Journal of King Saud University – Computer and Information Sciences (2011) **23**, 45–58

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Assessment of the status of spam in the Kingdom of Saudi Arabia

Mishaal Abdullah Al-Kadhi

Communications and Information Technology Commission, Saudi Arabia

Received 13 June 2009; accepted 27 October 2010
Available online 8 May 2011

KEYWORDS

Spam;
Spam statics;
Spam current state;
Spam baseline;
SMS spam

Abstract Spam is a serious threat to Information and Communications Technology (ICT) worldwide. It is used to not only transmit unsolicited messages, but also malware of every stripe and to propagate various types of phishing schemes. Spam has become so internationally wide-spread that in some regions it represents over 90% of the total e-mail traffic.

The purpose of this paper is to report the findings of the study commissioned by the Communications and Information Technology Commission to ascertain the magnitude of spam in the Kingdom of Saudi Arabia and formulate a comprehensive multi-pronged solution for handling spam in Saudi Arabia based upon best international practices, current situation and national requirements.

This paper will only focus on determining the current state of spam in KSA, focusing on obtaining a good understanding of the nature and prevalence of spam within Saudi Arabia. This information will then form the basis upon which the anti-spam national strategy framework will be based.

The study was compiled using the statistics that were gathered from stakeholders via different means including questionnaires, interviews and meetings. It covers e-mail, mobile and fax spam. It also highlights some of the stakeholders' concerns and recommendations regarding spam, as well as the measures taken by these stakeholders to control spam in their networks.

1. Introduction

Internet service was introduced into the Kingdom of Saudi Arabia pursuant to Royal Decree number 163 (1997), with the actual service itself coming online on 28/8/1419H (15th December 1998).

The construction of the national infrastructure, the related awareness efforts and the learning curve being experienced by all key stakeholders necessitated a gradual uptake of Internet service in KSA. Therefore, both the full benefits and the drawbacks of this service took some time to come to light.

E-mail address: mkadhi@citc.gov.sa

Peer review under responsibility of King Saud University.
doi:10.1016/j.jksuci.2011.05.001

Production and hosting by Elsevier

A few years later, Internet service in KSA began to achieve maturity and stability and it was deemed time for oversight of this service to be transferred from KACST[1] to the CITC[2], with the physical handoff occurring in 10/1427H (November 2006), pursuant to Royal Decree 229 (2004). At this point, core Internet service was considered to have achieved stability and CITC initiated numerous national projects to develop added-value services to the core Internet service. Among them was the national KSA anti-spam framework. Following further consideration, this initiative was expanded to cover the whole spectrum of ICT services, including fax and mobile spam.

In parallel to the above developments, during the Geneva phase of the World Summit on the Information Society (WSIS)[3], spam was identified by the international community as a potential threat to the full utilization of the Internet and e-mail. Accordingly, WSIS participants recognized that spam is a "significant and growing problem for users, networks and the Internet as a whole" (WSIS Declaration, 2003, paragraph 37) and that, in order to build confidence and security in the use of ICTs, there is a need to "take appropriate action at both national and international levels" (WSIS Plan of Action, 2003, paragraph C5, d).

The acknowledgment that spam is a problem at the global level, contributed to the fostering of various activities in the field. Countries, including KSA, became aware of the need to take action on this issue, and recognized the fundamental importance of international cooperation and coordination.

In October 2004, the World Telecommunication Standardization Assembly (WTSA, 2004), adopted resolution 51 – combating spam. This resolution instructs the TSB Director, in cooperation with the Directors of the other Bureaux and the Secretary-General to prepare urgently a report to the Council on relevant ITU and other international initiatives for countering spam, and to propose possible follow-up actions for consideration by the Council.

The second phase (Tunis phase) of the World Summit on the Information Society (WSIS) held from November 16 through 18, 2005, in Tunis, Tunisia, witnessed the adoption of the "Tunis Commitment (2005)" and the "Tunis Agenda for the Information Society (2005)" During this summit, attended by representatives from KSA, deliberations were made upon (i) concrete measures and mechanisms for implementation of the "Geneva Declaration of Principles" and the "Plan of Action" and (ii) issues not yet decided at the Geneva Phase, including the Internet Governance. At the closing plenary, the "Tunis Commitment" and the "Tunis Agenda for the Information Society," were adopted.

Paragraph 41 of the WSIS Tunis Agenda finally stated:

> "*We resolve to deal effectively with the significant and growing problem posed by spam. We take note of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul Melbourne Anti-Spam Memorandum of Understanding and the relevant activities of OECD and ITU. We call upon all stakeholders, to adopt a multi-pronged approach to counter spam that includes, inter alia, consumer and business education; appropriate legislation, law enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.*"

Regardless of methodology undertaken in combating spam in KSA, it was immediately recognized that any proposed framework solution would require certain core information to be present beforehand. Most prominent among this information is:

(1) Official, unified and legal definition of spam in KSA.
(2) Identification of the key stakeholders, and subsequently.
(3) Identification of the size of the problem.

As such a study had never before been conducted in KSA, therefore, it is hoped that the results of this study will be invaluable not only in the development of this national anti-spam national framework, but also as a basis for the work of other researchers in future, Allah willing.

In this study, all pertinent stakeholders were identified, an official definition of spam was proposed and a framework for the collection of spam-related statistics was developed. This framework covers e-mail, SMS and fax and is focused on three aspects. First, the definition of spam and related spam indicators where "spam rate" is defined as the percentage of spam compared to the total number of received messages. Second, the identification of sources for spam related statistics where, in addition to interviews, filters and anti-spam tools used by organizations and ISPs were the main source for determining e-mail spam while gateways and servers owned by mobile service providers were used to calculate SMS spam. Third, the collection of spam statistics achieved by inspecting published reliable data and by conducting survey, interviews and discussions with relevant personnel including CITC, KACST, MOC, MOI, SAMA,[4] companies, financial services institutions, Internet service providers, data service providers, bulk SMS licensees, mobile operators, solution providers and others.

It was decided that the necessary background information needed to formulate an effective national KSA anti-spam policy framework could be broken down into the following studies:

(1) The current state of SPAM in the Kingdom (summarized in brief in this research paper).
(2) A comprehensive international study of noteworthy anti-spam efforts in eight short-listed countries of relevance.
(3) A comprehensive international study of noteworthy anti-spam efforts in international bodies of relevance.
(4) A study of current and emerging anti-spam technologies.
(5) A study of past legal cases in KSA, plus current anti-spam-related legislation in the Kingdom and identification of key stakeholders.

As recommended by the well know international bodies, to combat spam, different areas shall be addressed in the final comprehensive policy framework, such as legal, enforcement, technical, awareness, industry assistance, codes of conduct, etc.

[1] King Abdulaziz City for Science and Technology.
[2] Communications and Information Technology Commission.
[3] The World Summit on the Information Society (WSIS) held in Geneva. 10–12 December 2003.
[4] -CITC, Communications and Information Technology Commission; SAMA, Saudi Arabian Monetary Agency; KACST, King Abdulaziz City for Science and Technology; MOC, Ministry of Commerce; MOI, Ministry of Interior.

By developing an anti-spam framework coupled with robust enforcement, ensuring industry assistance, running awareness programs, implementing technical solutions, ongoing monitoring of spam rates and focusing the control on commercial spam we can reduce the amount of spam significantly in the Kingdom of Saudi Arabia. This study comprises the first step in that direction.

2. Methodology and implementation

This study used a three step approach to collecting the required information on the status of spam in the Kingdom. These three steps were:

Agree on an initial definition of spam that could be used as the basis for collecting information.
Identify and agree to the likely sources of spam related statistics and the stakeholders who could be of assistance in this regard. This was done by exhaustively identifying all stages of the spam lifecycle and then, for each stage of that lifecycle, identifying all key stakeholders.
Collection of the spam statistics from the identified stakeholders. The key method used for collecting the data was questionnaires and interviews targeted at selected organizations, vendors and ISPs. Some additional statistics were also collected by service providers on their SMS gateways focusing on the number of SMS messages received by mobile phones in Saudi Arabia.

2.1. Identification spam lifecycle and stakeholders

The typical spam activity lifecycle can be broken down as follows:

(1) The recipient address (e-mail, fax number and mobile number) is captured and stored in a repository for a specific purpose
(2) The spammer harvests specific address details, which is then used for spamming activities.
(3) The spam message is carried by certain media (ISPs, mobile service providers, etc.).
(4) The message is received by a mail host (mail service provider, banks, etc.).
(5) The end-user (receiver) receives the message.
(6) If required, the receiver reports the spam to the appropriate authority.
(7) The designated authority enforces the applicable laws (prosecution and sentencing).

