EMAIL SPAM IN SAUDI ARABIA AND HOW DO END USERS DEAL WITH IT?


* Computer Science Department, College of Computer Science and Information Technology, King Faisal University, P.O. Box: 400 Al-Hass, 31982, Kingdom of Saudi Arabia hsalkahtani@kfu.edu.sa

** School of Computer Science, Engineering and Mathematics, Faculty of Science and Engineering, Flinders University, GPO Box 2100, Adelaide SA 5001, Australia paul.gardner-stephen@flinders.edu.au, robert.goodwin@flinders.edu.au

ABSTRACT

This paper presents the results of a survey of email users in Saudi Arabia about email SPAM. The survey investigated the nature of email SPAM, how email users dealt with it, and the efforts made to combat it. It also investigated the effectiveness of existing Anti-SPAM filters in detecting Arabic and English email SPAM.

1,500 participants located in Eastern, Western, Central, Southern and Northern regions of Saudi Arabia were surveyed and completed surveys were collected from 1,020 of the participants.

The results showed that there were different definitions for email SPAM based on different users’ opinions in Saudi Arabia. The results indicated that the majority of email SPAM received was written in English. The results showed that the most common type of email SPAM received in Arabic was emails related to forums and in English was business advertisements.

The results indicated that Yahoo was better than Hotmail, GMail and other email account providers in classifying email SPAM as the results revealed that the number of emails SPAM received by email users who used Yahoo was lower compared to other email account providers.

The results revealed that email users who have used email for long time were more aware of SPAM and using Anti-SPAM programs than users who used email for short time.

The results revealed that the most of the email users were not aware of the use of Anti-SPAM software to combat SPAM. The results indicated that the existing Anti-SPAM filters were not completely effective in detecting English and Arabic email SPAM and that these filters were more effective in detecting English SPAM than Arabic SPAM.

The results indicated that most email users were not aware of government and ISPs efforts to combat email SPAM in Saudi Arabia.

KEYWORDS: SPAM, email, Arabic, users, English, Saudi.

1. INTRODUCTION

Email is an important tool for many people and they consider email as a necessary part of their daily lives. Email enables people to communicate with each other in a short time at low cost. Although email gives benefits for people who use it, some people, called spammers, have exploited email for their personal purposes. They send so-called SPAM to a large number of recipients. They can use programs known as spam-bots to catch email addresses on the internet or they can buy email addresses from individuals and organizations to send email SPAM to these addresses [11]. They also use many methods to bypass SPAM filters such as tokenization and obfuscation [27].

Email SPAM is defined as “Unsolicited, unwanted email that is sent indiscriminately, directly or indirectly, by a sender having no current relationship with the recipient” [12], [13]. It is also defined as Unsolicited Bulk Email (UBE) that is sent to a large number of recipients who were not asked if they wanted to receive it [4], [14], [18]. Some studies [6], [7], [25] defined email SPAM as Unsolicited Commercial Email (UCE) that contains business advertisements sent to a large number of recipients.
There are legal and technical methods [2] to combat SPAM. Legally, some countries enacted laws against SPAM. Examples of these countries include the United States of America [26], European Union countries and Australia [5]. However, there are no laws in Saudi Arabia to combat SPAM although research and projects were conducted to assess the problem of SPAM in the country.

Technically, there exist many filters to combat SPAM. Examples of these filters include content based filters such as Bayesian [24], keywords [11] and genetic algorithms [15], and origin based filters like black lists [11], white lists [22], origin diversity analysis [16] and challenge response systems [21]. However, some of these techniques need to be updated to detect new types of email SPAM due to spammers developing ways to bypass these techniques.

This study aimed to gain an understanding about:

a. The nature of email SPAM, its definition based on email users’ opinions, its volume and its types.
b. Differences between Arabic SPAM and English SPAM.
c. The effects of email SPAM on email users.
d. How email users deal with email SPAM.
e. The efforts of government to combat email SPAM.
f. The efforts of ISPs to combat email SPAM.
g. Evaluation of email users’ perception of the effectiveness of Anti-SPAM filters in detecting Arabic and English email SPAM.

2. METHODOLOGY

2.1. Measures

It was decided that the best way to answer the research questions was through a questionnaire. Therefore, a questionnaire was distributed to the participants and the responses were analyzed.

