بسم الله الرحمن الرحيم

# Combating SPAM

Prepared by

**Mohamed M. K. Elhaj**

**National Telecommunications Corporation**

**NTC – SUDAN**

**mohamed.elhaj@ntc.gov.sd**

March 2009

# Combating SPAM

According to the internet world stats[9] the total number of internet users in the world reached 1,581,571,589 user, more than 70% of them have broadband connections. As ICT networks develop, however, besides the creation of an increasing range of opportunities, a host of new challenges arise. In particular, application and services, and the confidence of users in their utilization, are fundamental elements in enabling the benefits ICT can bring to economic and social development. However, today the reliability of e-mail and other electronic communication tools - and consequently users' trust and confidence in these technologies - is threatened by the escalation of unsolicited/unwanted electronic messages, commonly known as spam, which are flooding the Internet and causing significant harm to both individuals and businesses.

## Definition of Spam

Developing an accurate and useful definition of spam is more complicated than it might appear. In fact, the Working Group on Internet Governance (WGIG) notes in draft working paper, "there is not at present an international consensus on the definition of spam, the specific governance issues it raises, or the most appropriate methods of resolving these issues".

In the following section I will provide some definitions stated by Australia, European Union, France and United States.

**Australia:** defined as "unsolicited commercial electronic messages" (though the word "Spam" is not specifically mentioned), judicial provisions are technologically neutral: legislation includes Email, SMS, MMS and instant messaging; while faxes and voice-to-voice telemarketing are excluded, no reference to bulk messaging - a single unsolicited commercial electronic message could be Spam.

**European Union:** term Spam is neither defined nor used, the term "electronic mail for the purposes of direct marketing" is used, judicial provisions are technically neutral: legislation includes Email, calling machines, faxes and SMS messages.

**France:** the Commission Nationale de l'Informatique et des Libertés (National Data Processing and Liberties Commission) refers to "spamming" or "spam" as the practice of sending unsolicited e-mails, in large numbers, and in some cases

repeatedly, to individuals with whom the sender has no previous contact, and whose e-mail address was harvested improperly.

**United States:** term Spam is neither defined nor used, a FTC-definition of a "Commercial Electronic Mail Message" exists, judicial provisions not limited to Email: inclusion of mobile Spam subject to implementation (Action by the Federal Communications Commission on mobile Spam)[1]

Despite the confusion and disagreement on a precise definition there is a fairly widespread agreement that spam exhibits certain general characteristics. These characteristics may include all or some of the following:

- **Electronic messages:** spam messages are sent electronically (e-mail, SMS, ..)
- **Bulk**: spam messages are typically sent in bulk
- **Unsolicited**: spam is sent without the recipient's request or consent
- **Commercial**: typically spam has a commercial purpose, with some exceptions to other usages i.e. political, sexual , fraudulent …etc
- **Uses addresses collected or sold without the owner's consent**
- **Unwanted**: spam is usually considered to be unwanted or even useless by its recipients
- **Untargeted or indiscriminate:** typically spam is sent in an indiscriminate manner, without any knowledge about the recipient other than the e-mail address
- **Repetitive**: many spam messages are repetitive, either exact duplicates of prior messages (or containing very slight variations)
- **Contain illegal or offensive content**
- **Anonymous or disguised:** are often sent in a manner that disguises the originator by using a false address or header information. Spammers frequently use unauthorised third-party e-mail servers. [4]

## Spam .. history

Over the last few years, the use of and delivery of spam has evolved. Initially, spam was sent directly to computer users. In fact, spammers didn't even need to disguise the sender information. This early spam was easy enough to block – if you blacklisted specific sender or IP addresses, you were safe. In response, spammers began creating mock sender addresses and forging other technical information.

