
Hong Kong, January 2004

# WHITE PAPER

**"Legislation: One of the key pillars in the fight against spam"**

**Developed by the Hong Kong Anti-Spam Coalition**

# WHITE PAPER

## "Legislation: One of the key pillars in the fight against spam"

# TABLE OF CONTENTS

# White Paper

## "Legislation: One of the key pillars in the fight against spam"

---

### Summary


- Globally, more than 50% of all e-mail traffic is now spam.
- The problem in Hong Kong is escalating, at high cost to consumers and businesses. 50% of all e-mail in Hong Kong is spam, with a significant 5% of it originating in Hong Kong itself, and a further 20-40% from other Asian sources (mainly China).
- Calculations based upon international research figures reveal that spam could cost the Hong Kong economy as much as HK$10 billion per year, with the cost of lost productivity alone estimated at approximately HK$6 billion.
- A Coalition of Internet-related businesses and associations has formed to help protect consumers and businesses by combating spam in Hong Kong.
- The Coalition is calling for the Hong Kong government to begin public consultation on anti-spam legislation.
- Such legislation is one of the key pillars in the fight against spam, along with training of IT professionals, consumers and business users; industry best practices; message filtering and blocking technology.


### The Hong Kong Anti-Spam Coalition

The Hong Kong Anti-Spam Coalition was formed during the summer of 2003. The coalition brought together a group of concerned industry participants such as the Hong Kong Internet Service Providers Association (HKISPA), the Asia Digital Marketing Association (ADMA) and business leaders from a variety of organisations including Microsoft and Time Warner.

The Coalition aims to make a real difference to consumers, businesses and government by bringing together powerful local market knowledge and contacts to foster effective industry self-regulation, legislative solutions, information sharing, and other global best anti-spam practices.

As leaders in the industry, these companies and associations recognize they must share responsibility for dealing with spam.

The group's efforts have initially focused on the following areas:

- Discussion and development of **industry best practices for commercial e-mail**;
- **Evaluation of extent of the spam problem** in Hong Kong (and elsewhere in Asia), through both short and longer term projects;
- Developing information highlighting the problem of spam vis-à-vis computer users in Hong Kong and identifying key elements of effective **anti-spam legislation**;
- Development and sponsorship of **training programs** to educate local IT professionals on the dangers of spam and how to avoid having their systems abused by spammers;
- Where possible, sharing of information that would facilitate **enforcement** action against high-volume spammers;
- **Liaison with the Hong Kong government** in these areas.

## Scope of the Problem

While the purpose of e-mail is to make communication more convenient, e-mail does not always provide the increased efficiency desired. Worldwide, spam (Unsolicited Bulk and Unsolicited Commercial Email) is estimated to comprise up to 50% of all e-mail traffic, and is a growing problem in Hong Kong and throughout the Asia region. In the United States alone, the cost of spam to recipient organizations is believed to exceed US$9 billion annually in lost productivity (Ferris Research 2003).

A survey conducted by the Hong Kong Internet Service Providers Association (HKISPA) in December 2003 [Annex I], gathering data from eleven ISP's, which represent over 90% of Internet users in Hong Kong, revealed that 50% of all e-mail in Hong Kong is spam, with a significant 5% of it originating in Hong Kong itself, and a further 20-40% from other Asian sources (mainly China). Based on international calculation methodology, the annual economic costs of spam to Hong Kong could be as much as HK$10 billion, with the cost of lost productivity alone estimated at HK$6 billion.

Another survey, conducted by the office of Mr. Sin Chung Kai in December 2003 [Annex II], revealed that almost 60 percent of respondents said that over a quarter of the messages in their private email accounts is unsolicited, and more than 80 percent of respondents said that

unsolicited e-messages annoy them. Although many of respondents said they had already adopted some type of anti-spam measures, the vast majority (more than 80 percent) agreed the government should regulate unsolicited e-mail activity.

Of those supporting government intervention, 70 percent favor the introduction of anti-spam legislation in Hong Kong, indicating that respondents do not consider the technology now available to combat spam to be an adequate answer to the problem and that a more comprehensive solution, including some form of regulation, is needed. Of those respondents who did not favour regulator measures, many expressed a concern that government intervention may limit freedom of speech and the free flow of information in society.

Below is a table prepared by MessageLabs showing ratios for industry verticals in Asia Pacific most at risk of receiving spam emails. These can be taken as indicative of the size and scope of the problem.

**Table: Industry verticals most at risk of receiving spam emails in Asia Pacific (excluding Japan)**

| Vertical Market | June 2003 | September 2003 | October 2003 |
|---|---|---|---|
| Marketing, media, publishing | 1 in 9.27 | 1 in 4.05 | 1 in 1.67 |
| General services | N/A | 1 in 6.58 | 1 in 4.46 |
| Manufacturing | 1 in 7.99 | 1 in 6.14 | 1 in 3.01 |
| Public Sector | 1 in 16.64 | 1 in 4.55 | 1 in 4.48 |
| Transport and Utilities | 1 in 3.55 | 1 in 5.96 | 1 in 5.09 |
| Finance and Banking | 1 in 11.04 | 1 in 8.07 | 1 in 4.37 |
| IT Services | 1 in 5.62 | 1 in 2.27 | 1 in 1.82 |

Beyond costs associated with lost productivity, spam poses dangers for computer users. Spam is frequently fraudulent, deceptive, or highly offensive. Additionally, there is an increasing and alarming convergence of the spamming and hacking communities, and spam is often used as a delivery vehicle for malicious worm and virus attacks and other forms of computer-related crime.

