ABSTRACT

This paper presents the results of a survey of businesses in Saudi Arabia. The survey investigated email SPAM and the efforts made to combat it.

Three hundred businesses were surveyed and completed surveys were collected from 92 of the businesses. The businesses completing the survey were located in central, eastern and western Saudi Arabia. There were no completed questionnaires from businesses in the southern and northern regions because businesses in these regions notified us to conduct our survey in their head offices which are located in central, eastern and western regions of Saudi Arabia.

The survey aimed to understand the definition of email SPAM based on businesses opinions, its volume, its types, and its effects on businesses operating in Saudi Arabia. It also aimed to evaluate the effectiveness of existing Anti-SPAM filters in detecting Arabic and English email SPAM. The survey also investigated the efforts of government, Internet Service Providers (ISPs) and businesses to combat email SPAM.

The results showed that there were different definitions for email SPAM based on different businesses opinions in Saudi Arabia. The results indicated that the volume of email SPAM was very high in Saudi Arabia and the majority of email SPAM received was written in English. The results showed that the most frequent type of email SPAM received in both Arabic and English was business advertisements. The results showed that email SPAM had many effects on businesses. 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 businesses were not aware of government and ISP efforts to combat email SPAM. The results showed that most businesses did not inform their customers and employees about email SPAM and the methods used to combat it.

Keywords: SPAM, email, Arabic, businesses, English, Saudi.

1. INTRODUCTION

Email has become one of the significant uses of the internet today. It allows users to communicate with each other by sending and receiving text and multimedia messages. However, the use of email has some problems; the most common problem is email SPAM.

Email SPAM is an international problem and it has caused many effects in different countries. An example of these effects was a report that indicated SPAM cost companies in the USA $10 billion in lost productivity in 2003.[11] Ferris Research indicated that the cost of SPAM for companies around the world was about $14 per user per month in lost productivity.[17]

Email SPAM is defined as Unsolicited Bulk Email (UBE) which means sending a large number of emails that are not requested by recipients.[15], [22], [14], [25], [16], [32], [5]. It is also defined as Unsolicited Commercial Email (UCE) which contains promotional advertisements from different businesses sent to a large number of recipients.[10], [28], [9]. The Text Retrieval Conference (TREC) SPAM Track defined SPAM as "Unsolicited, Unwanted email that was sent indiscriminately, directly or indirectly, by a sender having no current relationship with the recipient"[12], [13]. [31], [24], [18] have considered both Unsolicited Bulk Email (UBE) and Unsolicited Commercial Email (UCE) as email SPAM definitions.

There are two ways to combat email SPAM. One of these ways is legislation and the other way is technical. Some countries have enacted laws to combat email SPAM. Examples of these countries are the United States of America[29], Australia[6], European Union countries such as Spain and Italy, and Asian countries like Japan and India[29]. However, there are no clear laws in Arabic countries including Saudi Arabia to combat SPAM and this will lead to an increase in the volume of SPAM in these countries.

The second way to combat email SPAM is various technical measures [2]. Many companies and researchers have developed techniques and filters to combat email SPAM.

These techniques include origin based techniques and content based techniques. Origin based techniques classify SPAM based on network information, such as the source IP and email addresses[18]. Examples of origin based techniques are black lists[11], white lists[26], [11], [20], challenge response systems[25], [11] and origin diversity analysis[19]. Content based filters detect SPAM by examining the content of email.
messages, irrespective of the origin[11]. Examples of these techniques include rule based filters[11], Bayesian filters[5], [27], genetic algorithms[18], [21], artificial neural networks[18],[16], decision tree technique[16], maximum entropy models[23], [32], boosting algorithms[32], [8], [10],K-nearest neighbors clustering techniques[16]and honey pots techniques[4]. However, some of these techniques are not effective in detecting email SPAM and need to be updated to detect new types of SPAM. This is because of the continuous work of spammers to develop techniques to bypass the existing techniques.

