Abstract — This paper presents the key findings of surveys of email users, businesses, and ISPs in Saudi Arabia. The surveys were to investigate the nature of email SPAM in Saudi Arabia, its effects, methods and efforts taken to combat it. They also aimed to investigate the Anti-SPAM filters used to combat email SPAM, and their effectiveness in detecting Arabic versus English email SPAM.

In all, 1,500 email users, 300 businesses, and 27 ISPs were surveyed, and completed surveys were collected from 1,020 email users, 92 businesses, and 11 ISPs.

The results indicated that there was no single definition of what constitutes email SPAM in Saudi Arabia, and definitions of respondents differed among groups of participants. The results showed that the volume of email SPAM was high in Saudi Arabia compared to other countries; and most email SPAM was written in English. The percentages revealed that the most common type of email SPAM for both Arabic and English was business advertisements. The percentages also revealed that most Arabic email SPAM was sent from Saudi Arabia and other Arabic countries; while most English email SPAM was sent from non-Arabic countries.

The results have shown that most email users were not aware of SPAM and the appropriate ways to combat it. The results showed that email SPAM caused many effects, and most participants were affected by SPAM through the unwanted filling of their email inboxes with SPAM.

The results showed that while many efforts and methods were conducted by government, ISPs and businesses to combat SPAM; most of the email users and businesses were not aware of these efforts.

The results revealed that many types of Anti-SPAM filters were used to combat email SPAM, and these filters were not 100% effective. The results indicated that these filters were more effective in detecting English email SPAM than Arabic email SPAM, suggesting the need to develop Arabic-specific SPAM detection technologies.

Keywords — SPAM, Email, Arabic, English, Users, Businesses, ISPs, Saudi.

I. INTRODUCTION

Email is a significant service for communication, and is the most common use of the Internet today. One of the issues related to using email is SPAM.

Email SPAM has been defined as Unsolicited Bulk Email (UBE) [3, 24, 32, 42]. It has also been defined as Unsolicited Commercial Email (UCE) [5, 37]. Email SPAM has many effects on email users, businesses, and ISPs such as reducing productivity [28, 40, 42], consumption of Internet resources [3, 10, 42], and infection of computers and systems by malicious programs such as Viruses and Trojans [16, 17, 33]. Many efforts and solutions are used to reduce the volume of email SPAM and its effects. These efforts can be broadly categorized into legal and technical measures. Laws were enacted by some countries such as the USA [9, 28, 36], EU States [23, 28, 30], and Australia [4, 9, 31] to combat SPAM. The technical efforts included producing Anti-SPAM filters to block SPAM. Some of these filters depend on email content, and some depend on email origin [15, 19].

The main aim of this research was to answer the following questions:

1. What was the definition of email SPAM based on opinions of email users, businesses, and ISPs in Saudi Arabia?
2. Was there a significant volume of email SPAM in Saudi Arabia?
3. What were the proportions of common languages of email SPAM in Saudi Arabia?
4. What were the types of Arabic and English email SPAM in Saudi Arabia?
5. What were the sources or origins of Arabic and English email SPAM in Saudi Arabia?
6. What were the keywords and phrases, if any, did respondents of English and Arabic email SPAM think might be worth targeting with a new SPAM filter?
7. How was Saudi society informed about SPAM, and methods of combating it?

This question was divided to the following sub-questions:

a. Was Saudi society aware of email SPAM and methods of combating it prior to reading the study survey?
b. What were the sources of knowledge in Saudi society about email SPAM, and the methods for combating it, (if they were aware of it)?
8. How did email users deal with SPAM in Saudi Arabia?
9. What were the effects of SPAM on email users, businesses, and ISPs in Saudi Arabia?
10. What were government, ISPs, and businesses efforts to combat SPAM in Saudi Arabia?
II. METHODOLOGY

It was decided that the best way to answer the research questions was through surveys. There were three different surveys: one each for email users, businesses and ISPs. The surveys covered the research questions and were distributed to email users, ISPs and businesses. The responses were analyzed.

Initially pilot surveys were prepared and distributed to a small sample of email users, ISPs, and businesses to get their comments about the questions. Then email users completed a 10 page survey, ISPs completed a 12 page survey, and businesses completed a 9 page survey. The surveys included both yes/no questions and open ended questions.

A. Aims of the Surveys

This section describes the primary aims of the email users, businesses, and ISPs surveys, and how the research aimed to achieve them.