Initially a pilot questionnaire was prepared and distributed to a few participants to get their comments about the questions. Then all the participants completed the 10 page questionnaire which included both yes/no answers and open ended answers. The questionnaire consisted of three main parts as follows.

2.1.1. General information questions

In this part, the participants were asked for the following information: gender, age, nationality, speaking language, highest level of education, major area of study, work status and the nature of the work. These questions helped in understanding and comparing the level of awareness of email users about email SPAM. Examples for the first part of questions of the survey can be seen in Figure 1.

| 1. Gender:  
| O Male  
| O Female |
| 2. What is your age?  
| 3. Nationality:  
| O Saudi  
| O Other |
| 4. What is your current work status?  
| O Student  
| O Employed  
| O Self employed |

Figure 1: Examples of questions of the first part of the survey

2.1.2. Email SPAM questions

At the beginning of this part, the participants were asked for a definition of email SPAM in their own words in order to understand the definition of email SPAM based on their opinions. Then the study defined email SPAM as “an unsolicited, unwanted, commercial or non-commercial email that is sent indiscriminately, directly or indirectly, to a large number of recipients without their permission and there is no relationship between the recipients and sender.” This definition was in the survey and used to provide a reference point for the remainder of the questions. Care was taken to ensure that the respondents did not see the study supplied definition until after they had supplied their own definition of email SPAM to prevent introducing a strong bias. The variety of responses to the question of what is SPAM is evidence that this approach was successful. Some examples of email SPAM, keywords and phrases used in email SPAM were given in the survey.

The participants were asked if they knew about email SPAM prior to reading the survey, and what were the sources of their knowledge. The participants were also asked if they received email SPAM and how many email SPAMs they received on average weekly. They were also asked about the languages they received in email and types of Arabic and English email SPAM. The study focused on English and Arabic email SPAM because English is the main language in the world and Arabic is the native language in Saudi Arabia.

The participants were asked about their email account providers to provide an understanding
about the differences between email account providers in filtering email SPAM and the effectiveness of their filters in detecting email SPAM. The participants were also asked how long they have been with their current email account providers to gain an understanding of the experience of email users in dealing with SPAM and using Anti-SPAM filters.

The participants were asked about what they did when they receive email SPAM (i.e. the actions of email users in dealing with SPAM). The actions of emails users in dealing with SPAM described in the survey were as follows: reading the entire email SPAM, deleting the email SPAM without reading it, and contacting the ISP and notifying it about email SPAM. The participants were asked to choose one option from the following options to answer their action in dealing with SPAM. These options were as follows: never, sometimes and always. Figure 2 shows an example for questions of email users in Saudi Arabia about their actions in dealing with email SPAM.

The participants were asked if they purposely responded to an offer made by a SPAM email and what benefits they derived from email SPAM. They were also asked if they were affected by email SPAM and what were the effects of email SPAM on them.

The participants were asked if they were aware of Anti-SPAM filters to block email SPAM, what were the sources of their knowledge about these filters, and how effective these filters were in detecting Arabic and English email SPAM. Examples for the second part of questions of the survey can be seen in Figure 3.

<table>
<thead>
<tr>
<th>1. Everyone defines SPAM differently, in your own words, how would you define email SPAM?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Did you know about SPAM emails prior to reading this survey?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Have you received SPAM emails?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. What is the language of SPAM email you receive on average weekly? The percentages should add up to 100 %.</th>
</tr>
</thead>
<tbody>
<tr>
<td>O English</td>
</tr>
<tr>
<td>O Arabic</td>
</tr>
<tr>
<td>O Other language</td>
</tr>
<tr>
<td>O Languages I do not recognize</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Are you aware of Anti-SPAM programs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. If you have used Anti-SPAM programs, please rate their effectiveness in detecting English and Arabic email SPAM?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The effectiveness of current programs in detecting Arabic email SPAM</td>
</tr>
<tr>
<td>0% 25% 50% 75% 100%</td>
</tr>
<tr>
<td>The effectiveness of current programs in detecting English email SPAM</td>
</tr>
</tbody>
</table>

Figure 3: Examples of questions of the second part of the survey

### 2.1.3. Questions about the efforts of government and ISPs to combat email SPAM

In this part, the participants were asked if they were aware of government efforts to combat SPAM and which efforts they were aware of. The participants were also asked if they were aware of ISPs efforts to combat SPAM and which efforts they were aware of. Examples for the third part of questions of the survey can be seen in Figure 4.