In the mid-1990s all email servers were open relay - any sender could send an email to any recipient. Starting in 2000, spammers began switching to high-speed Internet connections and exploiting hardware vulnerabilities. Cable and ADSL connections allowed spammers to send mass email messages inexpensively and quickly. In addition, spammers quickly discovered that many ADSL modems had built-in socks servers or http proxy servers. Both are utilities that divide an internet channel between multiple computers. This important feature meant that anybody from anywhere in the world could access these servers since they had no protection at all. In other words, malicious users could use other people's ADSL connections to do whatever they pleased, including sending spam. Moreover, they could make the spam look as if it had been sent from the victim's IP address. Since millions of people worldwide had these connections, spammers had a field day. That was until hardware manufacturers began securing their equipment.

Since 2004 spammers start sending the majority of spam messages from machines belonging to unsuspecting users. Spammers use malware to install Trojans on users' machines, leaving them open to remote use.

Today, spam is increasingly being viewed as a more serious messaging threat, as it is coming to be used to deliver worms, viruses, and Trojans as well as scams of more directly financial nature. Spammers often trick even the savviest of e-mail users into opening these messages.

For this reason, spam has been considered as an issue that affects every email user, and by extension, every computer user. The use of email as a ubiquitous tool that lies at the heart of the Information Society, and any threat to the use of email will undermine user trust and confidence in the Information Society.

## Nature of Spam

One of the major characteristics of spam that has stimulated the current international intention on encountering its effects is its rapid increase and wide spread. Current statistic from Kasbersky and Symantec labs shows that Spam consists between 70% to 80% of the overall E-mail traffic in the internet.

While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media, e.g., mobile phone messaging spam, internet telephony spam, instant messaging spam, usenet newsgroup spam, web search engine spam, and

blog spam. The content of the spam messages ranges from advertisement of goods to offensive pornographic material. Email spam has various kinds of harmful effects to the email service users and Internet Service Providers.

## Spam Categories :

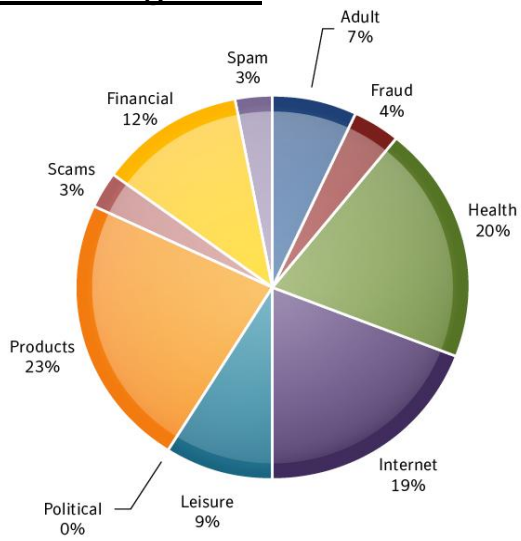


Figure (1) : source : kaspersky 2009

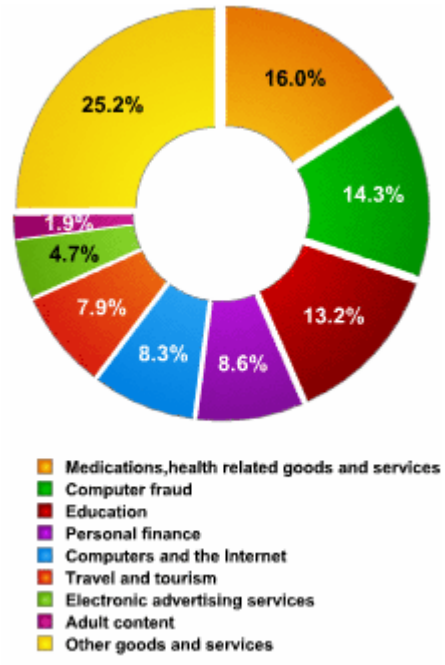


Figure (2) : source: kaspersky 2006

| Category | Description |
|---|---|
| Adult | containing offensive or/and inappropriate material like porn or sex |
| Fraud | email attacks that appear to be from a well-known company, but are not. Also known as "brand spoofing" or "phishing", these messages are often used to trick users into revealing personal information |
| Health | offering or advertising health-related products and Services |
| Internet | offering or advertising internet or computer related goods and services |
| Leisure | offering or advertising prizes, awards, or discounted leisure activities. Example vacation offers, online casinos, games |
| Political | messages advertising political issues like election |
| Products | advertising general goods and services like books, clothes etc.. |
| Scams | Email attacks recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender |
| Financial | contain references or offers related to money, market or other financial opportunities. |