Aims of the Email User Survey: The aim of the email user survey was to investigate the perceptions of email users about SPAM, and how they deal with it. It also aimed to investigate the effects of SPAM on email users, and the efforts to combat it in Saudi Arabia.

Aims of the ISP Survey: The ISP survey aimed to investigate the nature of email SPAM in Saudi Arabia, the efforts of the ISPs to combat it, and its effects on the ISPs. It also investigated the Anti-SPAM filters used by the ISPs to combat email SPAM, and their effectiveness in detecting Arabic and English email SPAM.

Aims of the Business Survey: The business survey goal was to investigate the nature of email SPAM, and how businesses dealt with it. It also investigated the effects of email SPAM on businesses, and the efforts to combat it in Saudi Arabia.

B. Questions of the Surveys

The questions in the surveys were designed to obtain information from the participants to cover all the research questions. Some of the survey questions were common for all three groups of participants, common between just two of them), or specific a particular survey.

The questions in the surveys were in three parts. The first part asked the participants for general information. The second part asked the participants about the nature of email SPAM, its effects, and their dealing with it. The third part asked the participants about efforts to combat SPAM in Saudi Arabia. These three parts were common for all surveys. Each part had some common questions for the three groups, and some specific questions for each group.

The ISPs survey had a fourth part, questions that were technical in nature. In this part, the ISPs were asked about the Anti-SPAM filters that they used to combat email SPAM, and their effectiveness in detecting Arabic and English SPAM.

Common Questions: This section describes the questions common to the email user, business and ISP surveys, and those which are common between two of them.

1. Common Questions for the Three Groups (Email Users, Businesses, ISPs):

There were no common questions in the first part of the surveys. There were only common questions between business and ISP surveys. The common questions between businesses and ISPs are presented in the next sections.

In the second part email users, businesses, and ISPs were asked about the nature of email SPAM, its effects, and their dealing with it, there were many common questions for all three groups as described below.

At the beginning of the second part, all three groups 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 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 to prevent introducing a strong bias.

All three groups of the participants were asked about the volume of email SPAM received by users and businesses, and blocked by ISPs on an average in a week. This question provided an understanding about the volume of email SPAM in Saudi Arabia. This also helped in making a comparison between this volume, and the volume of email SPAM in other countries in the world.

In addition, all three groups of participants were asked about the language of email SPAM received in Saudi Arabia. This helped in understanding the languages in which email SPAM is being written.
The three groups of participants were asked about the types of Arabic and English email SPAM received or blocked in Saudi Arabia. This gave an understanding about types of email SPAM, and any similarities or differences between Arabic and English email SPAM. This also helped in making a comparison between types of email SPAM in Saudi Arabia, and comparative types in other countries. The reason for the investigation of Arabic and English email SPAM was because Arabic is the native and official language in Saudi Arabia [8, 21], and English is the most used language in the world [2, 25, 29, 34].

The three groups of participants were asked about the effects of email SPAM. This helped in an assessment of the effects of email SPAM on email users, businesses, and ISPs in Saudi Arabia.

In the third part, which asked the participants about the efforts made to combat email SPAM in Saudi Arabia, all three groups were asked about the efforts of government and ISPs to combat email SPAM. These questions provided an understanding of the efforts of the government and ISPs in combating email SPAM, and the citizens and residents of Saudi Arabia perceived these efforts.

At the end of each survey, all three groups of participants were asked to provide their opinions about appropriate technical, legal and other ways to combat email SPAM in Saudi Arabia. These questions helped in providing some potentially useful suggestions to combat email SPAM.

The three groups of participants were asked to add anything that they think may be of value to this research. This question provided the research with further perspectives of the experiences of email users, businesses, and ISPs in combating SPAM.

2. Common Questions in the Email Users and Businesses Surveys:

This section presents and discusses common questions in the email user and business surveys.

There were no common questions between the email users and businesses surveys in the first part of the surveys. In the second part of the surveys, there were common questions. These questions are described below:

Email users and businesses were asked if they knew about email SPAM, and methods of combating it prior to reading the surveys. The question was to investigate their awareness of email SPAM and methods of combating it.

Email users and businesses were also asked about the source of their knowledge about email SPAM and the methods of combating it in Saudi Arabia. This question was to investigate the efforts of the government, private and public sectors in providing information about email SPAM, and the provision of information about appropriate ways to combat it.

Email users and businesses were asked about when the last time was that they received SPAM. This question gave an understanding of whether email users and businesses received SPAM continuously or intermittently. This provided insight into how to reduce the volume of email SPAM received by email users and businesses.