## A call to the Hong Kong Government for legislation to combat spam

The Hong Kong Anti-Spam Coalition urges the Hong Kong Government to initiate public consultation on the drafting of specific legislation to combat spam. The European Union, the United States, Korea, Japan, Australia and other countries around the world have either already enacted such laws or are well advanced in the process of deciding the best legislative route forward. The Coalition recognizes legislation alone will not prevent spam, but it would be a critical component of a comprehensive and effective solution to the problem. Appropriate legislation would also demonstrate Hong Kong's desire to combat spam and allow it to keep pace with other IT leaders in the region, as well as preventing Hong Kong from becoming a "safe haven" for spammers.

The Coalition understands that such legislation would need to complement existing laws and telecommunications regulatory guidelines. At present, there is no single legislation in Hong Kong that deals with all forms of computer-related crime, and no legislation addressing spamming specifically. Aspects of the spam problem may be covered by existing legislation only if, amongst other things, the actions, results and consequences brought about by the spammed communication are covered by existing offences within relevant Hong Kong ordinances (such as fraud, etc.). In short, it is the elements constituting the offences specified in existing relevant ordinances, rather than the fact that it is a piece of spammed communication per se, which may be prohibited under current Hong Kong law.

The existing piece-meal Hong Kong ordinances (which, again, were not designed specifically to address spamming) are not sophisticated enough to deal with the burgeoning spam problem and the techniques currently used by spammers. The result is uncertainty and dissatisfaction.

Current spamming issues, such as the misuse of headers, subject lines and sender's names, spamming techniques such as harvesting e-mail names and so-called "dictionary attacks," require effective legal regulation and enforcement. In addition, we recommend specific regulation requiring effective means of opting out of receiving future e-mail messages and protection for individuals and businesses from these practices.

We understand jurisdiction is also a critical issue, which must be effectively yet pragmatically dealt with in the legislation as many forms of computer-related crime may be initiated from abroad. We recommend detailed discussion and consultation on this important issue.

The Coalition therefore supports comprehensive but targeted legislation that includes:

- Meaningful civil and criminal penalties for fraudulent e-mails: Anti-spam legislation should apply to both individuals and companies and should prohibit the use of false or misleading header information, false or misleading subject lines, and the misuse of third-party domain names. Spammers use tactics such as these to avoid detection and to encourage unsuspecting consumers to open spam mail.
- Requirements that unsolicited commercial e-mail messages include a functioning mechanism for opting out of receiving future e-mail messages, valid contact information, and identification of the message as an advertisement through an "ADV" label.
- A "safe harbour" to the "ADV" labelling requirement for digital marketers who follow e-mail best practices: The Coalition believes that technology can and should be used to help differentiate messages that are sent by legitimate marketers from those that are not. Legislation can create incentives for online marketers to adopt e-mail best practices and to certify themselves as trusted senders who can be more easily identified by both filtering technologies and consumers.
- Rigorous measures to prevent harvesting and the use of "dictionary attacks," and prohibitions on the use of scripts to establish large volumes of e-mail accounts from which to send spam.
- Effective ISP enforcement and language preserving ISPs' rights to combat spam: ISP enforcement is an important means of combating the spam problem. Anti-spam legislation should facilitate, and not create barriers to, such enforcement efforts. Further, the law should not obligate ISPs to block or carry certain types of e-mail messages, nor should it inhibit an ISP's ability to enforce its anti-spam policies.
- Sufficiently broad scope to cover all bad actors involved in sending unlawful spam: Anti-spam legislation should capture not only individuals and entities whose products are advertised in spam mail but also others who knowingly assist in the transmission of unlawful spam. The law should include an explicit and unambiguous exemption for mere routing activities.

The Coalition welcomes the opportunity to work with the Hong Kong government and the broader community of affected computer users in developing a legislative response to the spam problem.

## More Background on Spam

More and more people are now using the World Wide Web, making the Internet an increasingly integral part of everyday life. Many people now have Internet access and are using it to exchange text files, photos, videos and music. **During the past few years, the number of Internet users has increased worldwide with incredible speed**. As of the end of June 2003, 66.5% of households in the United States are online, **61% in Hong Kong**, 59.8% in Sweden, 58.9% in Netherlands, 51% in Australia, and 44.0% in Japan. (Source: Nielsen/NetRatings, Aug. 2003)

Since one of **the most widely used functions of the Internet is E-mail**, it is no surprise that as the number of individuals using the Internet increases, the number of E-mail accounts rises as well. Almost every individual and business, from large corporations to small enterprises, maintain multiple E-mail addresses. **Email volume will continue to explode** as person-to-person emails are joined by rapidly-growing numbers of spam and email alerts and notifications, according to IDC. In **2006**, the **total number of email messages sent daily** is **expected to exceed 60 billion worldwide**, up from **31 billion in 2002**, and slightly more than half of these messages will be person-to-person emails. **E-mail is a powerful medium** for expressing ideas, receiving information, sharing opinions, and supporting commerce. E-mail is a **convenient** way for businesses to address customer service issues, send invoices and receipts, and maintain intra-office communications. The dramatic explosion in E-mail use should surprise no one and can be attributed to its role as a **quick** and relatively **inexpensive form of communication**. Hand-written letters and waiting for postal services to deliver important documents all seem somewhat archaic in today's technological world. **E-mail has developed as the primary method of communication for personal** and, more importantly, **business** use in 2003 and will surely increase in the future. It is therefore critical to protect the viability of e-mail and legitimate e-commerce by proactively addressing the spam problem in a variety of ways.

