World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:4, No:7, 2010

Spam e-mail: How Malaysian e-mail Users Deal with It?

Yanti Rosmunie Bujang and Husnayati Hussin

Abstract**—**This paper attempts to discuss the spam issue from the Malaysian e-mail users' perspective. The purpose is to discover how Malaysian users handle the spam e-mail problem. From the experiences we hope to discover the necessary effort needed to be undertaken to face this problem in the context of Malaysia. A survey was conducted to understand how Malaysian individual perceived spam and what they actually do with the spam e-mail they received in their daily life. The findings indicate that the level of awareness on spam issue in action is still low and need some extra effort by government and relevant agencies to increase their level of awareness.

Keywords**—**e-mail, Malaysia, spam, users' perspective

I. Introduction

SPAM is also known as Unsolicited Commercial E-mail (UCE) [3] or unsolicited bulk e-mail (UBE) [15]. The definition shows that the main characteristics of spam are the e-mail is sent without recipient's permission, from unknown sender, has commercial value and always sent in bulk. The main problem of the spam e-mail is that it is an 'unwanted' e-mail, or in other words, the content is not requested by the recipients. For this survey, spam is defined as unwanted message(s), also known as unsolicited commercial e-mail (UCE), which means these e-mails are sent without consent (permission) by the unknown sender. Normally the contents are related to promoting products or services of health, adult, finance and education.

Most researchers highlight that many issues need to be discussed further in order to understand the world of spam. Spam is not a new phenomenon in information and communication technology and in fact, spam is considered as information pollution [6]. Nowadays there are many types of spam exist even though many efforts have been undertaken to eliminate them, and even worse, spam become more advanced over time as stated by MessageLabs [11]. In the past, spam-related researches only considered four major concerns namely: ethical, social, technical and legal issues of the spam problem [10].

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).

The authors would like to thank Research Management Centre, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Malaysia to sponsor and support this research project and the respondents of the survey for their feedback.

However, most of the researchers focused on the technology to control spam; very scarce literature reports on the other aspects, particularly the social aspect.

II. Anti-spam Strategies

In general, anti-spam technique can be classified as adopting two major strategies namely, (i) technological approach, or (ii) legislation approach. Even though many anti-spam technology methods were created to control spam but they were only effective in the early stages. Once the spammers know how the technology works then they will create new technique to bypass the system. To ensure the effectiveness of anti-spam technology, it requires careful effort in updating and monitoring of the method [17]. These makes the efforts to fight spam is never ending and a continuous process. The following subsections discussed the two strategies in more detail.

A. Technology

Filtering and blocking are the common technology approach to reduce the spam in the e-mail users' inbox. The basic principle is that the system will filter all the messages, if the message contents match with the criteria which has been identified as spam, the system will blocked those e-mail entering the mailbox. Filtering such as rule-based (keywords matching) or heuristic is an analysis that uses regular expression rules to detect phrases or characteristics of spam such as Bayesian filtering [8]. However, this technology is based on a static rule set, which means it cannot adapt to the new spam characteristics [8] and false positive existence could not be avoided.

Other filtering method is signature-based techniques which generates a unique hash value (signature) for each known spam message. Two common softwares which use this technique are Cloudmark and Vipul's Razor [8]. As mentioned by Carpinter and Hunt [8], Cloudmark provides a commercial implementation of a signature filter, integrating with the network mail server and communicating with the Cloudmark server to submit and receive the spam signatures. Whereas Vipuls's Razor is an open source software using a distributed, collaborative mechanism to distribute signatures with appropriate trust safeguards that prohibit the network's penetration by a malicious spammers. The disadvantage is the inability of the method to identify new spam e-mail until it has been reported as spam and its signature distributed [8].

Interactive filters also known as 'challenge-response' is one of the filtering method to control the incoming spam e-mail in the inbox. The assumptions or belief made on the development of this filter is that the spammers are not interested to complete the given challenge. However, many e-mail users refuse to use the system because it slows down the message delivery [8]. One of the well known methods under this category is the Completely Automated Public Turing Test to Tell Computers and Humans Apart or CAPTCHA. While this method has provided many benefits, a recent study by Yan and Ahmad [19] has indicated the weaknesses for CAPTCHA as standard security technology. It seems CAPTCHA has to go through the process of evolutionary to be a more robust system. In their study CAPTCHA can be attacked with a present new character segmentation technique.