In addition, email users and businesses were asked to rate the effectiveness of the existing Anti-SPAM filters in detecting Arabic and English email SPAM. This question helped in understanding the effectiveness of the existing Anti-SPAM filters in detecting Arabic and English SPAM, and in comparing the effectiveness of filters in detecting Arabic and English SPAM. This could thus lead to proposals to develop more effective filters to detect Arabic and English SPAM.

In the third part of the surveys, email users and businesses were asked if they were aware of efforts by the government and ISPs to combat SPAM. These questions gave an understanding about the awareness of email users and businesses regarding the efforts the government and ISPs to combat SPAM in Saudi Arabia.

3. Common Questions in the Businesses and ISPs Surveys:

This section describes and discusses the common questions in the businesses and ISPs surveys.

In the first part of the surveys, which asked businesses and ISPs for general information, there were common questions in the surveys. These questions are described below.

Businesses and ISPs were asked about the year of establishment of their organization. This question allowed of the classification of the organization into old and new, and thus a comparison of the results based on the organization age.

Businesses and ISPs were asked about the organization size to compare the results of the study based on the organization size.

Businesses and ISPs were asked about the number of employees in the organization. This question allowed for the classification of the organization size into small, medium and large, allowing for the comparison of the results based on the organization size.

Businesses and ISPs were asked about the number of customers that the organization deals with, to investigate the volume of SPAM received by businesses, or that were blocked by ISPs based on the number of customers.

In addition, businesses and ISPs were asked if they had special units or teams to manage network security, what were the responsibilities of these units or teams, and how many employees were involved in these units or teams. These three questions assisted in investigating the efforts of businesses and ISPs in combating network security threats in Saudi Arabia.
Moreover, businesses and ISPs were asked if they had employee positions to combat email SPAM, and (if so), what were their tasks. Answers of these two questions provided insight into the efforts of businesses and ISPs in combating email SPAM in Saudi Arabia.

There were no common questions between the businesses and ISPs surveys in the second part of the surveys.

In the third part of the surveys, businesses and ISPs were asked if they provided awareness programs for their customers and employees about email SPAM and the appropriate methods to combat it. This question provided an understanding of the efforts of businesses and ISPs in ensuring the awareness of their customers and employees about email SPAM, and the appropriate ways to combat it.

Specific Questions: The previous section described and discussed the common questions for all three surveys, and those that are common between two of them. This section presents and discusses the specific questions for each survey. Questions specific to email users, businesses, and ISPs surveys are described below:

1. Email Users Survey:

   The email users' survey had many specific questions. In the first part of the survey, users were asked for the following information: their gender, their age, their nationality, their education level, their study area if they had a tertiary qualification (Diploma, Bachelor, Master, and PhD), their work status, and the nature of work as employees. These questions helped in comparing the results of perceptions of email users about SPAM, their methods of combating SPAM, and how they deal with it, based on the aforementioned factors.

   Email users were asked about the language that they speak. This question helped in the analysis of results of how email users deal with the various types of Arabic and English SPAM.

   In the second part, email users were asked about the principal email account providers that they used. This was to investigate the volume of email SPAM received by users who used different email account providers, and to investigate the effectiveness of Anti-SPAM filters used by these various email account providers in detecting Arabic and English email SPAM.

   Email users were asked how long they have had their email account, to investigate the experience of users in using email. This helped in understanding the awareness of users who have used email for a long or a short and how they dealt with email SPAM, including their awareness about using Anti-SPAM filters.

   Email users were asked about what they did when they received email SPAM. This question helped in investigating the actions taken by email users against SPAM in Saudi Arabia.

   Also, email users were asked if they have responded purposely to some offers made by email SPAM and what were the benefits they derived from email SPAM to investigate if email users interacted with SPAM, and to investigate purposes of their interaction with it.

   There were no specific questions for email users in the third part of the survey.

2. ISPs Survey:

   The ISP survey had several specific questions. In the first part, the ISPs were asked if there were workshops, conferences, or other ongoing training conducted for employees of their organization about email SPAM and the control of it, and (if so), when they were conducted. These two questions were to investigate the efforts of the ISPs to educate employees regularly about SPAM, and the methods of combating it.

   In the second part, the ISPs were asked about the sources of Arabic and English email SPAM that they blocked to find out the sources of Arabic and English email SPAM received in Saudi Arabia. This helped in comparing sources of Arabic email SPAM to English email SPAM and improving origin based filters.

