Email SPAM Related Issues and Method of Controlling Used by Internet Service Providers [ISPs] in Saudi Arabia

Hasan S. Alkahtani
Robert Goodwin
Paul G. Stephen
This paper presents the results of a survey of ISPs in Saudi Arabia about email SPAM and how they deal with it. We have surveyed all ISPs in Saudi Arabia and we have received 11 responses from 27 ISPs. This survey investigated the nature of email SPAM, its volume, its types and its sources in Saudi Arabia. It also investigated the effects of email SPAM on operating ISPs. This survey aimed to understand the efforts of government and ISPs to control SPAM. Finally, this survey aimed to assess the effectiveness of current filters in detecting Arabic and English SPAM.

The results showed that there was a large volume of SPAM in Saudi Arabia and this volume varied from organization to organization. The results showed that the major of languages of SPAM were Arabic and English and that these Arabic and English SPAM emails have different types and were sent from different sources in the world. The results showed that the email SPAM affected the operation of the ISPs.

The survey also showed that the effectiveness of current filters varied from method to method in detecting Arabic and English SPAM emails. Finally, the results showed that some of the ISPs were not aware of government efforts to combat SPAM while others said that there were efforts by the government and they contributed to these efforts. The results also showed that ISPs made attempts to control SPAM such as implementing and updating filters and informing customers about SPAM.

**Keywords:** SPAM, Arabic, Filters, E-Mail, ISPs, English.

**1. INTRODUCTION**

The internet is considered an important tool for the world today. It has provided several facilities for users such as, the selling and purchasing goods, searching for information, acquiring knowledge, and communication between people.

One significant use for the internet is email which allows users to send and receive text and multimedia messages. However, some people have exploited email for personal purposes. These people, called Spammers, send so-called SPAM.

Email SPAM can be defined as "Unsolicited, unwanted email that was sent indiscriminately, directly or indirectly, by a sender having no current relationship with the recipient" [3].

To achieve huge benefits in a short time at low cost spammers collect a large number of email addresses in various ways. 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 and send email SPAM to these addresses [2]. For example, the New York Times interviewed "One of the Most Prolific Senders of Junk Email Messages in the World" in 2003. His name is Alan Ralsky, and he reported that he has over 150 million email addresses from about 24 countries and he could send email SPAM to 70 million of users per day. He also said that he gained about $500 from each one million emails sent [8]. In addition, spammers have used many methods to bypass SPAM filters such as tokenization and obfuscation [13].
Email SPAM causes several impacts on users and companies. Firstly, deleting email SPAM from an inbox wastes the time of users, and reduces employees' performance in firms as well as reducing the productivity of companies. For example, reports indicate that SPAM cost companies in the USA $10 billion in lost productivity in 2003 [2]. The cost of email SPAM was estimated 10 billion euro for internet users a year worldwide [9]. Moreover, Ferris Research indicated that the cost of SPAM for companies around the world was about $14 per user per month in lost productivity [5]. Furthermore, the Singapore Infocomm Development Authority (IDA) indicated that the total cost of SPAM for consumers is about $23 million in lost productivity each year [6]. Secondly, resources of email servers are consumed by SPAM messages such as wasting the capacity of the email systems of ISPs and wasting bandwidth, and it costs Internet Service Providers (ISPs) a lot of money to increase their email systems capacity and to buy extra bandwidth [4].

Moreover, email SPAM has significantly increased, and the content of the email SPAM is now written in different languages such as, English, Chinese and Arabic. For example, Jamie Cowper who is a technology consultant at Mirapoint estimated that about 13.5 billion emails sent around the world each day are SPAM [5]. In the Middle East, 90% of the 1.5 million emails received by companies daily were detected as SPAM in 2009 [11]. In addition, the number of SPAM messages touched 92 million every day in Oman in 2009 [11]. In Saudi Arabia, the number of emails detected as SPAM is 54% in 2006 [7]. The level of SPAM email in the United Arabic Emirates averaged 83.4% in 2009 [12].

