study of Spam and Spam Vulnerable email Accounts, IEEE Computer Society, 2007.

[16] D. Fallows, "How It Is Hurting Email and Degrading Life on the Internet," *Book How It Is Hurting Email and Degrading Life on the Internet*, Series How It Is Hurting Email and Degrading Life on the Internet, ed., 2003.

[17] S. Hansell, "Totalling up the bill for spam," *Book Totalling up the bill for spam*, Series Totalling up the bill for spam, ed., 2003.

[18] E. Moustakas, C. Raganathan, and P. Duquenoy, "E-mail marketing at the crossroads - A stakeholder analysis of unsolicited commercial e-mail (spam)," vol. 16, 2006, pp. 38 - 52.

[19] M. Siponen, and C. Stucke, "Effective Anti-Spam Strategies in Companies: An International Study," *39th Hawaii International Conference on System Sciences*, pp. 10.

[20] T. Takemura, and H. Ebara, "Spam Mail Reduces Economic Effects," *Book Spam Mail Reduces Economic Effects*, Series Spam Mail Reduces Economic Effects, IEEE Computer Society, 2008.

[21] L. Uys, "Voice over Internet Protocol (VOIP) as a communications tools in South African business.," *African Journal of Business Management*, vol. 3, no. 3, 2009, pp. 89-94.

[22] S. Gaudin, "90% of e-mail will be spam by year's end," *Book 90% of e-mail will be spam by year's end*, Series 90% of e-mail will be spam by year's end, ed., 2007.

[23] A. Leung, "SPAM The Current State," *Book SPAM The Current State*, Series SPAM The Current State, ed., Telus Corporation, 2003, pp. 29.

[24] D. Gefen, E. Karahanna, D.W. Straub, and A.M. Trust, "Trust and TAM in online shopping and integrated model," *MIS Quarterly*, vol. 27, no. 1, 2003, pp. 51-90.

[25] D.H. Mcknight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: an intergrative approach," *Information Systems Research*, vol. 13, no. 3, 2002, pp. 334-359.

[26] A. Bhattacherjee, "Individual trust in online firms: scale development and initial test," *Journal of Management Information Systems*, vol. 19, no. 1, 2002, pp. 211-231.

[27] P.M. Doney, and J.P. Cannon, "An examination of the nature of trust in buyseller relationship," *Journal of Marketing*, vol. 61, 1997, pp. 35-51.

[28] N.K. Malhotra, S.S. Kim, and J. Agarwal, "Internet user's information privacy concerns (IUIPC): the construct, the scale and causal model," *Information System Research*, vol. 15 no. 4, 2004, pp. 336-355.

[29] Z. Lin, X. Hu, and H. Zhang, "Myth or reality? Effect of trust-promoting seals in electronic commerce," *11th Workshop on Information Technologies and Systems,*.

[30] A. Ruban, "Online shopping scams in Selangor on the rise," *Book Online shopping scams in Selangor on the rise*, Series Online shopping scams in Selangor on the rise, ed., Star Publications (Malaysia) Bhd, 2012. (accessed on 29 March 2012)

[31] "Teacher poorer by RM17,100 after falling prey to e-mail lucky draw scam," *Book Teacher poorer by RM17,100 after falling prey to e-mail lucky draw scam*, Series Teacher poorer by RM17,100 after falling prey to e-mail lucky draw scam, ed., Bernama Media, 2013. (accessed on 2 February 2013)

[32] T. Herath, and H.R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, 2009, pp. 154-165.

[33] R. Herardian, "Fight Back Against Spam. The evolution of anti-spam technology,"2004; http://www.dominopower.com/issueprint/issue200408/00001340.html. (accessed on 15 Jun 2012)

[34] R.D. Gopal, Z. Walter, and A. Tripathi, K. , "Admediation: New Horizons in Effective Email Advertising," *Commun. ACM*, vol. 44, no. 12, 2001, pp. 91-96.

[35] E. Rose, "Balancing Internet Marketing Needs with Consumer Concerns: A Property Right Framework," *Book Balancing Internet Marketing Needs with Consumer Concerns: A Property Right Framework*, Series Balancing Internet Marketing Needs with Consumer Concerns: A Property Right Framework, 2001.

[36] M. Workman, W.H. Bommer, and D. Straub, "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior*, vol. 24, no. 6, 2008, pp. 2799-2816.

[37] J. Pearsall, "Oxford Dictionaries," *Book Oxford Dictionaries*, Series Oxford Dictionaries, ed., Oxford University Press, 2013.

[38] Y.R. Bujang, and H. Hussin, "Investigating Email Users Behavior against Spam: A Proposed Theoretical Framework," *Journal of Internet and e-Business Studies*, vol. Volume 2012 (2012), 2012, pp. 10.