## Spam content types

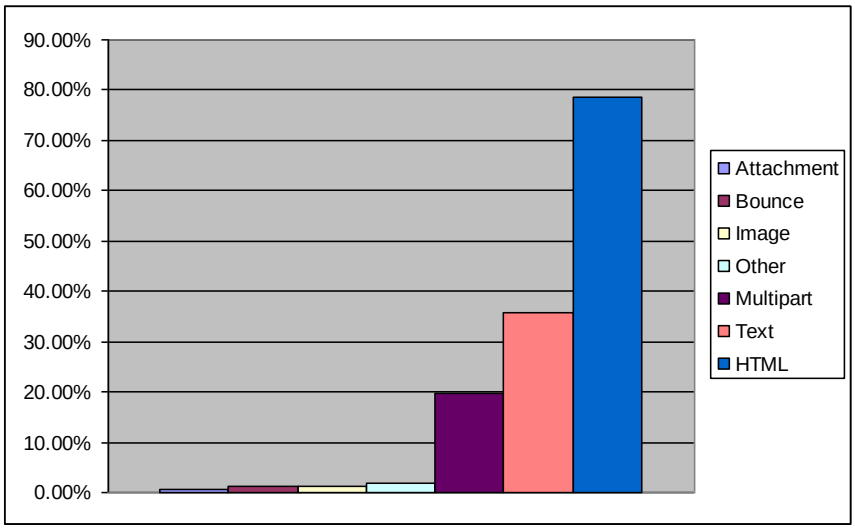


Figure (3) Spam content types (Symantec 2008)

## Size of Spam mail

The size of spam mails varies, just like that of legitimate correspondence: Approximately 35% of both spam and legitimate emails range from 1 – 5 KB in size. A second clearly delineated category is the 28.4% of spam which varies in size from 10 – 20 KB. This phenomenon was not mirrored in legitimate correspondence. The large number of spam mails ranging from 10 – 20 KB is partly due to graphical spam (see figure 4 for more information on this).

The vast majority of spam mails (95.6%) vary from 5KB to 40 KB in size. Spam contains fewer small messages than legitimate email. A small message is less than 1 KB in size (1% of spam, 13.7% of legitimate email), while a large message may be over 80 KB (3.4% of spam, 16.3% of legitimate email),[2]

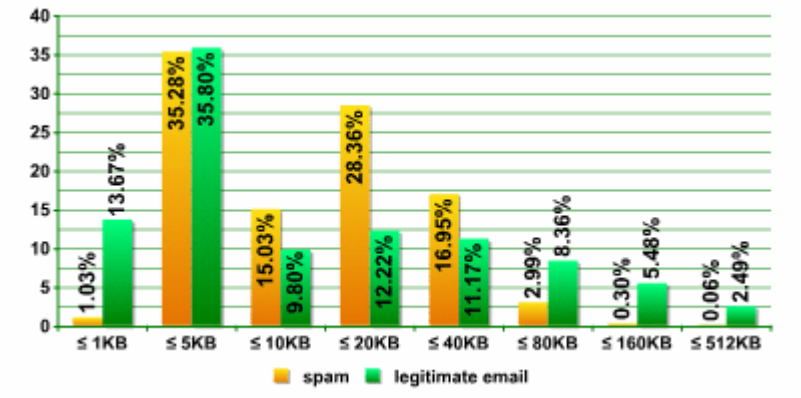


Figure (4) : the sizes of email spam and legitimate email

## Top Level Domains in Spam Emails

Most spam emails contain links to web sites. The percentage of unique domains in different top level domains or IPs is shown in the following table according to securecomputing[10]. This data is taken in October 2008.

