Webology, Volume 4, Number 1, March, 2007

Home	Table of Contents	Titles & Subject Index	Authors Index

A Study of Email Spam and How to Effectively Combat It

Mansoor Al-A'ali
Ph.D., Department of Computer Science, College of Information Technology, University of Bahrain, PO Box 32038, Kingdom of Bahrain. E-mail: malaali (at) itc.uob.bh

Received December 2, 2006; Accepted January 15, 2007

Abstract

This paper presents the results of researching the issues pertaining to email spam on Bahrain's email society and how to combat it. We have surveyed the status of spam amongst the Bahraini community through a carefully prepared questionnaire and studied the effects of spam on the social and economical welfare of Bahrainis. The research results stress the need to regulate spam spread through the introduction of a spam law. The overwhelming majority of the Bahraini email community expresses concern with receiving spam but some would still prefer to continue to receive some sort of controlled spam especially commercial advertising spam. The paper addresses the different concerns expressed by the email community and measures the levels of these concerns in terms of age, gender, work productivity. This paper is aimed at setting the pace for regulating and raising the level of awareness of email spam in the Arab countries.

Keywords

Spam; Spamming; Unsolicited email; Email pornography; Email ethics; Arab countries

Background

Email has become one of the most frequent means of communication with customers, employees and friends. However, the fact that it is generally a free form of communication for the sender, has made email one of the favored means of soliciting customers for a wide variety of goods ranging from financial services to pornography and drugs. These days, unsolicited commercial email (spam) makes a sizable percentage of emails. You can get spammed for a wide variety of reasons: commercial, personal, criminal, religious and political.

Checking spam has become part of our daily life such that unsolicited bulk emails have become unmanageable and intolerable. The situation is such that bulk volume of spam emails delivering to mail transfer agents is equivalent to the effect of denial of services (Wu et al., 2005; Zhang, 2004). Spam provides a real threat to our computer systems and drain systems and people resources (Hinde, 2002). Spam consumes bandwidth, disk space and there is a concern that it affects productivity at work, it can expose children to pornography and not to mention that it is very annoying if it takes the major bulk of your email account and prevents you from receiving important emails because there is no space left in your inbox (Hammonds, 2003). Spam emails have become a serious technological and economic challenge. So far we have been reasonably able to resist spam emails and use the Internet for regular communication by deploying complementary anti-spam approaches. However, if we are to avert the danger of losing the Internet email service as a valuable, free, and worldwide medium of open communication, anti-spam activities should be performed more systematically than is done in current, mainly heuristic, anti-spam approaches. A formal framework, within which the modes of spam delivery, anti-spam approaches, and their effectiveness can be investigated, may encourage a shift in methodology and pave the way for new, holistic anti-spam approaches. In this context, the effectiveness of anti-spam approaches in terms of coverage of spamming modes need to be assessed (Schryen, 2006).

Technological progress has greatly enhanced the freedom of speech, and less so the freedom of silence (Hoanca, 2005). With this tilted balance, the implications of freedom of silence on information security are more and more apparent: computer crimes are increasingly using misleading speech, for example phishing emails and denial of service. The implications of the freedom of silence, and the evaluation of the technological and legal solutions were studied in (Hoanca, 2005). Technology-supported speech can more readily be contained by appropriate defending technologies than by legal means.

As adoption of VoIP service increases, concern about spreading VoIP spam is also increasing. The applicability of traditional spam regulations to VoIP spam was studied by (Park et al., 2006). They chose several representative countering spam regulations - opt-out, opt-in, labeling and pricing. As the result of their analysis, they see that the applicability differs according to the type of regulation and the type of VoIP spam.

In view of the recent enactment of anti-spam legislation in the US (the Can-Spam Act) and South Korea (Information & Communications Act), which are two of the largest sources of spam in the world, some researchers claim that the runaway increase in spam cannot be stemmed by technical change alone. Although most see spam as a personal problem, some suggest it is a social problem that needs a social response, although it is a fact that traditional social responses - law, courts, and the judiciary seem to work poorly in cyberspace. Whitworth and Whitworth (2004) propose bridging the gap between society and technology by applying social concepts to technology design.

Email advertising was discussed by Gopal et al. (2006). Their analytical model examines the incentive structures for all participating entities, and derives pricing strategies, profit implications and characteristics of the email lists. They develop and model a form of price discrimination; they term sequential elimination price discrimination that can be practiced via email. Their results indicate that the transactions facilitated by the admediary can create significant value whereby every participating entity realizes increased benefits. These findings underscore the potential of admediation to restore email as an effective communication media for online advertising. Along with other business functions, there has been a remarkable boost in online-marketing activity, with companies attempting to develop new methodologies to more effectively market their wares online.

The sending of unsolicited emails is an inexpensive form of direct marketing. It can reach a broad public and the costs are mostly borne by the receiving end, paying for the Internet connection. Specific software packages make it possible to collect large numbers of email addresses through the Internet. Such so called harvesting tools systematically gather email addresses from discussion groups and websites. It is also possible to buy lists of email addresses from professional 'collectors' or service providers.

