

**Response to the
OFTA Consultation Paper 2004
on Unsolicited Electronic
Messages**

Date: 24 Oct 2004



Professional information security Association

Tel: (852) 8104-6800

Fax: (852) 2900-8338

Email: info@pisa.org.hk

Address: Unit 1211, Hang Shing Building, 363 Nathan Road, Hong Kong

Table of Content

<u>Introduction</u>	4
<u>PISA Intention to Contribute</u>	4
<u>Scope of Comment</u>	4
<u>Overview</u>	5
<u>Spamming interweaving with Other Attacks</u>	5
<u>Problems of Combating Spam</u>	5
<u>PISA's Proposed Approaches on Combat Spamming</u>	6
<u>Comment on the possible Legislation</u>	7
<u>Proposed Definition of Spamming</u>	7
<u>Principle of Anti-SPAM Legislation</u>	7
<u>Technical Measures</u>	10
<u>Black Lists (Real-time Blackhole Lists)</u>	11
<u>Technology to enforce identifiable Sender</u>	12
<u>Technology to close down Open Relay</u>	13
<u>Technology to filter mail content</u>	14
<u>Technology measures against Directory Harvesting</u>	15
<u>Industrial Partnership</u>	16
<u>ISPs collaboration and OFTA regulation</u>	16
<u>Corporation and eMarketer</u>	16
<u>Software developers</u>	16
<u>Education of the Public on anti-spam practices</u>	17
<u>International Cooperation</u>	18
<u>Conclusion</u>	19

INTRODUCTION

PISA Intention to Contribute Professional Information Security Association (PISA) was founded in 2001 with the mission to contribute to the community utilizing our expertise in the domain of information security.

The problem of spamming has affected the Internet user. There were cases where spammers exploit the vulnerability of personal and company computers in order to send huge amount of spam mails. Spam mail is also a medium of spreading virus and phishing attacks. As professionals in the information security sector and Netizens we do understand the risk of this uncontrolled beast. Members at PISA take the issue of spam seriously and organized an anti-spam email workshop to investigate the issue and related technologies on 07 Aug 2004.

We hope that our comment on anti-spam legislation and our technical researches will contribute to the effort to lay down a strategy for Hong Kong to combat spam.

Scope of Comment

Spam is hitting more and more people. As stated in the beginning of the consultation paper, Spam is interfering with many people's life through different channels including email, SMS, fax or other forms of spam. In our response to the consultation paper, we will focus on email spam; however, the general principle and spirit behind our stand on whether to legislate and the goals behind such legislations are generally applicable to other forms of spam.

OVERVIEW

Spamming Interweaving with Other Attacks

- Spamming has become a major problem, causing mail system paralysis and lowering the productivity. Furthermore, we would point out that spamming also breeds other kinds of Internet crimes and attacks.
2. Phishing is a special kind of spamming with fraudulent intent. Phishing was previous only serious in USA but has been spreading to Europe and Asia in the past year. Phishing is powered by the spamming business that provides abundant business targets (victim email addresses) as well as the IT infrastructure (open mail relays to send out the spamming emails).
 3. Spamming and worms have also formed a kind of symbiosis relationship. Some of the worms use available spamming technologies in the initial birth phase to gather a critical mass of infected machines to start a reaction chain in the Internet. On the other hand, more and more worms are now programmed to open the infected machines as open mail relays to serve the spammers.
 4. A certain portion of spammers choose to make use of the open mail relays on compromised machines. These compromised machines are either hacked or infected by computer worm. That implies these spammers may involve in hacking directly or indirectly.

Problems of Combating Spam

1. The implementation of the current Internet mail technology allows unauthenticated email to a great extent. The sender of an email can be spoofed easily and there is no enforcement of policy to validate the sender or sending domain.
2. The internet is distributed and decentralized. Technical controls on combating spam requires lots of coordination and time-consuming.
3. Spammers choose to send out spam mail from locations where there are barriers to effective close down of the sending sources, for example, places with
 - a. different language and/or time zone to the receivers
 - b. no or lax legislation against spamming activity or hosting of facility for spamming
4. Legislation against spamming does not exist or is not mature in many places of the world. Even when there is legislation, jurisdiction has difficulty when spammers come from another country or another province/state with different laws.
5. The victims of spam have difficulty in reporting the case, either because they have no technical skill to identify the source of spam or they do not know who to report to.