| Domain | Percentage |
|---|---|
| .COM | 51.70% |
| .CN | 19.10% |
| .INFO | 8.70% |
| .NET | 5.40% |
| .VE | 3.10% |
| .SG | 3.10% |
| .ORG | 2.20% |
| .RU | 1.20% |
| IP Number | 1.20% |
| .TK | 1.00% |
| .BIZ | 0.40% |
| .EU | 0.30% |

## Spam effects

The problematic nature of spam evolves from the destructive effects it has on many public and private resources and its real socio-economic threats, basically in developed environments. Some of these effects are ultimately justified and agreed, while others need to be carefully studied and reevaluated. The main effects are:

- SPAM Cost
- Privacy violation
- Drop of On-line Consumer trust
- Spam content; viruses and worms, sexual contents, fraud.
- SCAMMING; Identity theft through spam
- Spam victims; These are individuals , enterprises, ISPs or even countries whose e-mails or servers are used as either a falsified SPAM origins or as an intermediate SPAM vehicles due to security weaknesses .Yet another victims are legitimate spammers who join the set up regulations of anti-spam. All of these are innocent victims to anti-spam technologies or laws , a phenomenon known as ‘false positives’.

According to a study by Radicati Group report, "European E-mail Security Market, 2006-2010" [6], the European email traffic considered as "spam" in 2006 is 16 billion messages per day this number will increase to 38 billion messages per day in 2010, Despite aggressive spam filter technology, 66 percent of e-mail reaching user inboxes is spam according to Nucleus Research, a global provider of information technology research and advisory services, in 2007 announced that the spam epidemic is costing US businesses $712 per employee each year in lost worker productivity.
According to a survey of 849 e-mail users conducted during March 2007, Nucleus Research and KnowledgeStorm found that two out of every three e-mail messages received by today's business users are spam.
As a result, users are spending 16 seconds identifying and deleting each spam e-mail, which translates into an annual cost of $70 billion to all US businesses.
"Although most organizations have deployed some spam filtering technology, it clearly has not solved the spam problem - in fact, in some cases it's made it worse," said Rebecca Wettemann, VP of Research of Nucleus Research. "Spam is no longer just a technology problem - it's a problem that we should be attacking with more than just technology."
"The Companies and their employees are beyond fed-up with the spam problem," said Jeff Ramminger, executive vice president, KnowledgeStorm. "In fact, almost 20 percent of respondents believe jail time is an appropriate punishment for serial spammers. While that's probably not a realistic outcome, it indicates that frustration with spam has reached a boiling point.

## Tool for direct marketing

The development of sophisticated databases has made telemarketing and e-marketing increasingly popular as a direct marketing strategy. The forms of direct marketing include postal mail, telephone, fax, automatic calling machines and e-mail. Direct marketing is viewed by companies as an important tool to approach, inform and retain customers, as well as provide customer relationship services. Electronic messages including e-mail provide a cheap and easy way to contact a large group of customers. E-mail has also become one of the most cost-efficient ways to provide customer support and assistance. The recognition that the internet has decreased customer-switching costs in many cases has highlighted the importance of customer relationship

management and permission marketing. However, these benefits have been put at risk by the continued flood of spam, by reducing the customer confidence in, and effectiveness of, e-mail marketing.

## Spam cost

Internet users incur a direct cost resulting from the time spent consulting, identifying and deleting unwanted messages. In addition, they are concerned about the reliability of communications and the content of spam messages. The new possibilities offered by broadband, fast internet connections are hampered by dangers linked to spam; deceptive or misleading messages, offensive content, goods and services of a dubious nature offered for sale.

For professional and business users, spam represents a loss of productivity, and imposes direct costs by increasing the need for technical support and software solutions such as filters. Spam imposes more general societal costs by reducing the reliability of e-mail as a communication tool (legitimate messages can be blocked by filters or be lost among a large number of unsolicited e-mails), and threatening the security of a company's internal network.

The other major victims of spam are ISPs and other network operators, which process e-mails. Increased costs derive from the need to implement anti-spam solutions, such as filters, the increased necessity of technical support, costs associated with expanding infrastructure to handle the amount of messages, and the risk - in cases where ISPs are used by spammers, or computers in their networks are hijacked - to lose reputation or even to be blocked by other ISPs. Many of these costs will subsequently be passed on to the consumer in the form of higher access fees or poorer service.

The actual cost of spam is difficult to calculate, as some of the damages are only indirect, and whether and how to cost the time of private individuals is controversial. In addition, the fraudulent nature of spam, or the malware carried by spam messages, can result in more important financial damages to users and companies.

Unwanted messages are creating problems and additional costs to users all around the world. Individuals in developing economies often access internet through dial-up connections, or from community access points, such as cybercafés, where the user pays on the basis of the time spent online. Under these conditions it is easy to see how

spam takes up a valuable part of the already limited resources, increases the cost of internet access, and reduces the quality of service.

## Mail address gathering and sending technology

A spammer can obtain e-mail addresses from the following sources:

1) Customers or prospective customers who supply their e-mail address to the spammer themselves.
2) Third parties who obtained the addresses directly from the individuals and sell them to the spammer.
3) Public spaces such as web pages, directories or newsgroups on which the spammers harvest the addresses using spamware.
4) Third parties who used spamware to harvest individuals' addresses from public spaces and sell them to the spammer.
5) In some cases there are also formulas (automated guesses related to first or last name) used against a specified domain.

Among these sources, the third and fourth methods are the most common. Only the first method might result in a recipient being aware that their e-mail address was being used for spam. To obtain e-mail addresses, spamware tools automatically navigate web sites and public spaces such as Usenet or Chat rooms, using a list of URLs either specified in advance, created by means of keywords entered into search engines or recursively grabbed from web pages in a search-engine fashion. Then they collect all the e-mail addresses found on those spaces. They also distribute e-mail to lists created to circumvent filters put in place by the ISPs.

Some spamware programs use other techniques to gather e-mail addresses. One is the random e-mail address generator. A bulk e-mailer floods a particular domain name by using a program that generates millions of possible web addresses, such as aa@cdt.org, ab@cdt.org, and so on. This "brute force attack" attempts to send e-mails to every possible combination of letters that could form an e-mail address. The more elegant "dictionary attack" builds address lists through computer-generated alphabetic permutations combined with address suffixes or creates addresses by using common surnames and first initials (*i.e.* names are taken sequentially, for example bob@msn.com, abob@msn.com, bbob@msn.com, cbob@msn.com, etc.).

Major ISPs and corporate networks which handle a large volume of e-mail traffic on their servers everyday are highly vulnerable to the dictionary attack, because spammers often conduct the attacks undetected, hidden in normal traffic. Spammers sometimes use software which opens connections to the other mail servers and automatically submits millions of random addresses, such as "anne@hotmail.com", "michael@hotmail.com", recording which addresses succeed. These are then added automatically to the spammer's list. Spammers mainly target ISPs, but spammers also spam enterprises so as to reach the corporate inboxes of millions of e-mail users. Though the purpose of such attacks is not to alter the service of the attacked machines, its effect on ISPs or enterprises is similar to a denial of service (DoS) attack, wherein legitimate use of the ISP's services is denied by massive illegitimate traffic.

Some spammers gather lists of working e-mail addresses not for spamming, but for resale in bulk to other spammers worldwide. In fact, a fair number of spammers are not interested in selling goods and services. Instead, they make money selling e-mail addresses to other spammers.

## The difficulties of identifying Spammers

Identifying spammers is difficult. A number of methods are used by spammers to hide their identities. Source addresses are randomised so that they are not easily identified. Spamware programs automatically generate false headers and return address information. False headers allow spammers to ignore recipient requests to be removed from e-mail lists and to obscure their identities by making themselves untraceable. Other spammers scan the internet for open relays in foreign countries for their messages not to be traced. According to Spamhaus[11], direct spam sources "account for some 50% of spam received by internet mail relays worldwide, the other 50% comes via third-party exploits such as open proxies and open relays."

Some spammers open free e-mail accounts and abandon them before they're caught. Spammers also write programs that load in multiple accounts so when one account is terminated, another automatically kicks in. Quite a few spammers simply move on to another ISP when their accounts are terminated for spamming with another ISP. However, others pretend to their ISP providers to be small ISPs themselves, claiming that the spam is coming from non-existent customers. Spammers can send out

hundreds of thousands of messages, each with customised content and source addresses, and then quickly log out. “Spoofing” addresses is also used by spammers. This involves using false information as to the name of the sender. This can be either false information or in some cases using names of other commercial entities that are not involved with the spam operation.

## Approaches to countering and combating e-mail Spam

Since e-mail spam do great damage to e-mail service users, Internet Service Providers and Network Operators, technologies have been developed and regulations have been adopted in many countries to help counter spam. However, it is difficult to counter spam effectively through a single countering measure such as filtering or legal punishment since countering spam is not a simple problem. For that reason, ITU-T resolution 52, "countering spam by technical means"[8], suggests various kinds of methods to be applied simultaneously to counter spam effectively:

– Regulation: Anti-spam regulations should be adopted to facilitate appropriate response of service users for e-mail spam, and to increase the effect of anti-spam technologies such as filtering. In addition, regulation can help to protect service users and ISP from illegal spam.
– Technology: Anti-spam technology development is essential for countering large quantities of e-mail spam effectively. It is required to develop various kinds of technologies to prevent sending spam, and to identify and filter spam effectively.
– Legislation: it is important to adopt an antispam law or include it in the existing e-crime laws (in next section legislation issue will be discussed in detail)
– Industrial Actions: various kinds of anti-spam technologies, including blacklist or whitelist and filtering functions, are appropriate to be developed and installed by industry participants such as ISPs or network operators. It is also possible for ISPs to adopt policies for countering e-mail spam.
– International Cooperation: international cooperation is required, since the Internet is borderless, and the generation and effect of spam are not domestic. International cooperation is also useful for information sharing about effective regulation adoption, anti-spam technology development, and education of service users and providers.

– Education: to minimize damage of e-mail spam, education to rise the awareness of service users and ISPs is vital. The education is expected to make e-mail users take appropriate actions for e-mail spam, and ISPs to adopt anti-spam policies and technologies. [3]

## The need for anti-spam legislation [5]

Spammers clearly cannot be stopped easily; consequently, governments across the world started to realize this, and have begun to intervene in the spam war.

Since the enactment of the first anti-spam law in 1997, spam has grown from a mere nuisance into a global plague. The intention of such all laws has been to empower action against spammers in order to stop the problem at its source and, thereby, to substantially reduce the amount of spam clogging networks and irritating corporate users and consumers.

As the volume of spam increased in recent years, so did the number of spam laws across the world. However, while the laws proposed to combat spam were put forth with good intentions they are not actually addressing the problem in a substantive way.

In 1997, the average e-mail user received was approximately one unsolicited commercial e-mail message per week, today according to MessageLabs accounts for a large portion of all electronic mail traffic.

emerged from the Survey results that there are a number of countries that have already implemented anti-spam legislations, such as Australia, Austria, Belgium, China, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Japan, Lithuania, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, United Kingdom and the United States.

It was also found that several other countries use alternative laws, such as Data Protection laws or Consumer Protection laws to cope with spam issues; these are, for example, Argentina, Armenia, Brazil, Bulgaria, Canada, Chile, Colombia, Costa Rica, South Korea, Hong Kong, Luxemburg, Malaysia, Mexico, New Zealand, Peru, Russia, Switzerland, Turkey.

In other countries the enforcement of laws applicable to spam falls, however, under the jurisdiction of communication regulators and other related bodies.

The following countries are currently discussing the implementation of a specific anti-spam legislation: Argentina, Brazil, Canada, Colombia, Hong Kong, New Zealand, Russia, Singapore and Turkey.
Further results of the survey revealed that several countries have not developed any anti-spam legislation yet.

## OPT-IN or OPT-OUT? [5]

The fight against spam is made even more difficult by the fact that as there is no agreed definition of spam commonly accepted by all stakeholders, and of what constitutes illegal spam activities, this means that it varies depending on national jurisdiction.
In this regard, the focus of most discussions over anti-spam law to this point has revolved around "opt-in" versus "opt-out" approaches.
The difference between these two philosophies of anti-spam law is easy to understand; Governments that adopt an "opt-in" approach announce to the world their sentiment that marketers should not send messages to a recipient unless the recipient has affirmatively asked to receive them. The European Union has chosen to adopt an opt-in requirement for e-mail, which became effective October 31, 2003. The EU directive sets the broad policy, but each member nation must pass its own law as to how to implement it.
On the other hand, an "opt-out" approach declares that a sender may send a message to a recipient even if there is no existing business relationship and the recipient has not specifically opted in to receiving the messages. Opt-out laws typically require senders to honor the requests of recipients to remove them from a sender's mailing list. In other words, completely unsolicited messages may be sent; however, senders must stop their messages once they have been asked to do so. This is, for example, the approach followed by the United States, South Korea, Japan and some others.
Another approach to restraining spam is requiring that senders of commercial e-mail use a label, such as "ADV," in the subject line of the message, so the recipient will know before opening an e-mail message that it is an advertisement. That would also make it easier for spam filtering software to identify commercial e-mail and eliminate it.

## Spam & developing countries

The following points reflect the current situation in developing countries (specially Africa and Mid-East) in regard to SPAM:

- **Not a recognized source** ; The contribution of this region in sourcing SPAM activities is of no concern. The ultimate majority sources are in Europe, America (N and S) and East Asia. see the map in figure (5).
- **Not a current recognized destination**; Due to the limited internet usage and lack of professional E-services.
- **Suspicious to be an intermediate relay;** Due to open relays, open proxies, small amount of traffic (attractive response time) or network security weaknesses as general.


Figure (5) : Spam sources by country (the number in brackets is the rank)

In order for developing world to better combat Spam, these countries should make more efforts so as to maximize the portion of local internet traffic volume this will increase the network security and privacy. Some suggestions to reach this objective are :

- Activation of country code top level domains (ccTLD) and making them the favorite choice for domain holders.
- Encouraging local hosting by offering suitable hosting services.
- Encouraging local mail servers.
- Establishing an Internet Exchange Points (IXP) in national and regional levels to keep traffic local and thereby reduce international traffic and related costs.
- Installation of moderate technical anti-SPAM solutions to help encounter international, and possible local, illegitimate SPAM with a major funding from developed countries.

- Drafting an opt-out (not opt-in) regulations in developing countries to encounter possible future local threats while supporting the idea.
- Public awareness for reasonable security and filtering solutions.

## References


1. Workgroup of Internet Governance (WGIG)
2. Kasbersky lab annual report 2006 and 2009 http://www.viruslist.com/en/analysis?pubid=204791920
3. ITU-T Recommendation X.1240 (X.gcs), Technologies involved in countering email Spam-2007
4. OECD task force on spam final report, 2006, http://www.oecd.org/dataoecd/63/28/36494147.pdf
5. ITU survey on anti-spam legislation worldwide, 2008, http://www.itu.int/osg/spu/spam/legislation/background_paper_itu_bueti_survey.pdf
6. Radicati Group report, "European E-mail Security Market, 2006-2010", http://www.radicati.com
7. Nucleus Research, 2007, http://www.nucleusresearch.com
8. WTSA 2008 ITU-T resolution 52 "countering email spam by technical means", http://www.itu.int/ITU-T/wtsa/resolutions04/res52E.pdf
9. Internet World Statistics, 2008, http://www.internetworldstats.com/
10. Secure-computing monthly report on Spam 2008, http://www.securecomputing.com/pdf/mail-monthly-rep-nov08.pdf
11. Spammhaus, 2008
12. Spam .. a different perspective, 2004, Ammar Kabashi, NTC Sudan