## Definition of Spam

**Spam = Unsolicited Bulk E-mail or Unsolicited Commercial E-mail**

Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent and has no pre-existing business relationship with the sender. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content.

Both unsolicited bulk e-mail and unsolicited commercial e-mail (whether or not sent in bulk) may be seen to constitute spam.

## The Costs

The tangible and intangible **impact of spam on both individual and business Internet users** is rising, and is estimated to **cost over US$9 billion annually** in the United States and possibly as much as HK$10 billion each year in Hong Kong.

| | Marketers | ISPs/Portals | Companies | Recipients |
|---|---|---|---|---|
| **Tangible Costs** | - Low response rates<br>- Increased costs<br>- Decreasing opt-in rates<br>- IT security | - Storage space<br>- Hardware/Software<br>- Customer Service<br>- Management time<br>- Cancelled accounts<br>-IT security | - Storage space<br>- IT Upgrades<br>- Legal risks<br>- Productivity<br>- Profitability<br>-IT security | - Wasted time<br>- Cost of bandwidth, access time and storage<br>- Misused resources<br>-IT security |
| **Intangible Costs** | - Erosion of impact<br>- Worsening environment<br>- Clutter<br>- Customer dissatisfaction | - Pressure to switch ISP's<br>- Decline in trust<br>- Seen as source of problem | - User trust breakdown<br>- Distraction from core business | - Irritation and distrust<br>- Possible fraud<br>- Emotional upset at disturbing material<br>-Particular vulnerability of children to harmful content |

---

**If you wish to take part in this Coalition, please contact Sophie Lottefier at sophie@upstreamasia.com or +852 2973 0222**

## Glossary

| | |
|---|---|
| **Bulk** | Means that the message is sent as part of a larger collection of messages, all having substantively identical content. |
| **Domain name** | Means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority, and that is included in an e-mail message. |
| **Harvesting (e-mail addresses)** | Harvest is defined as compiling or stealing e-mail addresses through anonymous collection procedures such as via a web spider, through chat rooms, or from other publicly displayed areas listing personal or business e-mail addresses. |
| **Header information** | Means the source, destination, and routing information attached to an e-mail message, including originating domain name, the originating e-mail address, and technical information that authenticates the sender of an e-mail message for network security or network management purposes. |
| **ISP** | Internet Service Provider |
| **Opt-out** | Means opting out of receiving future e-mail messages. |
| **Spam** | Unsolicited bulk e-mail or unsolicited commercial e-mail |
| **Unsolicited** | Means that the recipient has not granted verifiable permission for the message to be sent and has no pre-existing business relationship with the sender. |

**ANNEX I - Result of Survey on "Unsolicited E-Messages" by The Office of Mr. Sin Chung Kai**


# RESULT OF SURVEY ON "UNSOLICITED E-MESSAGES "

**By THE OFFICE OF MR. SIN CHUNG KAI – LEGISLATIVE COUNCILLOR (IT)**

Office of Mr. **Sin Chung Kai** Legislative Councillor (I.T.)

**單仲偕**立法會議員（資訊科技界）辦事處

Empowering Hong Kong in the Information Age

# Result of Survey on "Unsolicited e-messages "

**13, January, 2004**

## 1. Introduction

The survey aims to reflect the scope of problem of unsolicited e-messages, and to gauge public opinion about regulating spam in Hong Kong.

## 2. Research Methodology

The study was conducted from 3 November to 10 December 2003. A questionnaire was sent to some 2 500 potential recipients via e-mail. To facilitate the public's participation in the study, the questionnaire was also uploaded to the official website of Mr. Sin Chung-kai, the legislator representing the IT sector. A total of 99 completed questionnaires were received.

## 3. Summary of Survey Findings & Conclusion

**Email is the most prevalent form of "Unsolicited e-messages" (Q1)**

- Of 4 types of unsolicited e-messages, namely, e-mail, fax, SMS and phone calls which are commonly received by the general public, e-mail is identified as the most prevalent form of unsolicited e-messages activity.
- Over 95.8 percent of respondents received this type of unsolicited e-messages each day.

**People are very annoyed about receiving unsolicited e-messages (Q2)**

- While almost 60 percent of respondents said that over a quarter of incoming messages in their private e-mail accounts is unsolicited, more than 80 percent of respondents expressed that unsolicited e-messages annoyed them. (Option 4 and Option 5 of Q2)
- This indicates that the problem of unsolicited e-messages has already become a nuisance to the vast majority, albeit some of them were yet to be hit seriously by spam.

**The problem of unsolicited e-messages has imposed additional costs to users (Q3)**

In general, respondents use the following methods to deal with the problem of unsolicited e-messages:

- Almost 90 percent of respondents would delete and ignore e-messages or just cut the line off when they received unsolicited phone call.
- Nearly 50 percent of respondents would use filtering tools.