PISA's Proposed Approaches on Combat Spamming

At PISA, we believe anti-spam legislation is a right starting point on combating spam. However legislation alone is not the only and most effective solution to stop spamming which is highly sophisticated, is crossing borders in nature and is evolving with new technologies. Like other social and economical problems, an integrated approach will help us to win this battlefield.

Mr. Robert Horton, chairperson of the United Nation ITU WSIS Thematic Meeting on Countering Spam in July 2004, laid down a five-layered approach to address the problem of spam.

- a. Legislation
- b. Technical Measures
- c. Industry Partnerships, esp. with ISPs, carriers and direct marketing associations
- d. Education of consumers and industry players
- e. International Cooperation at the levels of government, industry, consumer, business and anti-spam groups

This framework provides a more thorough view of the efforts required to combat spamming. We will follow such framework to deliver our comments from this point onwards.

COMMENT ON THE POSSIBLE LEGISLATION

Proposed Definition of Spamming Spamming, should be defined as an act of sending messages without fulfilling all the requirements of the “opt-out” provision or an act of not enforcing opt-out requests while being the originator of such messages. Spam is the product or result of spamming.

Principle of Anti-SPAM Legislation

Objective of Legislation

The objective of the legislation should be

- setting an enforceable definition to spamming;
- sending a clear signal to the public that spamming is illegal, to deter spamming activity. By deterrence, we do not mean proactive investigation. We want the public and business community to be aware of their legal liability when sending mass mail and realize their responsibility in flight against spamming.
- positioning Hong Kong as a “good neighbour” in the development of Internet. Legislation cannot effectively solve all the problem of cross border spamming which is the major source of spams in Hong Kong. However, failing to establish enforceable anti-spam laws, Hong Kong could make herself a potential safe harbour for international spammers.

Criteria for Legislation

- We agree that in the introduction of additional legislation or regulation on spamming, we need to strike a balance between the socio-economic impact of spam and the effectiveness and efficiency of the telecommunication medium for the general community and the business sector.
- The legislation should be clear and practical. It should grant the local law enforcement authority the necessary power.
- It should enable Hong Kong courts to exercise overseas jurisdictions.
- On the other hand, we have to avoid and minimize the adverse effect and side effect of legislation. We have to avoid over-broad definition of spam that might crossfire normal business promotion activities. We should also appreciate the self-regulation of industry sector, instead of replacing it by legislation, Last but not the least, legislation should not impact the rights and freedoms currently enjoyed by the citizens, to advocate their belief and religion.

Adopt “Opt Out” System as control mechanism

1. There are two distinct approaches to enforce anti-spam legislations. They are commonly known as “opt-in” and “opt-out” mechanisms. In essence, “opt-in” is considered a more stringent approach as it requires all recipients to grant the sender explicit consent before the sender can send the recipient any message. The advantage of “opt-in” is the ease of enforcement. The sender will have to prove the innocence of sending every mail, and the mechanism could shut down all the “cold calls”. The “opt-out” approach is more lenient than the all-out, “opt-in” approach. The direct marketing industry can still make cold calls, but at the same time, the recipients are given the right to opt out further communication with the direct marketer. We are recommending the “Opt-Out” approach when legislate for anti-spam and the law should be applied to commercial mail only. We regard this approach more acceptable to the community of Hong Kong who conduct intensive business activities.
2. The law should require the sender of mail to comply with ALL the provisions of “Opt out”.
 - a. The mail content must contain a real and effective reply email address of sender so that the receiver can contact the sender to unsubscribe from the mailing list.
 - b. The sender email address and the email header shall not be spoofed.
 - c. The mail subject line should be labeled with words like “ADV” to identify it is a promotion email.
3. The “Opt out” mechanism should be reasonable and easily achievable for receivers.
4. The law should avoid the possible abuse of the un-subscription mechanism. Here are some example of possible abuse which are reported after the USA CAN-SPAM Act:
 - a. Recipient being forced to act against their free will, when they must choose from certain menus to unsubscribe.
 - b. Recipient being forced to interact more than merely confirming the unsubscription (e.g. answering a survey or solving a puzzle)
 - c. Recipients being bombarded by pop-up advertisements of a web-based unsubscription mechanism.