This study aimed to gain an understanding about:

a. The nature of email SPAM, its definition based on businesses opinions, its volume and its types.
b. Differences between Arabic email SPAM and English email SPAM.
c. The effects of email SPAM on different businesses.
d. How businesses 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 the effectiveness of Anti-SPAM filters in detecting Arabic and English email SPAM.

2. METHODOLOGY

2.1. PARTICIPANTS

The questionnaire was designed and distributed to 300 different businesses in central, eastern, western, southern and northern regions of Saudi Arabia. Completed questionnaires were received from 92 businesses that were located in central, eastern and western regions of Saudi Arabia. No completed questionnaires were received from businesses in the southern and northern regions. Businesses in these regions notified us to conduct our survey in their head offices which are located in central, eastern and western regions of Saudi Arabia. Central, eastern and western regions are the largest regions. The businesses included production and manufacturing, finance and investment, technology and telecommunication, consultation services, and other businesses. The size of businesses that participated in this study ranged from small to medium and large.

2.2. 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 organizations to get their comments about the questions. Then all the participants completed the 9 page questionnaire which included both yes/no answers and open ended answers. The questionnaire consisted of three main parts as follows.

2.2.1. GENERAL INFORMATION QUESTIONS

In this part, businesses were asked the year in which the business was established to enable comparison between old and new businesses. Businesses were also asked about the size of the business which could help in understanding the efforts of small, medium and large businesses in combating email SPAM. In addition, businesses were asked about the nature of their business activity. Businesses were asked if they have business units, centres or teams to control network security, what are the responsibilities of these units, centres or teams in this regard, and how many employees are involved. Businesses were also asked if they have specific employees whose roles are to combat SPAM. Examples for the first part of questions of the survey can be seen in Figure 1.

<table>
<thead>
<tr>
<th>1. What year was the company established?</th>
</tr>
</thead>
<tbody>
<tr>
<td>O Yes</td>
</tr>
<tr>
<td>O Medium</td>
</tr>
<tr>
<td>O Large</td>
</tr>
</tbody>
</table>

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

2.2.2. EMAIL SPAM QUESTIONS

At the beginning of this part, businesses 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 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.

Businesses were asked if they knew about email SPAM prior to reading the survey, and what were the sources of their knowledge. Businesses 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.

Businesses were asked if they used Anti-SPAM filters to block email SPAM 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 2.

<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>
3. Have you received SPAM emails?
   O Yes
   O No

3. What is the language of SPAM email you receive on average weekly? The percentages should add up to 100%.

<table>
<thead>
<tr>
<th>Language</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>O English</td>
<td></td>
</tr>
<tr>
<td>O Arabic</td>
<td></td>
</tr>
<tr>
<td>O Other language</td>
<td></td>
</tr>
<tr>
<td>O Languages I do not recognize</td>
<td></td>
</tr>
</tbody>
</table>

5. Do you use Anti-SPAM programs to block email SPAM?
   O Yes
   O No

6. If you have used Anti-SPAM programs, please rate their effectiveness in detecting English and Arabic email SPAM?

<table>
<thead>
<tr>
<th>Current Programs\Percentage</th>
<th>0%</th>
<th>25%</th>
<th>50%</th>
<th>75%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>The effectiveness of current programs in detecting Arabic email SPAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The effectiveness of current programs in detecting English email SPAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Examples of questions of the second part of the survey

2.2.3. QUESTIONS ABOUT THE EFFORTS OF GOVERNMENT AND ISPs TO COMBAT EMAIL SPAM

In this part, businesses were asked if they were aware of government efforts to combat SPAM and which efforts they were aware of. Businesses were also asked if they were aware of ISPs efforts to combat SPAM and which efforts they were aware of. Finally, businesses were asked if they provided awareness programs for employees and customers about email SPAM and effective methods to control it and what specific programs they provided. Examples for the third part of the survey can be seen in Figure 3.