- More than one-third of them (37.4 percent) would request the sender to opt-out their name from the mailing list.
- This suggests that the problem of unsolicited e-messages has imposed additional costs to respondents, as they have to invest a great deal of time and resources on anti-spam tools and activities.

**The problem of spam is far more serious than we imagined (Q4)**

- Since nearly 70 percent of respondents have used some sort of anti-spam measures, such as filtering software to delete and block unsolicited e-messages automatically, the actual problem of spam could be more serious than we found in the study.

**Internet users support the Government to regulate spam as they do not consider technology available to date to be an adequate answer to the problem (Q5)**

- Despite 70 percent of respondents already adopted some sort of anti-spam measures, more than 80 percent of total respondents agreed the government to regulate unsolicited e-messages activities.
- Of those supporting government intervention, 70 percent of them suggested introducing an anti-spam legislation in Hong Kong.
- This indicates that respondents do not consider technology now available to combat spam to be an adequate answer to the problem. To reduce spam, they prefer some kind of regulatory measures.

**Freedom of speech is the major concern for those respondents who do not favor government intervention (Q7)**

- Of those opposing regulatory measures, 80 percent of them expressed that government intervention may limit freedom of speech and free flow of information in the society.

## 4. Findings

1. How many unsolicited e-messages have you received per day?

A1. Email received by your office email account (% of total email received)

| | Frequency | % |
|---|---|---|
| a. 0% | 8 | 8.2% |
| b. <5% | 21 | 21.4% |
| c. 6-10% | 24 | 24.5% |
| d. 11-15% | 4 | 4.1% |
| e. 16-20% | 7 | 7.1% |
| f. 21-25% | 5 | 5.1% |
| g. 26-30% | 9 | 9.2% |
| h. > 30% | 16 | 16.3% |
| i. Don't know | 4 | 4.1% |
| No response | 2 | 2.0% |
| **Total** | **99** | |

A2. Email received by your private email account (% of total email received)

| | **Frequency** | **%** |
|---|---|---|
| a. 0% | 2 | 2.1% |
| b. <5% | 8 | 8.2% |
| c. 6-10% | 13 | 13.4% |
| d. 11-15% | 7 | 7.2% |
| e. 16-20% | 4 | 4.1% |
| f. 21-25% | 2 | 2.1% |
| g. 26-30% | 19 | 19.6% |
| h. > 30% | 40 | 41.2% |
| i. Don't know | 2 | 2.1% |
| No response | 3 | 3.0% |
| **Total** | **99** | |

b. fax (% of total fax received)

| | **Frequency** | **%** |
|---|---|---|
| a. 0% | 21 | 21.4% |
| b. <5% | 24 | 24.5% |
| c. 6-10% | 10 | 10.2% |
| d. 11-15% | 3 | 3.1% |
| e. 16-20% | 3 | 3.1% |
| f. 21-25% | 4 | 4.1% |
| g. 26-30% | 4 | 4.1% |
| h. > 30% | 15 | 15.3% |
| i. Don't know | 14 | 14.3% |
| No response | 1 | 1% |
| **Total** | **99** | |

c. SMS (Number of SMS received)

| | **Frequency** | **%** |
|---|---|---|
| a. 0 | 31 | 32.3% |
| b. 1-3 | 53 | 55.2% |
| c. 4-6 | 8 | 8.3% |
| d. >6, please specify | 1 | 1.0% |
| e. Don't know | 3 | 3.1% |
| No response | 3 | 3.1% |
| Total | 99 | |

d1. Calls received by your office phone number (No. of calls)

| | Frequency | % |
|---|---|---|
| a. 0 | 31 | 31.3% |
| b. 1-3 | 49 | 49.5% |
| c. 4-6 | 9 | 9.1% |
| d. >6, please specify | 1 | 1.0% |
| i. Don't know | 9 | 9.1% |
| Total | 99 | |

d2. Calls received by your private phone number (No. of calls)

| | Frequency | % |
|---|---|---|
| a. 0 | 22 | 22.2% |
| b. 1-3 | 68 | 68.7% |
| c. 4-6 | 4 | 4.0% |
| d. >6, please specify | 1 | 1.0% |
| i. Don't know | 4 | 4.0% |
| Total | 99 | |

2. Generally speaking, do you think the unsolicited e-messages are annoying?

| | Frequency | % |
|---|---|---|
| 1 (Not annoying) | 1 | 1.0% |
| 2 | 4 | 4.0% |
| 3 (Half-half) | 12 | 12.1% |
| 4 | 21 | 21.2% |
| 5 (Very annoying) | 60 | 60.6% |
| N Don't know/ hard to say | 1 | 1.0% |
| Total | 99 | |

3. How would you handle unsolicited e-messages? (You may choose more than 1 answer)

| | Frequency | % |
|---|---|---|
| a. Send a reply to / request the sender to take you off from the distribution list | 37 | 37.4% |
| b. Delete / ignore the message / cut the line off (for phone calls) | 88 | 88.9% |
| c. Add the message sender into your own filtering list | 47 | 47.5% |
| d. Register your number on the "not-to-call list" of OFTA (for fax no. only) | 5 | 5.1% |
| e. Change your phone /fax number, email account | 5 | 5.1% |
| f. Lodge complaint to the service providers | 8 | 8.1% |
| g. Lodge complaint to the OFTA | 1 | 1.0% |
| h. Lodge complaint to other parties, e.g. Office of the Privacy Commissioner for Personal Data (PCO), Legislative / District Councillors, media, etc) | 4 | 4.0% |
| i. Others, please specify _____ | 8 | 8.1% |
| Total | 99 | |