   The ISPs were asked about the keywords or phrases used in Arabic and English email SPAM. The answers to this question helped in comparing the keywords and phrases used in Arabic SPAM to those used in English SPAM. This could lead to the development of improved filters to detect new types of Arabic and English email SPAM.

   The ISPs were also asked about the time they spent in fixing problems related to email SPAM which affects the ISPs productivity.

   In the third part of the survey, the ISPs were asked about the techniques that they used in their filters to detect email SPAM. This question was to investigate the types of Anti-SPAM filters used by the ISPs to block email SPAM in Saudi Arabia.

   The ISPs were asked about the types of content and origin based filters that they used to block email SPAM in Saudi Arabia.

   The ISPs also were asked about the effectiveness of the content and origin based filters in detecting Arabic and English email SPAM. This helped in comparing the effectiveness of the content filters to the effectiveness of origin based filters in detecting Arabic and English SPAM.

   In addition, the ISPs were asked if they updated their Anti-SPAM filters regularly to block new types of email SPAM.

3. Businesses Survey:

   There were some specific questions for the business survey. In the first part of the survey, businesses were asked about the nature of their company activities.
This question helped in comparing the results based on the activity of the company.

There were no specific questions for businesses in the second and third parts of the survey.

C. Participants in the Surveys

There were three groups of participants for the surveys used in this research. The participants were email users, businesses, and ISPs. Details about the three groups of participants are presented below.

Participants in the Email User Survey: The survey was designed and distributed to 1,500 participants in the Central, Eastern, Western, Southern and Northern regions of Saudi Arabia. The participants were from universities, colleges, schools, hospitals, public, and private sectors in Saudi Arabia. Incomplete surveys were discarded and were not considered in this research. Completed surveys were received from 1,020 participants. The participants varied in gender, age, nationality, speaking language, education level, study area, work status, and work nature. People who did not use computers, and thus did not use email, were not considered in the survey because they may give unfair responses.

Participants in the ISP Survey: There were 51 ISPs licensed by the Communication and Information Technology Commission (CITC) to provide Internet Service in Saudi Arabia [13]. 24 of the 51 ISPs changed their activity from providing Internet Service to other activities, while 27 still provide Internet Service. The 27 ISPs were located in different regions of Saudi Arabia. All these 27 ISPs were surveyed for this research. Completed surveys were collected from 11 ISPs. Responses from the other 16 were not received because they were not enthusiastic to participate in this survey. The 11 ISPs that participated in this study varied in the size and age.

Participants in the Business Survey: The survey was designed and distributed to 300 different businesses in the Central, Eastern, Western, Southern and Northern regions of Saudi Arabia. Incomplete surveys were discarded and were not considered in this research. Completed surveys were received from 92 businesses that were located in the Central, Eastern and Western regions of Saudi Arabia. No completed surveys were received from businesses in the Southern and Northern regions. Businesses in these regions requested that the survey be conduct at their head offices which were located in the Central, Eastern and Western regions of Saudi Arabia. These regions are the largest regions by area and population in Saudi Arabia [6, 38]. The participants varied in size, company activity, and age.

III. RESULTS

This section describes and discusses the main findings that were revealed by the survey responses of the three groups of participants (email users, businesses, and ISPs).

D. The Definition of Email SPAM

The results revealed a wide variety of definitions of email SPAM in Saudi Arabia.

The definition of users for email SPAM was different from user to user. The most common definition of users for email SPAM (42%) was: “an email that was sent randomly to numerous recipients, and contains Spyware, files, links, images or text that aims to hack the computer or to steal confidential information such as email passwords, and credit card numbers”.

The definition of email SPAM by businesses was different from business to business. The most common definition of businesses for email SPAM (49%) was: “Junk email, or Unsolicited, Bulk Email (UBE) that was sent indiscriminately to numerous recipients in a short time”.

The definition of the ISPs for email SPAM was different from ISP to ISP. The most common definition of ISPs for email SPAM (45%) was: “Unwanted, Unsolicited, and Bulk Email (UBE) that was sent from commercial advertisers”.

From the definitions of email users, businesses, and ISPs, it can be clearly seen that there was no specific definition for email SPAM in Saudi Arabia, and the definition was different from one group of the participants to another. The difference in definition of email SPAM could cause problems in enacting laws to combat SPAM, and in developing Anti-SPAM filters for detecting SPAM in different languages such as Arabic. The results indicated that some definitions by the participants for email SPAM agreed with two of the most commonly accepted international definitions of email SPAM as Unsolicited Commercial Email (UCE), and as Unsolicited Bulk Email (UBE).