Key stakeholders are involved in each of the spam activity lifecycle stages. The 7 stages are depicted below (in Fig. 1):

Profiles and examples of some of the stakeholder groups identified above are presented in the following:

2.2. Obtaining personal details

A number of organizations, such as banks, Retailers, ISPs, MSPs, Telcos, Mail service providers, etc. capture and store details of customers or subscribers. These details are mostly captured for specific purposes, which are typically authorized by the associated person. A number of these organizations are bound by internal Privacy policies, which prevent them from using the information for any purpose other than the purpose for which the information was collected. In some cases, some of these organizations may take the approval of the associated person to use these contact details for the purpose of e-marketing. Some of these organizations may also sell contact details of their subscribers to other bodies, who then use them for spamming purposes. The availability of this store of contact information and personal details is often a key source of contact information for spammers.

2.3. Media stakeholders

Having collected relevant information, the spammer then sends the spam messages over certain media to the receivers. The media used for this purpose could vary, and could involve media owned by stakeholders such as Internet service providers, mobile service providers, data service providers, Bulk SMS service providers, etc. These stakeholders are relevant because at times the media owner may knowingly or unknowingly provide the platform for the spammer to carry out his activities.

2.4. Mail host stakeholders

The spam mail is then received by the host of the mail box belonging to the receiver. The mail host could be either a mail

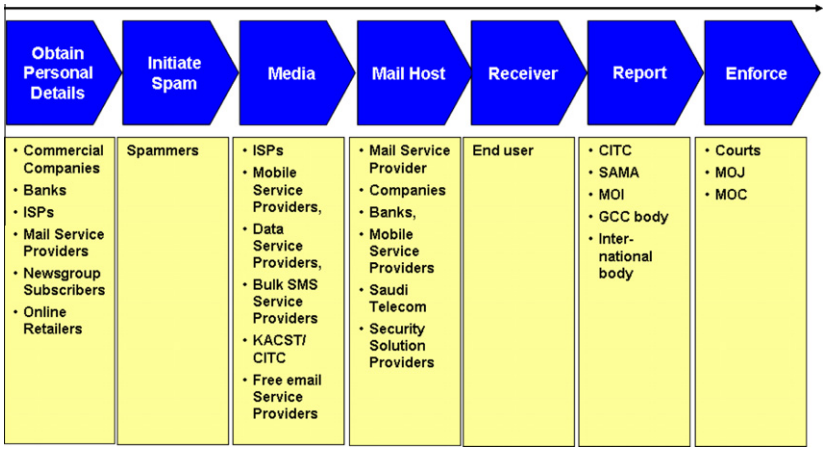

Figure 1 Spam activity lifecycle stages.

service provider or organizations that provide corporate mail service to their employees. These stakeholders are relevant because they often employ filters and such devices to control the spam addressed to their mail service subscribers.

2.5. Reporting process stakeholders

Once the receiver receives the spam message, he may wish to report this incident to a suitable organizational unit within the Kingdom, particularly if some damage was caused as a result of the spam. Typically the organizational unit to whom the receiver can report spam would vary by kind, origin and content of the spam. For example, the receiver may report such spam messages to banks, the company that he/she works with, or relevant Government agencies.

2.6. Enforcement process stakeholders

Once the report is submitted and it is determined that the spammer was guilty of sending the spam to the receiver, the spammer is punished by a stakeholder responsible for enforcement of the anti-spam regulations. The enforcement agencies could vary by severity and type of spam sent and would typically include agencies like Courts and/or relevant Ministries. There are two major enforcement agencies in KSA related to spam. They are the Ministry of Interior (MoI) and the Communications and Information Technology Commission (CITC).

2.7. Summary of stakeholder role and scope

There are a number of stakeholders involved in the spam activity life-cycle. Each of them plays different roles in the context of the spam life cycle. In order to be effective, it is imperative that the anti-spam policy framework should address most, if not all, of these stakeholders. Identification of these stakeholders is also key to effective benchmarking of the state of spam in KSA. This study has short-listed in the following section the key stakeholders most relevant to the goals of this study. Those are the stakeholders who were contacted for participation in this study's questionnaire.

2.8. Stakeholders involved in the questionnaire

The following list represents the stakeholders who were included in the 'current state assessment' research (questionnaire based survey and/or interviews) conducted by the survey team:

Saudi Arabian Monetary Agency (SAMA).[5]
Data service providers (DSPs)/facility based providers (FBPs).[6]
Mobile service providers (MSPs).[7]
Bulk SMS licensees.[8]
Solution providers.[9]
Internet service providers (ISPs).[10]
Companies.[11]
Universities.[12]
Ministry of interior (MOI).[13]
Communications and Information Technology Commission (CITC).[14]
King Abdulaziz City for Science and Technology (KACST)/Internet Services Unit (ISU).[15]

2.9. Questionnaire-based survey results

This section highlights the findings that we generated using the statistics provided by stakeholders in the answers to our questionnaires.

(1) Spam definition question (Fig. 2).
(2) Questions related to the magnitude of the problem (Figs. 3–9).
(3) Questions related to methods of addressing spam (Figs. 10–22).

3. Findings and analysis

3.1. Stakeholders major concerns and recommendations

Interviews were conducted with the identified stakeholders, using structured questionnaires, in order to obtain feedback on their views and concerns on the status of spam in Saudi Arabia. The major concerns and recommendations of the various stakeholders with regard to spam have been summarized in this section.

All stakeholders mentioned the fact that there is currently no central law in Saudi Arabia to regulate spam. However, there are some spam-related provisions that are scattered over different laws and licensing requirements/agreements. For this reason, there are no regulations regarding the collections, use,

[5] The central bank of the Kingdom of Saudi Arabia, charged with supervising commercial banks.
[6] Licensed media stakeholders providing Internet gateway connectivity for ISPs to the Internet.
[7] Licensed to provide the SMS/MMS infrastructure required to transmit and receive messages between mobile phones. All MSPs were interviewed.
[8] More than 90 licensed companies (class B licenses) which allow them to resell SMS/MMS services in bulk from MSPs.
[9] They provide the technical solutions that are critical to reduce spam. Two solution service providers were met while others were contacted via e-mail and over phone (examples: Symantec, Sophos, ISS, CLEAR SWIFT, SurfControl, others).
[10] Licensed to provide Internet connections to corporations, individuals and governmental agencies, and hence, they are the carriers of electronic communications, mainly e-mails. Two major ISPs were interviewed while 15 other ISPs participated in the survey.
[11] Thirty-six companies of varying size and locality were included in the study and detailed meetings were conducted with two of them.
[12] Aside from the vast number of beneficiaries among the students, faculty and staff, university networks are generally vulnerable to hackers using the universities' machines as botnets. As such, universities computers become zombies where spamers find it attractive to launch their attacks.
[13] MOI is the owner of the Anti e-Crime Act and thus plays an important role in combating spam. MOI has recently established a new division in charge of investigating eCrimes. Cooperation between MOI, CITC, SAMA and other stakeholders is critical for ensuring that spam is efficiently combated.
[14] The CITC is charged with regulating the telecommunications sector in the Kingdom. It oversees the application of the Telecommunications Act, its Bylaw and the Ordinance of the CITC.
[15] Serving as the national "Academic/Research sector ISP" in KSA.

and trade of personal contact details such as e-mail addresses and phone numbers. Some stakeholders also highlighted the lack of cooperation between various agencies in combating spam. For instance, SAMA, MOI, and CITC have developed an informal procedure to cooperate regarding spam/phishing related issues. However, there is no formal process in place for handling complaints and forwarding them to the appropriate authorities. It was also raised that there is no code of conduct for ISPs or e-marketers in Saudi Arabia.

Spam e-mails, in addition to being an annoyance are causing capacity, bandwidth and staff performance problems. During the meetings held with the various stakeholders, many points were raised and some stakeholders suggested some technical controls as well.

Some stakeholders suggested that CITC should promote the establishment of Commercial Secure Mail Hosting providers who receive e-mails on behalf of companies and filter them before delivering them to the mail servers of the companies.

3.1.1. ISPs

ISPs highlighted their shortage of technically capable staff. They indicated that they are understaffed and thus are not capable of addressing the spam issue extensively. ISPs also indicated that they install tools/filters to protect the mailboxes of the customers who decide to use the e-mail servers of the ISPs. As such, ISPs do not filter all the traffic flowing through their networks due to the existing constraints in budgets, resources and capacities. However, one of the findings is that ISPs who have deployed RBLs on their routers or Gateways, report a lower spam rate, as do their clients.