There are many legal and technical solutions to fight the problem of SPAM. By looking at the legal aspect, some countries have enacted special laws against SPAM to reduce the volume of this attack. Examples of these countries include the United States of America, European Union countries, Australia [1] and some Asian countries. In the United States of America, there are two sets of laws against SPAM: Federal laws and State laws. The Federal laws were enacted on 16 December 2003 and it was the first attempt by the United States of America to combat SPAM. These laws are regulated by the Federal Trade Commissions (FTC). In addition, states in America such as Washington, Virginia, Georgia, California, Florida and Texas have enforced special laws to fight the problem of SPAM [10].

However, none of the Arabic countries have special laws to combat SPAM. In particular, Saudi Arabia has assessed the problem of SPAM, and has designed a framework to combat SPAM but this framework has not yet been applied as laws to fight SPAM in the country.

From the technical aspect, much research and many projects have been undertaken by experts and scientists in the area of information and network security to combat email SPAM. Examples of techniques and filters used to combat email SPAM include content based filters such as bayesian, keywords and genetic algorithms, and origin based filters like black lists, white lists and challenge response systems.

However, these filters and techniques for fighting email SPAM will not be effective as long as spammers work continuously to develop methods to bypass these filters. So, these filters need to be updated and developed regularly to detect new email SPAM and to detect new techniques used by spammers in sending these emails.

Therefore, this research aims to gain an understanding about:

- the nature of email SPAM, its volume, its type and its sources in Saudi Arabia
- the effects of email SPAM on ISPs in Saudi Arabia
- the efforts of government and ISPs to combat email SPAM
- the effectiveness of current email SPAM detection filters in detecting Arabic and English SPAM.

2. METHODOLOGY

2.1. PARTICIPANTS

There are 27 ISPs licensed by the Communication and Information Technology Commission (CITC) in Saudi Arabia. These ISPs are distributed in different regions of Saudi Arabia. All 27 ISPs were surveyed to achieve the aims of this research. Completed questionnaires were collected from 11 ISPs. Responses from the other 16 were not received because they were not keen to participate in this survey. The 11 ISPs that participated in this study varied in size of organization.

2.2. MEASURES

It was decided that the best way to answer the research questions was through a questionnaire and hence a questionnaire was distributed to the participants and their responses were analyzed. At the beginning, a pilot questionnaire was prepared and distributed to a few ISPs to get their comments and feedback about the questions.

Then the participants completed a 12 page questionnaire using both yes/no answers and open ended answers. The questionnaire was divided into four parts, general information about ISPs, the nature of email SPAM and its effects on ISPs, the effectiveness of current SPAM filters in detecting Arabic and English email SPAM, and the efforts of ISPs and government to combat email SPAM in Saudi Arabia. These parts are described in detail in the next sections.
2.2.1. GENERAL INFORMATION QUESTIONS

ISPs were asked about the establishment of the organization to enable a comparison between old and new organizations in combating SPAM. ISPs were asked about the organization size to understand the differences between large, medium and small organizations in combating SPAM. They were also asked about the number of employees and the number of customers.

They were asked if they have a special team or unit to manage and control network security, what are their responsibilities in this regard and how many employees are involved to give an understanding of efforts of ISPs to manage network security. They were also asked if they have specialist employees to combat email SPAM and what are their tasks to control SPAM. ISPs were also asked if workshops, conferences or other ongoing training on the control of email SPAM were conducted regularly for employees. This gave an understanding of the efforts of ISPs to reduce the amount of SPAM by informing employees of new types of SPAM and new methods to combat it. This data may lead to the development of new techniques to combat new types of SPAM or the update of current filters.

2.2.2. EMAIL SPAM QUESTIONS

At the beginning of this part, ISPs were asked to define email SPAM in their own words in order to understand the definition of email SPAM based on their judgment. The definitions of ISPs for email SPAM are described in results section.