The truth is that spam or junk email is seen as an extremely rude form of email marketing. It can be defined as: 'The practice of sending unsolicited emails, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact, and whose email address was found in a public space on the Internet, such as news group, mailing lists, directory or website'.

Spam statistics

Spam statistics are on the rise and it is difficult to put the spam problem in concrete figures. In 1997, America Online (AOL) estimated that 5-30% of its 10 million email messages per day were spam. That amounted to "only" 0.5-3 million spam messages per day (Oda et al., 2003; Hoanca, 2006). According to company news, the average daily number of spam messages peaked in 2003 at 2.4 billion, but dropped to "only" 1.2 billion by 2004. These figures refer to messages recognized as spam and blocked at the AOL gateway, not messages that actually reached the users' inboxes. According to the same AOL report, the amount of spam reported by users (spam that actually reached their inboxes) dropped by 75% from 2003 to 2004. Even this seemingly encouraging trend indicates an almost 100,000% increase in spam volume from 1997 to 2004. There are several costs associated with spam. First, the sheer volume of unwanted email is lowering the productivity of email users by an estimated 1.4-3.1% (Hoanca, 2006), a significant loss. The cost of transporting and delivering spam is not borne by spammers, but by ISP's and ultimately passed on to end-users.

Email is now the vehicle for delivering viruses and phishing attacks, which can lead to data loss, financial losses or even identity theft. Also, the use of filtering to reduce spam has led to the risk of false positives where legitimate and sometimes very important emails do not get delivered. Problems with false positives in email filtering have led to a decrease of users' confidence in email as a communications medium, and in some cases to a higher churn rate among ISP customers.

In an estimate made in a European Commission study on unsolicited commercial communications and data protection (Schaub, 2002), it was estimated that junk email costs Internet users 10 billion Euros a year world wide. This study investigated email marketing and the legislative approach of the European Union with regard to it. It is virtually impossible to make an exact calculation of the costs caused by junk email. Even so, this estimate indicates that there is a problem at hand. According to Interactive Advertising Bureau, online advertising revenue in the U.S. totaled nearly $2.99 billion in the second quarter of 2005, up more than 26% from the same period in 2004, and increased 6.6% over the first quarter of 2005. For all of 2004, this number totaled $9.6 billion, up 31.5% from the 2003 total of $7.3 billion. As the number of Internet users, estimated at 729.2 million as of March 2004, and continues to grow, this trend is expected to continue (Gopal et al., 2006).

From all indications, it does not seem like the tidal wave of spam will subside in the near future (Grimes, 2004). Some spam industry experts estimated about two trillion spam messages were sent in 2003. In a June 2003 *USA Today* article, one of the busiest spammers in the USA, Ronnie Scelson, known as the "Cajun king of spam", says he "spits out 60 million to 70 million ads a day, or about 2 billion ads a month". According to the *Spamhaus Project* (www.spamhaus.org) "90% of all spam received by Internet users in North America and Europe is sent by a hard-core group of under 200 spam outfits".

Spam Protection techniques

Anti-Spam Laws

The United States of America has both a federal law against spam and a separate law for each state. Many individual states have their own spam laws, e.g., Alaska, Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon., Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin and Wyoming. The European Union has its anti-spam law. Each of the following European countries has its own spam law: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden and the United Kingdom. Other countries with anti-spam laws are: Argentina, Australia, Brazil, Canada, Czech Republic, India, Japan, Russia, South Korea and Yugoslavia. Like all other Arab countries, Bahrain has no spam law which puts the Bahraini public and Bahraini organizations at risk from open spam attacks from any source.

Recent amendments to the Virginia Computer Crimes Act are significant for two reasons. First, they contain anti-spam provisions which are more robust than most. Second, Virginia is the home state of several major Internet service providers including America Online and it is estimated that around half of all Internet traffic flows through the state. It is therefore suggested that the potential jurisdictional reach of the legislation is enormous both within and outside the U.S. Nevertheless, enforcement will always be a problem (Hammonds, 2003). We have selected Virginia State law as an example of anti-spam laws. Figure 1 gives an excerpt from that law.

Figure 1: Excerpt from Virginia Spam Law

18.2-152.3:1. Transmission of unsolicited bulk electronic mail; penalty.
VIRGINIA CODETITLE 8.01. CIVIL REMEDIES AND PROCEDURE CHAPTER 9. PERSONAL JURISDICTION IN CERTAIN ACTIONS SECTION 8.01-328.1 (2003)
A. *Any person who:*
1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or
2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. *A person is guilty of a Class 6 felony if he commits a violation of subsection A and:*
1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or
2. The revenue generated from a specific UBE transmission exceeded $1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded $50,000.

C. *A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.*

Anti-Spam filtering

In a paper by Wu et al. (2005) an anti-spam system which utilizes visual clues is proposed which determines whether a message is spam. They analyzed a large collection of spam emails containing images and identified a number of useful visual features for this application.

Garg et al. (2006) suggest that leveraging social networks in computer systems can be effective in dealing with a number of trust and security issues. Spam is one such issue where the "wisdom of crowds" can be harnessed by mining the collective knowledge of ordinary individuals. In their paper, they present a mechanism through which members of a virtual community can exchange information to combat spam. Previous attempts at collaborative spam filtering have concentrated on digest-based indexing techniques to share digests or fingerprints of emails that are known to be spam. They further recommend users to share their spam filters, thus dramatically reducing the amount of traffic generated in the network. The resultant diversity in the filters and cooperation in a community allows it to respond to spam in an autonomic fashion. As a test case for exchanging filters they use the popular SpamAssassin spam filtering software and show that exchanging spam filters provides an alternative method to improve spam filtering performance (Garg et al., 2006).

Some researchers have been trying to separate spam from legitimate emails using machine learning algorithms based on statistical learning methods. A spam filtering model was proposed based on support vector machine (Islam et al., 2005).

We need to also develop an approach towards spam filtering that seeks to exploit the nature of spam messages that allow them to be classified into different communities. The working of a possible implementation of such approach needs to be evaluated. Some researchers suggest that users may want selective blocking of spam mails based on their interests (Deepak & Sandeep, 2005).

Approximately 40% of all email in the Internet is spam, and its volume is growing rapidly. Blackhole list and mail filter are the main measures to defend the spam at present. But as a matter of fact, the situation of spam flooding tends to be more and more terrible. Technology of anti-spam based on flows, which could detect spam and abnormal email behaviors in the network, according to the type of email flows and their respective characteristics (Qiu, 2004).

A new spam detection technique using the text clustering based on vector space model was proposed in (Sasaki & Shinnou, 2005). Their method computes disjoint clusters automatically using a spherical k-means algorithm for all spam/non-spam mails and obtains centroid vectors of the clusters for extracting the cluster description. For each centroid vectors, the label ('spam' or 'non-spam') is assigned by calculating the number of spam email in the cluster. When new mail arrives, the cosine similarity between the new mail vector and centroid vector is calculated. Finally, the label of the most relevant cluster is assigned to the new mail. By using this method, the authors claim that they can extract many kinds of topics in spam/non-spam email and detect the spam email efficiently.

A number of anti-spam products are listed by Hinde (2002). These are commercial systems which can be purchased to stop the unwanted spam. Dealing with spam is like fighting a battle against a large army; the most effective approach is to employ multiple tactics (Agrawal et al., 2005). However, almost all spam control methods that have been proposed and implemented follow the same basic theme of establishing a "front line" of defense at the end-user level and therefore we need a method for blocking the supply lines. We need to identify spam at the router level and control it via rate limiting. Spam identification can be done in two phases. In the first phase, identify the bulk stream of email messages and in second phase identify whether it is a spam. If a bulk email stream is classified as a spam then rate will limit it (e.g., no more than one copy per minute).

Bright mail currently dominates the anti-spam market with a market share of 45%. Mail-Filters.com has launched SpamCure, which claims to utilize Mail-Filters' 11-step spam detection process that allows enterprises to achieve up to 95% effectiveness at finding and removing spam. DigiPortal Software Inc. whose new product, 'Choicemail', defeats spam by requiring the sender to first ask the recipient's permission. Vanquish Inc. proposes a different approach which addresses the root cause of spam - sending it costs nothing but even a very small response rate to a spam offer results in an astronomical return on investment. Even worse, its costs are borne by those who distribute it. Habeas' service works by trademarking and copyrighting a unique set of lines, known as the warrant mark, which is embedded in the headers of outgoing email. Mail-Filters have SpamRepellent system for filtering out junk email (spam) messages. Mail-Filters.com claims every email is subjected to 11 different categories of tests resulting in over 95% of all spam messages being identified. McAfee has launched SpamKiller which helps stop spam email, tracks the mail back to the source ISP and sends complaints to the spammer's service provider. SurfControl uses the concept of 'RiskFilter' database, part of its email filtering software.

An anti-spam scheme using pre-challenges was proposed in a paper by (Roman et al., 2006) where they introduce the pre-challenge scheme, which is based on the challenge-response mechanism and takes advantage of some features of email systems. It assumes each user has a challenge that is defined by the user himself/herself and associated with his/her email address, in such a way that an email sender can simultaneously retrieve a new receiver's email address and challenge before sending an email in the first contact.

Methods

Participants

A convenience sample of three hundred participant volunteers was selected from a wide variety of organizations and the general public. The sample included college and university students, school teachers, engineers, university lecturers, lawyers, medical doctors, nurses, marriage councilors, house wives, final year school students, social workers, shop workers and managers. The sample also included some randomly selected people regardless of their status. We had to make sure that the sample represented the society in Bahrain as much as possible so that our results reflect the views of the average Bahraini. The age group ranged from 15 to 60. Youth below sixteen years were not considered because we felt that they are not mature enough for this investigation. People older than 60 were not considered because most of this age group in Bahrain are not Internet users and would therefore not give fair answers. The survey did not consider people who did not read and write, people who did not use the Internet and people outside the selected age group.

Of the participants in this survey, 71% were male and 29% were female. The ages of the participants were as follows: 38% between 15 and 21, 32% between 21 and 31, 12% between 31 and 39, 15% between 39 and 49 and 3% older than 49.

Spam questionnaire

The questionnaire began with a definition of spam as 'unsolicited email messages offering or attempting to sell you a product or service or attempting to give you information that you never requested or interested in where such information could be offensive to your person or your belief.' Participants were asked if they receive spam and if they ever purchased anything as a result of a spam advertisement. They were asked questions about their gender, age and their views and stance with regards to spam.

It was decided that a good method of answering these research questions was through a questionnaire and hence a questionnaire was distributed to a carefully selected sample of email users in Bahrain and their feedback was analyzed. The questionnaire focused on people from the ages of 15 to 60. First, a pilot questionnaire was prepared and distributed among a few people to get their feedback on any adjustments or any comments they had about the questions. Then a questionnaire containing 16 questions was prepared to cover all the research questions that this research aims to answer.

It was first thought that a questionnaire sent by email to various people was the best way to distribute the questionnaire but based on the prototype findings it was decided that this method had a few drawbacks such as the sincerity in answering the questionnaire could not be verified and there was not certainty that anybody would answer the questionnaire in the first place as it may ironically be considered as spamming. Therefore, a face to face, one by one, each participant was handed the questionnaire in order to answer any questions they had about the questionnaire and to explain some of the terminology used.

It was made clear in the questionnaire that we were researching the effects of email spam on Bahrain's email users and identifying effective ways to combat it. The major questions of this research are: What percentage of users in Bahrain receives spam messages and how many? Are spammers mainly from outside the Arab world? Do Bahraini people get any benefit from spam? How much do people actually get bothered by spam? What do users do when they are spammed? Do people use any anti-spam software to reduce the spam they receive? How much does spam affect work productivity? What is the role of spam email in spreading pornography? Should there be a Bahraini law against spam?

In total we received 300 responses, and although this might be thought of as a small sample, it is a highly accurate one to some degree since the Bahraini population is only half a million people.

Results Summary

In this section, only the results obtained from the questionnaire will be shown and discussed briefly, a more detailed analysis of the results will be carried in the next section.

1. Of the participants in this survey, 71% were male and 29% were female.
2. The ages of the participants were as follows: 38% between 15 and 21, 32% between 21 and 31, 12% between 31 and 39, 15% between 39 and 49 and 3% older than 49.
3. When asked how long they have been using the Internet, 3% said that they have been using the Internet for less than 1 year, 3% between 1 year and 3 years and the majority which is 94% have been using the Internet for more than 3 years.
4. When asked about how many spam emails they get everyday, 12% said less than 5, 46% said between 5 and 15, 24% received between 15 to 25 and 18% more than 25 spam emails per day.
5. When asked about the language of the email spam they mostly receive, 18% said Arabic, 18% said both Arabic and English and 64% said English.
6. When asked about the reasons in their opinion for people to send spam, 73% said for marketing products and services, 21% said for fun and 6% thought that they got their emails by mistake.
7. When asked how much they benefited from email spam, 56% said they got no benefit or up to 20% benefit from the total email spam they received, 38% said up to 40% benefit and 6% said up to 60% benefit.
8. When asked about how much the spam email bothered them, 6% said they were not bothered or just up to 20% bothered, 21% said up to 40% bothered, 24% said up to 60% bothered, 25% said up to 80% bothered and 24% said that they were 100% bothered by Spam email.

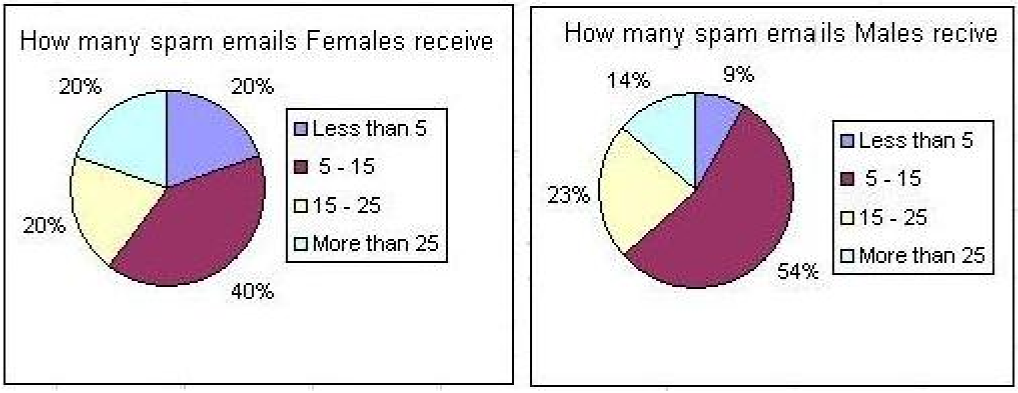
9. When asked what they do with the spam email, 82% said that they read the header and delete the email, 6% said that they read the whole email and delete it and 12% said that they keep the spam email.
10. When asked if they know about any software to combat email spam, 26% said yes and 74% said no.
11. When asked about their preference on how spam should be stopped, automatically or manually, 65% said they would like it to be stopped automatically and 35% said that they would like to delete it themselves.
12. When asked about how much email spam affected their work productivity, 58% said that they did not get affected or up to 20% effect on their work productivity, 13% said up to 40% affected, 21% said up to 60%, 4% said up to 80% and 4% said that email spam 100% affect their work productivity.
13. When asked if they get spam emails related to pornography, 76% said yes they get spam related to pornography and 24% said they did not get any pornographic emails.
14. When asked about how much they got disturbed from these pornographic emails, 8% said that they were not disturbed at all or just 20% disturbance level was felt, 12% had a disturbance of up to 40%, 27% up to 60%, 4% up to 80% and 49% were extremely disturbed at a 100% level.
15. Of the parents' who answered this questionnaire, 83% said that they are worried that this pornographic spam emails will have an effect on their children and 17% said that they did not know, but nobody agreed that it had no effect.
16. When asked if they thought that there should be a law to stop the email spammers, 56% said yes there should be a law, 12% said no and 32% said that they were not sure about the mater.

Results Analysis

Analysis by Gender

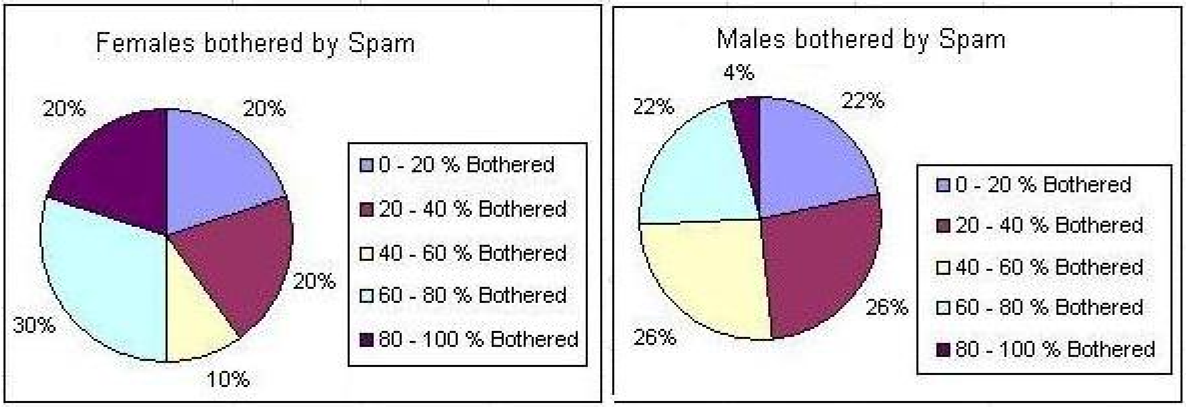
Spam generators do not really differentiate between males and females, but the question is do men and women recognize what spam is in the same way. Figure 2 shows the results to the question about how many spam emails are received by men and women. The results are slightly different for the two genders.

Figure 2: How many spam emails females and males receive



It can be seen in Figure 3 that females are a little less bothered by spam than males and this might be due to the fact that males receive more spam emails in general than females or that they use the email service more than females. Another possibility is that females like shopping and since many emails are of a commercial marketing nature; this may suit women more than men and that they do not consider marketing spam emails as spam anyway. Another reason might be that the females who answered the questionnaire are only 29% of the total number of participants.

Figure 3: How Females and Males are bothered by spam emails



With regards to the question who gets more pornographic spam content, males or females, and how much each gender is bothered by this kind of spam, see Figures 4 and 5.

Figure 4: How many females and Males are receiving pornography

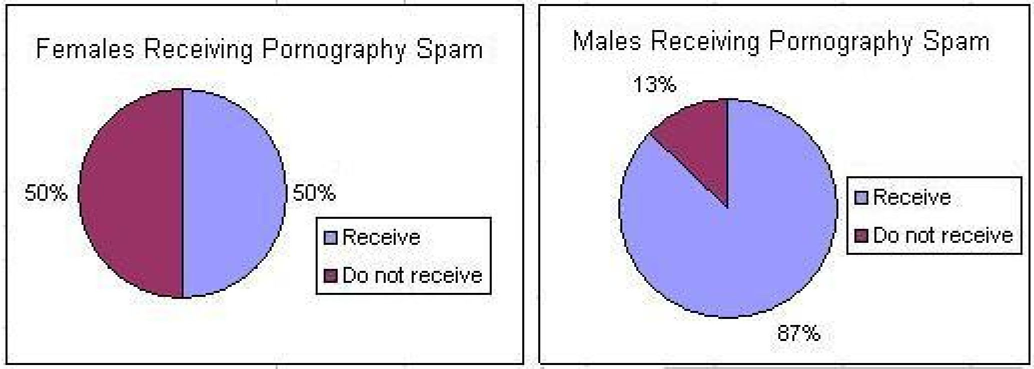
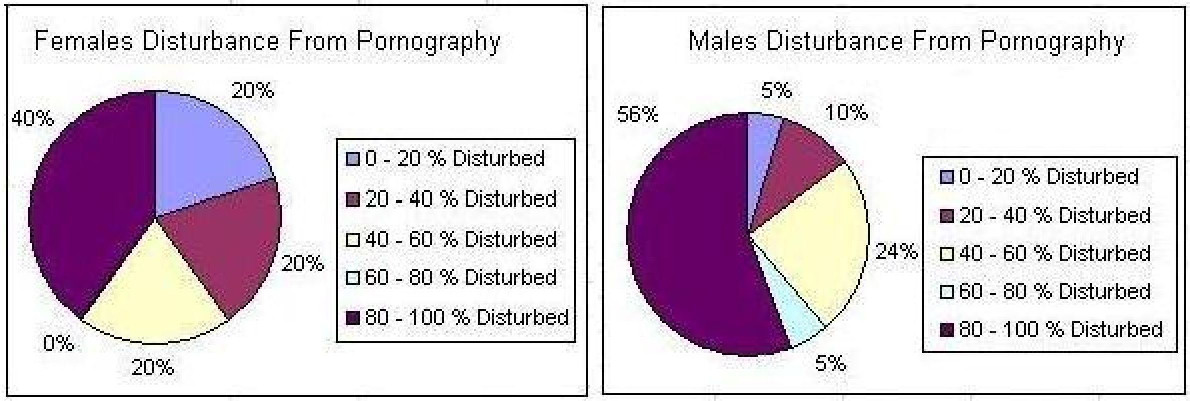


Figure 5: How much females and Males are disturbed by pornography



It is very clear that because males receive a larger percentage of pornographic spam emails than females that they are more disturbed by these emails. This can be for a number of reasons, such as:

1. Arab males visit pornography sites more often than females where their email address was found out and used by the spammers.
2. Arab females feel ashamed about admitting visiting such sites.

Analysis by Age

In this part we would like to make a comparative analysis between the different age groups in terms of how much they are bothered by spam, if they receive pornographic spam emails and how much they are disturbed by such emails.

Figure 6 shows how much younger users are more tolerant of spam in general

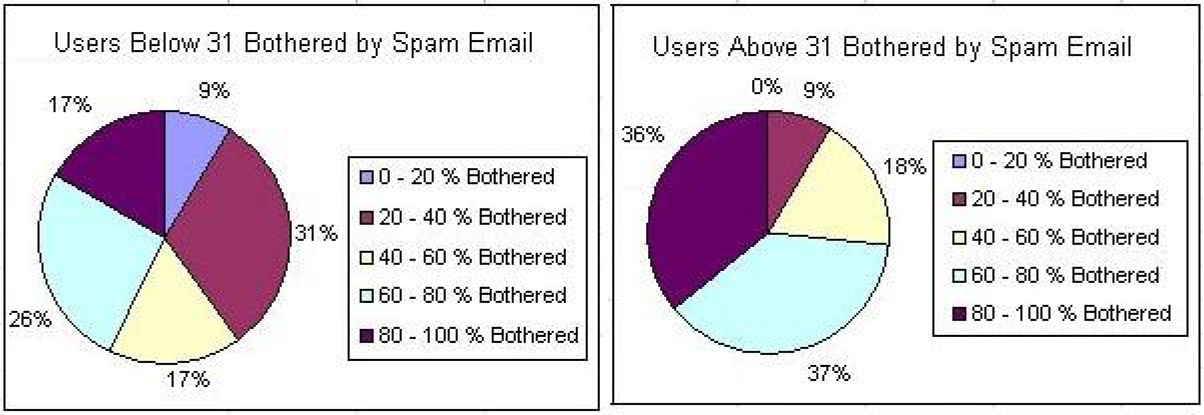
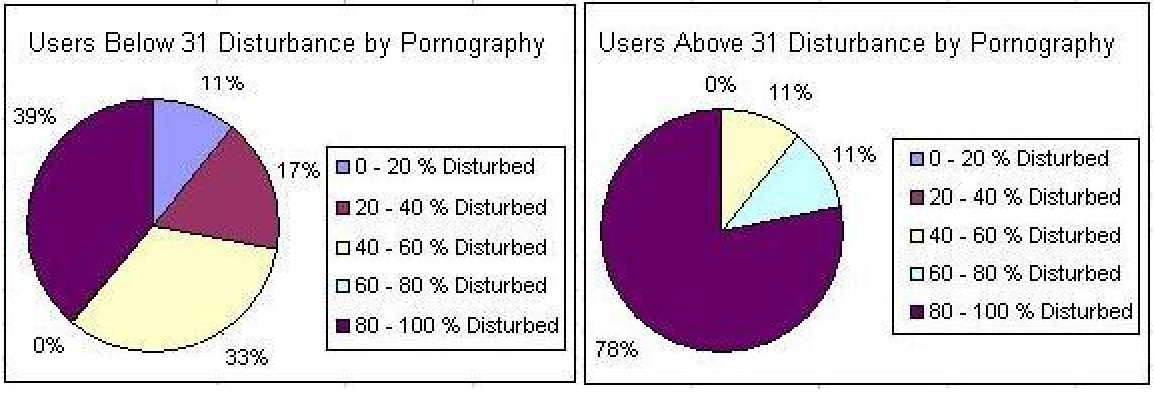
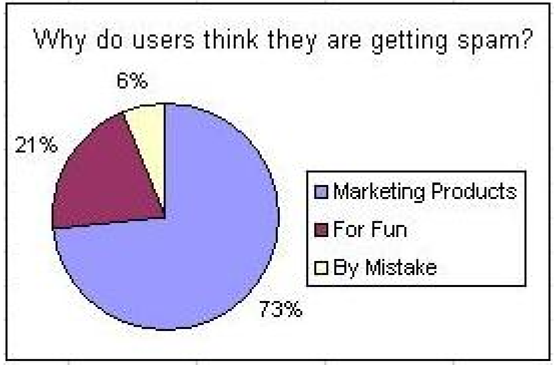


Figure 7 shows how much younger users are more tolerant of pornography



It can be seen from Figures 6 and 7 that young users are more tolerant than older users of spam and younger users are also more tolerant of pornography than older users. Older users are probably married and with children and they are more concerned about other family members viewing pornography and they are more mature than younger users who tend to like viewing this kind of material.

Figure 8 shows that most spam we get is commercial in nature



As shown in Figure 8, the majority of email users, 73%, are of the opinion that they get spammed mostly for commercial purposes. 56% of the email users surveyed thought that there should be a law against spammers. This means that a large percentage of users are very bothered by spam that they think these spammers should be prosecuted for wasting their time and disk space. Also exposing them to pornographic emails and the fear that these emails will fall into the hands of their children is a very big concern as you can watch where your children surf and advice them not to enter pornographic sites but when the pornography is emailed to them, that is dangerous and hard to stop even with email filters. Most users are not aware of the existence of anti-spam software, and in any case this software is not 100% effective and to fight the source of the spam through spam laws is one good way to battle spam. If the spammers get big penalties and very tough laws applied on them, they might think twice before spamming people to market their products or to spread viruses.

Analysis of other factors

Spam is an invasion of privacy as the email users never gave authority to these spammers to send them all theses emails. In the United States, an anti-spam law has become affective starting January First 2004, other countries have anti-spam laws, but in our search of the Internet, we found that there is no law against spam in the Arab world. There is already a comprehensive list of countries with anti-spam laws or that are working to develop one (www.spamlaws.com).

It is clear from the results obtained in this research that email users at varying levels in Bahrain are bothered by spam (94%), that pornographic spam is disturbing a majority of the users (92%) at varying levels and that parents are very worried about their children getting exposed to such material (83%).

It is also clear that the majority support the existence for an anti-spam law in Bahrain, as most people seem to support it (56%) and because the spam wastes time and is a danger to youths, therefore authorities in Bahrain should consider developing such a law in the Kingdom.

Most of the users who work did not have their work productivity affected by this spam emails as 58% said that the spam emails had no or little effect on their work productivity. But since more than 42% suffer a substantial affect on their work productivity, this would mean that spam has gotten to be a time waster for the work force of Bahrain.

People and especially parents hate pornographic spam emails. It is a very big problem since 76% of the email users in Bahrain receive a form of pornography in their emails. It is seen as a very dangerous phenomenon especially in our *Islamic culture*; these pornographic emails are a major disturbance as 49% of the users were extremely disturbed by these kinds of emails.

Parents are the most disturbed by pornographic emails as 83% of parents thought that these emails will have an affect on the children and 17% were unsure about the effect of pornographic emails on their children. It is worth mentioning that from the parents that were surveyed, none said that the pornographic spam emails will have no effect on their children.

An anti-spam law is definitely needed as spam comes in English and Arabic which means that it comes from all over the world and recently it started to come from within Bahrain to offer services and offers from companies.

This phenomenon is expected to grow by time and a law dealing with email spam specifically and spam in general should be developed to put a stop to this annoying and time wasting practice.

It can be deduced from the results found that only 12% of the email users got less than 5 spam emails per day and the majority which is 88% receive more than 5 spam emails per day and that is a lot of unwanted emails that uses up bandwidth and disk space and consumes time to read and delete. This is apparent because 82% of the users read the header first and then delete it which takes time if you receive more than 25 emails per day as 18% of users do receive.

These emails do more harm than good. 56% of the users do not benefit at all or just about 20% benefit from these spam emails. Only 6% of the users are not bothered by them. That means that 94% of the users are bothered by spam. Most users (74%) are not aware that anti-spam software exists and a large percentage of these (65%) would prefer that this spam be stopped automatically.

On the other hand 35% of the users prefer that they read and delete these emails manually due to their curiosity that these emails may have some benefit for them because some (44%) said that they got some benefit from these spam emails, but this benefit did not carry more than 60% importance in the most extreme cases and only by 6% of the users.

Conclusion

This paper presented an analysis of a survey about email spam in the Bahraini society. The survey clearly indicates that the Bahraini society would welcome an anti-spam law in line with other leading nations such as the USA and Europe. The survey shows that a lot of time wastage is caused by spam for men and women and that all adults have a concern about their time and disk space wastage as well as their children welfare. Further, awareness of anti-spam software must be increased amongst the public. The paper identified and analyzed the major issues pertaining to spam and measured their effects on the Bahraini community. In the absence of an anti-spam law in Bahrain and the other Arab countries, we hope to do further research on this subject in order to bring a balanced and culturally fit anti-spam law.

References

- Agrawal, B., Kumar, N., & Molle, M. (2005). Controlling spam emails at the routers. *Proceedings of the IEEE International Conference on Communications*, (ICC 2005), Volume 3, pp. 1588-1592.
- Deepak, P., & Parameswaran, S. (2005). Spam filtering using spam mail communities. *Proceedings of the 2005 Symposium on Applications and the Internet*, 2005, pp. 377-383.
- Garg, A., Battiti, R., & Cascella, R.G. (2006). May I borrow your filter? Exchanging filters to combat spam in a community. *20th International Conference on Advanced Information Networking and Applications*, 2006. AINA 2006, 18-20 April 2006, Vol. 2, pp. 489- 493.
- Gopal, R.D., Tripathi, A.K., & Walter, Z.D. (2006). Economics of first-contact email advertising. *Decision Support Systems*, 42 (3), pp. 1366-1382.
- Grimes, G. (2004). Issues with spam. *Computer Fraud & Security*, 24(5), 12-16.
- Hammonds, M. B. (2003). Spam- the meat of the problem. *Computer Law & Security Report*, 19(5), 388-391.
- Hinde, S. (2002). Spam, scams, chains, hoaxes and other junk mail. *Computers and Security*, 21(7), 592-606.
- Hoanca, B. (2005). Freedom of silence vs. freedom of speech: Technology, law and information security. *Proceedings of International Symposium on Technology and Society*, 2005. Weapons and Wires: Prevention and Safety in a Time of Fear. ISTAS 2005. 8-10 June 2005, pp. 37-45.
- Hoanca, B. (2006). How good are our weapons in the spam wars? *IEEE Technology and Society Magazine*, 25(1), 22-30.
- Islam, Md.R., Chowdhury, M.U., & Zhou, W. (2005). An innovative spam filtering model based on support vector machine. *Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce*, Vol. 2 (CIMCA-IAWTIC'06), 28-30 Nov. 2005, pp. 348-353.

- Oda, T., & White, T. (2003). Increasing the accuracy of a spam-detecting artificial immune system. *Proceedings of the 2003 Congress on Evolutionary Computation*, 8-12 December 2003, Canberra, Australia, Vol. 1, pp. 390-396.
- Park, S.Y, Kim, J.T., & Kang, S.G. (2006). Analysis of applicability of traditional spam regulations to VoIP spam. *The 8th International Conference on Advanced Communication Technology*, ICACT 2006, 20-22 February 2006, Vol. 2, pp. 1215-1217.
- Qiu, X., Jihong, H., & Ming, C. (2004). Flow-based anti-spam. *Proceedings IEEE Workshop on IP Operations and Management*, 11-13 October 2004, pp. 99-103.
- Roman, R., Zhou, J., & Lopez, J. (2006). An anti-spam scheme using pre-challenges. *Computer Communications*, 29 (15), 2739-2749.
- Sasaki, M., & Shinnou, H. (2005). Spam detection using text clustering. *International Conference on Cyberworlds*, 23-25 November 2005, pp. 316-319.
- Schaub, M.Y. (2002). Does Europe allow spam? State of the art of the European legislation with regard to unsolicited commercial communications. *Computer Law and Security Report*, 18(2), 99-105(7).
- Schryen, G. (2006). A formal approach towards assessing the effectiveness of anti-spam procedures. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, January 2006.
- Spam Laws. Available at: http://www.spamlaws.com
- Whitworth, B., & Whitworth, E. (2004). Spam and the social-technical gap. *Computer*, 37 (10), 38-45.
- Wu, M-W., Huang, Y., Lu, S-K., Chen, I-Y., & Kuo, S-Y. (2005). A multi-faceted approach towards spam-resistible mail. *Proceedings. 11th Pacific Rim International Symposium on Dependable Computing* (PRDC'05), Changsha, China, December 2005.
- Wu, C-T., Chengy, K-T., Zhuy, Q., & Wux, Y-L. (2005). Using visual features for anti-spam filtering. *IEEE International Conference on Image Processing 2005* (ICIP 2005), September 11-14, 2005, Vol. 3, pp. 509-12. http://www1.engr.ucsb.edu/~zhuq/paper/icip05.pdf
- Zhang, Y. (2004). Age, gender, and Internet attitudes among employees in the business world. *Computers in Human Behavior*, 21(1), 1-10.

Bibliographic information of this paper for citing:

Al-A'ali, Mansoor (2007). "A Study of Email Spam and How to Effectively Combat It." *Webology*, **4**(1), Article 37. Available at: http://www.webology.org/2007/v4n1/a37.html

Alert us when: New articles cite this article