3.1.2. DSPs

DSPs highlighted their shortage of technically capable staff. They indicated that they are understaffed and thus are not capable of addressing the spam issue extensively. DSPs also indicated that they do not have existing controls for spam e-mails and they strongly advise that spam filters should be decentralized at the ISP level and below since these filters might introduce degradation in the quality of service offered by DSPs if installed on their backbones. However, DSPs agreed that RBLs might be deployed on their routers to ensure that known spammers cannot send e-mails to users in the Kingdom, yet they stressed on the fact that these blacklists need to be very accurate since they might result in blocking legitimate traffic.

3.1.3. MSPs

Mobile service providers (MSPs) suggested that SMS spam regulations should focus on bulk SMS licenses and should exclude advertisements. They also suggested that it is important to control websites' registries as an ancillary element to setup accountability and to control websites sending SMS spam.

MSPs receive daily huge numbers of SMSes originating from outside Saudi Arabia. Some of these messages are spam messages. Although their current systems do not contain sophisticated filters to identify spam SMSes, MSPs have developed some controls to ensure that bulk SMS sent internationally are inspected and blocked if deemed spam. Additionally, the MSPs are upgrading their systems to ensure that they can apply smarter controls to combat spam. The mobile operators reported that the SMS spam rate ranges between 1.25% and 1.75%. This rate is, however, suspect due to many considerations, among them that MSPs tend to shy away from defining revenue-generating SMS messages, regardless of content, as spam, and thus, deserving of combat.

3.1.4. Bulk SMS service providers

Bulk SMS providers suggested the development and enforcement of an anti-spam law with severe penalties as the best way to control SMS spam. Moreover, in order to know the Bulk SMS providers who originated the message, Bulk companies suggested that this could be achieved by tracking the premium numbers included in the messages sent. The tracking should be done in coordination with the mobile service providers.

3.1.5. SAMA

SAMA took many initiatives targeted at fighting phishing, whether by encouraging the banks to join international organizations to fight phishing, or by coordination the efforts with CITC to block access to the phishing source website. SAMA also does regular follow-ups with banks which have been subject to phishing attacks, after closing the phishing website to assess any possible damage that could have happened as a result. Additionally, SAMA stated that they have strict measures to be undertaken by banks operating under SAMA's license and the Saudi Banking Law. SAMA does conduct regular audits to ensure that all financial institutions are adhering to SAMA's regulations.

Moreover, SAMA has published security guidelines for the banks on its website www.sama.gov.sa and has recorded 72 phishing attacks on Saudi banks during the last year.

SAMA also mentioned that the current cooperation in law enforcement is not efficient as SAMA has to coordinate between MOI and CITC in order to issue an order for blocking a phishing website through CITC. The bureaucracy sometimes causes severe delays before an action could be taken against the offenders.

3.1.6. MOI

MOI suggested that either CITC or the newly established eCrimes Fighting Unit is to be contacted for reporting spam. Then, the case would be forwarded to the Bureau of Investigation and Prosecution who might use the technical skills of other agencies including CITC.

3.1.7. Universities

Universities recognized that their networks and machines are attractive to spammers since they can turn them into Zombies[16]. Thus Universities have deployed various security controls to mitigate the issues of spam. However, some of the universities do not allow the students to use their Laptops to access the Internet using the University networks due to the shortage of existing resources. Once this access is granted, the threats of spam might increase and thus additional security controls might be needed. Universities also suggested that a Cybercrime law should be in place to combat spam. Universi-

[16] A Zombie computer (often abbreviated zombie) is a computer attached to the Internet that has been compromised by a security cracker, a computer virus, or a trojan horse. Most owners of zombie computers are unaware that their system is being used in this way. Zombies have been used extensively to send e-mail spam.

ties also suggested that an awareness program for spam is very critical to educate people.

3.1.8. KACST–ISU

The ISU division in KACST indicated that currently they do not filter the bandwidth provided to universities to clean it from spam, however, they might consider the idea of offering filtered bandwidth to universities especially that universities do not have the required technical resources needed to deploy those technically complex solutions.

ISU stressed on the importance of signing agreements with other countries and already existing international enforcement agencies. ISU suggested the cooperation with regional bodies in the GCC. Moreover, it also suggested that the reporting mechanism should be clear and straightforward while enforcement should be very simple and international cooperation is critical to achieve this.

3.1.9. Companies

Most companies use anti-spam softwares to filter spam e-mails. Although some companies have huge databases of customer related information on their databases, these companies have not invested heavily to protect the secrecy of this information and thus prohibit spammers from harvesting this information. This is also due to the fact that the protection of this information is not enforced by law.

Companies that are hit by spam have not developed programs to educate users on how to use the Internet while minimizing the entities who know their e-mail addresses and thus minimize the probability that spammers can discover their e-mail addresses.

3.1.10. Banks

Banks suggest that control measures and a clear reporting procedure should be enforced in case the spam is originated using a local ISP. Additionally, a formal procedure for reporting phishing complaints is being developed currently in conjunction with the banks as are user education and awareness guidelines.

3.2. Key survey findings

Our findings are divided into three main categories:

Spam definition.
Magnitude of the problem.
The manner in which stakeholders currently address spam.

3.3. Spam definition

One of the key issues which needs to be resolved when dealing with spam is the formal definition of what is meant by the word and when a message is or is not considered to be spam. Without such a formal definition, it would be impossible to measure spam, calculate spam rates, classify spam categories prosecute spam, or perform any useful study or analysis of spam.

Therefore, and due to the absence of any formal and legal definition of spam in the Kingdom of Saudi Arabia, it was deemed necessary to generate a proposed definition which could subsequently be suggested to the participants of this survey with a solicitation of their feedback on its wording.

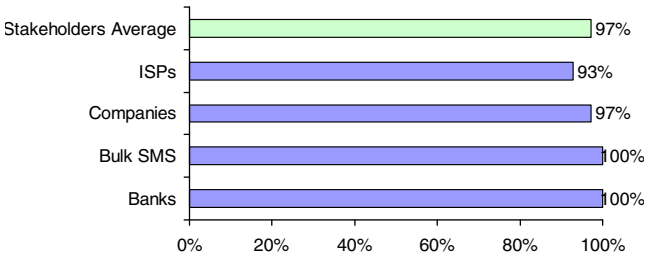

Figure 2 Spam definition agreement.

In order to arrive at an initial suggested formal definition for spam, a preliminary international survey was performed specifically targeting nine prominent and carefully selected countries around the world to gain insight into the definitions adopted by other nations in their anti-spam initiatives. Due to the scope and breadth of that study and the need to remain focused in this one, it was deemed appropriate to separate that study into an independent research paper on international spam best practices and benchmarking, which will, Allah willing, be published in the near future.

Once the preliminary suggested spam definition was formalized, it was introduced into the list of survey questions and opinions were solicited regarding its appropriateness, comprehensiveness and focus. As illustrated in Fig. 2, the majority of stakeholders in Saudi Arabia agree on the definition of spam that we have proposed in our questionnaire (97.4% approval rate). The definition of spam used in the survey was:

> *unsolicited*[17] *bulk*[18] *messages and communications containing commercial, abusive or objectionable content and which are sent out in bulk to people or individuals without their consent by e-mail, fax, or instant messages such as SMS.*

This preliminary definition was also used as a basis upon which the respondents could frame their responses to the subsequent survey questions.

Note: As an aside, this definition was later further slightly refined into its current formal and accepted form by adding the "technology neutrality" concept, greater clarity of the "opt-in" concept, and clearer alignment with the recently-introduced anti eCrimes law to the definition as follows:

> "*Any unsolicited electronic message that contains commercial or objectionable content transmitted without prior consent through any communication media including, but not limited to, e-mails, Mobile Messaging, fax, Bluetooth and instant messaging services.*"

3.4. Identifying key stakeholders

Further, in order to perform a comprehensive national study of spam and its impact, it is necessary to define a representative

[17] Electronic messages that was sent without the stated or inferred consent of the recipient and are of an advertising or promotional nature.

[18] Messages that are sent in numbers exceeding a predefined threshold in a predefined period of time.

and comprehensive grouping of key stakeholders and participants. To this end, much effort was expended in identifying the national entities directly involved in regulating, selling, transmitting, enforcing, restricting, monitoring, generating or receiving spam in KSA. This grouping of key stakeholders was instrumental and pivotal in the success of this survey and the list may further be re-utilized in the future for follow-up surveys in this field.

3.5. Magnitude of the problem

This section of the study shows the magnitude of the spam problem in the Kingdom.