1. Are you aware of efforts by the government in Saudi Arabia to combat email SPAM?
   O Yes
   O No

2. Are you aware of efforts by ISPs in Saudi Arabia to combat email SPAM?
   O Yes
   O No

3. Is there awareness provided by the company for employees and customers about email SPAM and appropriate methods to combat it?
   O Yes, please explain
   O No

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

3. RESULTS

The results obtained from the questionnaire are presented based on the three parts of the questionnaire.

3.1. OVERVIEW OF RESPONDENT BUSINESSES AND SPAM RELATED UNITS

The first part showed that 40% of the businesses that participated in this study were large, 39% were medium and 21% were small.

Among the respondents, 46% of businesses were production and manufacturing, 16% were technology and telecommunication, 10% were consultation services, 9% were finance and investment, and 19% were other businesses.

When businesses were asked if they have units, centres or teams to manage network security, the results revealed that 59% of the businesses have units, centres or teams to manage network security while 41% did not have units, centres or teams to control network security.

The results showed that the security units, centres and teams have a number of responsibilities to protect businesses networks and systems. 86% of businesses with them said that the security units, centres and teams monitor and protect networks and systems of head offices and branches of the business from dangerous attacks by Viruses, Worms, Trojans or other malicious programs. They also said that these units, centres and teams apply advanced software and hardware such as Anti-Virus and Anti-SPAM filters to secure internal and external networks and connections to the internet.

23% of businesses said that the security units, centres and teams check the firewall and routers of the company network, and monitor ports, web server, email server and database of the business. They said that these units, centres and teams also manage the proxy server, the internet and businesses applications such as Enterprise Resource Planning (ERP) systems.

6% of businesses said that the security unit, centre and team for the business secure the internet connection, wireless network connection and Virtual Private Network (VPN) connection. They also design security policies and security enhancements for the business.

14% of businesses said that the security unit, centre and team set up the security between the company and internet inside the company and report or send alerts when network security issues were found. They also said that these units monitor activities on the internet and intranet users and manage the trouble shooting for the network.

When different businesses were asked if they have special employees to combat SPAM, the results showed that only 18% of businesses have employees with specific responsibility to combat email SPAM while 82% do not have employees with specific responsibilities to combat email SPAM.

The results showed that the employees of combating of email SPAM in the businesses have many responsibilities to combat SPAM. 80% of businesses who had employees specifically to combat email SPAM said that their tasks were to manage, control and monitor email systems and to protect the email servers from any dangerous activities such as Viruses, Trojans and SPAM. These employees also regularly apply and update Anti-SPAM filters to catch new email SPAM.

13% said that the tasks of employees in combating email SPAM were tracing the causes of email SPAM, fixing the problem and generating a daily report of the activity. Based on
the report, the problem is analyzed and necessary actions taken like updating Anti-SPAM software and hardware.

13% said that the employees check the logs regularly, get users complaints for new SPAM and add the specific words in email SPAM to blacklists.

7% said that the tasks of employees were to protect end users inboxes from dangerous attacks and separate email addresses for different online activities.

3.2. RESPONDENTS DEFINITION AND AWARENESS OF EMAIL SPAM

In the second part of the questionnaire, the different businesses were asked about the definition of email SPAM. The responses showed that 16% of businesses defined email SPAM as email sent by unknown senders.

49% of businesses defined email SPAM as junk email or unwanted, unsolicited, bulk email (UBE) that was sent to numerous numbers of recipients indiscriminately in a small time.

46% have defined email SPAM as unsolicited, commercial emails (UCE) that contain advertisements for products and services sent to numerous recipients and their purposes were to collect money from recipients.

16% said that email SPAM is email that contains some suspicious or strange links, hidden attachments or components and some malicious programs such as Viruses, Worms and Trojans which aim to affect the speed and efficiency of networks and computers and to steal confidential data.

4% of businesses defined email SPAM as email that was sent from adult and sexual websites, different forums and newsgroups to individuals.