Oversea Jurisdiction

The law should enable Hong Kong courts to exercise overseas jurisdictions. A good example in the adoption of overseas jurisdictions in Hong Kong legislation was the Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 that deals with three computer related offences, which are prohibited by the Telecommunication Ordinance and Crimes Ordinance.

Make service providers responsible and empower them

The law should empower the ISP to suspend or terminate the network or email services of a spamming source, whether it is operated by a spammer or not.

The law should empower law enforcement to investigate spamming case with cooperation from ISP, network providers, corporations and individuals involved in spamming activities.

The Expected Effect & Reaction of Proposed Legislation

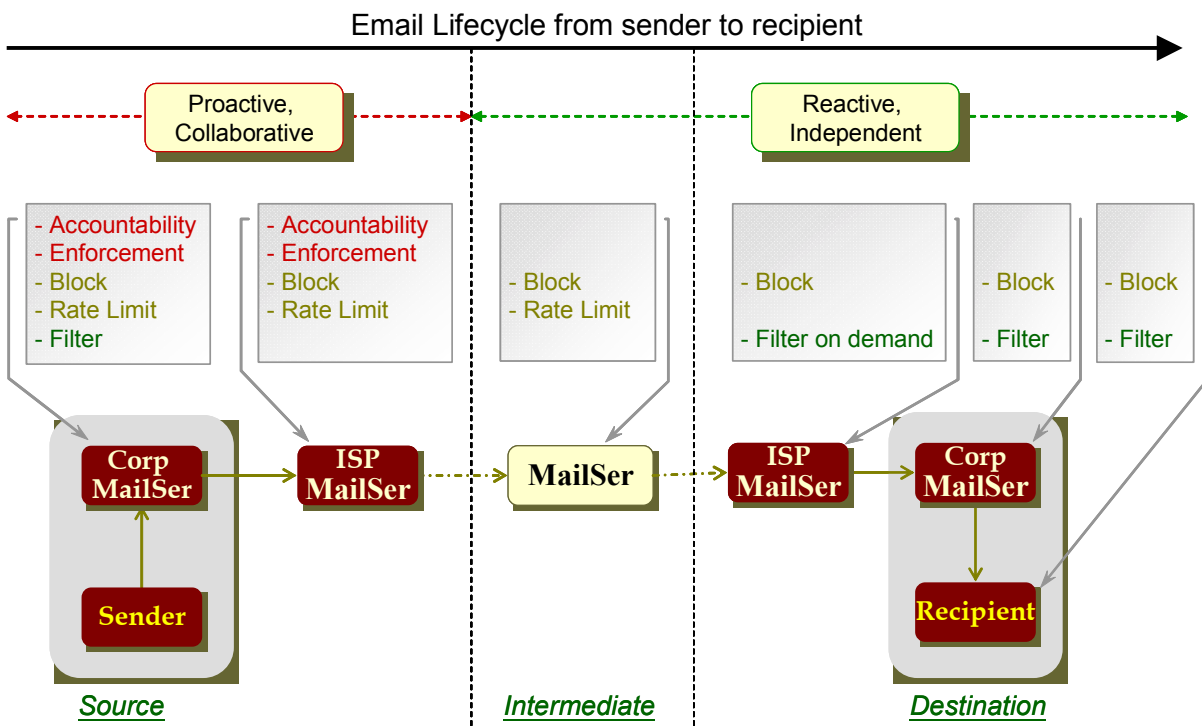
The matrix below shows the anticipated consequences and possible reactions of the parties under our proposed legislation directions.