B. Legislation

To deal with the evolvement of spam, some countries has identified legal act to control them. For example, Australia has introduced the Spam Act 2003 and United States implemented CAN Spam Act. They either adopt opt-in or opt out method anti-spam laws. In Australia's Spam Act 2003 [3], it adopts opt-in approach which means the receiver's consent must be obtained before sending a message, whereas US practise opt-out which means it does not require consent of the recipient of a message but requires request removal from the list in future [7]. In 2002, Casal suggested to reject opt-in as a sensible basis for International regulation [9]. His reason is to achieve a compromise among user companies and would protect user's privacy and property and indirectly protect market competition. However, the problem with opt-out is when the recipients reply the e-mail to request removal from the list in the future, it indicates the e-mail is active and can attract more spam [9]. In addition, it also indicates the ISP filters is not effective, confirms the users responded to the spam e-mail and follow the spammers instruction [15].

Whatever the reasons are, it depends on each country to set their own legislation regarding the spam because different countries have different culture in handling their e-mail communications. Some study stated that legislation had little effect to stop spammers' activities [16] and some other study said it was effective [3].

In Korea, the government enforces spammers to note 'Advertisement' for general commercial e-mail and 'Adult Advertisement' for adults' contents of commercial e-mail [20]. Unfortunately it seems this method was not successful because the legitimate e-mail can be blocked for a certain phrase related with spam mails

Furthermore according to the study by Young and Tae et. al, although Korea has adopted opt-out and labelling method to decrease the number of spam e-mail but these were only effective in the first place [20]. The number decreased drastically in 2003 but after a year, the number has increased constantly. It makes Korea ranked as second after US among countries creating spam e-mails. Thus, the authors have proposed opt-in and register with pricing to fight spam.

However, the effectiveness of the legislation still can be questioned by e-mail users based on the number of spam e-mail they received in the mailbox.

III. Spam In Malaysia

Currently, Malaysia is relying on the Communication and Multimedia Act, 1998 to control this problem but as mentioned in a "Report on a Public Consultation Exercise Regulating Unsolicited Commercial Messages" by Malaysian Communications and Multimedia Commission (2004), there are some insufficient aspect to handle the spam issue [1]. Although Malaysia has no specific law to fight against spam, there are some actions taken by a few agencies to control spam. Malaysia Computer Emergency Response Team (MyCERT) is a unit under the National ICT Security and Emergency Response Centre (NISER), which is responsible to receive the report of spam cases through Cyber 999 hotline. NISER also has produced a document namely Anti-Spam Framework of Best Practices and Technical Guidelines as an effort fight spam problem [2]. However, the awareness of the public on these efforts and their effectiveness is yet to be determined. It is hoped that the findings of this study will shed light on these issues.

Although there are anti-spam software effective to control spam but the research on how the e-mail users accept or use the technology is unknown. There is no use to have advance technology if it is not well adopted by the society. Currently, only ISPs, ESPs, and technology-related companies follows the evolution of these technologies. But this is not enough because the e-mail user himself must play important role to protect his own e-mail address. It is hoped that the results from this study will depict the real perceptions, and eventually the next step to develop control measures on the spam issues can be developed.

IV. Methodology

This research has adopted a survey method to study the perception of people in Malaysia on spam problem. In addition, the survey attempts to reveal their attitudes towards spam e-mails and how they handle spam e-mail in their daily communication.

A. Sampling

The sample consists of e-mail users in Malaysia with the minimum age is 15 years old. For this purpose, the sampling method used was simple random sampling. The sample population included students from various institutions and employees were from any organisations in Malaysia.

For the pilot study, the sample was 30 and we managed to get 19 respondents. For the main survey, the sample was 350 respondents, of which 250 were students in any schools or higher educational institutions and 100 were employees in any organisations in Malaysia. The selected sample population attempts to represent the general Malaysian e-mail users in the whole country.

B. Data Collection Strategy

Prior to the distribution of the questionnaires, each potential respondent was checked to ensure that he/she has an e-mail account. The distribution of the questionnaire was done in both hardcopy and softcopy, whichever is convenient to the sample based on their preference. The soft copy was distributed through e-mail, and the hard copy was distributed either hand-delivered or through the snail mail. The distribution of questionnaire has taken approximately six weeks between February to March 2010, including the pilot study.