<table>
<thead>
<tr>
<th>1. Are you aware of efforts by the government in Saudi Arabia to combat email SPAM?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Are you aware of efforts by ISPs in Saudi Arabia to combat email SPAM?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O No</td>
</tr>
</tbody>
</table>

Figure 4: Examples of questions of the third part of the survey

### 2.2. Participants

The questionnaire was designed and distributed to 1,500 participants in central, eastern, western, southern and northern regions of Saudi Arabia. Completed questionnaires were received from 1,020 participants in Saudi Arabia.
The participants were from different regions in Saudi Arabia. 34% of the participants were from the Central region, 20% were from the Eastern region, 20% were from the Western region, 13% were from the Southern region and 13% were from the Northern region.

60% of the participants were male and 40% were female.

The ages of the participants ranged between 15 and 62. 45% were between 15-25, 35% were between 26-35, 15% were between 36-45, 4% were between 46-55, and 1% were more than 56.

The nationality question revealed that 84% of the participants were of Saudi nationality and 16% were other nationalities. The other nationalities included Egyptian, Sudanese, Iraqi, Syrian, Yemeni, Thais, Palestinian, Emirates, Algerian, Jordanian, American, Omani and British.

All the participants (100%) speak Arabic, 67% of the participants speak English and only 2% speak other languages such as Turkish, French, German, Hindi, Chinese, Italian, Moldovan, Malaysian and Persian.

The participants were different in the level of education. 58% of the participants had a Bachelor degree, 14% had a High School, 14% had a Master degree, 9% had a PhD and 5% had a Diploma.

The participants who had Diploma, Bachelor, Master and PhD have different area of study. 33% of 875 participants who had Diploma, Bachelor, Master and PhD studied Computer Science and Information Technology, 18% studied Education and Teaching, 17% studied other majors, 11% studied Social Sciences, 11% studied Physical and Biological Sciences and 10% studied Health Sciences and Medicine. The other majors included Accounting, Psychology, Library Administration, Islamic Studies, English Language, Mathematics, Marketing Management, Agriculture and Holy Quran studies.

The work status of the participants was 54% of the participants were employees, 45% were students and 1% were self-employees. The participants were from universities, colleges, schools, hospitals, public and private sectors in Saudi Arabia.

The employed participants worked in number of different areas. These areas included the following positions. 49% of 554 participants who were employees worked in Educational positions, 18% worked in Management positions, 16% worked in Technical positions, 11% worked in Medical positions, and 6% worked in other positions. The other employment positions were in academia, administration, banks, transport, research, information systems analysis, engineers and laboratories.

3. RESULTS
This section described the results of the email users’ survey.

3.1. Respondents Definition and Awareness of Email SPAM
Email users were asked for a definition of email SPAM based on their opinions. The responses showed that only 428 of 1,020 participants answered this question.

42% of the participants who answered this question defined email SPAM as an email that was sent randomly to numerous recipients and contained Spyware, files, links, images or text that aims to hack the computer or steal confidential information such as email passwords, credit card numbers and bank account numbers.

39% defined email SPAM as an email that did not contain an email address or that was sent randomly, directly or indirectly by unknown senders or sources to a large number of recipients without their permission to receive it.

33% said that email SPAM was an email that was sent randomly and contained malicious programs such as Viruses, Trojans, Worms, or contained hidden links, strange contents and untrusted attachments that aimed to damage computer, software and hardware, or aimed to delete important information in a computer.

29% defined email SPAM as Unsolicited Commercial Email (UCE) or email that was sent to a large number of recipients and aimed to promote commercial advertisements which contained attractive words that were used to encourage the recipient to buy medical, technical and sexual products.

9% said that email SPAM was annoying and unimportant email that was sent from friends, but it was not sent in person and contained jokes, greetings, invitations to subscribe to forums, invitations for friendship by social networks such as Facebook, competition, puzzles, political and religious reviews, news, and scandals of famous people in the world.