Party	Legal Liability	Challenges and Difficulties	Benefit to party	Possible reaction to new legislation
User	N/A	Unable to distinguish sending what is spamming Afraid of committing the new anti-spam law when sending message to large group of receipts.	Save time and effort to deal with spam. Receive less email with malicious intent.	More careful when using email and internet.
Corporate	May be liable for damages caused by unprotect systems which enable spamming	Both administrative and technical compliances are required; 1. Enforce security policy on using network and emails 2. Protect email server from spammers	More efficient use of company resources such as time, internet bandwidth. Improvement of company image – good email citizen and good respect of the Internet infrastructure	Worry about cost implications for compliance. Stop hiring spammers.
eMarketer	Criminal charges when not comply with new law	Implement controls to comply with opt-out requirements.	eMarketer will enjoy a sustainable growth of the eMarketing industry as promotional message will reach potential clients and also does not mixed with malicious messages.	May move operation center from HK Transfer the compliance cost to clients Deliver more sophisticated solutions to clients
ISP and network providers	Fine if failed to cooperate in investigations	Consensus on the sender identification technology to adopt; additional cost for compliance;	More efficient use of resources like bandwidth, technical support: reduce cost; improve customer satisfaction; ultimately elevated the competitiveness	Worry about cost implication for compliance Consider collaborations among industry.

TECHNICAL MEASURES

Strategies at Points of Control of Spam

The diagram below shows a life cycle of an email message. A mail message travels from the sender to the recipient along a path. If the sender has a corporate email server, the email passes through the corporation mail server (Corp MailSer) and in some cases, the email also passes to the ISP mail server (ISP MailSer) for delivery. If the sender has no corporate email server, the mail will be passed to ISP mail server (ISP MailSer). The email message may pass through intermediate mail server (MailSer) before reaching the ISP's or corporation's mail server at the recipient side. The email finally reaches the recipient's ISP or corporate mail server. The recipient then retrieves the email.



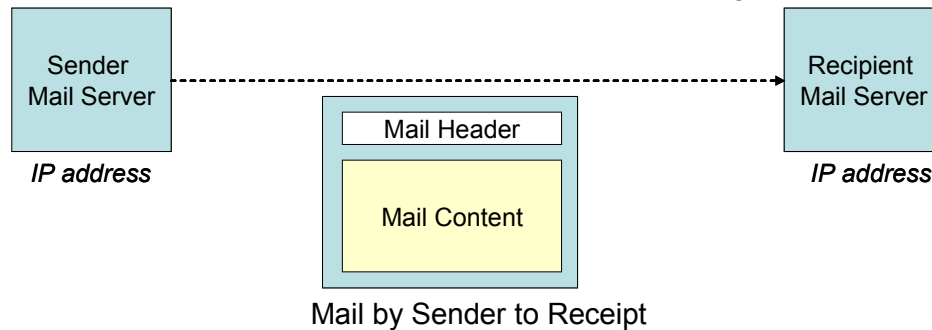
Anti-Spam Strategy in the Life Cycle of an email message

Remark: In the typical spamming attack where a spammer has his controlled mail server, there is neither ISP mail server nor intermediate mail servers involved. The spammer uses his own mail server to connect directly to the mail server of the recipient. The life cycle of the email message is a reduced version of the one shown above.

The effort of legislation mainly targets at the sending side where the sender can be held accountable for his action. It is a more proactive approach and can save bandwidth. However, legislation and enforcement of law take time to develop and always require cross-border collaboration.

PISA believes a proactive and collaboration measures at the origin of spam mail are more effective and efficient.

At the recipient end, it is more reactive to deal with the spams but the recipient can take more independent action. The recipient can use different technologies to combat spam.



1. The recipient can determine to block all mail from the sending mail server using its IP address or email domain. This is the approach taken by Black List.
2. The recipient can determine if the sender mail server is the valid mail server to send out the email for the domain. This approach is called Mail Server Validation.
3. The recipient can also filter the email message if the mail header does not comply with the standard way, or if the content is verified to contain advertisement or spam like features. This approach is called Content Filtering.
4. The recipient may suspend communication with sender who is trying to send testing email to non-existent user of the domain. This approach is called email address harvesting prevention.
5. The email server administrator may stop external party from abusing their email server as mail relay for spam. This approach is called Closing Down Open Relay.

Black Lists (Real-time Blackhole Lists)

Black List (or Real-time Blackhole List, i.e. RBL) can be of two types: spam sources (IP address or domain) black list and the open mail relay servers black list. There are various black lists around the world. They are operated by commercial and voluntary entities.