With regard to scope of the problem, it became clear after tallying the results that e-mail suffers noticeably from spam in KSA. International estimates peg spam rates at above 80%[19], with some industry experts' metrics setting the bar closer to 95%[20]. Therefore, although the KSA survey average rate of 51%[21] may appear to be comparatively mild, it is still a significant threat in that one out of every two e-mail messages in KSA on average is a spam message.

Statistics collected from other sources such as companies, was ignored since it was considered that:

> Some of the companies provided guesstimates since they did not procure reporting tools that can generate such information readily.
> Other companies have reported their statistics, however, their spam rate was skewed by the fact that some ISPs do deploy RBLs on their gateways and thus block a substantial amount of spam messages before they reach these companies.

Figures obtained from anti-spam product vendors, such as Message Labs and Symantec, appeared quite close to the numbers obtained from the panel of ISPs. Message Labs[22] reported the spam rate in KSA for the year 2006 to be around[23] 48.3% whereas Symantec[24] reported the spam rate for the year 2006 to be around 59%. Message Labs reports the spam rate for the year 2007 (till July) to be around 42.7%.

Further, it is quite likely that the use of RBLs at some ISPs has skewed-down the actual KSA spam rate.

As regards spam content classification, "Direct Marketing/commercial" rose to the top of the list at 64% making it the number one type of e-mail spam, as shown in Fig. 3. 25% of the respondents considered Sexual e-mail to be the most common type of spam, while only 5% considered religious spam to be a major type of spam received. Accordingly, controlling commercial spam has the potential to reduce the amount of spam substantially.

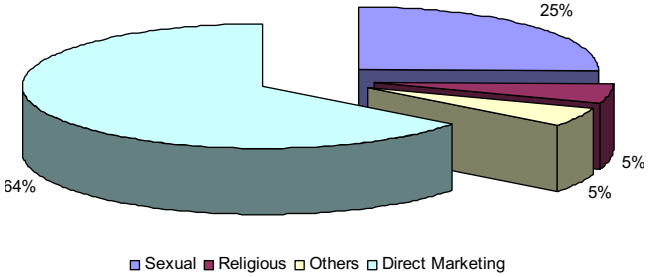

Figure 3 Respondents' views on most common types of spam.

There was no real surprise regarding the dominance of direct marketing and sexual content in spam as this is the general trend worldwide. Further breakdown of direct marketing revealed that the majority of the message contents fell under the "other" category, which appears to indicate a weakness in our initial selection of suggested categories.

Also, since most recipients categorized messages promoting the sale of "Viagra" (or alternatives) under "direct marketing → other" categories rather than under the "sexual" category, perhaps it would be beneficial to study the combination of such content under one "sexual" heading in the future (via printed instructions to the survey respondent). Performing this calculation here, we find that roughly $25\% + (65\% \times 64\%) = 67\%$ of e-mail spam could be classified under the broad heading of "sexual services, products or pictures". In other words, it is a matter of perspective. If we are looking at the issue from the financial vs. non-financial perspective, then "non-financial sexual" content represents 25% of all spam e-mails. However, if we remove the "financial" attribute as a classification criterion, then fully 67% of the e-mail spam messages deal with sexual topics service or products in one fashion or another. Again, this appears to follow the general international trend and is actually not unexpected as almost all of these messages are sources overseas and do not discriminate across country boarders.

On the other hand, at the time of the collection of the raw spam survey statistics (8 months in 2007), SMS spam appears to have been a relatively trivial issue with the reported spam rate ranging between 1.25% and 1.75%[25]. However, due to the high dependence of this study on data voluntarily provided by commercial mobile providers, and due to the lucrative revenue-generating nature of SMS spam to these companies and their narrow focus on combating only foreign-sourced SMS messages (i.e. non-revenue generating SMS spam) in their voluntary spam-combating efforts, therefore, the final accuracy of these numbers may justifiably be called into question.

[19] http://www.messagelabs.co.uk/resources/press/8413.

[20] http://www.barracudanetworks.com/ns/news_and_events/index.php?nid=232.

[21] Multiple ISPs participated in the survey for the duration of 8 months. However, we only considered the statistics of the months where multiple ISPs provided us with accurate numbers. Also, this number represents the spam average across these months.

[22] The data provided by Message Labs are based on statistics and analysis on a range of e-mail security threats worldwide. MessageLabs Intelligence is based on live data feeds pulled from its global network of control towers that scan millions of e-mails daily.

[23] This number was obtained by averaging various spam rates collected from different physical sensors.

[24] The data used in this analysis are based on the spam messages detected by Symantec Probe Network sensors deployed in over 180 countries.

[25] It is interesting to note that at the time of the conduction of this survey, SMS spam was still a relatively novel concept in KSA. One year later, informal observation confirms that the rate of SMS spam has risen dramatically. Possibly over tenfold. It would be beneficial to re-conduct the survey again now to compare the results. Also, it is believed that this study will be of value in providing a fairly accurate estimation of when SMS spam actually began its rise in KSA and in providing an initial base benchmarking value against which we can compare future spam rate values.

The same general reasoning applies to the Bulk SMS Licensees contacted in this survey as the generation of bulk SMS messages is their core business. Strict conformance is not always observed at all times by all these companies to license regulations requiring them to obtain prior consent of the recipient. These companies further state that they receive no more than about 100 complaints per month from end users, however, since the product/service advertisements broadcast by these companies relate to third parties, it is not easy for an end-user to identify the bulk messaging company responsible for sending them the message in question and they will need to expend time and effort to track them down. A task likely not deemed justifiable except by those recipients with the greatest grievances. Thus it becomes clear that the proposed KSA anti-spam framework will need to include provision for clearly identifying the bulk messager to the end user as well as clear, swift and effective opt-out mechanisms.

To be fair, a mobile provider will be justifiably hesitant to classify as spam SMS all messages sent by licensed bulk marketers. The national bulk marketers may or may not have obtained prior approval from the end recipients to receive their messages, but from the mobile company's perspective these national bulk marketing companies have signed commercial agreements with them to utilize their mobile networks to transmit × number of SMS messages at a given monetary rate. Similar contracts do not exist between the mobile provider and the end users, therefore, subsequent individual user complaints are handled on a reactive basis as deemed appropriate.

Regardless, one year down the road (the end of 2008) a general consensus was conveyed both in the public media and on the street that SMS spam had increased dramatically in KSA. This could not be scientifically and objectively confirmed at the time of the publication of this study so it is suggested that a new study be performed to compare the current state with the results published here, and optimally to benefit from the lessons learned in this study with regard to possible conflicts of interest.

Respondents considered that Finance (11%). Sports (8%) and Computer Software related messages (8%), were the predominant types of commercial spam messages. The other types of spam were either related to phishing or education. A big part of the spam messages received were clubbed under the "Other marketing messages". Respondents indicated that by "Other marketing messages" they were referring to messages promoting for the illegal sales of products (e.g. Viagra) (Fig. 4).

As shown in Fig. 5, 78% of companies that responded to the survey believe that the primary impact of spam was on their e-mail server resources. 72% believed that it congested their network. Other major impacts included the time spent by their technical people to deal with spam (61% of the respondents). Surprisingly, only 42% stated that spam reduced employee's performance.

When ISPs were asked to specify the impacts that spam has on their organizations, the results came in as shown in Fig. 6. 67% of ISPs believed that customers were most affected by spam. Bandwidth and productivity were also highly affected as per 42% of the ISPs. Respondents also reported that the bandwidth consumed by spam ranged from 5% to 25% of the total bandwidth.

Fax spam was not considered by any of the respondents to be a major source of spam in the Kingdom. Fig. 7 represents

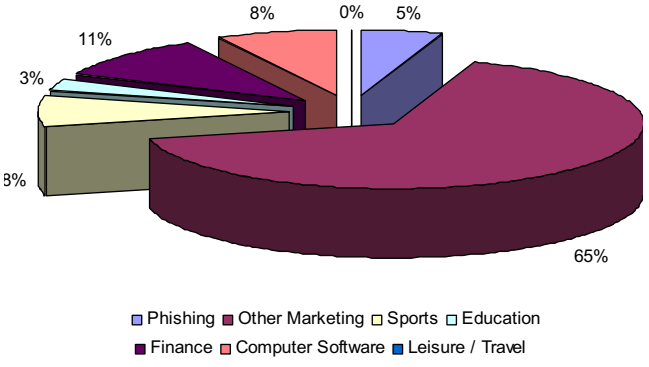

Figure 4 Breakdown of respondents' views on direct marketing types of spam.