C. Measurement Items

The questionnaire contains 44 questions consist of both qualitative and quantitative items. Some of the questions are adopted from other study [5], [10] and Pew Internet & American Life Project (2007) and selected based on the appropriateness of the study purpose. The quantitative questions are using seven point Likert Scale whereas qualitative questions use open ended questions. It has four sections namely: (i) demographic information; (ii) Internet and e-mail experiences; (iii) spam experience; and (iv) opinion and recommendations.

V. RESULT ANALYSIS

For analysis purposes, data from the pilot study was also considered due to only minor changes have been done after the pilot test. Out of 380 questionnaires sent out, only 260 questionnaires returned and usable for analysis.

A. Demographic Information

The first part of the questionnaire asked demographic information of the e-mail users. Table 1 summarize the data:

TABLE I
GENDER

Gender	Frequency	Percentage (%)
Male	108	41.5
Female	152	58.5
Total	260	100.0

TABLE II
AGE

Age	Frequency	Percentage (%)
15-20	33	12.7
21-30	199	76.5
31-40	18	6.9
41-50	7	2.7
Above 50	3	1.2
Total	260	100.0

TABLE III
EMPLOYMENT CATEGORY

Employment Category	Frequency	Percentage (%)
Student	207	79.6
Self-employed	2	0.8
Private	16	6.2
Public	32	12.3
No Answer	3	1.2
Total	260	100

TABLE IV
LEVEL OF EDUCATION

Education	Frequency	Percentage (%)
Secondary school	42	16.2
Certificate/Diploma/College	48	18.5
First Degree	152	58.5
Postgraduate	12	4.6
No answer	5	1.9
Other	1	0.4
Total	260	100

Table I, II, III and IV summarize the demographic information from the survey. As seen from the above tables, most participants of this survey are females, which is 58.5% (Table I) although not much different with the males. Since the focused population is more on students, therefore, 79.6% (Table III) of them are students and 76.5% (Table II) of them are between 21-30 years old of age. In addition, 58.5% (Table IV) of the participants have first degree as their highest education level.

B. Internet and E-mail Experience

Based on the belief of IT experience is very important as a foundation to use IT application specifically e-mail application for this research context. In this survey they were asked their experiences on Internet and e-mail application as an indicator to measure their skills on these areas.

An assumption was made, the more experience they have in using the Internet, the less spam e-mail they received due to more knowledge and information they gain from Internet. As shown in Fig. 1, 79% of the e-mail users have more than 5 years experience using Internet and 66% experienced using e-mail (Fig. 2).

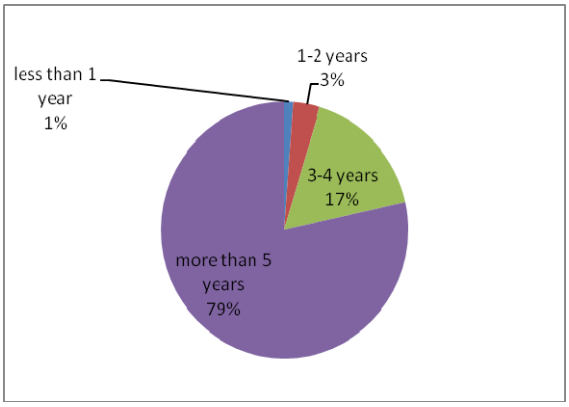

Fig. 1 Experience using the Internet

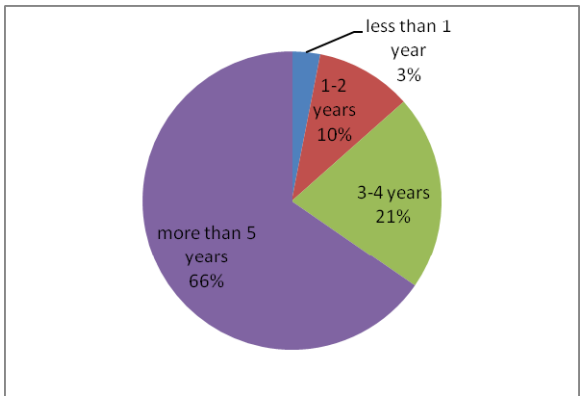

Fig. 2 Experience using e-mail

Fig. 3 and 4 represent the frequency of the participants using Internet and e-mails. Contrast to prior assumption, it was found that the more frequent they use Internet and e-mail, the more spam they received since they are exposed to the online threat and become spammers victims. The finding indicate that most of the participant are active users which they use Internet (62%) and e-mail (39%) everyday.

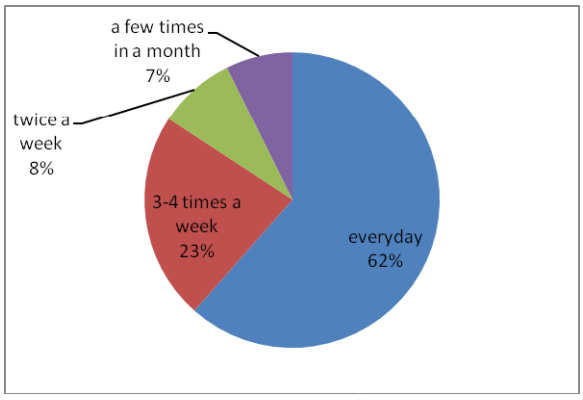

Fig. 3 Frequency using the Internet

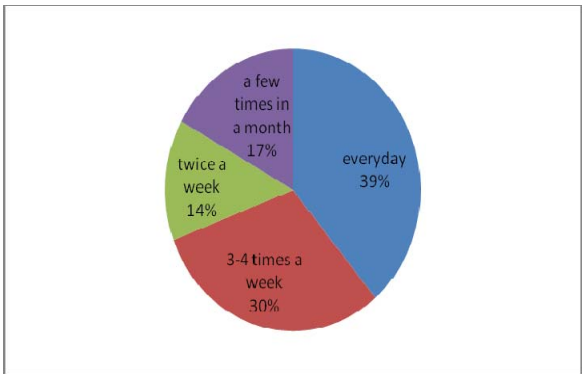

Fig. 4 Frequency using an e-mail

TABLE V
NUMBER OF E-MAIL ACCOUNT

No. of e-mail account	Frequency	Percentage (%)
1	92	35.4
2	96	36.9
3	47	18.1
4	12	4.6
5 to 10	9	3.5
11 to 20	0	0.0
Above 20	1	0.4
No Answer	3	1.2
Total	260	100.0

By referring to the Table V above, most e-mail users have two e-mail accounts (36.9%) and those with single e-mail account represents 35.4%. When the participants were asked with the probing question why they have that number of e-mail account(s), the main reason was because it is easy to manage as having many e-mail accounts (more than two) mean that they need to remember many passwords. However, they prefer to have more than one e-mails account because each e-mail account has different purposes and the main purposes is for formal activities like work or study and personal purpose such as social network.

It seems e-mail users prefer to have free e-mail account which is 73.1% of them instead of having formal e-mail account only provided by their organisation or institution that is 1.2%. Then, 25% of them have both type of e-mail. The most popular free e-mail account among e-mail users in Malaysia are Yahoo (55.8%), secondly Yahoo and Gmail (17.3%) and followed by Yahoo and Hotmail (11.2%).

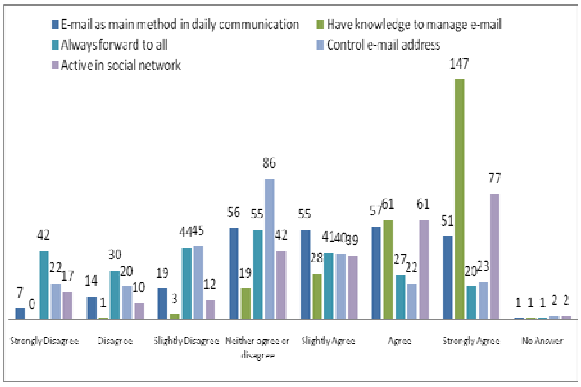

Fig. 5 Internet and e-mail experience

Figure 5 depicts the result of the background of the respondents' Internet and e-mail experiences. Most of them consider e-mail as one of the main methods for their daily communication with 21.2% slightly agree, 21.9% agree and 19.6% strongly agree. To manage e-mail account, 147 (56.5%) of them strongly agree they can manage their e-mail account by themselves.

Most of the e-mail users give neutral answer when they were asked if they always forward e-mail message to all in their contact list (21.2%). This is similar with the question that asked did they protect their e-mail addresses by making it more difficult for others to find them, 33.1% of them give neutral responses as well. Most of them disagree to publish their e-mail address. In using e-mail application, ethically the e-mail users are not encouraged to forward any email to all in their contact list because this will expose the listed e-mail address to the spammers. Surprisingly, 33.9% of them did this. As can be seen from the above diagram, 68.1% of them involve actively in social networks such as Facebook, Friendster and Twitter, with the detail results of 15.0% slightly agree, 23.5% agree and 29.6% strongly agree.