We have 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 a sender”. This definition was in the survey and used for the purpose of this research. Some examples of email SPAM, keywords and phrases used in email SPAM were given in the survey.

ISPs were asked if they have blocked email SPAM recently and how many SPAM messages they block on average weekly. This gave an understanding of the volume of email SPAM in Saudi Arabia. They were also asked about the language of email SPAM, types of email SPAM, sources of SPAM and its keywords, phrases or unique features if they have blocked Arabic or English SPAM. We have focused in this study on English and Arabic email SPAM because English is the first language in the world and Arabic is the mother language for Saudi Society. We gained an understanding of the nature of email SPAM in Saudi Arabia, the differences between English and Arabic SPAM, their types and their sources which may be useful in developing filters to combat email SPAM. Additionally, ISPs were asked about the effects of SPAM on their performance and how much time they spent in fixing SPAM related problems.

2.2.3. QUESTIONS ABOUT THE EFFECTIVENESS OF EMAIL SPAM DETECTION TECHNIQUES IN DETECTING ARABIC AND ENGLISH SPAM

This part of the survey began with the definition of the two main techniques used in classifying email SPAM and some examples of these techniques. The two techniques were content based filters and origin based filters. ISPs were asked about the techniques or filters that they have used to detect SPAM. They were also asked about the effectiveness of the filters used in detecting Arabic and English email SPAM. The results may lead to proposals of more appropriate and effective methods of classifying English and Arabic SPAM. Finally, they were asked if they update their filters regularly because updating filters regularly enables the detection of new SPAM based on new keywords or features.

2.2.4. QUESTIONS ABOUT THE EFFORTS OF ISPs TO COMBAT EMAIL SPAM

In this part, ISPs were asked about the efforts of government and ISPs to control and combat email SPAM. ISPs were also asked if there was information provided by them to customers about email SPAM and the appropriate methods to combat it. We requested from ISPs their opinions about the appropriate ways to control email SPAM in Saudi Arabia either technical or legal, and to add anything that they thought might be of value to this study.

3. RESULTS

This section summarizes the results obtained from the questionnaire for each of the four parts of the survey. The first part of the survey showed that the size of the organizations ranged between small, medium and large. The percentages of organization size can be seen in figure 1. The size was based on the opinions of the actual ISPs.

![Figure 1: Organizations Size](image)

The results indicated that there were no differences between small, medium and large or new and old organizations in combating SPAM email in Saudi Arabia.

Figure 2 shows that 82% of ISPs have a business unit or team to manage the network security of
the organization while 18% do not have a unit to control security of the organization. The results showed that there were different responsibilities for these units to manage security. Some of the responses said that security units protected networks of companies from intrusions and malicious programs such as viruses and Trojans. Some said that these units strengthen the organizations network security, detect email SPAM by using software or hardware, protect the organization’s business, and save business time. Some of the ISPs said that the security units verify the current connections, look at the network traffic, read the security logs on the domain, look at the authorizing logs, and update the security patches. We have also found that the responsibilities of security units included following up reports sent from security devices on the internal and external networks and the development of security systems with the latest versions software and hardware.

The results showed that 45% of ISPs have employees with specific responsibility to combat email SPAM while 55% do not (See figure 3). The results showed that the tasks of those employees were: monitoring of relay, email systems support, check unwanted bulk unsolicited commercial emails, and emails sent from pornographic sites or similar. Some of the responses said that the tasks were updating black lists and creating special lists when the known international lists are inadequate.

The workshops, conferences and ongoing training were conducted regularly for employees of ISPs to understand the new keywords, features and phrases of email SPAM and the new detection methods to control it. Some of the ISPs conducted these activities every 4-6 months, some of them every 7-9 months and the others every 10-12 months.