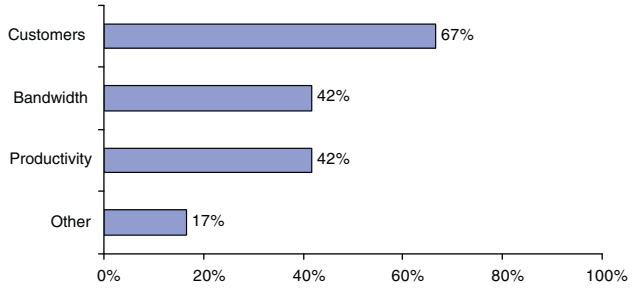

Figure 6 Percentage of ISPs who consider that spam impacted them as per the criteria in the graph.

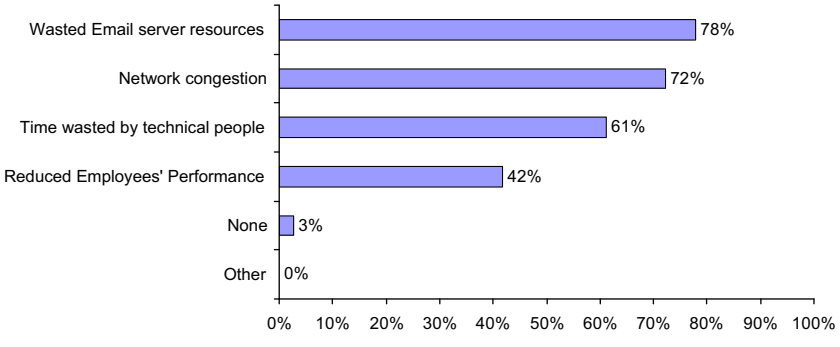

Figure 5 Percentage of companies who consider that spam impacted them as per the criteria in the graph.

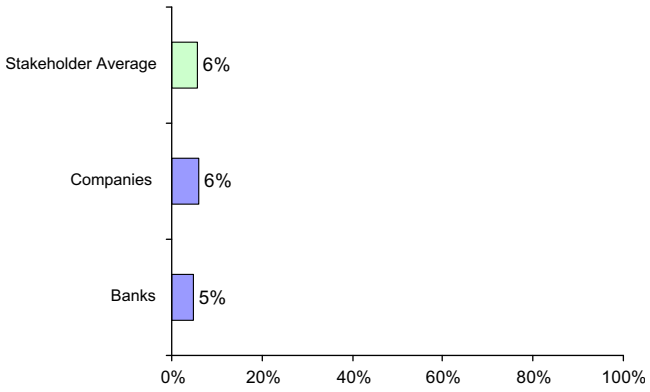

Figure 7 Fax spam received.

the percentage of faxes received that are reportedly considered to be spam. According to respondents, fax spam is not a major issue in Saudi Arabia. Most of the fax spam received tended to be commercial in nature, with 84% of the respondents confirming that commercial spam was the most common form of spam received by fax. So, here again we see the trend toward "Direct Marketing" being the major culprit (Fig. 8).

Bulk SMS providers offer 3 main types of services: product promotions, service promotions, and advertisements on behalf of others. Messages sent through their respective units are usually either Direct Marketing, religious or political as shown in Fig. 9. It is obvious that the vast majority of Bulk SMS Licensees send Direct Marketing Messages.

Interestingly, Bulk SMS Licensees stated that they only receive around 100 complaints per month. Some of them (17%) even state that they donot even receive any complaints. This may be due to the fact that users cannot tell who is the real originator of the SMS that they have received.

Regarding company network resources, it was clear from the responses received that a very significant impact was observed by the participants on their underlying infrastructures (e-mail server, network, etc.) as a result of spam proliferation, up to an observed 78%. Therefore, an effective Anti-spam national policy framework will (Allah willing) have a significant impact on reducing this negative effect and returning the wasted resources to these companies to be utilized in more productive avenues.

It is further revealed from the results that the negative impacts of spam are not confined to internal company infrastructure such as bandwidth utilization and absorbed therein, rather the external ripple effects continue to be far-reaching, materially negatively impacting the end-user and general productivity at rates of up to 67%.

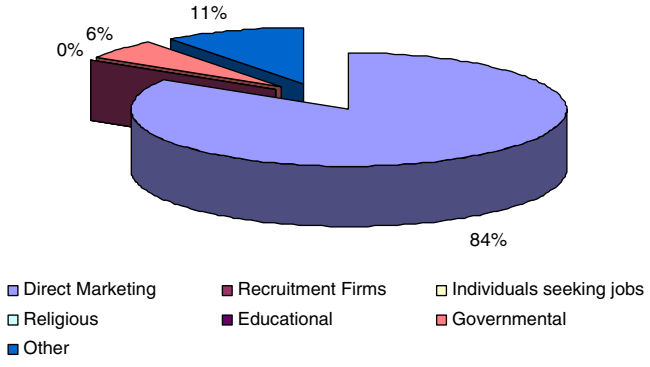

Figure 8 Types of fax spam received.

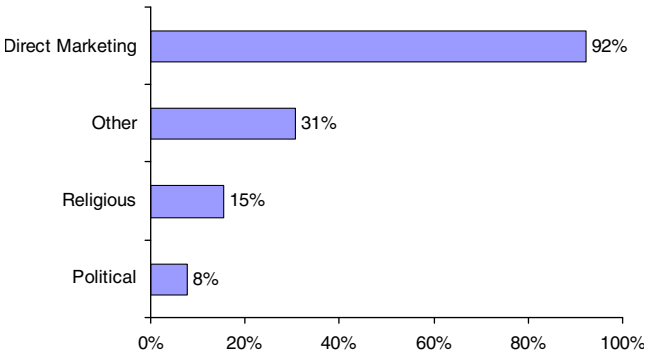

Figure 9 Percentage of bulk SMS licensees who send bulk SMS messages as per the criteria in the graph.[31]

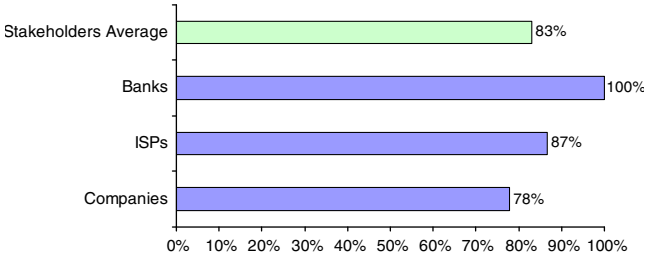

Figure 10 Percentage of respondents who deployed e-mail anti-spam Tools/filters (Incoming).

3.6. The manner in which stakeholders currently address spam

Addressing the issue of spam needs a multi-level approach, not just deployment of tools and filters to prevent spam. There is also a need to have proper processes in place to report and deal with spam on a higher level as well as the availability of proper awareness and education to end-users and customers. To be able to present a comprehensive view of how stakeholders currently address spam in the Kingdom, we have looked into three areas.

First, we looked at the existence of anti-spam solutions. This also included the location at which the solution is deployed and how the solution is configured. Second, we looked at processes that are in place to control spam. This includes procedures to report spam to other agencies. Finally, we looked into whether stakeholders carry out spam awareness programs within their organizations.

3.6.1. Anti-spam tools

It is revealed in Fig. 10 that the majority of respondents are concerned about spam and thus they employ one or more layers of spam technical counter-measures (83% average). Natu-

[31] According to the stakeholders, examples of others include, but are not limited to, the following categories, Sports, Entertainment services, Education services, Subscription services from mobile operators.

rally banks featured the highest coverage rate at 100% sector coverage. This is to be expected due to the sensitivity of their core business and the potential threat spam poses to that core business and clientele. What was surprising though was that not all ISPs employ such countermeasures even though it is commonly expected that not only would ISPs be among the companies most technically adept and likely to recognize the threat posed by spam to themselves and their customers, but that such a service is commonly expected as an integral part of an ISPs core added-value services. Therefore, although at first glance 87% coverage for ISPs may appear to be a high percentage, it is indeed quite low for this sector. Further, it was discovered that ISPs appear more concerned with protecting their internal e-mail accounts (47% deployment of e-mail server-level countermeasures) than with preventing the usage of their networks to relay spam on to others (only 13% e-mail gateway countermeasures).

The 78% adoption of anti-spam countermeasures in "companies" indicates a fairly high awareness level in the private sector in general.

In general, it was also observed that on average more survey participants are likely to filter incoming e-mails for spam (83%) than are likely to filter outgoing e-mail for potential spam generated on their own systems and networks targeting others (51%). Thus, taking into consideration the rampant software piracy problem observed in KSA, these two factors combine to make KSA a fertile breeding ground for bot-nets and zombies.