E. The Volume of Email SPAM

The results indicated that the volume of email SPAM was varied in Saudi Arabia. The results revealed that email users estimated they received an average of 108 SPAM emails weekly. A study conducted by CNNIC in 2004 revealed that the average number of email SPAM received by every user in China was 7.9 weekly [11]. Another study conducted by [18] showed that the average number of email SPAM received in China was 19.33 SPAM weekly. By comparing the results of this study to results of other studies, it can be seen that the average number of email SPAM received by users in Saudi Arabia was larger than that received by users in China.
Please note that the years in which the studies were conducted affected the comparison of the results. No more recent studies could be found for comparison purposes.

Businesses estimated receiving a weekly average of 4,200 SPAM emails on average.

ISPs estimated receiving a weekly average of 1,400,000 SPAM emails.

Many recent studies and reports such as [27, 39, 41] have discussed the volume of email SPAM in Saudi Arabia. These studies and reports revealed that the volume of email SPAM in Saudi Arabia was high compared to other countries both regionally and internationally.

From the results shown above, it can be seen that the volume of email SPAM in Saudi Arabia was high compared to other countries.

F. The Languages of Email SPAM

The results indicated that email SPAM received by users and businesses, and blocked by the ISPs in Saudi Arabia was written in a number of different languages (See Table I).

<table>
<thead>
<tr>
<th>Language of SPAM</th>
<th>Users (%)</th>
<th>Businesses (%)</th>
<th>ISPs (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>59</td>
<td>66</td>
<td>59</td>
</tr>
<tr>
<td>Arabic</td>
<td>34</td>
<td>21</td>
<td>24</td>
</tr>
<tr>
<td>Not Recognized</td>
<td>4</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Other Language</td>
<td>3</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

From the results shown in Table I, it can be clearly seen that the largest percentage of email SPAM in Saudi Arabia was written in English. This agrees with another study conducted in Bahrain by [1] which also showed that the largest percentage of email SPAM received in Bahrain was written in English.

G. The Types of Arabic and English Email SPAM

The results indicated that there were many types of Arabic and English email SPAM received in Saudi Arabia. The volume of each type was different in Arabic to English, and also was different from one surveyed group to another.

The results indicated that there were differences between Arabic and English SPAM in the percentage of types of email SPAM. The results, as seen in Table II, revealed that the percentage of business advertisements, religious and political emails, and emails related to forums was larger in Arabic than English.

The possible reason for the percentages of emails related to forums, and religious and political emails being higher in Arabic than in English is that all participants (100%) speak Arabic which help them to subscribe to Arabic forums, religious and political groups. This may add their addresses on mailing lists of forums, religious and political groups which could result in receiving more Arabic SPAM of this type than English SPAM.

On the other hand, the results revealed that the percentage of pornographic emails, phishing and fraud emails, and products and services emails was larger in English than Arabic.

The reason for the percentage of pornographic email being lower in Arabic than the percentage in English could be because pornographic email conflicts with the Arabic culture which forbids this content of emails.

The reason for the lack of phishing and fraud email in Arabic could be because organised criminal elements behind most email phishing and fraud attempts are not yet operating or established in Arabic speaking countries to the same extent as elsewhere.

The results indicated that all types of English email SPAM occurred in Arabic email SPAM; while there were some types of Arabic email SPAM that respondents did not observe in English email SPAM. These types included news, fun, greetings, donation, marriage advertisements, subscription to forums, and scandals about famous people such as actors and singers.

In Table II, it can be seen that the most common type of Arabic and English email SPAM received by email users, businesses, and blocked by ISPs in Saudi Arabia was businesses advertisements.

H. The Sources (Origins) of Arabic and English Email SPAM

The results indicated that Arabic and English email SPAM received by email users and businesses, and blocked by the ISPs in Saudi Arabia were sent from different sources.
Most of the Arabic email SPAM was sent from Saudi Arabia, and other Arabic countries; while little of the Arabic email SPAM was sent from non-Arabic countries, and unknown sources. Most of the English email SPAM was sent from non-Arabic countries; while little of the English email SPAM was sent from Saudi Arabia, other Arabic countries, and unknown sources.

I. The Keywords and Phrases Used in Arabic and English Email SPAM

The results identified some keywords and phrases used in Arabic and English email SPAM which could help in producing effective Anti-SPAM filters for Arabic and English email SPAM.