C. Spam Experience

From the analysis, it shows 86.5% of them are aware of the existence of spam e-mail and the average number of spam e-mail they received daily is 5 e-mails. Over the last 6 months, 43.5% said the number of spam e-mail has increased, 44.2% said they were about the same and 9.6% of them indicated it has decreased.

Generally, English is the most popular language used by the spammers which is 90.0% and the second popular language is Malay (82.9%) due to the sampling are done in Malaysia. This question asked the e-mail users to rank the language of spam e-mail they frequently received.

Table VI reveals how actually the e-mail users handle spam e-mails in their daily life. As we can see, most of them are aware on the spam existence (86.5%) as mentioned in previous discussion and aware of the existence of anti-spam technology (66.9%) as shown in Table VI. The result shows that only 8.1% of the respondents have responded to the spam e-mail and 30.8% have ever clicked on the spam link. When asked about the anti-spam technology, only 50.4% of them have used filter which is provided by ESP (Email Service Provider) and employer. Although they are aware of anti-spam technology, surprisingly, only 25.8% of them have ever applied their own filter by purchasing licensed security software or get it free from Internet. For false positive cases, where legitimate e-mail was misclassified as spam e-mail, 45.4% of them have experienced that situation and 53.8% do not have. This indicates that e-mail users are aware on the false positive cases as a weakness of the filtering technology because they also check their spam folder which is under quarantine.

Unfortunately, 91.9% of Malaysian e-mail users did not report any spam cases and only a small minority (7.7%) actually did. Even though they perceived that they are aware on spam issue, they did not do much or take any action to solve the problem. Some possible reason is they do not know how to go about doing it and to whom they should report to. In fact Malaysia has Cyber 999 as a channel to report any online criminal to the Cyber Security Malaysia under Ministry of Science, Technology and Innovation (MOSTI). This fact is supported by the result on the awareness of the existence of anti-spam services which shows that only 14.6% of them are aware on these services. This shows the

TABLE VI
SPAM EXPERIENCE

Experiences	Yes	No	No Answer
Ever responded to the spam	21 (8.1%)	237 (91.2%)	2 (0.8%)
Ever clicked on spam link	80 (30.8%)	178 (68.5%)	2 (0.8%)
Awareness of the existence of anti-spam technology	174 (66.9%)	83 (31.9%)	3 (1.2%)
Ever used filters offered by ESP or employer	131 (50.4%)	126 (48.5%)	3 (1.2%)
Ever applied own filters	67 (25.8%)	191 (73.5%)	2 (0.8%)
Ever experienced false positive	118 (45.4%)	140 (53.8%)	2 (0.8%)
Have reported any spam cases	20 (7.7%)	239 (91.9%)	1 (0.4%)
Awareness of anti-spam services	38 (14.6%)	218 (83.8%)	4 (1.5%)

level of awareness on spam services is still low among Malaysians and most do not know what they can do to prevent spam from coming into their inbox.

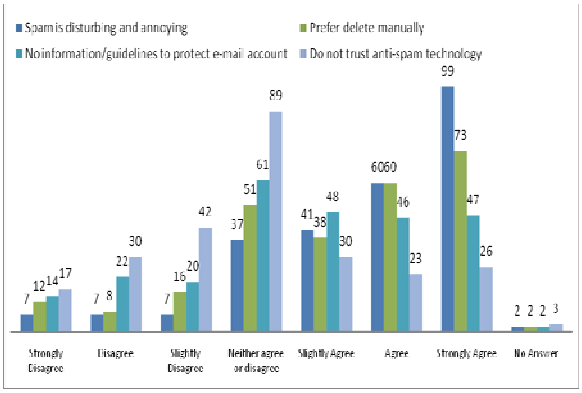

Fig. 6 Spam experience (II)

By referring to Fig. 6, mostly of the e-mail users (38.1%) strongly agree that spam is disturbing and annoying. Although, most of them (23.5%) are neutral, in general, 54.3% of them agree they did not have information/guidelines to protect their e-mail account. Similar with that, most of them also give neutral feedback when asked about the trust of using anti-spam technology which indicates that they are not sure on the effectiveness of anti-spam technology to control spam e-mail. This is in line with the result that a majority (65.8%) of them prefer to delete e-mail manually rather than depend on the filtering method provided by ESP, with the fraction 14.6% slightly agree, 23.1% agree and 28.1% strongly agree.