In the case of ISPs, in addition to the fact that most of the ISPs do not filter the e-mail traffic sent by their customers without passing through the ISP's e-mail server, not all ISPs check whether their own mail servers are generating spam. Fig. 14 illustrates this point.

Detecting spam is an automated process involving automatic live inspection of massive numbers of electronic messages followed by an automated response when a potential spam message is detected. The survey classified the possible responses as being either "tag and deliver," "delete," "quarantine," "no tool," or "other". "Delete" is obviously the most dangerous approach as it potentially can result in irretrievable loss of important messages if the anti-spam program wrongly classifies such an e-mail as spam (false-positives). We notice, however, that "delete" is applied more in ISPs (where the e-mail is directed not to the company itself but to its customers) than in banks or private companies (where the e-mail is directed to their own employees). It appears, therefore, that the more "personal" the status of the e-mail the more likely the entity is to default to "quarantine" as opposed to "delete". "Tag and deliver" features a more uniform distribution across survey participants (13–17%) and places a higher filtering requirement on the end user in addition to an assumed higher "technical savvy" level at the end-user level to deal appropriately with potential spam phishing or malware threats.

Therefore, on average, most survey participants prefer to quarantine suspect spam messages and have qualified experts manually deal with them later on. "Tag and deliver" and "delete" tie for second place and appear to come down to internal policy regarding whether they trust end users or the expert system more in making the final decision.

Another important finding that our survey revealed was the location where the anti-spam solution is deployed to filter incoming traffic. Stakeholders average show that almost the same percentage of respondents deploy tools on their servers[26] (37%) and on their gateways (36%).

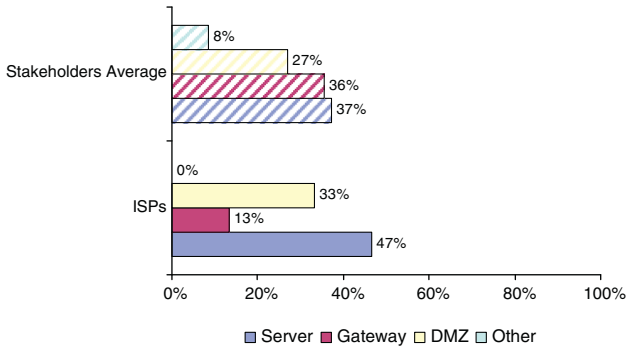

Figure 11 Percentage of respondents who instal their anti-spam Tool/Filters (Incoming) as per the criteria in the graph.

However, as indicated in Fig. 11, ISPs tend to have a different approach. Most ISPs tend to deploy anti-spam solutions on their servers (47%) in order to protect the mailboxes that they host on their servers, while they tend to focus less on protecting or filtering the traffic going through their network. Only 13% of the ISPs tend to deploy anti-spam solutions on their gateways. This means that spam originating or targeting the clients of the ISPs can pass through the network of the ISPs' without being detected or filtered.

Fig. 12 shows that banks and companies prefer to quarantine the suspected spam e-mail messages. ISPs, on the other hand, are divided as to whether to delete the e-mail messages that are suspected to be spam or whether they quarantine them.

Real-time blackhole lists (RBLs)[27] are considered to be efficient in blocking a big percentage of spam e-mails. These lists need to get updated regularly and it also needs regular maintenance in order to ensure that legitimate traffic is not blocked accidentally. In our survey, we also checked if stakeholders utilize RBLs alongside their anti-spam solutions. Sadly however, as seen in Fig. 13, we can see that on average in KSA, only 17% tend to use RBLs separately from their anti-spam solutions. A higher percentage is shown in case of banks (25%). The reason for the low adoption rate is not known and it is suggested that this could be a prime target for an awareness campaign. It may be that the reason for the low adoption rates is the fear of the possible negative effects of blackholing entire networks, or it may be that the participants simply are not familiar with this technology. In any case, RBLs are a proven technology and an awareness campaign is likely warranted.

Looking at the location where the tools are implemented on the outgoing traffic, our survey shows that only 8% of average stakeholders are concerned with protecting the outgoing traffic on their gateways and in the case of ISPs only 13% are con-

[26] When the anti spam solution is deployed on the server, only incoming and outgoing e-mails are inspected and cleaned. Whereas, when the solution is deployed on the gateway, then all the traffic flowing out or into the network is inspected and cleaned. For instance, Zombies might send e-mails that pass unidentified by a server-based solution.

[27] Realtime Blackhole List (RBL) is a list of IP addresses whose owners refuse to stop the proliferation of spam. The RBL usually lists server IP addresses from ISPs whose customers are responsible for the spam and from ISPs whose servers are hijacked for spam relay.

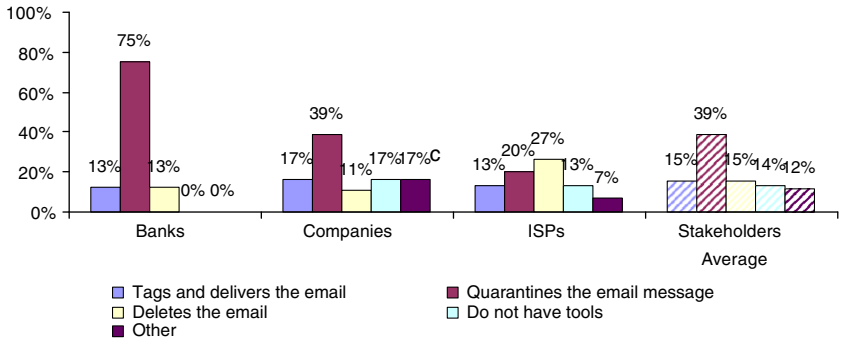

Figure 12 Percentage of respondents who configure their anti-spam tools as per the criteria in the graph.

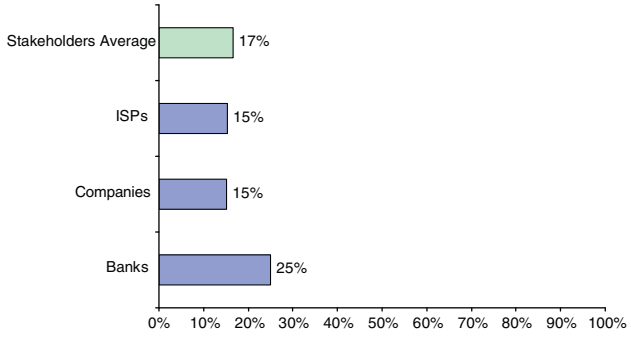

Figure 13 Percentage of Respondents who use a RBL solution separately from the anti-spam Solution.

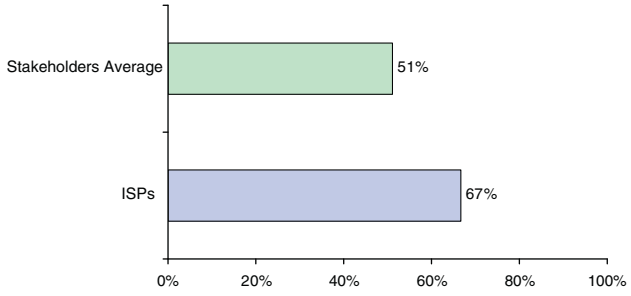

Figure 14 Percentage of respondents who deployed e-mail anti-spam Tools/filters (Outgoing).

cerned with protecting their gateways. This means that if a subscriber instals a mail server, he/she can send spam e-mails undetected. Additionally, this means that spam bots can send spam e-mails undetected. Figs. 15 and 16 give a clearer picture of the situation.

3.6.2. Processes to control spam

The second aspect that we have covered in our survey was the processes that stakeholders have to control spam. This includes dealing with spam initially, spam reporting procedures, any Acceptance Use Policy (AUP) with customers and code of conduct among entities.

Our survey has showed that in the absence of a formal complaints reporting process, it is not surprising (contrary to banks) that most of the organizations deal with spam internally or do not do anything about spam complaints. Around

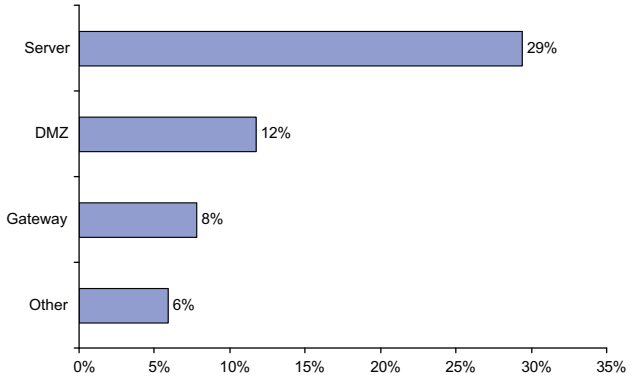

Figure 15 Percentage of respondents who installed their anti-spam Tools/Filters (Outgoing) as per the criteria shown in the graph.