1. Black list is effective because it consumes only little resources like network bandwidth, disk space and processing time. The benefits of a local black list are that:
 - a. it provides transparency of the local spammer or open relay to local and external parties, making Hong Kong a friendlier place of business.
 - b. it helps building up a culture of reporting and responding to spamming

- c. if the list is available free of charge to the public, it can lower the cost of deployment of black list.
2. The disadvantages of a local black list are that:
 - a. it will discourage the development of commercial black list service
 - b. Mandatory enforcement of black list will require investment from ISPs. Small ISPs may be at disadvantage.
3. **PISA is open to the option of a local black list. We would highlight that, if a local black list is to be set up, several aspects need to be observed:**
 - a. Transparency There must be clear and published criteria and the tests applied for classifying a mail server as open relay or spam source.
 - b. Authority The black list management organization should have the authority to handle the report and appeals, and to liaise with ISP and network providers.
 - c. Neutrality The black list management organization should be a neutral body to handle the report and appeals impartially.
 - d. Handling Unavoidable Error The black list mechanism can make mistakes in putting an innocent entry into black list. Effective appeal system must be in place.
 - e. Resources The update and monitoring of black list is resource intensive. Sufficient resources must be allocated to the black list management organization.

Technology to enforce identifiable Sender

Mail Server Validation

"Mail server validation" makes use of specific information stored in Domain Name Server (DNS) for validating the origin of an email. One traditional way is to have receiving server performs reverse PTR record lookup of the sending server's IP address in DNS. Receiving server only accepts email if the sender's claimed domain name matches the DNS information. While this method is not originally designed for anti-spam purpose and it has some limitation, some service providers have published a number of proposals on domain-level authentication framework with similar concept. Three well-known proposals are: (1) Sender Policy Framework (SPF); (2) Sender ID; and (3) DomainKeys. SPF is designed to fight email address forgery by establishing a policy framework and a sender authentication scheme with the help of DNS. Sender ID is a combination of the SPF and Microsoft's Caller ID technology. Domainkeys is proposed to use public-key technology and DNS to prove the origin and contents of an email. It involves authentication framework for email that stores domain based public-key in DNS for digitally signing of email.

Microsoft, Yahoo and some other organizations have submitted Sender ID, Domainkeys and other relevant proposals to the Internet Engineering Task Force (IETF) for seeking the Internet standard approval. However, IETF has rejected Microsoft's Sender ID proposal in

middle of September due to Microsoft refuses to reveal details of a possible patent application on its proposed technology. The other recently submitted proposals are still in draft stage and waiting for approval.

Advantages:

- a. The configuration is done at the DNS server and is transparent to user.
- b. It can validate sending server before accepting email. Therefore spam sender cannot be anonymous.

Issues:

- a. A universally accepted standard or pool of standards is not yet available. The recent disbandment of the IETF RFC committee on Sender ID technology implied such standard might not be in the near future.
- b. It takes a long time, if not forever, to have every DNS server to add the capability to be compliant with the new standard.
- c. It is not applicable to third party mail services, e.g. some companies assign a third party, for example, email virus filtering service provider to act as mail forwarder for them to filter out viruses.

PISA is happy to see the development of mail server validation technology. The government should encourage universities of Hong Kong to research on applicability of these technologies to the community of Hong Kong. The government should also encourage ISPs and email service providers to join the research and adopt some of these technologies in their platforms.

Mail Sender Validation

"Mail sender validation" makes use of digital signature of either public key infrastructure (e.g. S/MIME) or web of trust (e.g. PGP) to validate the source of the email and the integrity of the email message. The technology is proven and is accepted in the technical and information security community. Serious corporations like CERT teams are using this technology to communicate prudent information. The technology, however, has not been popularized to common user. Furthermore, the recipient needs to check the digital signature for each email. This is more time-consuming. Some spam email messages forge to be signed email, e.g. adding "PGP begin" and "PGP End" delimiters in an email message, to fool recipients. The technology is very useful but not a cure for the general public at this moment.

Technology to close down Open Relay

There are simple ways to stop mail server from being used as open mail relay.