D. Impact of Spam

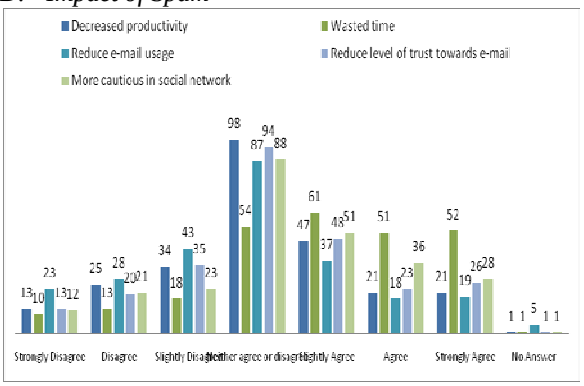

Fig. 7 Negative impacts of spam

Out of eight impacts of spam listed in the questionnaire, five negative impacts were compiled in a single graph for easy comparison as shown in Fig.7 above. It seems Malaysian e-mail users are not really aware of the impacts of spam. Most of e-mail users are not sure about the spam impact as indicated by a majority of them choosing 'neutral' as their responses. Nevertheless, about two thirds indicated that they were very sure that spam e-mail has wasted their time (63.1%) The possible reason is that they have spent their precious time to open, read and delete the spam e-mail in their inbox. This is relevant with the result that 65.8% of them prefer to delete their e-mail manually rather than depend on the filtering tools to avoid false positive cases.

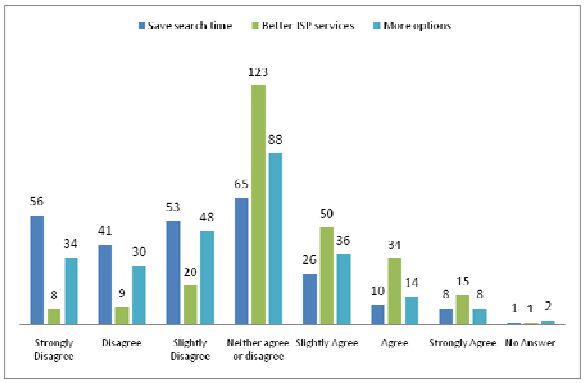

Fig. 8 Positive impacts of spam

There are three positive impacts of spam listed and the result is shown in Fig. 8 above. Similar to the previous result, most of them give neutral response for all the positive impacts. Among them 38.1% agree the benefits that they get from the spam issue is they found the ISP has better competition to give better services to overcome spam bandwidth. They might be influenced by many broadband and wireless promotions in Malaysia recently.

In the last section of the questionnaire, their perceptions towards using anti-spam software alone, their concern about the privacy of their e-mail address and the level of awareness of the spam issue were asked. The result from Figure 9 shows that most of them give a neutral answer and when comparison between the negative answers and positive answers were made, most of them in agreement for all the questions.

E. Opinions and Recommendations

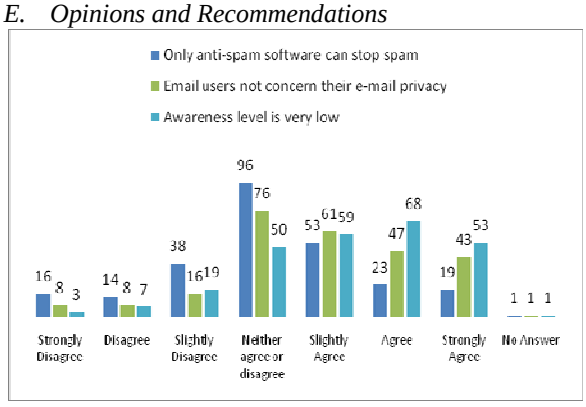

Fig. 9 Opinions and recommendations

They admit they are not too concern about the privacy of their e-mail address and Malaysian e-mail users awareness on spam issue is very low.

VI Conclusion and Future Works

From the result analysis, Malaysian e-mail users consider e-mail as one of the main communication method. Most of them prefer to have free and less than three e-mail accounts for ease of management. Although they are aware of the spam issue, they do not know what they should do to avoid spam and protect their e-mail address. In fact, in Malaysia some action has been taken by respective organisation but unfortunately it seems that the information does not reach the people. In view that Malaysia is a developing country, this may be due to the fact that most Malaysians are not really sure on the negative impact of spam which can indirectly affect the economic progress of the country.