17% of stakeholders do not even have a proper process to deal with spam as we can see from Figs. 17 and 18.

However, the observation is different in the case of banks. Fig. 17 shows that almost half the banks have procedures in place to report phishing complaints to CITC and SAMA. By developing an anti-spam framework it is expected that other industry sectors will develop such processes as well to report spam.

In our survey, we also tried to confirm the views of stakeholders on the best method to combat spam. As indicated in Fig. 19:

- 32% of the stakeholders see that having an anti-spam law was the most effective manner in which their organizations could combat spam.
- 26% of stakeholders also agreed that having a proper code of conduct between service providers would help substantially in preventing spam, though interestingly, only 13% of ISPs believed that having a code of conduct among them will help in combating spam.[28]
- 24% of stakeholders (especially ISPs and Companies) saw that deploying anti-spam tools was a sufficient measure to prevent spam.

[28] Possibly, this is because ISPs are aware of the fact that having a code of conduct with no enforcement and audit will not help to reduce spam.

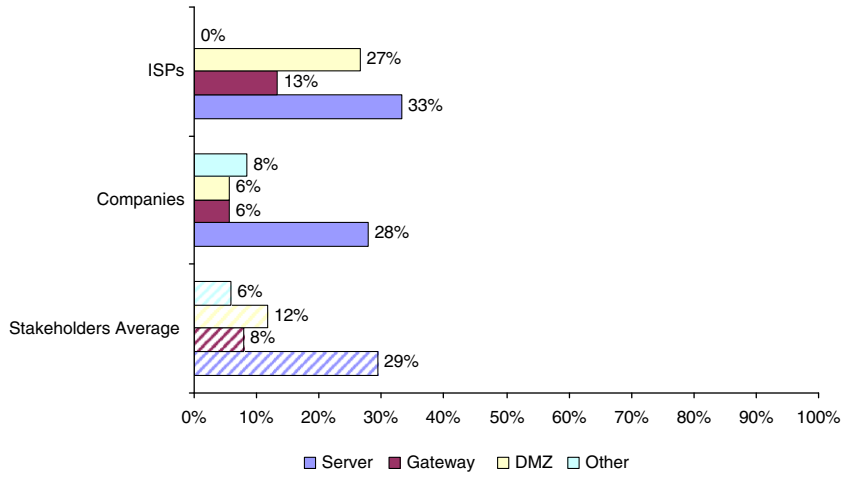

Figure 16 Percentage of respondents who instaled their anti-spam Tools/Filters (Outgoing) as per the criteria shown in the graph by Stakeholders' types.

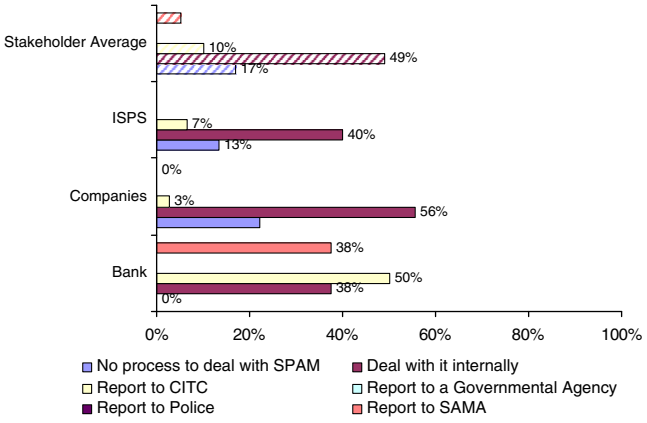

Figure 17 Percentage of the stakeholders who take one of the actions listed in the graph when spam is detected by stakeholders' type.

- 15% of stakeholders agreed that having strict eMarketing rules, including possibly a code of conduct, between e-marketing service providers could help in controlling spam.[29]

This led us to have a look at two other aspects: do service providers ensure that their customers do not abuse the services offered to them, and do service providers cooperate among each others in combating spam? First, we noticed in our survey that 46% of service providers (Fig. 20) do not have any anti-spam provisions in their Acceptance Use Policy (AUP). The inclusion of such clauses can help greatly in controlling spam originating from Saudi Arabia. Second, we have also discovered that 93% of service providers (Fig. 21) are not aware of any existing code of conduct among service providers. This means that there is no cooperation between service providers to control spam.

[29] This reflects the importance of the industry assistance in the battle against spam. Although legislation is critical, having an industry-specific guideline which is more customized to a specific industry is of great importance.

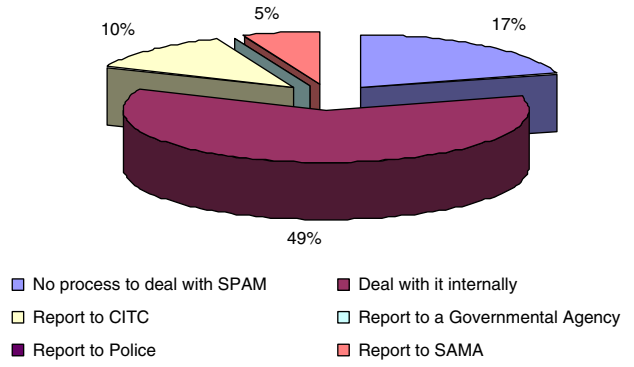

Figure 18 Percentage of the stakeholders who take one of the actions listed in the graph when spam is detected.

3.6.3. Spam awareness programs

Finally, in this survey we tried to identify the level of awareness that stakeholders provide to their customers/employees. The results were very surprising as we can see from Fig. 22. The stakeholders' average of 24% shows that organizations are not putting much effort in educating their employees and customers on how to deal with spam, revealing a prime candidate for a quick win action plan. However, banks have scored very high (86%) in conducting awareness programs to their employees and customers.

4. Conclusions and recommendations

The purpose of this study, commissioned by the Communications and Information Technology Commission, is to ascertain the magnitude of spam in the Kingdom of Saudi Arabia, its formal definition and the key stakeholders involved. The focus of the study was to obtain a good understanding of the issue of spam within Saudi Arabia. This study comprises one core module of an overarching "Anti-spam policy framework study" aimed at providing a comprehensive multi-tiered solution for handling spam in Saudi Arabia based upon best international practices, current situation and national requirements.

A wide swath of relevant stakeholders was contacted during the course of this study in commercial, governmental and

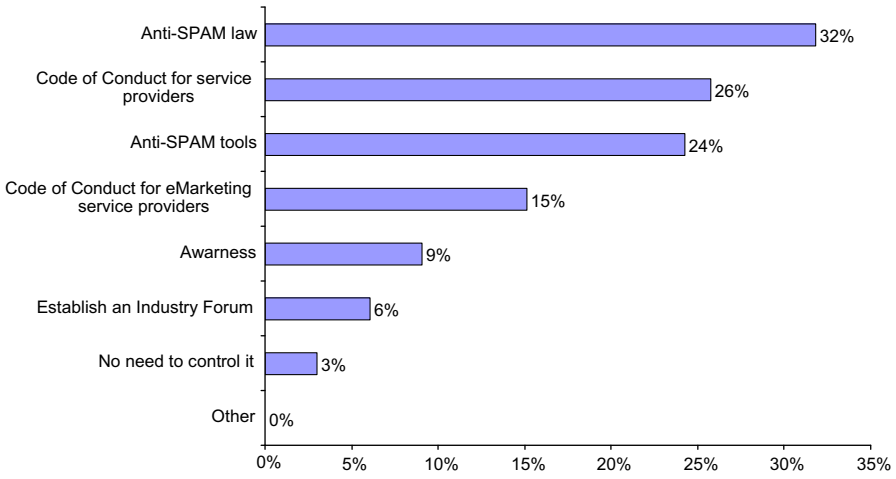

Figure 19 Stakeholders' View on How to Combat spam.

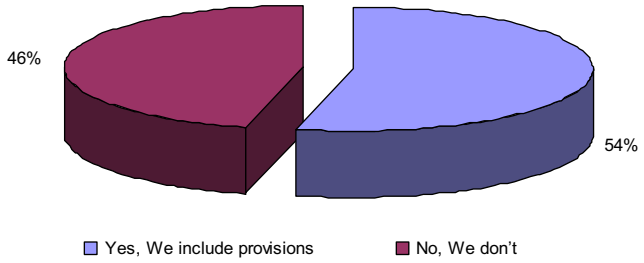

Figure 20 Provisions in the Acceptable use section of the contracts restricting sending of spam.