7% defined email SPAM as junk email or as Unwanted, Unsolicited Bulk Email (UBE) that was sent randomly to a large number of recipients.
1% defined email SPAM as an email that was not related to recipients’ work or was not related to their interests.

From the definitions described above, it can be clearly seen that there was no a specific definition for email SPAM by email users and that the most common definition for email SPAM was that “an email that was sent randomly to numerous recipients and contained Spyware, files, links, images or text that aims to hack the computer or steal confidential information such as email passwords, credit card numbers and bank account numbers”. The definitions described above indicated that some definitions of email users in Saudi Arabia for email SPAM agreed with the international definitions for email SPAM by defining email SPAM as Unsolicited Commercial Email (UCE) and as Unsolicited Bulk Email (UBE).

The differences in definition of email SPAM could cause problems in enacting laws to combat SPAM in Saudi Arabia and developing Anti-SPAM filters for different languages such as Arabic. This suggests that there is a scope to specify an agreed definition for email SPAM which could be used for enacting laws to combat SPAM and developing Anti-SPAM techniques in Saudi Arabia.

When the participants were asked if they knew about email SPAM prior to reading the survey, the results revealed that 62% of the participants knew about email SPAM prior to reading the survey while 38% did not know about it.

The results of the survey revealed that only 62% of the participants indicated prior awareness of SPAM, suggesting that the survey itself has acted as a means of educating the participants about SPAM and its impact. This suggests that a broader survey or information campaign about SPAM would have a further positive impact in Saudi Arabia. Also, this suggests that conducting research related to SPAM and funding researchers who work in the field of SPAM could help in increasing the awareness of email users about email SPAM and hence reducing the impact of email SPAM in Saudi Arabia.

When the participants were asked about the source of their knowledge about email SPAM, the results revealed that email users were informed about email SPAM by different sources. These sources can be seen in Figure 5.

As seen in Figure 5, the results indicated that most email users in Saudi Arabia had knowledge about SPAM by self-educating through researching and reading about email SPAM in the internet and forums, and through asking and discussing with friends and relatives about SPAM. Also, the results indicated a deficiency of efforts by government ministries and commissions, ISPs and broadcast media such as newspapers and magazines in informing email users about email SPAM. This suggests that these sectors should focus on the awareness of email users about SPAM and should collaborate with each other to publish information about SPAM in different regions in Saudi Arabia.

3.2. Volume and Nature of Email SPAM in Saudi Arabia

When the participants were asked if they received email SPAM, the results showed that 73% of the participants (747 of the 1,020 participants) received email SPAM while 27% did not receive email SPAM. Email users estimated they received an average of 108 SPAM emails per week. Another study, conducted by [17], showed that the participants received an average of 94.5 emails SPAM per week. By comparing the volume of email SPAM received in Saudi Arabia to the volume of email SPAM in that study [17], it can be clearly seen that the volume of email SPAM in Saudi Arabia was broadly similar to the volume in that study.

When the participants were asked about the language of email SPAM that they received, the results, as shown in Figure 6, showed that most email SPAM received by email users (59%) was in English, 34% was in Arabic, 4% was not recognized and 3% was in other languages such as Chinese, Japanese, Russian, Turkish, French, Brazilian, Spanish, Persian, German, Italian, Hindi, Urdu and Hebrew. The percentages
indicated that most email SPAM received in Saudi Arabia was written in English.

A study conducted in Bahrain indicated that 64% of the respondents said that they received English SPAM, 18% said that they received Arabic SPAM and 18% said that they received both Arabic and English SPAM [1]. The results of this study indicated that the volume of English SPAM received in Bahrain was similar to the volume of English SPAM that received in Saudi Arabia. The results of the study also revealed that the volume of Arabic SPAM received in Bahrain was less than that received in Saudi Arabia.

![Figure 6: Language of email SPAM received by email users in Saudi Arabia](image)

When the participants were asked about the types of Arabic and English emails SPAM that they received, the results showed that there were many types for both Arabic and English email SPAM and these types were different from Arabic to English SPAM. Types of Arabic and English SPAM and the differences between them can be seen in Table 1.