Not surprisingly, Malaysia also has its own spammers due to the result shows that Malay is the second language frequently used by the spammer other than English as the most popular language. It indicates many e-mails users also received spam from local spammers regarding local commercial advertisement.

By discovering the real perception of Malaysian toward the spam issue, any lacking or gaps can be filled by developing an appropriate framework in the future. Thus, it is necessary to determine all the factors that influence the low awareness and attempt to indicate and guide them what can be done to help Malaysians handle this phenomenon. Although currently Malaysia still does not have specific law related to spam, this should not be a reason why spam problem could not be curbed. Spam problem is initiated by human, therefore, it is believed that only human can control the issue from becoming worst.

However, it should be noted this study is not without any limitations. One of the limitations is the representativeness of the sample, whereby most of the respondents were university students. They were chosen because students are known to be very active e-mail users in Malaysia other than working employees. Relatively, university students have easier access to e-mails and generally more cooperative in participating in surveys as they have more spare time compared to the working adults. Nevertheless, working employees were included in the sample despite having some challenges in getting their responses. Reminders have to be sent in order to get their feedbacks on time. However there appear to be no significant difference between the responses from employees and students. Therefore, it may be concluded that the findings can represent Malaysian e-mail users' perspective in general.

References

[1] (2004). A Report on a Public Consultation Exercise "Regulating Unsolicited Commercial Messages", Malaysian Communications and Multimedia Commission.

[2] (2005). Anti-Spam Framework of Best Practices and Technical Guidelines. NISER Report. Kuala Lumpur, National ICT Security and Emergency Reponse Centre. Issue 2.00: 42.

[3] (2006). Report on the Spam Act 2003 Review. Department of Communications, Information Technology, and the Arts

[4] (2006). "spamcop.net." Retrieved 10/04/2010, from http://spamcop.net/ces/setup.shtml

[5] Al-A'ali, M. (2007). A Study of Email Spam and How to Effectively Combat It. Webology. 4(1).

[6] Alstyne, M. V. An Economic Answer for Spam. Volume, 4 DOI:

[7] Bender, M. R. (2006). Australia's Spam Legislation: A modern-day King Canute? Working Paper Series, Corporate Law & Accountability Research Group, Department of Business Law & Taxation, Faculty of Business and Economics, Monash University.

[8] Carpinter, J. and R. Hunt (2006). "Tightening the net: a review of current and next generation spam filtering tools." Science Direct Vol. 25(8): 19.

[9] Casal, C. R. (2002). "Regulating Spam: opting in or opting out?" 4(2): 7.

[10] Chigona, W., A. Bheekun, et al. (2005). Perceptions on SPAM in a South African context. Proceedings of the 5th International Business Information Management Conference,, Cairo, Egypt.

[11] Eliminate Spam, Gain Productivity: E-mail Spam Is Growing Faster Every Year, Especially in The United States. White Paper. M. Labs.

[12] Gopal, R. D., Z. Walter, et al. (2001). "Admediation: New Horizons in Effective Email Advertising." Commun. ACM 44(12): 91-96.

[13] Moustakas, E., C. Raganathan, et al. (2006). "E-mail marketing at the crossroads - A stakeholder analysis of unsolicited commercial e-mail (spam)." 16.

[14] Fallows, D. (2007). The volume of spam is growing in American's personal and workplace e-mails accounts, but e-mail users are less bothered by it. , Pew Internet & American Life Project.

[15] Schryen, G. (2007). Anti-Spam Measures Analysis and Design. New York, Springer-Verlag Berlin Heidelberg 2007.

[16] Shlomo, H. and J. S. Salvatore (2004). "Identifying spam without peeking at the contents." Crossroads 11(2): 3-3.

[17] Siponen, M. and C. Stucke (2006). Effective Anti-Spam Strategies in Companies: An International Study. 39th Hawaii International Conference on System Sciences, Hawaii.

[18] Wood, P. (2003). A spammer in the works. White Paper. M. w. paper, MessageLabs.

[19] Yan, J. and A. S. E. Ahmad (2008). A Low-cost Attack on Microsoft CAPTCHA. CCS'08, Alexandria, Virginia, USA.

[20] Young, P. S., K. J. Tae, et al. (2005). Proposal of a new effective spam mail regulation.