Promote Best Practices in Mail Server Counter Open Relay Management

PISA would propose that more education is required for system administrators to close down their email server relay feature. The best practices are:

1. For Sendmail running on Linux, disable the "VRFY" and "EXPN" Sendmail commands. For Microsoft Exchange on Windows, use the more current version with updated patch which have the two commands disabled.
2. Use email server software that only accept email where either recipient or sender is within their domain (by default) unless relay enabled (e.g. Sendmail 8.9 or later).
3. The email server software should not accept email if the "From:" address has a domain that is not real.
4. The email server software should be smart enough to verify the claimed "From:" address matches the numeric IP that is connecting to the email server (e.g. Sendmail 8.9 cannot pass this requirement, use newer versions).
5. Ensure the latest security patches or hot fixes are applied in order to prevent the servers being hacked and turned into open-relay by attackers.
6. Perform periodic health check of Internet accessible machines, including the check of whether unexpected service ports are opened and whether email server allows open relay.

Advocate the use of Authenticated SMTP technology

PISA would propose to use Authenticated SMTP mail. Everyone accepts logging in a POP3 mail server to retrieve email. In the same way, it is easy to implement authenticated SMTP for sending out email. Even if the mail server is mis-configured, it will be much harder for spammer to abuse the use of the server as relay if they need to crack the password of an email account before using it. This can be applied in email servers of both ISP and Corporation.

Technology to filter mail content

Content filtering technology is the last line of defense when the email server has no clue if the sender is a spammer. Content filters analyze email messages and tag messages that are suspected spams and let the user to delete or accept them. Currently, content filter technologies involve more than simple keyword matching. Statistical analysis of mail content like Bayesian filter is very popular. Its advantages are (1) the ability to look at the email message as a whole to give a more accurate rating and (2) the ability to learn from user feedback to fine tune the rating scheme. There are also content filters using heuristic analysis of mail content to catch evasion tricks. Some content filtering technologies employ collaborative spam identification and response to improve their performance. Content filtering is very processing intensive. The best approach is to integrate first line defense technology like RBL with content filtering to screen out identifiable spammer sources.

Technology measures against Directory Harvesting

Spammers use email directory harvesting techniques to exploit the available email addresses of a company. Directory harvest attack occurs when a spammer uses publicized or known email addresses to steal other valid e-mail addresses from corporate or ISP mail servers. The technique takes advantage of network vulnerabilities that allow the spammer to send e-mails to randomly generated e-mail addresses. The spammer then collects all the e-mail addresses that the receiving mail server acknowledges as being valid. Some email servers have feature to minimize directory harvesting attack by temporary suspending the session of failed mail recipients scanning attempts. The government can provide more technical guidelines for system administrators to make use of the features.

Technology is an important arm of the Anti-Spam strategy. The anti-spam technology is new and complex. There is a huge gap in the technology know-how in business sectors and the general public. PISA would recommend the Government to provide support to close the gap. More guidelines, seminars and resources can be collaborated by the industry sector, the professional association and Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to provide information on how to choose the appropriate technologies and how to apply them in their environment.

INDUSTRIAL PARTNERSHIP

ISPs collaboration and OFTA regulation “Code of Practice from HKIPSA” is becoming ineffective to stop SPAM. Apart from the anti-spam legislation, OFTA needs to take more active role to regulate.

Regulation must be provided to enforce some of the Anti-Spam Code of Practice of HKISPA. The regulatory requirements for compliance should include:

1. ISPs and other Internet network providers (e.g. Internet Data Centre) shall have in the Acceptable User Policy a mandatory clause to prohibit users carrying out virus & hacking attack and spam activities on the provided network; to grant ISP right to apply rate limiting, or suspend, or terminate the services provided to user in case user violates such terms; to empower ISP to refer case to the law enforcement.
2. ISPs and other Internet network providers shall provide an abuse contact by email and otherwise to the public for reporting abuse of use cases. Appropriate actions should be taken upon receiving complaints via these channels.
3. OFTA as the regulatory body to monitor and enforce the requirements and receive complaint reports of non-compliance.

Remark: the anti-spam legislation might include some of the above improvements in regulatory requirements, e.g. granting ISP right to suspend or terminate the network service provided to a user who is sending out spams.