4. Have you adopted any prevention measure for dealing with unsolicited e-messages? (You may choose more than 1 answer)

| | Frequency | % |
|---|---|---|
| A. Yes, (You may choose more than 1 answer) | N=68 | |
| a. Use filtering software for email | 63 | 92.6% |
| b. Use "anonymous call blocking feature" or "calling number display" services for phone calls | 25 | 36.8% |
| c. Register your fax number on the "not-to-call list" of OFTA | 6 | 8.8% |
| d. Register your phone number on the "not-to-receive list" of the services providers | 6 | 8.8% |
| e. Others, please specify _____ | 1 | 1.5% |
| B. NO, because | N=31 | |
| f. Don't know which prevention measures are available | 12 | 38.7% |
| g. The prevention tools cannot effectively block the unsolicited messages | 16 | 51.6% |
| h. Others, please specify | 4 | 12.9% |
| Total | 99 | |

5. Do you support that the Government should regulate the activities of sending unsolicited e-messages?

| | Frequency | % |
|---|---|---|
| A. Yes (please also answer Q6) | 85 | |
| a. introduce anti-spam legislation | 61 | 71.8% |
| b. issue a new code of practice | 51 | 60.0% |
| c. tighten the relevant terms in the license of the service providers | 46 | 54.1% |
| d. Others, please specify _____ | 4 | 4.7% |
| B. No (please skip Q6 and answer Q7) | 13 | |

6. What are your major reasons of supporting the Government to get involved in banning unsolicited e-messages? (You may choose more than 1 answer) N=85

| | Frequency | % |
|---|---|---|
| a. Waste of Internet / Telecom network resource | 66 | 77.6% |
| b. Increase the operation cost of the business (e.g. Internet / Telecom services charges) | 52 | 61.2% |
| c. Decrease the productivity of the business | 66 | 77.6% |
| d. Information security, such as spread of virus | 63 | 74.1% |
| e. Those messages are annoying and wasting time | 69 | 81.2% |
| f. Others, please specify _____ | 5 | 5.9% |
| g. no special reason | 0 | |

7. What are your major reasons of NOT supporting the Government to get involved in banning unsolicited e-messages? (You may choose more than 1 answer) N=13

| | Frequency | % |
|---|---|---|
| a. The IT & T sector itself would handle the problem in a more efficient way | 5 | 38.5% |
| b. Too costly for the Government to fight against the senders | 3 | 23.1% |
| c. Government may not have enough skills and technology to deal with the problem | 6 | 46.2% |
| d. Government involvement may impair freedom of speech and free flow of information | 10 | 76.9% |
| e. Others, please specify _____ | 5 | 38.5% |
| f. no special reason | 1 | 7.7% |

## 濫發電子訊息問卷調查結果
## 2004 年 1 月 13 日

### 1. 簡介
問卷調查的目標是爲了解濫發電子訊息的情況，以及使用者對監管上述活動的態度。

### 2. 調查辦法
調查在 2003 年 11 月 3 日至 12 月 10 日間進行。問卷透過電子郵件，發予約 2500 位人士，並上載至單仲偕議員辦事處的網頁。問卷以英文進行，共收回 99 份有效回覆。

### 3. 調查結果及分析

**A. 濫發電子郵件是最普遍的濫發行爲(第一題)**

- 公眾最常接觸到的四類濫發電子訊息中，包括：電子郵件、傳真、手提電話短訊(SMS)及電話，以濫發電子郵件的情況最嚴重
- 超過 95%回應者每日均會接收到這類未經許可的濫發電郵。

**B. 使用者認爲未經許可的電子訊息非常滋擾 (第二題)**

- 約有六成回覆者表示，在私人電郵信箱收到的電郵中，超過四分一是未經許可的濫發電郵。然而，認爲未經許可的電子訊息很滋擾(第 2 題答案 4 及 5)的回覆者則達八成。
- 結果顯示，即使一些回覆者並未被濫發電子訊息嚴重地影響，他們仍認爲該類電子訊息非常滋擾。

**C. 未經許可濫發電郵增加企業成本 (第三題)**

- 大多數回覆者以下列方法處理收到的濫發電子訊息：
  - 近九成回覆者會刪除或不理會濫發的電子訊息，或將電話掛斷。
  - 近一半回覆者使用過濾軟件
  - 約三分一回覆者(37.4%)要求發出訊息的人士將他們從分發名單中刪除。
- 這顯示使用者需花時間和資源處理濫發的電子訊息，因而增加使用者的成本。

**D. 濫發電子訊息的情況可能遠較我們所知的嚴重(第四題)**

- 近七成回覆者表示已採用不同的措施阻截或刪除未經許可的電子訊息，故濫發電郵的真實情況可能遠較我們所得的結果嚴重。

**E. 互聯網使用者認爲科技未能解決濫發電子訊息的問題，因而支持政府監管濫發電子訊息 (第五題)**

- 雖然近七成回覆者已採用某種方式減輕受濫發電子訊息的滋擾，但八成半回覆者認爲政府應監管濫發電郵活動。

- 在支持政府監管濫發電子訊息的回覆者當中，七成認爲香港應引入監管濫發電子訊息的法例。
- 上述結果顯示回覆者不認爲現時的科技，是解決濫發電子訊息的最有效方法。

**F. 部份回覆者憂政府介入濫發電子訊息問題，可能會損害言論自由 (第七題)**

- 超過八成不支持監管濫發電郵的回覆者，擔心政府介入監管濫發電子訊息，可能會削弱言論自由及資訊流通。

## 4. 結果

1. 你每天收到多少個未經許可的電子訊息?