7% have defined email SPAM as annoying email sent directly or indirectly to recipients without their permission or without their subscription.

4% of businesses said that email SPAM is email that slows down the processes of the network, consumes bandwidth, and waste the time of employees.

3% defined email SPAM as emails that are irrelevant to the businesses work or that has nothing to do with the main functions of businesses.

From the definitions described above, it can be clearly seen that there was no specific definition for email SPAM and this could cause problems in enacting laws to combat SPAM in Saudi Arabia and in developing Anti-SPAM filters for different languages such as Arabic. In addition, the responses showed that most of the definitions of email SPAM agreed with the international definitions for email SPAM through their definition of email SPAM as Unsolicited Bulk Email (UBE) and as Unsolicited Commercial Email (UCE).

When different businesses were asked if they knew about email SPAM prior to reading the survey, the results revealed that 90% of businesses knew about email SPAM prior to reading the survey while 10% did not know about it.

By comparing these results with advanced countries such as Australia, it was found that all businesses in Australia were aware of email SPAM, its impacts and the legislation of the government to combat it [7]. The results of the survey revealed that only 90% of respondents indicated prior awareness of SPAM, suggesting that the survey itself has acted as a means of educating the respondents about SPAM and its impact.

Figure 4 shows the sources of knowledge of businesses about email SPAM.

The results showed that 75% of businesses were informed about email SPAM by the internet and forums, 40% were informed about email SPAM by friends and relatives, 25% of businesses were informed by ISPs, 25% informed by other companies and organizations, 24% informed through broadcast media such as radio, TV, newspapers and magazines, 21% were informed from other sources and 8% of businesses were informed by government ministries and commissions. The other sources of awareness about email SPAM were from the work in the information technology department, ongoing training conducted by companies, school and university education, experiences, some workshops and conferences related to email SPAM and reading about email SPAM.

3.3. VOLUME AND NATURE OF EMAIL SPAM IN SAUDI ARABIA

When the businesses were asked if they received email SPAM, the results showed that 95% of businesses received email SPAM and 5% did not receive email SPAM. A report released by Symantec in 2012 indicated that Saudi Arabia remains the most spammed country in the world with a SPAM rate of 75.5% of email traffic in the country[30].

When the participants were asked about the number of email SPAM received on average weekly, the responses were different from company to company. Some of businesses have received thousands of email SPAM emails, some of them have received hundreds, some received tens and some have not received any SPAM email. The number of email SPAM received in different companies depends on many factors such as the number of employees, the number of customers and the filters used by the business to combat email SPAM. Businesses estimated they received an average of 4,208 SPAM emails weekly. Another study conducted on ISPs in Saudi Arabia estimated that ISPs blocked an average of 1,466,027 SPAM emails weekly [3].

When the participants were asked about the languages of email SPAM that they have received, the results showed that 66% of email SPAM received was in English, 21% was in Arabic, 5% was not recognized and 10% was in other languages such as Chinese, Russian, Turkish, French, Hebrew, German, Persian and Urdu (See Figure 5).

The results on the language of the email SPAM received in Saudi Arabia were similar to the results of a study conducted in the Bahraini society about email SPAM emails which indicated that the percentage of English email SPAM was 64% and the percentage of Arabic email SPAM was 18% [1].
As seen in Figure 5, the majority of email SPAM received by businesses in Saudi Arabia was in English.

![Language of Email SPAM received by businesses in Saudi Arabia](image)

**Figure 5:** Language of email SPAM received by businesses in Saudi Arabia

When businesses were asked about the types of Arabic email SPAM that they have received, the results shown in Table 1, revealed that 36% of email SPAM were business advertisements, 33% were from forums, 10% were products and services, 7% were from religious and political parties, 6% were phishing and fraud emails, 5% were from pornographic websites and 3% were other types. The other types of Arabic email SPAM included emails for fun, jokes and greetings, educational consultation advertisements, puzzle and invitations from social networks sites such as Facebook and LinkedIn.