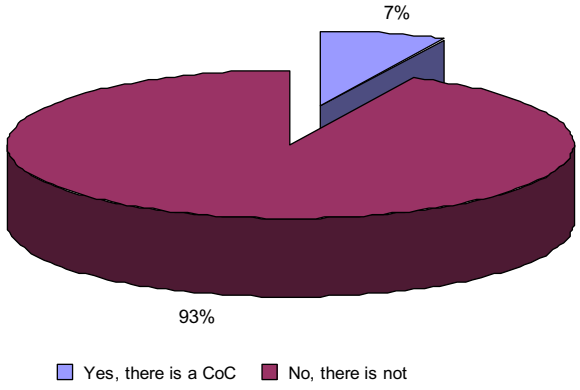

Figure 21 Existence of an inter-ISP code of conduct for spam?

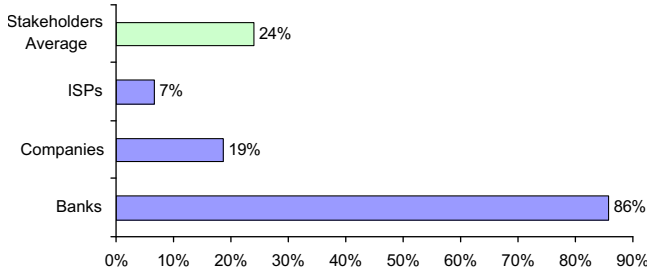

Figure 22 Stakeholders running an Awareness Program.

academic organizations via questionnaires, interviews, and meetings. The study covered multiple transmission mediums of spam such as fax, SMS and e-mail, multiple categories based upon content, such as phishing, sports, direct marketing, religious, sexual, and multiple others, and finally the state of spam countermeasures and awareness overall in these organizations. An additional benefit of this study was to formalize a universally accepted definition for spam and also highlights some of the stakeholders' concerns and recommendations regarding spam.

During this study, all pertinent stakeholders in a proposed "national Anti-spam framework" were identified and a framework for the collection of spam-related statistics was developed. This framework covers e-mail, SMS and fax and is focused on three aspects. First, the definition of spam and related spam indicators where "spam rate" is defined as the percentage of spam compared to the total number of received messages. Second, the identification of sources for spam related statistics where, in addition to interviews, filters and anti-spam tools used by organizations and ISPs were the main source for determining e-mail spam while gateways and servers owned by mobile service providers were used to calculate SMS spam. Third, the collection of spam statistics achieved by inspecting published reliable data and by conducting survey, interviews and discussions with relevant personnel including CITC, KACST, MOC, MOI, SAMA[30], companies, financial services institutions, Internet service providers, data service providers, bulk SMS licensees, mobile operators, solution providers and others.

Although the spam rate differs depending on where the spam is being measured, spam appears to be a serious problem in the Kingdom of Saudi Arabia. According to the data gathered by ISPs, the average e-mail spam rate in the Kingdom was 54%. On the other hand, fax spam was not considered to be a major source of spam with less than 6% spam rate. The Direct marketing messages constitute the major type of spam received in the Kingdom reflecting the majority of commercial spam in the globe. As for the SMS spam, mobile operators reported that the SMS spam rate ranges between 1.25% and 1.75%,

[30] CITC, Communications and Information Technology Commission; SAMA, Saudi Arabian Monetary Agency; KACST, King Abdulaziz City for Science and Technology; MOC, Ministry of Commerce; MOI, Ministry of Interior.

Table 1 Breakdown of SPAM rates in KSA.

	E-mail spam rate	Dominant spam type	Fax spam rate	SMS spam rate	Using RBLs	Spam tools deployed
Average	54%	Commercial	6%	1.25–1.75%	17%	83%

although it was informally observed one year after the conduction of this survey that the SMS spam rate appears to have risen dramatically, possibly over tenfold, and it would, therefore, be beneficial to re-conduct this survey to compare results as it appears that we have hit the leading edge of the SMS spam wave in KSA in this survey.

The main findings are summarized in the Table 1.

Spam e-mails, in addition to being an annoyance to individuals, cause capacity, bandwidth, and staff performance problems. While most of the companies believe that the primary impact of spam was on their e-mail server resources, network, and time wasted, ISPs considered that their customers were most affected by spam. Bandwidth and productivity were also highly affected.

Considering the impact of spam in the Kingdom, it appeared that most organizations, with the exception of banks, did not expend much effort in educating their employees and customers on how to deal with spam. Most banks conduct awareness programs to their employees and customers.

Noticeably, almost 83% of stakeholders have tools targeted at combating spam. However, it is worthwhile noting that ISPs focus on filtering the e-mail traffic hitting the mail servers hosted in the ISP's Data center. They do not filter all traffic (especially outgoing traffic) due to the existing constraints in budgets, resources and the shortage of technically capable staff. Indeed, ISPs employing Real-time blackhole lists (RBLs) reported lower spam rates.

With the absence of a formal complaints reporting process, it is not surprising that most organizations deal with spam internally or even ignore the spam complaints. On the other hand, the observation is different in the case of banks where half of them have procedures in place to report phishing complaints to CITC and SAMA.

When it comes to industry, it was obvious that there is no code of conduct for ISPs or e-marketing in Saudi Arabia. Moreover, half of the service providers do not have any provisions in their acceptable use policy (AUP) covering spam.

As recommended by the well-known international bodies, to combat spam, different areas shall be addresses, such as legal, enforcement, technical, awareness, industry assistance, etc. According to the majority of stakeholders, the legal side is of most importance to combat spam in the kingdom while having a proper code of conduct between service providers would help substantially in preventing spam.

As indicated by the study, spam constitutes a serious problem as being an annoyance to people, organizations and service providers. As mentioned, there is little awareness of spam, no codes of conduct for service providers and e-Marketers. Moreover, stipulations provided through licenses granted to ISPs, bulk SMS service providers and Bluetooth providers are not audited or enforced.

This justifies the need to develop an anti-spam framework for the Kingdom of Saudi Arabia. By developing an anti-spam framework coupled with robust enforcement, ensuring industry assistance, running awareness programs, implementing technical solutions, ongoing monitoring of spam rates and focusing the control on commercial spam we can reduce the amount of spam significantly in the Kingdom of Saudi Arabia.

Spam e-mails, in addition to being an annoyance to individuals, cause capacity, bandwidth, and staff performance problems. While most of the companies believe that the primary impact of spam was on their e-mail server resources, network and time wasted, ISPs considered that their customers were most affected by spam. Bandwidth and productivity were also highly affected.

Considering the impact of spam in the Kingdom, it appeared that most organizations, with the exception of banks, did not expend much effort in educating their employees and customers on how to deal with spam. Most banks conduct awareness programs to their employees and customers.

Noticeably, almost 83% of stakeholders have tools targeted at combating spam. However, it is worthwhile noting that ISPs focus on filtering the e-mail traffic hitting the mail servers hosted in the ISP's Data center. They do not filter all traffic (especially outgoing traffic) due to the existing constraints in budgets, resources and the shortage of technically capable staff. Indeed, ISPs employing Real-time Blackhole Lists (RBLs) reported lower spam rates.

With the absence of a formal complaints reporting process, it is not surprising that most organizations deal with spam internally or even ignore the spam complaints. On the other hand, the observation is different in the case of banks where half of them have procedures in place to report phishing complaints to CITC and SAMA.

When it comes to industry, it was obvious that there is no code of conduct for ISPs or e-marketing in Saudi Arabia. Moreover, half of the service providers do not have any provisions in their acceptable use policy (AUP) covering spam.

Where to go from here? Action is required to utilize this information in the development of a targeted national anti-spam policy framework which will utilize the above spam definition and findings to (Allah willing) effectively combat spam in the Kingdom of Saudi Arabia. It is also suggested that further benchmarking studies be conducted in line with this one to gauge the effectiveness of the application of that policy framework and the possible need to redirect or fine-tune it in order to best achieve the envisioned goals.

References

Royal Decree number 163 dated 24/10/1417H (4th Mar 1997).
Royal Decree number 229 dated 13/180/1425H (27th Sep 2004).
World Summit on Information Technology, Declaration of Principles, WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003.
World Summit on Information Technology, Geneva Action Plan, WSIS-03/GENEVA/DOC/0005, Geneva, 12 December 2003.
World Telecommunications Standardization Assembly, Resolution 51 – Combating spam, Florianopolis, 5-14 October 2004.
World Summit on Information Technology, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, Tunis, 18 November 2005.
World Summit on Information Technology, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, Tunis, 18 November 2005.