A1. 從公司提供的電郵信箱收到的電郵 (全部電郵的百分比)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0% | 8 | 8.2% |
| b. <5% | 21 | 21.4% |
| c. 6-10% | 24 | 24.5% |
| d. 11-15% | 4 | 4.1% |
| e. 16-20% | 7 | 7.1% |
| f. 21-25% | 5 | 5.1% |
| g. 26-30% | 9 | 9.2% |
| h. > 30% | 16 | 16.3% |
| i. 不清楚 | 4 | 4.1% |
| 沒有回答 | 2 | 2.0% |
| **總數** | **99** | |

A2. 從私人電郵信箱收到的電郵 (全部電郵的百分比)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0% | 2 | 2.1% |
| b. <5% | 8 | 8.2% |
| c. 6-10% | 13 | 13.4% |
| d. 11-15% | 7 | 7.2% |
| e. 16-20% | 4 | 4.1% |
| f. 21-25% | 2 | 2.1% |
| g. 26-30% | 19 | 19.6% |
| h. > 30% | 40 | 41.2% |
| i. 不清楚 | 2 | 2.1% |
| 沒有回答 | 3 | 3.0% |
| **總數** | **99** | |

b. 傳真 (全部傳真的百分比)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0% | 21 | 21.4% |
| b. <5% | 24 | 24.5% |
| c. 6-10% | 10 | 10.2% |
| d. 11-15% | 3 | 3.1% |
| e. 16-20% | 3 | 3.1% |
| f. 21-25% | 4 | 4.1% |
| g. 26-30% | 4 | 4.1% |
| h. > 30% | 15 | 15.3% |
| i. 不清楚 | 14 | 14.3% |
| 沒有回答 | 1 | 1.0% |
| **總數** | **99** | |

c. 手提電話短信(SMS) (收到的 SMS 的數目)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0 | 31 | 32.3% |
| b. 1-3 | 53 | 55.2% |
| c. 4-6 | 8 | 8.3% |
| d. >6, | 1 | 1.0% |
| e. 不清楚 | 3 | 3.1% |
| 沒有回答 | 3 | 3.1% |
| **總數** | **99** | |

d1. 致電到公司的電話號碼 (電話數目)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0 | 31 | 31.3% |
| b. 1-3 | 49 | 49.5% |
| c. 4-6 | 9 | 9.1% |
| d. >6 | 1 | 1.0% |
| i. 不清楚 | 9 | 9.1% |
| **總數** | **99** | |

d2. 致電到私人電話號碼 (電話數目)

| | 頻數 | 百分比 |
|---|---|---|
| a. 0 | 22 | 22.2% |
| b. 1-3 | 68 | 68.7% |
| c. 4-6 | 4 | 4.0% |
| d. >6 | 1 | 1.0% |
| i. 不清楚 | 4 | 4.0% |
| **總數** | **99** | |

2. 一般來說，你會否因收到未經許可的電子訊息而感到受滋擾?

| | 頻數 | 百分比 |
|---|---|---|
| 1 (不滋擾) | 1 | 1.0% |
| 2 | 4 | 4.0% |
| 3 (一半一半) | 12 | 12.1% |
| 4 | 21 | 21.2% |
| 5 (非常滋擾) | 60 | 60.6% |
| N 不清楚/ 難說 | 1 | 1.0% |
| **總數** | **99** | |

3. 你如何處理未經許可的電子訊息? (可選多於一項) N=99

| | 頻數 | 百分比 |
|---|---|---|
| a. 回覆/ 要求寄件人從分發名單中除名 | 37 | 37.4% |
| b. 刪除/ 不理會該類訊息/ 掛斷電話 | 88 | 88.9% |
| c. 將寄件者加入過濾名單內 | 47 | 47.5% |
| d. 將你的傳真號碼登記在電訊管理局的「不收傳真名單」 | 5 | 5.1% |
| e. 更改電話號碼/ 傳真號碼/ 電郵地址 | 5 | 5.1% |
| f. 向服務供應商投訴 | 8 | 8.1% |
| g. 向電訊管理局投訴 | 1 | 1.0% |
| h. 向其他機構投訴，如個人資料私隱專員公署、立法會議員、傳媒等) | 4 | 4.0% |
| i. 其他 | 8 | 8.1% |
| **總數** | **99** | |