When businesses were asked about the types of English email SPAM that they have received, the results shown in Table 1, revealed that 32% of email SPAM received was business advertisements, 25% were phishing and fraud emails, 18% were products and services, 15% were from pornographic websites, 6% from forums, 3% were from religious and political parties and 1% were other types. The other types of English email SPAM included invitations from social networks sites such as Facebook and LinkedIn and friendship requests.

Table 1: The differences between Arabic and English email SPAM received by businesses in Saudi Arabia

<table>
<thead>
<tr>
<th>Types of email SPAM</th>
<th>AR (%)</th>
<th>EN (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>36</td>
<td>32</td>
</tr>
<tr>
<td>Religious and Political Party</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Pornographic</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>Forums</td>
<td>33</td>
<td>6</td>
</tr>
<tr>
<td>Products and services</td>
<td>10</td>
<td>18</td>
</tr>
<tr>
<td>Phishing and Fraud</td>
<td>6</td>
<td>25</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

From Table 1 shown above, it can be clearly seen that the largest proportion of email SPAM in both English and Arabic was from business advertisements. The results showed that businesses reported receiving email SPAM from forums, religious and political parties in Arabic more than English. The results also showed that the volume of other types of email SPAM such as friendship request of social networks such as Facebook was more in Arabic than English. The results also revealed new types of Arabic email SPAM containing jokes, greetings, fun and puzzles. These types of email SPAM did not exist in English. Additionally, the results revealed that the volume of pornographic, products and services, and Phishing and fraud emails was larger in English than Arabic.

3.4. EFFECTS OF EMAIL SPAM ON THE OPERATION OF BUSINESSES IN Saudi ARABIA

When the participants were asked about the effects of email SPAM on their operations, the study found that 83% of businesses said that the email inbox filled with SPAM, 72% said that email SPAM wasted time and reduced the productivity of employees, 64% of businesses said that the computers of the company were infected by Viruses, Worms or other malicious programs, 50% said that they had spent a lot of money to implement and update filters to combat email SPAM, and 7% of businesses said that email SPAM had other impacts on the operation of the business. These other impacts of SPAM included reducing the internet speed, consumption of bandwidth, slowing down the main server for the company and stealing or losing confidential data. Figure 6 shows the effects of email SPAM on businesses.

![Effects of email SPAM on businesses](image)

**Figure 6:** Effects of email SPAM on operating businesses

3.5. THE EFFECTIVENESS OF ANTI-SPAM FILTERS IN DETECTING ARABIC AND ENGLISH EMAIL SPAM

The businesses were asked if they used Anti-SPAM programs to block email SPAM and the responses showed that 80% of businesses have used Anti-SPAM filters while 20% did not use Anti-SPAM filters to block email SPAM (See Figure 7).

![Do you use Anti-SPAM programs to block email SPAM?](image)

**Figure 7:** Do you use Anti-SPAM programs to block email SPAM?

When the participants were asked about the effectiveness of Anti-SPAM filters in detecting Arabic and English email SPAM, the results found that the effectiveness of the filters was 56% in detecting Arabic email SPAM and 80% in detecting English email SPAM (See Figure 8).
The results in Figure 8 indicated that Anti-SPAM filters were not effective enough in detecting Arabic and English email SPAM, but they were more effective in detecting English email SPAM than Arabic email SPAM. The lower effectiveness of Anti-SPAM filters for Arabic SPAM combined with current low levels of Phishing and Scams indicates that there is the very real risk of exploiting of the Saudi community through Phishing and Scams. To prevent the negative effects of this, better Arabic language Anti-SPAM filters are required.