<table>
<thead>
<tr>
<th>Types of email SPAM</th>
<th>AR (%)</th>
<th>EN (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>31</td>
<td>30</td>
</tr>
<tr>
<td>Religious and Political Party</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Pornographic</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>Forums</td>
<td>36</td>
<td>3</td>
</tr>
<tr>
<td>Products and services</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Phishing and Fraud</td>
<td>6</td>
<td>28</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

As described in Table 1, it can be clearly seen that the volume of business advertisements, emails from religious and political parties, and emails related to forums was larger in Arabic SPAM than English SPAM. The percentages indicated that there was a significant difference in composition between Arabic and English SPAM, for example in the volume of forum emails where this volume was much more in Arabic SPAM than English SPAM.

Also, the results showed that the volume of pornographic emails, products and services emails, and phishing and fraud emails was larger in English SPAM than Arabic SPAM. The percentages indicated that there was a significant difference between Arabic and English email SPAM in the volume of pornographic and phishing and fraud emails where this volume was much more in English SPAM than Arabic SPAM.

The results revealed other types of Arabic SPAM that did not exist in English SPAM. These types included news, training consultation, jokes, scandals of famous people, puzzles, greetings, competition, and invitations by social networks websites such as Facebook.

A study conducted by the Communication and Information Technology Commission (CITC) in Saudi Arabia in 2007 showed that 64% of email SPAM received in Saudi Arabia were direct marketing, 25% were sexual emails, 5% were religious emails, and 5% was other types [20]. However, this study did not specify if the email SPAM received was written in Arabic or English. The results of the CITC study indicated that the volume of religious emails, pornographic emails and other types of email SPAM was similar to the volume of the same types in this study.

The results, seen in Table 1, showed that the volume of pornographic emails for both Arabic and English email SPAM was lower compared to the same type in other countries such as Bahrain. The results of a study conducted in Bahrain by [1] revealed that 76% of the participants received pornographic emails while 24% did not receive pornographic emails. The results of this study did not specify if the volume of pornographic emails was larger in English or Arabic. Therefore, the results of this study indicated that the volume of pornographic emails in Saudi Arabia was lower and this could be because the access to pornographic websites is not allowed for public in Saudi Arabia and this could be contributed in reducing the volume of SPAM email that sent from pornographic websites.

A study conducted by [3] described some keywords and phrases used in Arabic and English email SPAM in Saudi Arabia. These keywords and phrases were collected from different ISPs in Saudi Arabia.

Examples of Arabic SPAM keywords and phrases are as follows: "ادوية" (pharmacy), "ألعاب" (games), "فوارق" (diversities), "مسابقة" (competition), "فرصة للربح" (winning chance), "ريجيم" (dietary).
When the participants were asked about how long they have been using their emails, the results showed that 45% of the participants said that they have been using their emails between 4-6 years, 28% between 7-9 years, 13% between 1-3 years, 11% between 10-12 years and 3% of the participants for more than 12 years.

The results revealed that 88% of email users who used email for more than 12 years were aware of email SPAM prior to reading the survey of this research, 85% of the users who used email between 10-12 years were aware of email SPAM prior to reading the survey, 71% of the users who used email between 7-9 years were aware of email SPAM prior to reading the survey, 52% of the users who used email between 4-6 years were aware of email SPAM prior to reading the survey and 48% of the users who used email between 1-3 years were aware of email SPAM prior to reading the survey. This indicated that email users who used email for long time were more aware of email SPAM than users who used email for short time. This suggests that email users who had a short experience in using email should inform about email SPAM and its impacts and this could help in reducing the effects of email SPAM in Saudi Arabia.

3.3. Actions of Email Users in Dealing with SPAM

The participants were asked about the appropriate action for dealing with email SPAM. In the survey, the participants were given three actions for their dealing with SPAM. These actions were as follows. The first action was that reading the entire email SPAM. The second action was that deleting the email SPAM without reading it. The third action was that contacting with the ISP and notifying it about email SPAM. To answer this question, the participants were asked to evaluate their actions in dealing with SPAM by choosing one of the following options for each action. The options for each action were as follows: never, sometimes and always.