Corporation and eMarketer

Corporation should enforce employee policy and security policy to avoid spamming activities. Direct Markets should enforce a common policy to use massive electronic direct mail. Failing to achieve this would invite more intervention from the government. Government should include corporation and eMarketer as target in the anti-spam promotion campaign.

Software developers

Email server and client developers should make their software “anti-spam friendly”. Email servers should come with anti-spam feature turned on by default. Email clients should be equipped with simple user interface to examine the sending source of an email in order that the user can locate the spammer source easily and make a complaint to the relevant party.

EDUCATION OF THE PUBLIC ON ANTI-SPAM PRACTICES

The success of Internet is that it is easy to use. A person knows how to use mouse and keyboard will be able to surf the web and send/receive email. The low learning barrier produces a general misimpression in the public that Internet and email is safe. The public is attracted by the benefit is not being told about the inherent risk. A casual user of the Internet exposes himself to malicious code, identity theft and spamming.

The other reason for user not aware of technology risk is that behind the user friendly interface there are complicated technical mechanisms. It is a difficult task to explain to users from various backgrounds on the enabling technology and the design faults. For example, spamming involves the use of domain name server, electronic mail protocol and mail servers. There is no easy way to explain to the public on the possible misuse and risk, without hours of lectures.

The challenge we face is a remarkable one. If we are not able to raise the public awareness of Internet security, the future of Internet will be on the hands of the irresponsible users and criminals. Education on responsible and cautious use of Internet and email must be introduced to different segments of the public.

General users should be reminded that in order to stop their email address being abused, they should

- Do not list more email addresses on web site than you need to. Each additional email address will attract spam
- Consider having your users not supply valid email addresses (company email address) if they post to newsgroups
- Educate user on the advantages of "bcc" when sending emails.

General users should be educated how to use extract the email header to report spamming.

INTERNATIONAL COOPERATION

Spam is an international issue. An effective system to combat spam must be a globalized one. We are delighted to see the United Nation taking the spam problem serious. For example, U.N. had held the ITU WSIS Thematic Meeting on Countering Spam in July 2004. We hope that U.N. can take the lead

- to facilitate the standardization of legislation against spam
- to facilitate the enforcement of anti-spam law cross-border. For example, an international anti-spam convention which requires signing nations or economic entities to share information, exchange evidence and coordinate enforcement against cross-border spam violations with all other signing countries, can greater reduce the cost of multilateral negotiation.

We hope that the Hong Kong and every other government will set themselves an example to commit to stop spam. We should be a good player and a good neighbour to the Internet community. Hong Kong should be cooperative to oversea governments to chase spammers and close down spamming sources located in Hong Kong.

Hong Kong government can take initiatives to build up relationship (e.g. signing bilateral agreement or memorandum of understanding) with mainland China and strategic international business partner states to share information and coordinate enforcement against cross-border spam violations.

CONCLUSION

PISA has provided our comments on anti-spam strategies under the five layered framework of Legislation, Technical Measures, Industry Partnerships, Education and International Cooperation. We consider a multi-dimensional approach is the right strategy to combat spam.

In legislation, PISA proposes to take an "Opt out" system with a number of considerations for effective implementation and better acceptance. PISA also commends that oversea jurisdiction is required to make the legislation enforceable.

In technical measures, PISA examined the various technologies available and concluded that they are effective to different points of control. The industry sector, professional associations and HKCERT can play a role, with government support to educate the public when and where to apply what technologies. Government can also play a role in encouraging universities to research on the applicability of new anti-spam standards to Hong Kong.

In Industrial Partnership, PISA would point out ISP collaboration and OFTA regulation is vital.

In Education, PISA cannot emphasize more that the challenge we face is remarkable. Education on responsible and cautious use of Internet and email must be introduced to different segments of the public.

In International Cooperation, PISA would emphasize Hong Kong's participation in the international community, to modernize our anti-spam law, to stay ahead of the anti-spam international taskforce and build up relationship with our Internet neighbours to combat spam.

PISA hopes that our comments contributing to Hong Kong and the global Internet village and is willing to collaborate with any party to achieve a safer and more productive Internet.