3.6. EFFORTS OF GOVERNMENT AND ISPs TO COMBAT EMAIL SPAM

In the third part of the questionnaire, businesses were asked if they were aware of efforts by the government in Saudi Arabia to combat SPAM. The results revealed that 25% of businesses were aware of government efforts to combat SPAM while 75% were not aware of these efforts. The results showed that the government efforts that the participants were aware of were as follows: 20% of businesses said that the government had enacted regulations and laws to combat electronic crimes which included SPAM. 50% of businesses said that the Communication and Information Technology Commission (CITC) as a government sector provided some information about SPAM and methods of controlling it in brochures and designed a website to inform people, companies, and the public and private sectors about SPAM and effective ways to combat it. 10% said that one of the responsibilities of the government was to block suspicious and untrusted websites that may send email SPAM such as pornographic websites. 20% of businesses said that there were some efforts by King Abdulaziz City for Science and Technology (KACST) to combat email SPAM and other electronic attacks by making people aware of SPAM, and by blocking some untrusted websites. The businesses were also asked if they were aware of efforts by ISPs in Saudi Arabia to combat email SPAM and it was found that 24% of businesses were aware of ISPs efforts to combat SPAM while 76% were not aware of the ISPs efforts. The ISPs efforts that the participants were aware of were as follows: 79% of businesses said that the ISPs block any email SPAM and its source before it arrives in customers’ inboxes by using advanced software, hardware and firewall or combinations of them. 14% of businesses said that if there were some problems regarding SPAM, they contacted their ISP for assistance. The ISP obtained an email SPAM report from them and took appropriate actions. These actions were either legal or technical actions. 7% said that some ISPs in Saudi Arabia do not use port 25 which is normally used to send email. They said that closing port 25 reduces the amount of email SPAM that is sent onto their networks.

When different businesses were asked about the awareness of their employees and customers about email SPAM and the appropriate ways to combat it, the results showed that 39% of businesses informed employees and customers about email SPAM and methods of controlling it while 61% did not inform customers about email SPAM (See Figure 9).

4. CONCLUSION, RECOMMENDATIONS AND FURTHERWORK

This paper presented the results of a survey of different types of businesses about email SPAM and how they deal with it in Saudi Arabia.

The survey showed that only 59% of businesses in Saudi Arabia have businesses units, centers or teams for controlling network security. The responsibilities of these units or centers differ from business to business depending on the available capability in different businesses, the age of businesses, the nature of activity in businesses and the business size.

The survey showed that relatively few businesses in Saudi Arabia have special employees to combat SPAM. The responsibilities of those employees differ from one company to another depending on the available capability in different businesses and the experience of those employees in dealing with SPAM.

The survey showed that there were different definitions for email SPAM based on different businesses opinions in Saudi Arabia. Most business definitions of email SPAM agreed with international definitions for email SPAM, i.e., email SPAM is Unsolicited Bulk Email (UBE) and is Unsolicited Commercial Email (UCE).

The survey also showed that 10% of different businesses in Saudi Arabia did not know about email SPAM before reading the survey. The survey showed that there were many sources of knowledge for awareness about email SPAM for businesses and the most used source was the internet and forums. The survey showed that few businesses were informed about email SPAM by government ministries and commissions which indicated that deficiencies in the efforts of government ministries and commissions to make businesses aware of SPAM.

The survey showed that the most businesses in Saudi Arabia, 95% of the participants, received email SPAM and indicated a rise in volume of email SPAM. The volume of email SPAM
was different from one company to another because of many of factors such as the effectiveness of Anti-SPAM filters used, the awareness of employees and customers about email SPAM, and the experience of employees in dealing with email SPAM.

The survey showed that most of the email SPAM received by different businesses in Saudi Arabia was in English and Arabic. The most numerous English email SPAMs were businesses advertisements, Phishing and fraud emails. The most common Arabic email SPAMs were businesses advertisements and forums emails.

The survey showed that email SPAM caused many effects on the work of different businesses in Saudi Arabia and the level of these effects were different from one company to another. The main effect of email SPAM on the work of businesses was that filling email inboxes with SPAM. The second main effect of email SPAM was losing time and reducing the productivity of businesses. There were other effects of email SPAM on businesses such as spending a lot of money for updating Anti-SPAM filters and removing infections of businesses computers by malicious programs like Viruses, Trojans and Worms.