When the participants were asked about their evaluation for the first action of dealing with SPAM, the results showed that 56% of the participants said that they sometimes read the entire email SPAM, 35% said that they never read the entire email SPAM and 9% said that they always read the entire email SPAM (See Figure 7). The responses indicated that only 35% of the participants did not read the entire email SPAM. This suggests that email users should inform about SPAM, its impacts, and the safe ways in dealing with it. Examples of safe ways in dealing with SPAM included awareness of users not to open strange or untrusted emails. This could reduce the impacts of SPAM on email users.
When the participants were asked about their evaluation for the second action of dealing with SPAM, the results showed that 54% of the participants said that they sometimes delete the email SPAM without reading it, 38% said that they always delete the email SPAM without reading it and 8% said that they never delete the email SPAM without reading it (See Figure 8). The responses indicated that a few of the participants did not delete email SPAM without reading it. This suggests that email users should inform about SPAM, its impacts and the safe ways to combat it. Examples of the safe ways in dealing with SPAM included awareness of users to delete SPAM before reading it. This could reduce the impacts of SPAM on email users.

When the participants were asked about their evaluation for the third action of dealing with SPAM, the results showed that 81% of the participants said that they never contact with ISP and notify it about email SPAM, 14% said that they sometimes contact with ISP and notify it about email SPAM and 5% said that they always contact with ISP and notify it about email SPAM (See Figure 9).

When the participants were asked if they purposely responded to an offer made by a SPAM email, the results showed that 21% of the participants responded to offers made by SPAM emails while 79% did not respond to offers made by emails SPAM (See Figure 10).

The participants who responded to offers made by emails SPAM were asked about the benefits that they derived from SPAM emails. The results revealed that 60% of the participants said that they enjoyed fun emails involved in email SPAM, 43% said that they learnt by email SPAM, 18% said that they purchased and sold by email SPAM, and 1% said that they got other benefits from email SPAM such as friendship (See Figure 11).

The results indicated that as long as some users responded to some offers of SPAM, email SPAM could be increased and caused problems for other users unless those users combat it. This suggests that laws against SPAM in Saudi Arabia could reduce the incidence of SPAM by greatly reducing the ability of spammers to make sales without fear of penalties.
3.4. Effects of Email SPAM on End Users

When the participants were asked if they affected negatively by email SPAM, the results showed that 45% of the participants said that they affected negatively by email SPAM while 55% said that they did not affect negatively by email SPAM (See Figure 12).

The participants who affected negatively by email SPAM were asked about the impacts of email SPAM on them. The results revealed that 62% said that email inbox was filled with SPAM, 54% said that computer was infected by a Virus, Worm and other malicious programs, 43% said that email SPAM lost the time and reduced the productivity, 20% said that personal information such as user name, passwords and credit card numbers were stolen by email SPAM, 19% said that they felt less confidence in using email and 3% said that email SPAM caused other impacts. The other impacts included annoying, bothering, and tension and nervousness upon searching for important emails in the inbox (See Figure 13).

3.5. Awareness of Anti-SPAM Filters and the Effectiveness of Anti-SPAM Filters in Detecting Arabic and English SPAM

When the participants were asked if they were aware of Anti-SPAM software, the results revealed that only 38% of the participants were aware of Anti-SPAM software while 62% were not aware of Anti-SPAM software (See Figure 14). The results indicated that most email users were not aware of Anti-SPAM programs and this suggests that there should be a focus on the awareness of email users about Anti-SPAM programs and how Anti-SPAM programs work. This awareness could be done by the government and the private sectors in Saudi Arabia.

A study conducted in Bahrain [1] revealed that 26% of the participants knew about Anti-SPAM software while 74% did not know about Anti-SPAM software. By comparing the results of Bahraini study to the results of this study, it can be clearly seen that Saudi society was more aware of Anti-SPAM software than Bahraini society, but still most Saudi society were not aware.

The results showed that 71% of email users who used email for more than 12 years were aware of Anti-SPAM filters, 53% of the users who used email between 10-12 years were aware of Anti-SPAM filters, 49% of the users who used email between 7-9 years were aware of Anti-SPAM filters, 30% of the users who used email between 4-6 years were aware of Anti-SPAM filters, 30% of the users who used email between 7-9 years were aware of Anti-SPAM filters, 30% of the users who used email between 1-3 years were aware of Anti-SPAM filters. This indicated that email users who used email for long time were more aware of Anti-SPAM filters than users who used email for short time. This suggests that the users who had a short experience in using email should inform about Anti-SPAM filters and how these filters work to detect SPAM.
When the participants were asked about the source of their knowledge about Anti-SPAM programs, the results revealed that email users were informed about Anti-SPAM programs by different sources. These sources can be seen in Figure 15.