The results indicated that there were keywords and phrases common to both Arabic and English SPAM. Examples of common keywords and phrases used in both Arabic and English email SPAM were as follows: “مبارك”, “Congratulations you won”, “Viagra”, “training”, “viagra”, and “Gift”.

The results indicated that there were specific keywords and phrases for each language. Examples of specific keywords and phrases used in Arabic email SPAM included “مبارك”, “Congratulations you won”, “Viagra”, “training”, “viagra”, and “Gift”. The English translations for the previous Arabic keywords are: “MARRIAGE”, “DONATIONS”, “SUBSCRIBE TO FORUMS”, and “REVOLUTION”.

Examples of the specific keywords and phrases used in English email SPAM involved “cialis”, “INCOMPLETE PERSONAL INFORMATION”, “LOTTERY”, and “SUSD”.

The results indicated that the keywords and phrases used in Arabic email SPAM focused on the religious and political issues, training and education consultation, and subscription to forums. The keywords and phrases used in English email SPAM focused on the pornographic materials, investments, credit cards, bank loans, phishing and fraud, and medical products such as Viagra.

J. The Awareness of Users and Businesses about Email SPAM and Methods of Combating it

The results found that the awareness of users about email SPAM and Anti-SPAM filters was different from one group of email users to another depending on factors such as their experience in using email, the nature of their work, and their area of study. The results revealed that over half of the users knew about email SPAM prior to reading the survey, while about one third of users were aware of the Anti-SPAM filters.

The results indicated that the awareness of businesses about email SPAM and Anti-SPAM filters was different from one group of business to another depending on factors such as the business size, business age and business activity.

The results indicated that most businesses knew about email SPAM and Anti-SPAM filters prior to reading the survey.

As seen above, many Saudis are still not aware of email SPAM, and effective ways to combat it. The results have shown that parts of Saudi society had knowledge about SPAM by self-education; through researching and reading about email SPAM on the Internet generally and forums specifically, and through discussing the issue with friends and relatives. The results indicated the deficiency of efforts by government ministries and commissions, ISPs, and broadcast media such as newspapers and magazines in making Saudi society aware of SPAM.

K. How Email Users Deal with SPAM

The results indicated that email users dealt with SPAM in various ways, and this could be because of many factors such as their experiences in using email, their awareness of SPAM, and their area of study.

The results have shown that over half of the participants (65%) read the entire SPAM email.

The results revealed that most of the participants (92%) deleted the SPAM email. A study conducted by [20] revealed that 66% of 205 participants deleted SPAM email. Results of a survey conducted by [22] revealed that 82% of the participants deleted SPAM email. By comparing the results of this study to results of studies described above, it can be seen that the percentage of the participants, who deleted email SPAM, was larger in this study, than the percentages in other studies.

The results found that few email users (19%) contacted their ISPs and notify them about SPAM. The results of a study conducted by [20] showed that 11.7% of the participants contacted their ISPs when they received email SPAM. By comparing the results of the two studies, it can be clearly seen that the percentage of the participants, who contacted the ISP and notify it about SPAM email, was better in this study than the percentage in the other study.

The results showed that a few email users responded to offers made by SPAM, and the greatest benefits that participants derived from email SPAM were fun and learning materials emails.

The results revealed that about one third of participants used Anti-SPAM filters to combat SPAM email.

As described above, it can be clearly seen that users dealt with SPAM email in various ways, and they were not aware of the appropriate ways to deal with SPAM. This requires work to increase the awareness of email users about effective methods in dealing with SPAM.

L. The Effects of Email SPAM in Saudi Arabia

The results indicated that email SPAM had a large effect on email users, businesses, and ISPs.
The results revealed that the most common effects of email SPAM on email users were the filling of their email inboxes with SPAM, and the infection of their computer by Viruses, Worms, and other malicious programs.

The results indicated that the main effects of email SPAM on businesses were the filling of email inboxes with SPAM, and causing lost time and reduced productivity.

The results found that the main effects of email SPAM on the ISPs was the large increase in spending needed to update Anti-SPAM filters to combat SPAM, and dealing with the filling of email systems with SPAM.

From the results shown above, it can be clearly seen that the most common effect of email SPAM on the participants was the filling of email inboxes, or email system capacity with SPAM. As long as some people consider email SPAM as just advertisements, and they remain ignorant in how to deal with it, the volume of email SPAM and its effects are likely to increase. This indicates the need for appropriate ways to combat it in Saudi Arabia.