The survey showed that 20\% of different businesses in Saudi Arabia did not use Anti-SPAM filters to block email SPAM. The survey showed that the effectiveness of Anti-SPAM filters was more effective in detecting English email SPAM than Arabic email SPAM.

The survey showed that most of the businesses in Saudi Arabia were not aware of the government efforts to combat SPAM. Most of the government efforts to combat SPAM were at the Communication and Information Technology Commission (CITC) and King Abdulaziz City for Science and Technology (KACST).

The survey showed that most of the businesses in Saudi Arabia were not aware of ISPs efforts to combat SPAM. The survey showed that most of businesses in Saudi Arabia did not provide awareness programs for employees and customers about SPAM.

The study results have revealed several actions and suggestions that could be taken into account to reduce the impact of email SPAM in Saudi Arabia. First of all, businesses in Saudi Arabia should establish security units or centres to reduce security attacks such as Viruses, Trojans and SPAM in businesses. The study results suggest that recruitment of qualified employees who have expertise in the field of network security in general, and spam in particular would help in reducing the volume of SPAM and Saudi Arabia businesses.

The study results also suggest that there is scope to specify an agreed definition for email SPAM which could be used for enacting laws to combat SPAM and developing Anti-SPAM filters in Saudi Arabia. The study results suggest that consultation and collaboration between different businesses, government, ISPs and other businesses in Saudi Arabia about SPAM and methods of combating it would reduce the volume of SPAM. The study results suggest that creating a scientific forum related to SPAM and methods of combating it could help in reducing SPAM through providing awareness for employees, customers or other subscribers, answering questions regarding SPAM problems and publishing a daily updated email SPAM list. The study results suggest that the publishing of information about SPAM by different communication media such as magazines, TV and radio could be helpful in mitigating SPAM in Saudi Arabia. The study results also suggested that conducting and sharing in workshops, ongoing training and conferences related to SPAM and the effective methods to combat it, and educating people through school or universities about SPAM would help in reducing SPAM in Saudi Arabia.

The study results suggest that the existing Anti-SPAM filters need to be updated and improved regularly to catch new types of email SPAM. The study results also suggest that work is required to create specific filtering techniques for Arabic email SPAM. This is critical given that Phishing and Scams are not yet as prevalent in Arabic language and thus there is the potential for significant exploitation of the Saudi Arabia community.

The study results suggest that concerted efforts between all government ministries, commissions and sectors and private sectors could be effective way to reduce the volume of email SPAM in Saudi Arabia. Examples for the suggested efforts for government and private sectors include: improving the awareness of people who work on these sectors about SPAM, distributing free Anti-SPAM software to employees, and funding research projects related to SPAM and publishing them for researchers and the public who interested in SPAM issues.

The study results suggested that the government should establish an internet security management, commission or create acyber-crimesdepartment which is responsible for enacting laws for information crimes, following up implementation of these laws, receiving complaints by internet users about security attacks, developing internet security software and providing awareness programs for people in the public and private sectors about security attacks such as viruses and SPAM.

Future work could include investigating effective ways to inform people in the public and private sectors in Saudi Arabia about email SPAM and methods of combating it. Government efforts in Saudi Arabia to combat email SPAM could also be investigated to find more effective methods. The legal and technical efforts of ISPs in Saudi Arabia to combat email SPAM could also be investigated.

Improving the performance of existing Anti-SPAM filters in detecting email SPAM could be investigated. This could be achieved by developing more effectiveAnti-SPAM techniques for detecting SPAM through testing their effectiveness in detecting SPAM and using more than one technique to design effective filters.

Part of the research would involve the listing of keywords and phrases used in Arabic email SPAM and applying techniques that are effective in detecting other SPAM in other languages. This could help in designing and creating specific Anti-SPAM filters for Arabic email SPAM.

REFERENCES