4. 你有沒有採用任何方法，阻截未經許可的電子訊息? (可選多於一項)

| | 頻數 | 百分比 |
|---|---|---|
| A. 有, (可選多於一項) | N=68 | |
| a. 使用過濾電郵軟件 | 63 | 92.6% |
| b. 使用「拒絕沒有來電顯示的電話」或「來電顯示」服務 | 25 | 36.8% |
| c. 將你的傳真號碼登記在電訊管理局的「不收傳真名單」 | 6 | 8.8% |
| d. 將你的電話號碼登記在電訊服務供應商，要求拒絕接收宣傳電話 | 6 | 8.8% |
| e. 其他 | 1 | 1.5% |
| B. 沒有, 因爲 | N=31 | |
| f. 不清楚有什麼方法可以使用 | 12 | 38.7% |
| g. 該類工具無法有效阻截未經許可的訊息 | 16 | 51.6% |
| h. 其他 | 4 | 12.9% |

5. 你是否支持政府監管發出未經許可的電子訊息的活動?

| | 頻數 | 百分比 |
|---|---|---|
| A. 支持 | 85 | |
| a. 引入法例監管 | 61 | 71.8% |
| b. 發出業務守則 | 51 | 60.0% |
| c. 收緊現時發牌條款 | 46 | 54.1% |
| d. 其他 | 4 | 4.7% |
| B. 不支持 | 13 | |

6. 你支持政府禁止濫發電子訊息的主要原因是 (可選多於一項) N=85

| | 頻數 | 百分比 |
|---|---|---|
| a. 該類訊息浪費互聯網及電訊網絡的資源 | 66 | 77.6% |
| b. 該類訊息增加業務成本(如 互聯網/ 電訊服務費用) | 52 | 61.2% |
| c. 減低企業的效率 | 66 | 77.6% |
| d. 資訊保安問題，如容易散播病毒 | 63 | 74.1% |
| e. 該類訊息非常滋擾且浪費時間 | 69 | 81.2% |
| f. 其他 | 5 | 5.9% |
| g. 無特別原因 | 0 | |

7.你不支持政府禁止濫發電子訊息的主要原因是： (可選多於一項) N=13

| | 頻數 | 百分比 |
|---|---|---|
| a. 資訊科技及電訊業會以更有效的方法處理 | 5 | 38.5% |
| b. 由政府處理成本太貴 | 3 | 23.1% |
| c. 政府沒有足夠技術水平處理問題 | 6 | 46.2% |
| d. 政府介入可能會削弱言論自由及資訊流通 | 10 | 76.9% |
| e. 其他 | 5 | 38.5% |
| f. 無特別原因 | 1 | 7.7% |

**ANNEX II - HKISPA's Survey of ISPs in Hong Kong**


# IS SPAM AN ISSUE IN HK?
# HKISPA'S SURVEY OF ISPS IN HONG KONG

**By THE HONG KONG INTERNET SERVICE PROVIDERS ASSOCIATION**

**January 2004**

***Is SPAM an issue in HK?***
***HKISPA's survey of ISPs in Hong Kong***

**Background to the Survey**

In the past year there has been a rising number of spam related complaints to OFTA, Consumer Council, Media and ISPs along with an increasing awareness of the commercial impact to online business (service providers, legitimate online marketers, vendors).

There has also been a noticeable overseas trend in 2003 towards legislation covering spam.

The above lead to several events; OFTA & HKISPA held meetings around midyear and OFTA asking the HKISPA to help gather statistics. The HK Anti Spam coalition was formed in July. This group was also hungry for some HK specific statistics to give backing to the recommendations it was considering. The Anti Spam Task Force (ASTF) under HKISPA came into being in September to help drive the anti spam efforts of the HKISPA.

Thus the survey was developed with the following broad objectives;

- To get some quantitative information on the size of the problem in HK. This would enable us to, among other things, compare to overseas data.
- To identify the key characteristics of HK spam. In particular to try and quantify how much spam is originated within HK.
- To understand what is being done today, if anything, by ISPs and what ISPs would consider as the most effective means to combat spam.

**HKISPA's survey of ISP's**

There were 11 respondents to the survey, covering a broad representation of all types of ISPs including some non-members of the HKISPA. It was well supported and the survey covers the majority of Internet users in HK, over 90%.

The survey was in 4 sections and covered the following questions;

Sect 1. Covering the area. Is SPAM regarded as a problem?

- SPAM ranking in severity as an issue versus other issues
- Number of complaints received on spam
- Nature of the complaints i.e. are they about receiving spam or unable to send email (as a result of the ISP email server being blocked by another ISP)

Sect 2. Asking. How big a problem in SPAM?

- How much email carried is spam
- How much is of HK origin
- How much is from other Asian sources (and where from?)
- How often is email being blocked?

Sect 3. Asking. What are ISPs doing?

- Have they implemented anti-spam procedures?
- What sort of procedures have they implemented?
- Which they consider is most effective?
- Have they a charged service and if so what is the take up

Sect 4. Asking ISPs opinions

- Would they see a benefit in ISPs working together?
- If so, what sort of things would be the most effective?
- Will legislation help address the problem?

**The survey's detailed Results**

The following are the detailed results of the survey.

Is SPAM is a major issue for ISPs in HK. YES. All but 1 agreed.