M. Efforts Related to Combating SPAM in Saudi Arabia

This section describes the efforts of the government, ISPs, and businesses to combat SPAM in Saudi Arabia that the participants were aware of.

The Efforts of the Government: The results indicated that the government undertook many efforts to combat SPAM in Saudi Arabia, and the efforts as perceived by email users, businesses and ISPs were as follows:

1. The King Abdulaziz City for Science and Technology (KACST) efforts: the surveyed participants said that KACST blocks unsecured websites and websites that send SPAM, informs people about dangerous security threats such as SPAM and their impacts, and conducts and funds research related to information security issues [26].

2. The Communication and Information Technology Commission (CITC) efforts: the surveyed participants said that CITC funded the Saudi National Anti-SPAM Program, creating a public website for it that includes information about SPAM, and methods of combating it. They also said that this program informed people about SPAM by publishing brochures or by the subscription of people to the mailing list of the CITC, which updated subscribers on new developments related to SPAM [12].

3. The surveyed participants said that the government established and funded centres to deal with information security issues. Examples for these centres are the Centre Of Excellence in Information Assurance [14], the Computer Emergency Response Team [7], and the Prince Muqrin Chair for Information Security Technologies [35]. They said that the aims of these centres were to inform people about security threats, and their impacts by conducting and funding research related to security issues, and by conducting conferences and workshops regarding security threats.

4. The surveyed participants said that the government recommended that the public and private sectors should apply a security policy within their organization. This policy should include tasks to achieve its aims such as providing the organization with software and hardware necessary to avoid security threats and ensuring the awareness of employees and customers about security threats and methods of combating them.

5. The surveyed participants said that some universities established centres for Information Security, which provide services for people such as providing awareness to people about security threats such as SPAM; and conducting workshops, conferences and ongoing training in the field of security issues and methods of combating it for people.

The Efforts of ISPs: The results indicated that the ISPs undertook many efforts to combat SPAM in Saudi Arabia, and these efforts as perceived by email users, businesses and ISPs were as follows:

1. The surveyed participants (email users, businesses and ISPs) said that the ISPs used advanced Anti-SPAM filters, which were either software or hardware, to block email SPAM before it reaches users inboxes, and that they updated these filters regularly.

2. The surveyed participants said that the ISPs blocked websites, email addresses, or forums that send email SPAM, and that they put them on specific black lists to stop the increased volume of SPAM.

3. The surveyed participants said that the ISPs informed customers about email SPAM, and about methods of combating it via email, brochures, and Short Message Service (SMS).

4. The surveyed participants said that there were some legal efforts by ISPs to combat SPAM such as receiving customers’ complaints regarding SPAM and dealing with them legally and submitting reports to the CITC if any Internet abuse occurs from their own IP allocations.

5. The surveyed participants said that the ISPs provided technical support for customers when they were contacted regarding SPAM problems.

6. The surveyed participants said that some ISPs created business units or teams to manage the network security of organizations, and to protect them from dangerous threats such as Viruses and SPAM.
The Efforts of Businesses: The study results indicated that businesses undertook a great deal of effort to combat SPAM in Saudi Arabia, and these efforts were as follows:

1. Some businesses established business units or created a team to manage the network security of the company and to protect it from security threats such as SPAM.
2. Some businesses employed specific employees to manage and combat SPAM in the company.
3. Some businesses informed employees and customers about email SPAM, and methods for combating it via the company website, brochures, or by information centres.
4. Some businesses used advanced Anti-SPAM filters, either hardware or software, to block email SPAM.
5. Some businesses trained employees in the effective ways to combat SPAM, and how they use Anti-SPAM filters to block email SPAM.

N. The Anti-SPAM Filters Used to Block Email SPAM, and their Effectiveness in Detecting Arabic and English Email SPAM

The results indicated that ISPs use both content and origin based filters to block email SPAM. Examples of content based filters used by ISPs were Iron port, Brightmail, Barracude, McAfee, Norman, Sophos, Forfront security, Symantec, NETASQ MFILTRO, and Kaspersky. The most common content based filter used by the ISPs was Iron port.

Examples of origin based filters used by ISPs to block email SPAM were Black Lists, White Lists, and Challenge Response Systems. The most common origin based filter used by the ISPs was Black Lists.

The ISPs evaluated the effectiveness of content and origin based filters in detecting Arabic and English email SPAM, and these evaluations can be seen in Figure 1 and Figure 2.

Figure 1: The Effectiveness of Content based Filters in Detecting Arabic and English Email SPAM based on ISPs' Evaluation

Figure 2: The Effectiveness of Origin based Filters in Detecting Arabic and English Email SPAM

As described in Figure 1 and Figure 2, the evaluation of the ISPs for the effectiveness of content and origin based filters in detecting Arabic and English email SPAM revealed that both content based filters and origin based filters were more effective in detecting English email SPAM than Arabic email SPAM. The results also indicated that the origin based filters were slightly more effective in detecting Arabic email SPAM than content based filters.

Email users and businesses also evaluated the effectiveness of the Anti-SPAM filters that they used in detecting Arabic and English email SPAM, and these evaluations are presented in Figure 3 and Figure 4.
As seen in Figure 3 and Figure 4, email users and businesses estimated that Anti-SPAM filters were more effective in detecting English SPAM than Arabic SPAM. The percentages revealed that the evaluations of email users and businesses of the existing Anti-SPAM filters in detecting English SPAM was the same; while the evaluation of email users of the effectiveness of Anti-SPAM filters in detecting Arabic SPAM was slightly higher than the evaluation of businesses.

IV. CONCLUSION AND FUTURE WORK

This paper presented the main findings of user, business, and ISP surveys for email SPAM, its effects, and methods of combating it in Saudi Arabia. The results indicated that there was no specific definition for email SPAM in Saudi Arabia. This could require specifying an agreed definition for email SPAM which could be used for enacting laws to combat SPAM, and in developing Anti-SPAM filters.

The results revealed that the volume of email SPAM in Saudi Arabia was high compared to other countries; and most of the email SPAM in Saudi Arabia was written in English followed by Arabic. This requires legal effort to control SPAM in Saudi Arabia, and more effective Anti-SPAM filters in detecting email SPAM, particularly in that written in Arabic, as most respondents indicated that the filters were less effective at detecting such SPAM. The results indicated that the most common type of Arabic and English email SPAM was businesses advertisements. The results have shown that most of the Arabic email SPAM was sent from Saudi Arabia, and other Arabic countries; while most of the English email SPAM was sent from non-Arabic countries. This suggests that improving origin-based filters to detect SPAM sent from different sources may be effective.

The results showed that most email users in Saudi Arabia were not aware of email SPAM and ways to combat it. This suggests that efforts by government, ISPs, and broadcast media in providing information to people about SPAM and methods of combating it are needed.

The results indicated that there were efforts undertaken by government, ISPs, and businesses to combat SPAM in Saudi Arabia such as awareness of people about email SPAM, using Anti-SPAM filters, and funding research related to SPAM. These efforts were not effective to combat SPAM, and the work to develop these efforts is necessary.

The results indicated Anti-SPAM filters were not completely effective in detecting Arabic and English email SPAM, and these filters were more effective in detecting English SPAM than Arabic SPAM. This suggests that work is required to improve the existing Anti-SPAM filters to be more effective in detecting email SPAM in different languages.

Future work is required to investigate other types of SPAM in Saudi Arabia such as web SPAM, image SPAM and Short Message Service (SMS) SPAM, and effective ways to combat them.

Future work could include investigating effective ways to inform people in the public and private sectors about email SPAM, Anti-SPAM filters, and methods for dealing with it.

Some countries have enacted laws against SPAM, and there are no laws to combat SPAM in Saudi Arabia. Therefore, laws to combat SPAM in Saudi Arabia could be investigated. This could be achieved by investigating laws in other countries in order to enact a new clear law to combat SPAM in Saudi Arabia.

Most participants were not aware of the ISPs efforts to combat SPAM in Saudi Arabia. Effective ways to encourage ISPs to collaborate with each other ISPs, organizations, the government and customers in combating SPAM in Saudi Arabia could be investigated.

Anti-SPAM filters were not completely effective in detecting Arabic and English email SPAM. Further research is needed to improve the performance of Anti-SPAM filters in detecting Arabic and English SPAM. This could be achieved by testing the effectiveness of Anti-SPAM filters in detecting Arabic and English SPAM, and then updating and developing Anti-SPAM filters to be more effective.

The existing Anti-SPAM filters were more effective in detecting English email SPAM than Arabic SPAM. Future work is required to create and produce more effective Anti-SPAM filters for Arabic SPAM. Part of the research would involve the listing of keywords and other characteristics of Arabic email SPAM, which could help in designing and creating specific Anti-SPAM filters for Arabic email SPAM.

REFERENCES