As seen in Figure 15, it can be clearly seen that most sources of knowledge about Anti-SPAM programs were from the internet and forums, school and university education, and friends and relatives. This indicated that most users had knowledge about Anti-SPAM programs by self-educating such as searching on the internet about SPAM, learning about SPAM in school and university, and discussing with friends about SPAM. The results also indicated that the deficiency of broadcast media, government and ISPs in awareness of users about Anti-SPAM programs. This suggests that the different government and private sectors in Saudi Arabia could be collaborated in the awareness of people about SPAM, its impacts, the appropriate ways to combat it, and providing necessary technical assistance when email users needed it.

When the participants who were aware of Anti-SPAM software were asked to rate the effectiveness of Anti-SPAM software in detecting Arabic and English email SPAM, the results, as seen in Figure 16, revealed that the effectiveness of Anti-SPAM software was 59% in detecting Arabic SPAM and 80% in detecting English SPAM.

As seen in Figure 16 above, the percentages indicated that the Anti-SPAM software were not completely effective in detecting English and Arabic email SPAM. This suggests that the existing Anti-SPAM filters need to be developed to detect SPAM in different languages such as Arabic and English. The percentages also indicated that Anti-SPAM software were more effective in detecting English email SPAM than Arabic email SPAM. This suggests that there should be a focus on producing and developing techniques to detect email SPAM in Arabic language.

3.6. Efforts of Government and ISPs to combat SPAM

When the participants were asked if they were aware of efforts by the government in Saudi Arabia to combat SPAM, the results revealed that only 24% were aware of government efforts to combat SPAM while 76% were not aware of these efforts.

The participants who were aware of government efforts to combat SPAM were asked about these efforts that they were aware of. Most of the participants (62%) said that the government efforts could be observed by King Abdulaziz City for Science and Technology (KACST). They said that KACST blocks unsecured websites and websites that send SPAM, informs people about dangerous security attacks and their impacts, and conducts and fund researches related to information technology [19].

24% of the participants said that the government recommended that each government sector and private sector in Saudi Arabia should apply security policy in the organization. The policy should include: providing the organization with
software and hardware that are necessary to avoid security attacks such as Viruses and SPAM, awareness of employees and customers about security attacks and methods of combating them, conducting researches related to security attacks and countermeasures for these attacks, conducting training and workshops related to security issues for employees, employment of qualified people in the field of networks security in the organization to deal with security attacks, providing financial budget to develop the work of security policy and reviewing the security policy regularly to find out the strengths and weaknesses of the work of security policy.

22% said that the government established and funded centres to deal with information security issues. Examples for these centres are Centre of Excellence in Information Assurance (COEIA) [8], Computer Emergency Response Team (CERT) [10] and Prince Muqrin Chair for Information Security Technologies (PMC IT SECURITY) [23]. They said the aims of these centres were to inform people about security attacks such as Viruses and SPAM and their impacts, conducting and funding researches related to security issues and conducting conferences and workshops regarding security attacks.

19% of the participants said that the government efforts could be observed by Communication and Information Technology Commission (CITC). They said that CITC funded Saudi National Anti-SPAM Program project and created a website for this project that includes information about SPAM, methods of combating it and published it for public on the internet. They also said that this project informed people about SPAM by publishing brochures or by subscription of people in mailing list of CITC to make people look for the new development in SPAM. The participants also said that the project conducted some researches regarding SPAM problems and publish the results of researches for public. They also said that CITC received complaints of people regarding SPAM problems and it processed these problems with the other responsible government sectors [9].

18% said that some universities in Saudi Arabia established centres for information security which provide the following services for people. First of all, information security centres provide awareness of people about security attacks. Second, these centres conducted workshops, conferences and ongoing training in the field of security issues and methods of combating it for people. Third, centres published valued researches in the field of security issues for people and different libraries in Saudi Arabia.

18% of the participants said that the government enacted law for combating electronic crimes in Saudi Arabia and there were no specific laws for SPAM. They said that the government sectors that are responsible to execute the electronic crime law are Communication and Information Technology Commission (CITC) with coordination with other legal sectors.