Spam was identified as in the top 3 issues for all but 1 ISP.

| | |
|---|---|
| Lots of spam complaints are received by ISPs: | |
| Half the ISPs receive | > 500 complaints per month |
| Majority relate to receiving spam | >40% of the complaints |
| Less are for unable to send email | >30% of the complaints |

**How much email is spam in HK**

| # ISPs | % Spam | Size |
|---|---|---|
| 2 | >70 | S |
| 1 | 60-70 | M |
| 1 | 50-60 | L |
| 0 | 40-50 | - |
| 3 | 30-40 | L&M |
| 2 | 20-30 | L&M |
| 2 | <20 | L&M |

S, M, L refers to the size of the ISP in that response category. (Small, Medium and Large)

Weighting the above responses we can say that HK spam is in the region of 50% of email handled by HK ISPs. This is in line with International trends.

**How much Spam is originating in HK**

| # ISPs | % HK Spam | Size |
|---|---|---|
| 1 | 30-40 | M |
| 1 | 10-20 | S |
| 4 | 5 -10 | L&M |
| 5 | <5 | L&M |

Weighting the above responses we can conclude that HK originating spam is in the region of 5% of the total spam.

**How much Spam is originating from other Asian sources**

| # ISPs | % Asian | Size |
|---|---|---|
| 1 | >60 | M |
| 1 | 50-60 | S |
| 3 | 40-50 | M |
| 1 | 30-40 | M |
| 2 | 10-20 | L |
| 2 | <5 | L&M |

It is difficult to draw a conclusion from the above, however it is clear that more Asian spam is coming from outside HK than inside. This was consistent across all respondents.
We would estimate that in the region 20-40% of the spam is Asian sourced. The Mainland is the most cited source with Taiwan next most prevalent. Korea was also cited. No other languages were cited.

Wide ranges of results were obtained regarding ISPs having their mail servers blocked because of sending spam.

| # ISPs | Freq | Size |
|---|---|---|
| 1 | weekly | L |
| 2 | monthly | M |
| 5 | yearly | LMS |
| 2 | never | M |

**Are ISPs addressing the issue**

All ISPs but one have implemented their own anti-spam measures. These include

| | |
|---|---|
| Self built blacklists | 10/11 ISPs |
| Commercial blacklists | 6/11 |
| Rate limiting | 6/11 |
| Content analysis | 6/11 |
| Info sharing | 1/11 |
| Other analysis | 5/11 |
| Commercial product | 1/11 |

However there was no consensus on the most effective method. Some noted that the method they considered the most effective was not what they had implemented.

Three of the ISPs provide chargeable anti-spam services and take up is considered good.

**Suggestions to address SPAM**

All the respondent ISPs think it's a good idea to work together. This was interesting as it is probably the first time that all ISPs have been united. Given the highly competitive nature of the industry, it is not common.

- All ISPs think a common blacklist is the most powerful means.

Other suggestions from ISPs include;

- Sharing information.
- A charging mechanism to send and deliver bulk email.
- Legislation.

**ISPs view on Legislation**

It appears ISPs are uncertain if will address the core issue of materially reducing the amount of spam. However the general feeling it would be a positive step. When asked if legislation would help or not, we received the following response;

| | |
|---|---|
| Help | 8 |
| Won't help | 2 |
| Unsure | 1 |

**The potential economic impact of SPAM to Hong Kong.**

Although not part of the survey the HKISPA have endeavored to place a potential economic impact on the local economy. Given that the level of spam is HK has been demonstrated as similar to international levels and that cost structures are in the same realm as the countries that have produced economic data, we thought it would be interesting to see the results. The HKISPA does not represent these figures as being the result of a proper economic study.

International studies put the impact between USD10-20 billion pa. There are at least two research findings that are at the lower end of this range and one at the upper end.

In overseas research, losses are also put at USD874 per employee pa. Other research findings have it less, but still of the same order of magnitude.

One study has also quantified lost time in the work place at 6.5minutes per employee per day. This is referred to as Spam related "absenteeism".

If we apply the above economic data to Hong Kong with the following assumptions, we can obtain an estimate of how large the economic impact might be to the Hong Kong economy.

We have used as an assumption that 44% of the active workforce is connected to the Internet. This is on the basis that government statistics say that 44% of businesses are connected. We used the workforce as being 3.5Million with an unemployment rate of 7.2%. Again these are based on current government statistics. For average monthly salary of an employee who uses email we have estimated at HK22K per month. Government statistic have the average of a non professional or managerial as 11K, so we have doubled this figure as an estimation.

Applying the above assumptions and data, the potential loss to the HK economy is in the region of HKD9.7Billion pa. And the loss due to spam "absenteeism" HKD6.8Billion pa or $22Million per day or $13 per employee per day.

The above figures could be argued in the details and the HKISPA would support a detailed study, however the point to note is that however the figures are calculated and whatever the assumptions, the losses to the HK economy are likely to be very high.

**In Summary**

- Spam IS a major problem in Hong Kong.
- It's a high priority issue for all ISPs.
- A large proportion (50%) of email in HK is spam.
- Though most of the spam is not from HK, a significant amount (5%) is.
- Even more is from other Asian sources (20-40%). Mainly China.
- All ISPs have procedures in place, but are not highly effective
- Varying views on most effective method to combat spam
- All ISPs think it's a good idea to work together – developing a common blacklist & info sharing info most popular idea
- Most, but not all, believe legislation would help
- SPAM could be costing Hong Kong economy as much as $10billion pa