In the second part of the survey when we asked ISPs about the definition of email SPAM, most of the responses from the ISPs defined email SPAM as unwanted, unsolicited and bulk emails that are sent from commercial advertisers and adult websites. Some of the ISPs defined SPAM as messages sent to recipients without their direct or indirect permission. Some responses have defined SPAM as messages sent to mailing lists that are not regularly maintained. Email SPAM was also defined by some ISPs as unknown language emails delivered to recipients. Some of the ISPs defined SPAM as messages that complicate work of server systems due to the large number of messages sent.

All 11 ISPs said that they have blocked email SPAM and the number of SPAM messages blocked varied from organization to organization. Some of the ISPs have blocked millions of SPAM messages, some have blocked thousands and others blocked hundreds on average weekly. The maximum number of blocked SPAM messages was 8,000,000 emails per week and the minimum was 100 emails per week.

The SPAM emails blocked by ISPs were written in different languages. It can be clearly seen in figure 5 that 59% of emails SPAM were in English, 24% were in Arabic, 7% were not recognized and 10% were in other languages such as Chinese, Japanese and Russian.
From figure 5, the majority of email SPAM blocked was English and Arabic. Both Arabic and English SPAM have many different types. These types are shown in figure 6 and 7. They included advertisements from businesses, religious and political parties, also for pornographic materials, forums, medical products and online gaming, phishing and fraud emails, and other types such as individual messages for fun, news and puzzles. As seen in figures 6 and 7, the highest percentages for both English and Arabic SPAM were from businesses.


When we asked ISPs about the sources of Arabic and English SPAM Emails, we have found that the sources of Arabic SPAM were as follows: 41% sent from Saudi Arabia, 30% sent from other Arabic countries, 8% sent from non Arabic countries and 21% sent from unknown sources (See figure 8).

We also found that the sources of English SPAM were as seen in figure 9: 16% sent from Saudi Arabia, 11% sent from other Arabic countries, 53% sent from non Arabic countries and 20% sent from unknown sources.

Email SPAM has caused many effects on the operation of ISPs in Saudi Arabia. Figure 10 describe the effects of email SPAM on ISPs.
From the results summarized in figure 10, we have found that 45% of the effects of SPAM on ISPs was losing time and reducing productivity. We have asked ISPs how much time they spend in fixing related SPAM problems on average weekly. The responses were different from organization to organization. Some of the ISPs stated that they spent between 6-10 hours per week to fix SPAM problems and some said that they spent between 1-5 hours while others said that the fixing of SPAM problems was done automatically by the filters used.

In the third part of the survey which asked ISPs about the filters that they have used and their effectiveness in detecting Arabic and English SPAM, we have found that all 11 ISPs used content based filters to classify email SPAM and 91% of the ISPs also used origin based filters. Examples for content based filters used by ISPs are shown in figure 11. We found that the majority of ISPs used Iron Port to classify email SPAM.

When we asked ISPs about the effectiveness of the content based filters in detecting Arabic and English email SPAM, we found that the effectiveness of the filters was 70% in detecting Arabic SPAM and 84% in detecting English SPAM (See figure 13).

The results also showed that the effectiveness of the origin based filters was 64% in detecting Arabic email SPAM and 77% in detecting English SPAM as shown in figure 14.
From the results in figures 13 and 14, we have found that both content based filters and origin based filters are more effective in detecting English SPAM than Arabic SPAM. We have also found that the content based filters are more effective than origin based filters in detecting Arabic and English email SPAM. From this study, we have also found that all 11 ISPs updated the SPAM filters used regularly to detect new features and types of email SPAM.

In the fourth part of the survey, when we asked about the efforts of government to combat email SPAM, the responses showed that most of the ISPs were not aware of government efforts to combat email SPAM. Some of the ISPs said that they have read Communication and Information Technology Commission (CITC) documents about SPAM and took part in CITC surveys related SPAM that were conducted by the government.