When the participants were asked if they were aware of efforts by the ISPs in Saudi Arabia, the results showed that only 14% were aware of ISPs efforts to combat SPAM while 86% were not aware of these efforts.

The participants who were aware of ISPs efforts to combat SPAM were asked about these efforts that they were aware of. 42% of the participants said that the ISPs used advanced Anti-SPAM filters to block email SPAM before it reaches end users inboxes.

26% said that the ISPs blocked websites or forums that send email SPAM for recipients and put them in black lists.

13% of the participants said that the ISPs informed people about email SPAM and methods of combating it by email, brochures, and Short Message Service (SMS).

13% said that the ISPs warned customers not to send SPAM, they received customers’ complaints regarding SPAM and they executed some legal actions against people who sent email SPAM such as disconnecting the internet service and cancellation of the contract.

4. CONCLUSION AND FUTURE WORK
This paper presented the results of a survey of email users about email SPAM and how they deal with it in Saudi Arabia.

The results showed that there was no a specific definition for email SPAM and the most common definition for email SPAM was that “an email that was sent randomly to numerous recipients and contained Spyware, files, links, images or text that aimed to hack the computer or steal confidential information such as email passwords, credit card numbers and bank account numbers”.

The results showed that most email users knew about email SPAM prior to reading the survey and the most source of their knowledge about SPAM was the internet and forums. The results revealed that approximately third of email users in Saudi
Arabia did not know about email SPAM and this is a significant and a risk for Saudi society. The results showed that the volume of email SPAM was high in Saudi Arabia compared to other countries. The results revealed that the most of email SPAM received by users in Saudi Arabia was written in English. The results indicated that there were many types for both Arabic and English email SPAM and the most common type of SPAM in Arabic was emails related to forums and in English SPAM was business advertisements.

The results indicated that Yahoo was possible marginally better than Hotmail, Gmail and other providers in classifying email SPAM where the results revealed that the rate of SPAM received by users who used Yahoo was lower compared to other email account providers.

The results revealed that email users who used email for long time were more aware of email SPAM, its impacts and methods of combating it than users who used email for short time.

The results showed that few email users purposely responded to an offer made by a SPAM email and the main benefit that they derived from email SPAM was fun.

The results revealed that approximately half of the participants were affected negatively by email SPAM and the main impact of SPAM was that filling inbox with SPAM.

The results revealed that few email users were aware of Anti-SPAM programs and the most source of their knowledge about Anti-SPAM programs was the internet and forums. The results also revealed that the Anti-SPAM software were not completely effective in detecting English and Arabic email SPAM. The results indicated that Anti-SPAM software were more effective in detecting English email SPAM than Arabic email SPAM.

The results revealed that most email users were not aware of efforts of the government and ISPs to combat SPAM in Saudi Arabia.

Future work could include investigating government efforts to combat SPAM to find more effective methods to combat SPAM.

Laws to combat SPAM in Saudi Arabia could be investigated. This could be achieved by taking the experiences of developed countries to combat SPAM. This could help in enacting a new clear law to combat SPAM in Saudi Arabia.

The legal and technical efforts of ISPs in Saudi Arabia to combat email SPAM, and ways to encourage ISPs to collaborate with each other ISPs, private sectors, government sectors and customers could be investigated.

Effective awareness programs to inform private sectors and government sectors about SPAM, its effects and methods of combating it could be investigated.

Improving the performance of existing Anti-SPAM filters in detecting Arabic and English email SPAM could be investigated. This could be achieved by testing the effectiveness of existing Anti-SPAM filters in detecting Arabic and English SPAM email and this could help in creating and developing effective filters to detect new types of Arabic and English SPAM.

A listing of keywords and phrases used in Arabic email SPAM were involved in this research and this could help in designing and producing special Anti-SPAM filters for Arabic SPAM.

5. REFERENCES

5. Australian Communications & Media Authority (ACMA), http://www.efa.org.au/Issues/Privacy/spam.html#acts
23. [23] Prince Muqrin Chair for Information Security Technologies (PMC IT SECURITY), http://pmc.ksu.edu.sa/AboutPMC.aspx