When we asked the ISPs about their technical and legal efforts to combat SPAM, most responses said that they used latest versions of software and hardware to classify email SPAM. Some of the ISPs said that there were no legal regulations set by ISPs to combat email SPAM while some of them said that there were few legal actions such as submitting a report to the CITC if any internet abuse occurs from their own IP allocations. The results showed that the legal and technical efforts of ISPs were warning the spammers who send SPAM, blocking the addresses that send SPAM and dealing with them in a quick and professional way. The results also showed that some of the ISPs when writing subscription contracts warned customers regarding misuse the internet service, and they applied penalties for the misuse of the internet like disconnecting the service and cancelling the contract.

When we asked the ISPs about the awareness of their customers, either individuals, or companies, about email SPAM and methods of controlling it, the responses showed that 55% informed customers about SPAM, 18% did not inform customers about SPAM and 27% did not answer the question (See figure 15).

We have found that some of the ISPs suggested some legal solutions. They said that it is necessary to enact clear laws to combat SPAM which include executive regulations and specific penalties for people who send SPAM email. They suggested that there should be clear conditions for the internet service usage for each internet subscriber regarding SPAM activities.

When we asked the ISPs about other appropriate ways to combat SPAM in Saudi Arabia, the ISPs said that it is important to establish an integrated authority, commission or management for network security and staff it with people who have experience in both software and hardware areas of information security. Some of the ISPs suggested focus on the awareness of people about SPAM and methods of controlling it, and conducting conferences and seminars to discuss email SPAM problems and the effective techniques to combat it.

4. CONCLUSION AND FUTURE WORK

In summary, this paper presented the results of the survey of ISPs about email SPAM and how the ISPs deal with it. This paper presented different definitions of email SPAM based on the ISPs judgment. The survey showed that most of the ISPs in Saudi Arabia blocked a large volume of email SPAM, the SPAM was mainly in...
English and Arabic. The survey also showed that most Arabic and English SPAM was in the form of businesses advertisements. The results showed that the Arabic email SPAM was sent from different sources to the English SPAM and the highest percentages of Arabic SPAM were from Saudi Arabia and other Arabic countries. The highest percentages of English SPAM were from non Arabic countries and unknown sources.

In addition, the results showed that email SPAM impacted on the operations of ISPs in Saudi Arabia. These impacts included: losing time and reducing productivity, spending a lot of money in implementing and updating filters used to combat SPAM, and to buy extra bandwidth and capacity for the email system, losing customers due to receiving a large volume of email SPAM, and filling email capacity with SPAM.

The results also showed that the ISPs used content and origin based filters to detect email SPAM. We have found that both content and origin based filters were more effective in detecting English SPAM than Arabic SPAM. We also found that content based filters are more effective in detecting Arabic and English SPAM than origin based filters. The results also showed that Anti SPAM hardware is more effective than Anti SPAM software.

The results showed that some of the ISPs were not aware of government efforts to combat SPAM while others said that there were efforts by government and they contributed to these efforts. The results also showed that ISPs tried to control SPAM by means of technical efforts like implementing and updating filters, legal efforts like warning spammers and applying penalties for misuse of the internet service, and other efforts like raising customers awareness about SPAM.

In future work, ways to improve the performance of current filters in detecting Arabic and English email SPAM will be investigated. This can be achieved by testing the effectiveness of current filters in detecting Arabic and English SPAM emails and this will lead to propose, update and develop the appropriate filters to detect Arabic and English SPAM.

Secondly, laws to combat SPAM in Saudi Arabia will be investigated. This can be achieved by looking to experiences of developed countries and their laws to combat SPAM and this will lead to enact a new clear law to combat SPAM in Saudi Arabia.

Thirdly, ways to encourage ISPs to collaborate with each other ISPs, organizations, government and customers will be investigated.

Finally, effective ways to inform customers, either individuals, or companies about SPAM in Saudi Arabia will be investigated.

REFERENCES: