ANTI-SPAM TOOLKIT

Version I.O

Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

Published by:
Malaysian Communications and Multimedia Commission
63000 Cyberjaya, Selangor Darul Ehsan Malaysia
Tel: 6 03 8688 8000 Fax: 6 03 8688 1000 Toll Free Number: 1-800-888030 http://www.mcmc.gov.my

TABLE OF CONTENTS

ACKNOWLEDGEMENT

MCMC would like to express its gratitude to all those who have contributed to the completion of this Anti-Spam Toolkit. They have selflessly shared their time, expertise and knowledge in the interest of the general public in Malaysia.

INTRODUCTION

The Information Sharing Forum (ISF) was set up by MCMC to bring together the relevant parties into a single forum to share their experiences and expertise for the benefit of the Malaysian network infrastructure and to establish an effective information sharing mechanism.

This coordinated effort enables different network operators, internet backbone providers and other interest groups to analyze and exchange data about attacks and thus stop exploits from escalating and causing damage or disrupting vital systems.

As one of its maiden task, the ISF has developed this Anti-Spam Toolkit. The Toolkit contains the policy and regulatory framework for curbing spam in Malaysia and includes best practices and technical guidelines for organizations and users to take preventive and precautionary measures against spamming.

POLICIES AND REGULATORY FRAMEWORK

POLICIES AND REGULATORY FRAMEWORK

1. Introduction

Spam has increased rapidly with the development of IT technology and the Internet. The spread of spam causes great harm to Internet users by interrupting work, spreading viruses and infringing upon privacy. Service Providers are also not spared as the proliferation of spam contributes towards wasted resources due to increased traffic. Spam is rapidly moving from being just a nuisance to serious problem in many countries.

In a worrying trend, spam is flooding the Internet in an attempt to force messages on people who would not otherwise choose to receive them.

The main reason for spam growth is the low cost of sending such material. Spam costs the sender very little as most of the costs are paid for by the recipient or the carriers rather than by the sender.

To prevent increased proliferation of spam, the government as well as public institutions, general users and providers must play their role effectively in curbing the increase of spamming activities.

1.1 Definition of Spam

All around the world various definitions has been adopted by different stakeholders to define spam. Although all these definitions share some common points, there is still no standard universal definition of spam.

A simple definition of spam would be “all unsolicited bulk e-mails”. Whatever definition is adopted, it all shares the common elements of non-consensual, indiscriminant, repetitious, illegal or unsound content or being forged or altered.

Under the policy framework adopted by the Malaysian Communications and Multimedia Commission, spam is defined as unsolicited electronic messages sent through various communication modes including but not limited to e-mails, mobiles short message (SMS) or instant messaging services where there is no prior relation ship between the sender and the recipient regardless of content whether commercial or non-commercial messages including malicious program and/or data.

2. Malaysia’s Policy against Spam

There is no single solution to the problem of spam. A multi disciplinary approach focusing on regulatory and self-regulatory measures, technical solutions as well as consumer and business education is required to develop sustainable solutions to spam.

In line with this Malaysia has always promoted a multi prong approach in its fight against spam. The success of the strategy depends on cooperative efforts of all stakeholders, from government to industry to civil society organisations and individual users.

2.1 Management of Spam

A comprehensive approach involving all parties (consumers, service providers, industry forums and the regulator) would be most useful in managing the problem of spam.

Consumers who are plagued by spam have the recourse of reporting it to their service providers. In the event the complaints remains unresolved at the service provider end, the complaint can be escalated to the Consumer Forum of Malaysia and thereafter can be further escalated to MCMC.

- Guidelines for Complaints Handling

MCMC released a Guideline on Complaints Handling in July of 2003. The Guideline provides information on making, receipt and handling of complaints and can be assessed at www.cmc.gov.my/consumer/complaint.asp

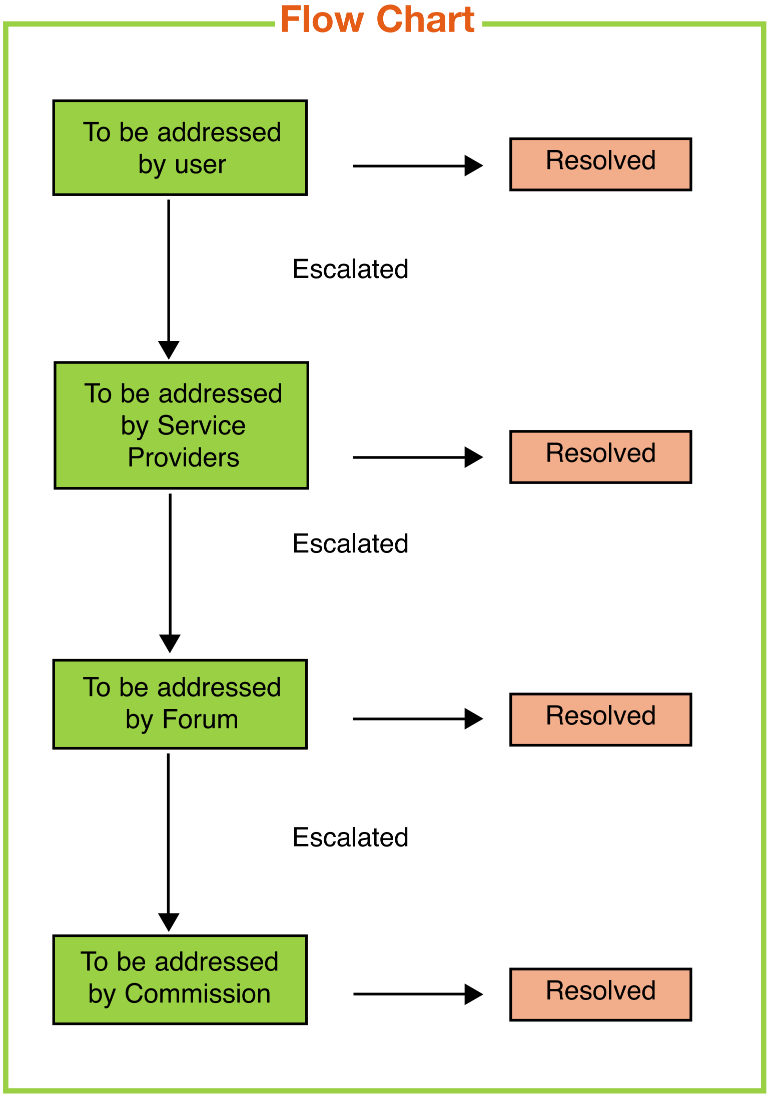
- Online Complaints Form

This online complaint form facilitates complaints from consumers on issues relating to spam. This form is to be read in conjunction with the Guideline for Complaints Handling and can be accessed from the spam portal at www.mcmc.gov.my/what _we_do/ins /ComplaintFormOnSpam.asp

A summary of the process is as below:-

First tier : Self management by users
Second tier : Forward complaint to Service providers
Third tier : If complaints remain unresolved, next recourse is complaint forwarded to Consumer Forum of Malaysia (CfM)
Fourth tier : Still unresolved, matter escalated to MCMC.

Flow Chart



3. Regulatory Framework

MCMC undertook a study in 2003 on Regulating Unsolicited Commercial Messages.

Based on the feedback and comments received, MCMC had adopted a multi-prong approach in dealing with spam:-

(i) Self regulation by users through education and awareness initiatives;

(ii) Management by Service Providers;

(iii) Legislative recourse; and

(iv) International Cooperation.

3.1 Self regulation

The first step towards self-regulation by users is education and the creation of awareness. Awareness and education play a vital role in helping to reduce damages caused by spam.

Users must be aware of the basic rules applicable to unsolicited communications and need to know how they can prevent spam by adapting their behavior.

End users must seek available options i.e. technology to fight spam. They need to know what filtering software available in the market and what service and software providers can do for them.

To create awareness among users, MCMC has developed a spam portal which can be accessed at www.mcmc.gov.my/what_we_do/ins/faq.asp. The portal contains information which is relevant to both the service providers and the end users.

MCMC had also set up the Information Sharing Forum (ISF) to bring together relevant parties into a single forum to share their experiences and expertise for the benefit of the Malaysian network infrastructure, and to establish effective information sharing mechanism.

MCMC has also designated industry forums whose main objectives are to promote self-regulation within the industry. The Consumer Forum of Malaysia is doing its part in the creation of awareness and education of consumers on issues affecting the consumers within the communications and multimedia industry.

One of the initiatives undertaken by the Consumer Forum of Malaysia is the drafting of Industry Voluntary Code for Internet Access Service Providers (sub code) which contains provisions for anti-spam measures.

The main aim of the sub code is to promote the free-flow of information and communications over the internet, to set out a code of practice for Internet Access Service Providers and to improve the standard of conduct within the industry.

Compliance to this sub code is mandated by the Communications and Multimedia Act 1998 (CMA) pursuant to the Schedule on License condition which states the following:-

"The licensee shall comply with any consumer codes registered under this Act which are relevant to the activities of the licensees."

One of the main provisions of this sub code is the anti-spam measures whereby the Service Providers can consider several methods in managing spam to ensure the protection of the user's interest.

The sub-code was duly registered on 1st June 2005 and a copy of the sub code is attached herewith as **Appendix A**.

3.2 Management by Service Providers

Service Providers must be able to act against spammers where they must discontinue subscription of consumers who abuse their networks. This will strengthen the service providers' positions and will deter spammers from using Malaysia as their base.

Management by Service Providers can be divided into two parts:-

(a) Service Providers to enforce the subscription contract between the service providers and their subscribers

Under this category, the Service Provider can impose obligation on the part of the customer not to engage in sending spam messages.

Specific guidance on the dos and the don'ts will be provided to the customer via the Acceptable Use Policy (AUP). In the said AUP, the service providers will provide information to the users on when sanctions or suspension and termination of account would be imposed.

As an example a Service Provider via the AUP could impose an obligation on its customer that all commercial e-mails sent out by the customer must be accompanied by accurate header information, valid return address, functional unsubscribe facility, identity of sender etc. Failure on the part of the customer to provider such information could constitute a breach of his/her obligation under the subscription contract and may result in suspension or termination of his/her account.

(b) Service Providers' obligation under General Consumer Code and the Content Code

The General Consumer Code (Consumer Code) and the Content Code are two codes developed by the Consumer Forum of Malaysia and the Communications and Multimedia Content Forum of Malaysia, two voluntary industry bodies designated as industry forums under Section 94 of the CMA.

Both these codes are registered as voluntary industry codes under Section 95 of the CMA.

Both the Content Code and the Consumer Code play a complementary role to agreements made between the service providers and the users of the service. Content code for example manages content that is provided across a variety of platforms and includes a specific chapter that deals with online guideline.

The Consumer Code likewise endeavors to promote, protect and enhance consumer and customer expectations and rights i.e. the importance of protecting personal information. It lists out good practices that must be employed in collecting and maintaining such information and the need for appropriate security and respect for consumers' preferences regarding unsolicited mails and telephone calls.

3.3 Legislative Recourse

Unlike most other part of the world, Malaysia has legislation in place to deal with spam whereby Section 233 of the CMA clearly deals with the use of "improper use of network facilities or network services.

Section 233 (1) of the CMA states-

A person who –

(a) by means of any network facilities or network service or applications service knowingly

(i) makes, creates or solicits; and
(ii) initiates the transmission of,

any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

(b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address,

commits an offence.

Section 233 (2) states-

A person who knowingly-

(a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or

(b) permits a network service or applications service under the person's control to be used for any activity described in paragraph (a)

commits an offence.

Section 233 (3) states-

A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.

Section 233(1) (b) is an appropriate section to deal with the problems faced by spamming activities.

The MCMC continues to monitor the development of spam laws and legislation in various jurisdiction around the world i.e. United States of America, Australia, South Korea, Singapore etc.

3.4 International Cooperation

MCMC believes that global cooperation and coordination in the implementation of spam related legislations are needed to tackle spam as they can originate in any country in the world where there is Internet access.

In a report released by the Malaysian National ICT Security Emergency Response Center (NISER) in 2004, almost 97% of spam that affects Malaysia comes from overseas mainly United States, China, South Korea, Canada, Japan and others. Only 3.17% of spam originates locally.

It is therefore imperative that Malaysia partake in global collaborative alliances to ensure the sharing of information to assist in enforcement and regulatory matters.

Malaysia via MCMC is very keen to have closer working relationship with other countries to minimize spam originating in each country, passing through each country and being sent to end-users in each country.

To encourage exchange of information on technical, educational and policy solutions to the spam problem, MCMC has signed a Multilateral Memorandum of Understanding on Cooperation in Countering Spam (MOU) with Australian Communications Authority of Australia and Korea Information Security Agency of South Korea on 27th April 2005.

A copy of the said MOU is attached as **Appendix B.**

The focus of the MOU is to allow greater cooperation on enforcement and geared towards cooperation and information sharing on technological, policy and educational solutions to spam.

The benefits of the MOU are many fold, among them:-

(a) Exchange of information about policies and strategies for establishing anti-spam regulatory framework and the establishment of links amongst the regulators;

(b) Industry collaboration by exchanging information relating to technical and educational solutions to spam; and

(c) Encouragement of liaison between industry and government agencies to promote area of interest and cooperation.

In becoming a signatory to the multilateral MOU, Malaysia is cooperating with those countries on the following area:-

(a) Establishment of working links amongst regulators;

(b) Sharing technical expertise, commercial intelligence, educational strategies and materials;

(c) For joint enforcement, use of existing and cooperative international and regional fora such as ITU, OECD and APEC;

(d) Support for technical enforcement partnerships;

(e) Enforcement and regulatory policy co-development; and

(f) Comparison and promotion of publicity message

Apart from the above, MCMC also endorsed the London Action Plan on 18th May 2005. The London Action Plan (LAP) was initiated in London, United Kingdom on 11th October 2004 to combat spam problem at international level through cooperation between regulators and related industry bodies.

The LAP sets a platform for cooperation at working level and sharing of information on issues which includes but not limited to the following:-

(a) New technology and trends in countering spam;

(b) Educational programs for both users and businesses;

(c) Legislative and law enforcement developments;

(d) Effective investigative techniques and enforcement strategies; and

(e) Problems related to spam such as online fraud and deception, phising and dissemination of viruses.

The LAP is non binding and encourages sharing of infomation and cooperation on spam related issues for the mutual benefits of thoseendorsing the LAP. A copy of the LAP is attached as **Appendix C**.

4. Conclusion

There is no magic bullet in the fight against spam. There is a need to have a combination of many things which includes regulation, self-regulation, technical measures, international enforcement cooperation, public-private partnerships and increased awareness and education.

The International Telecommunications Users Group (INTUG) in a report submitted during the 2nd OECD Workshop on spam in September 2004 in Busan, South Korea, cited user education as the “weakest link” in the chain of anti-spam solutions. The report stated that individuals or corporations need to have stronger links with their suppliers who should be providing education and information on how to combat fraud, spam and viruses.

Malaysia through MCMC had always promoted a multi-prong approach in the fight against spam emphazing on self regulation, management of service providers and creation of consumer awareness and will continue to do so.

APPENDIX A

Internet Access Service Provider (IASP) Sub-Code for the Communications and Multimedia Industry Malaysia

Part 1 - Introduction

Part 2 - General rules of the code for internet access services providers

Part 3 - Review and amendments

PART 1 INTRODUCTION

1. Background

1.1 The Communications and Multimedia Act 1998 (CMA 1998) seeks to establish a regime of industry self-regulation, supported by fallback regulatory standards that may be administered by the Malaysian Communications and Multimedia Commission (MCMC).

1.2 Pursuant to section 189 of CMA 1998, MCMC had designated the Communications and Multimedia Consumer Forum of Malaysia (Consumer Forum) as the consumer forum in March 2001. The Consumer Forum has been given the responsibility to develop sub-codes for dealing with matters relating to the protection and promotion of consumer interests in relation to specific services including, but not limited to, the matters listed in the CMA 1998.

(a) The Consumer Forum has identified the Internet Access Service Provider Sub-Code (here in after referred to as the "IASP Code") as being one of the important sub-codes for the Consumer Forum to be developed at this juncture.

(b) A permanent working committee appointed pursuant to Article 19 of the Constitution of Forum Pengguna Komunikasi dan Multimedia Malaysia made up of relevant parties from both the demand and supply side of the communications and multimedia services drafted the following IASP Code.

2. Preamble

2.1 This IASP Code is cognizant of the constant state of profound technological change that is characteristic of the communications and multimedia industry.

2.2 As technologies innovate new operating conditions, this IASP Code may need to be updated to nurture, conserve and protect the objectives of this IASP Code.

3. Objectives of the Code

3.1 To promote the free-flow of information and communications over the Internet;

3.2 To set out a code of practice for Internet Access Service Providers.

3.3 To improve the standard of conduct within the industry.

4. Definitions

4.1 All capitalised terms in this IASP Code shall bear the same definition as contained in the General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia (GCC) unless specifically otherwise provided herein.

4.2 For the purpose of this Code:

“Acceptable Use Policy” or **“AUP”** means a policy defined by the Service Provider as to the acceptable nature of use of a service subscribed.

“Child” means all persons under the age of 18 years as defined by the Child Act 2001.

“Code” means this IASP Code.

“Consumer Forum” means the Consumer Forum of Malaysia set up pursuant to the CMA 1998.

“CMA 1998” means the Communications and Multimedia Act 1998 including any amendments thereto from time to time.

“Consumer” means a person who receives, acquires, uses or subscribes to the Internet access service provided by any Service Provider. This includes a Customer.

“Customer” means a person who, for consideration, acquires or subscribes to the Internet access service provided by any Service Provider.

“GCC” means General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia.

“Guardian” means natural parent or any person having care and control over a child.

“Internet” means a global information system that is able to support communications using the Internet Protocol (IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols.

“Internet Access Service” means an applications service whereby a person is able to access Internet services and applications.

“Internet Access Service Provider” or **“IASP”** means a person who provides Internet Access Service.

“MCMC” means the Malaysian Communications and Multimedia Commission established under the Malaysian Communications and Multimedia Commission Act 1998.

"Personal Information" means any information collected by the Service Provider from the Customer that identifies the Customer.

"Service Provider" means the service provider as set out in Section 5.1 (Part 1).

"Spam" means unsolicited electronic messages sent through various communication modes including but not limited to e-mails, mobiles short message (SMS) or instant messaging services where there is no prior relationship between the sender and the recipient regardless of content whether commercial or non-commercial messages including malicious program and/or data.

"Website" means a file that contains text, audio and/or visual data accessible on the World Wide Web by a single Uniform Resource Locator (URL).

"World Wide Web" means the network of websites accessible on the Internet using including, but not limited to, the Hypertext Transfer Protocol ('http').

5. Scope

5.1 This Code shall be applicable to the following:-

(a) IASPs;

(b) Other persons or class of persons as may be directed by MCMC; and

(c) Members of the Consumer Forum.

(For the purposes of this IASP Code, the code subjects shall be referred to as "Service Providers".)

5.2 This IASP Code may be amended from time to time.

5.3 This IASP Code is developed pursuant to Clause 6.2, Part 1of the GCC to address the specific needs of the Internet services industry.

5.4 This IASP Code is to be read in addition to and not in derogation of the GCC. The GCC will govern all sub-codes unless expressly otherwise provided in the sub-codes.

5.5 This IASP Code shall come into effect upon registration in accordance with the CMA 1998. However, Service Providers shall be granted a grace period of six (6) months, or such period as may be extended by the Council of the Consumer Forum to comply with provisions of this IASP Code.

PART 2 GENERAL RULES OF THE CODE FOR INTERNET ACCESS SERVICE PROVIDERS

The IASP Code general rules are as follows:-

1. The IASP Code Guiding Principles
2. Protection of Personal Information
3. Provision of Information
4. Provisioning of Services
5. Anti-Spam Measures
6. Policy on Information Network Security
7. Content
8. Billing
9. Protection of Minor
10. Handling of Customer Complaints and Disputes
11. Principle of Compensation

1. The IASP Code Guiding Principles

1.1 The communications and multimedia industry will strive to achieve the following principles:

(a) The National Policy Objectives as set out in the CMA 1998;

(b) The Code objectives as set out in Clause 5, Part 1 of the GCC; and

(c) The Fundamental Principles for Service Providers as outlined Clause 1(A), Part 2 of the GCC for the communications and multimedia industry of Malaysia.

2. Protection of Personal Information

2.1 The relevant provisions in the GCC on protection of consumer information (namely the provisions of Clause 2, Part 2 of the GCC) are applicable to the IASP Code.

3. Provision of Information

3.1 Service Providers shall comply with all the relevant provisions contained in the GCC on the provision of information regarding services, rates and performance.

3.2 Consumers shall be provided with adequate description of the service offered prior to entering into the contract of sale. All material features of the services such as banwidth, speed and availability (i.e. coverage) should be described in simple language that is easily understood.

3.3 The IASP Code should impose an obligation on all Service Providers to publish and adhere to an acceptable use policy, which in all cases would be a condition of sale. This policy shall, at the minimum, include:

(a) Information to Consumers about their legal obligations and liabilities in making use of the services provided by the Service Provider;

(b) Information to Consumers about the responsibilities of the Service Providers in ensuring that the Customers adhere to their legal obligations;

(c) Information on Internet use etiquette;

(d) A description of practice, which are abusive and therefore prohibited; and

(e) Subject to the anti-spam measures herein provided, an indication of the type of remedial measures that may be taken by the Service Providers in respect of defaulting Customers.

3.4 Service Providers shall take reasonable steps to notify all Consumers of their policy on privacy prior to the entering into the contract of sale.

3.5 Any changes in policies developed by the Service Providers should also be communicated to the Consumers as soon as practicable.

4. Provisioning of Services

4.1 Service Providers will provide services and products in a responsible manner, ensuring that the services that they provide to their Customers meet the service levels as contractually agreed between the Service Providers and the Customers.

4.2 Service Providers shall endeavour to provide consistent and reliable access to the services.

4.3 Service Providers shall give adequate notice to their Customers of any planned interruptions of service.

4.4 Service Providers shall not discriminate unduly between persons or classes of persons in the provision of their services or any related matters and shall provide equal access to all Customers.

5. Anti-Spam Measures

5.1 The Service Providers should address concerns about spam and consider methods of managing such issues in such a way to ensure the protection of the Customers' interest.

The Service Provider may consider the following measures in dealing with these issues: -

(a) To articulate a specific definition for spam so as to be clear what is being addressed.

(b) To include the following general principles as contractual conditions in agreements entered into between the Service Providers and Customers who may have the propensity to produce spam:-

(i) The Customer shall not engage in sending spam messages;

(ii) Any breach of conditions shall result in the suspension and/or termination of the Customer account. Such Customer may appeal for reactivation of the said account in accordance with the Service Provider's prevailing policies and procedures;

(iii) Service Providers should provide specific guidance (in the form of an Acceptable Use Policy (AUP)) on when sanctions or suspension and termination of account would be imposed. The Acceptable Use Policy should impose an obligation on the Customer to ensure that all commercial e-mails sent out by the Customer are accompanied by or include the following information:-

(a) Header information that is not false, deceptive or misleading
(b) A valid return e-mail address
(c) Functional unsubscribe facility (ie "opt out" facility
(d) Identity of sender
(e) Message be clearly labeled as commercial communication
(eg [ADVERTISEMENT] for advertisements, [COMMERCIALS] for commercials etc.)

For the purpose of this provision, "commercial electronic message" shall mean any electronic message that can be concluded to be for the purpose of advertising, highlighting, promoting, selling and/or offering to supply any goods, property, service and/or business or investment opportunity.

(iv) The Service Providers should also provide their policies and procedures in reactivating the services suspended due to violation of the AUP.

5.2 In addition to the terms and conditions outlined above in the service contract with their Customers, Service Providers should also consider implementing some technical measures to assist in curbing spam.

5.3 In addition to Section 5.1(b)(iv), the Service Providers shall have a written procedure for handling incidents of spam. This procedure should be publicly available either in print and/or on a web site. Examples of such procedure may be as follows:-

(a) There shall be an ‘abuse’ account. Mail sent to this account shall be routed to a responsible person or those who have the ability to investigate and take action on such complaints;

(b) All complaints sent to the ‘abuse’ account shall be replied to. All complaints should be investigated within certain period of time and proper and timely replies should be given to complainants

(c) Complaints shall be investigated and action must be taken against users flouting the terms and conditions referring to spam. Even if investigation reveals no fault on the part of the Service Provider or user, the Service Provider is encouraged to help the complainant to resolve their complaint.

5.4 The Service Provider shall make available on its website information on anti-spaming measures regarding its Customers. Such information may include IP addresses suspended and/or blocked by the Service Provider and/or any anti-spamming monitoring bodies such as Spamhaus and Spamcop. The said information shall be updated on a weekly basis.

6. Policy on Information Network Security

6.1 Service Providers should have a guideline on how to implement security in their network and there must be some level of standard procedures to be followed. The policy may cover the following areas:-

(a) Business Continuity Planning

There must be a business continuity plan in place to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters

(b) System Access Control

Access Control System should be in place to ensure the following:-

(i) to control access to information
(ii) to prevent unauthorised access to information systems
(iii) to ensure the protection of networked services
(iv) to prevent unauthorized computer access
(v) to detect unauthorised activities.

(c) System Development and Maintenance

Service Providers should also put in place policies on system development and maintenance so as to ensure the following:-

(i) security is built into operational systems;
(ii) to prevent loss, modification or misuse of user data in application systems;
(iii) to protect the confidentiality, authenticity and integrity of information;
(iv) to ensure IT projects and support activities are conducted in a secure manner;
(v) to maintain the security of application system software and data.

(d) Physical and Environmental Security

Policies must be put in place to prevent: -

(i) unauthorised access;
(ii) damage and interference to business premises and information;
(iii) loss, damage or compromise of assets and interruption to business activities; and
(iv) compromise or theft of information and information processing facilities.

(e) Compliance

The policies in place must clearly set the following:-

(i) to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
(ii) to ensure compliance of systems with organizational security policies and standards
(iii) to maximize the effectiveness of and to minimize interference to/from the system audit process.

(f) Security Organisation

The policies in place must clearly set the following:

(i) to manage information security within the Company;
(ii) to maintain the security of organizational information processing facilities and information assets accessed by third parties
(iii) to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

(g) Computer & Network Management

The policies in place must clearly set the following:

(i) to ensure the correct and secure operation of information processing facilities;
(ii) to minimise the risk of systems failures;
(iii) to protect the integrity of software and information;
(iv) to maintain the integrity and availability of information processing and communication;
(v) to ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
(vi) to prevent damage to assets and interruptions to business activities;
(vii) to prevent loss, modification or misuse of information exchanged between organizations.

(h) Asset Classification and Control

To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

6.2 Service Providers are required to ensure that their policy on information and network security is in compliance with and subject to other general guidelines such as frameworks and determinations issued as well as framework and determinations to be issued by MCMC and Ministry of Energy, Water and Communications from time to time.

7. Content

Reference should be made to the relevant provisions of the Content Code in this regard.

8. Billing

Reference should be made to the relevant provisions of the GCC in this regard.

9. Protection of Minor

9.1 Service Providers will take reasonable steps to ensure that post-paid Internet access accounts are not provided to any child without the consent a Guardian. For the avoidance of doubt this obligation shall not be applicable to the pre-paid Internet access services.

9.2 Service Providers should take reasonable steps to provide Customers with:-

(a) information on supervising and controlling a child's access to Internet content;

(b) procedures which Guardians can implement to control a child's access to Internet content, including the availability, use and appropriate application of Internet content filtering software.

(c) notifying the Consumers : **"if you are below 18 years of age – prior consent of a guardian is required before you are allowed to subscribe to a post - paid Internet access account"** prior to the sale of the service.

10. Handling of Customer Complaints and Disputes

Reference should be made to the relevant provisions in the GCC in this regard.

11. Principle of Compensation

Reference should be made to the relevant provisions of the GCC in this regard.

PART 3 REVIEW AND AMENDMENTS

1. Review and Amendments

1.1 A review of this IASP Code shall be conducted by the Consumer Forum:

(a) Within 12 months from the date of implementation of this IASP Code; and/ or

(b) As and when the Consumer Forum deems it necessary. (In line with the stipulated review at least every three years as stated in Clause 4.1 of the GCC).

1.2 Any amendments to this IASP Code shall go through the process of public consultation for a minimum of 45 days. The Consumer Forum will inform the MCMC of any amendments made to this IASP Code. Any amendments to the IASP Code shall only be effective upon registration by MCMC.

APPENDIX B

Seoul - Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam

SEOUL-MELBOURNE MULTILATERAL MEMORANDUM OF UNDERSTANDING ON COOPERATION IN COUNTERING SPAM

The Signatories to this Memorandum of Understanding,

CONSIDERING that the protection of the information economy is a major factor for social, economic and environmental development and for the realisation of productivity and service delivery improvements in the government, business and community sectors of each country/region; and

CONSIDERING ALSO that spam can impair the infrastructure and viability of the information economy;

RECOGNISING the necessity for mutual cooperation for the minimisation of spam originating in and being sent to, or by way of, each country/region;

RECOGNISING ALSO that other organisation may in the future wish to be part of this Memorandum and to jointly combat the spam problem;

HOPING to work together to develop cooperative mechanisms to combat the spam problem, including technical, educational and policy solutions; and

DESIRING to enhance cooperative relations,

HAVE REACHED the following understandings:

Focus of Cooperation

1. Acting within the framework of their powers, interests and responsibilities, the Signatories will collaborate on countering spam (unsolicited commercial electronic messages).

2. The purpose of this Memorandum is to encourage closer cooperation among the Signatories in minimising spam originating in each country/region, passing through each country/region and being sent to end-users in each country/region. The Signatories will also encourage the exchange of information on technical, educational and policy solutions to the spam problem in accordance with the relevant laws and regulations of each country/region and on the basis of equality, reciprocity and mutual benefit.

Scope of Cooperation

3. The Signatories will promote cooperation in all spheres of activity defined by this Memorandum in order to derive maximum benefits for each and all Signatories.

4. Recognising that bilateral and multilateral cooperation can complement areas of mutual interest in reducing the spam problem, the Signatories have identified areas of common interest for cooperation including, but not limited to, the encouragement of:

   (a) the exchange of information about policies and strategies for establishing and enforcing anti-spam regulatory frameworks;

   (b) the exchange of information relating to technical and educational solutions to the spam problem;

   (c) the exchange of information and strategies about the effective use of regulation policies and in support of enforcement;

   (d) the exchange of intelligence, relating to the other countries/regions, gathered as a result of enforcement; and

   (e) industry collaboration.

Forms of Cooperation

5. Cooperation among Signatories in the field of countering spam may take the following forms:

   (a) establishment of channels for exchange of exchange of information on spam, anti-spam measures and emerging issues;

   (b) exchange of delegations and visits as appropriate;

   (c) encouragement of liaison between industry and Government organisations to promote areas of interest and cooperation; and

   (d) other forms of cooperation arranged bilaterally or multilaterally by the Signatories.

Designated Representative

6. In order to coordinate cooperative activities, each Signatory will appoint a representative who will act as a contact point, and who will be responsible for determining the particular directions of cooperation and for ensuring the effectiveness of all cooperative activities.

7. The representatives of the Signatories will consult with each other through the channel specified by the Signatories, to define activities and other related matters.

Activities subject to the Laws of the Signatories

8. All activities implemented pursuant to this Memorandum will be subject to the respective international obligations and domestic laws and regulations of the Signatories cooperating on any issue.

Changes in Anti-Spam Legislation and Signing of Other Agreements

9. In the event of a significant modification to a Signatory's anti-spam legislation, that Signatory will use their best efforts to consult with the other Signatories promptly, either directly or through the Secretary of Signatories as to whether these modifications may have implications for the operation of this Memorandum, and whether the Memorandum should be amended.

10. In the event of a Signatory considering becoming a party to another Agreement that may have implications for the operation of this Memorandum, the Signatory will use their best efforts to consult with the other Signatories promptly, either directly or through the Secretary of Signatories.

Funding and Resources

11. The cooperative activities carried out under this Memorandum will be subject to the availability of funds and resources of the Signatories. For those activities carried out under this Memorandum, unless otherwise jointly decided, each Signatory will provide resources adequate to carry out its own commitments in relation to those activities.

Treatment of "In Confidence" Material

12. No Signatory will disclose or distribute any information that is supplied and marked, or stated to be ‘in-Confidence’ by the originating Signatory, except as, and to the extent authorised, by the originating Signatory, or as required by law.

Settlement of Disputes

13. Any disputes between any Signatories arising from the interpretation or implementation of this Memorandum will be settled amicably through consultations between the affected Signatories. Should the dispute be of a kind that might warrant a revision of this Memorandum, the parties should advise the Secretary of Signatories so that the matter may be circulated to all Signatories for comment and consideration.

Secretary of Signatories

14. The Secretary of Signatories will be an officer of one of the Signatories and will be rotated subject to the agreement of the Signatories. The role of the Secretary will be to act as a contact point for joining this Memorandum and to inform the other Signatories when a new Signatory joins. When a new Signatory joins, the Secretary will include the name of the new Signatory on the List of Signatories and advise the contact points of all other Signatories.

Joining of New Signatories

15. Participation in this Memorandum is voluntary and is open to the relevant Government and industry organisation/s of any country/region. All Signatories have equal status.

16. New Signatories will become party to this Memorandum upon acceptance of their credentials by a majority of current signatories, and will signify their intention to participate by completing the details of the Signatory schedule and sending the schedule by facsimile or similar unalterable form to the Secretary of Signatories.

17. Where more than one Government regulator or industry organisation within one particular country/region is a Signatory to this Memorandum, those regulators and industry organisations will each nominate a single contact point for the purpose of correspondence with the Secretary of Signatories (i.e. where there are two or more government organisations in the same region, they will nominate a single government contact point; where there are two or more industry organisations within the same region they will nominate a single industry contact point).

Duration of Participation

18. Each Signatory's participation in this Memorandum will come into effect on the date of signature by that Signatory. It will remain in effect for a period of five (5) years thereafter unless terminated by the Signatory giving six (6) months prior notice in writing to the other Signatories.

19. Notwithstanding termination of participation in this Memorandum by any Signatory pursuant to paragraph 18, activities being undertaken pursuant to this Memorandum immediately before its termination will continue to be governed by this Memorandum until their completion, unless the Signatories that are party to the activity mutually determine otherwise.

Miscellaneous

20. This Memorandum may be amended or extended at any time by written mutual determination of the Signatories. To this end, signatures to any amendment or extension to this Memorandum may be circulated by facsimile, and any facsimile signature shall have the same effect as an original.

APPENDIX C

London Action Plan

THE LONDON ACTION PLAN

On International Spam Enforcement Cooperation

On October 11, 2004, government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international spam enforcement cooperation. At this meeting, a broad range of spam enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international spam enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting.

Global cooperation and public-private partnerships are essential to spam enforcement, as recognized in various international fora. Building on recent efforts in organizations like the Organisation for Economic Cooperation and Development (OECD) and the OECD Spam Task Force, the International Telecommunications Union (ITU), the European Union (EU), the International Consumer Protection Enforcement Network (ICPEN), and the Asia-Pacific Economic Cooperation (APEC), the Participants issue this Action Plan.

The purpose of this Action Plan is to promote international spam enforcement cooperation and address spam-related problems, such as online fraud and deception, phishing, and dissemination of viruses. The Participants also open the Action Plan for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement cooperation.

A. The participating government and public agencies (hereinafter “Agencies”), intend to use their best efforts, in their respective areas of competence, to develop better international spam enforcement cooperation, and intend to use their best efforts to:

1. Designate a point of contact within their agency for further enforcement communications under this Action Plan.

2. Encourage communication and coordination among the different Agencies that have spam enforcement authority within their country to achieve efficient and effective enforcement, and to work with other Agencies within the same country to designate a primary contact for coordinating enforcement cooperation under this Action Plan.

3. Take part in periodic conference calls, at least quarterly, with other appropriate participants to:

    (a) Discuss cases.

    (b) Discuss legislative and law enforcement developments.

    (c) Exchange effective investigative techniques and enforcement strategies.

    (d) Discuss obstacles to effective enforcement and ways to overcome these obstacles.

    (e) Discuss undertaking, as appropriate, joint consumer and business education projects addressing problems related to spam such as online fraud and deception, phishing, and dissemination of viruses. Such projects could include educational efforts addressing conditions facilitating the anonymous delivery of spam, such as the use of open relays, open proxies and zombie drones.

    (f) Participate as appropriate in joint training sessions with private sector representatives to identify new ways of cooperating and to discuss spam investigation techniques.

4. Encourage dialogue between Agencies and appropriate private sector representatives to promote ways in which the private sector can support Agencies in bringing spam cases and pursue their own initiatives to fight spam.

5. Prioritize cases based on harm to victims when requesting international assistance.

6. Complete the OECD Questionnaire on Crossborder Enforcement of Anti-Spam Laws, copies of which may be obtained from the OECD Secretariat.

7. Encourage and support the involvement of less developed countries in spam enforcement cooperation.

The participating Agencies intend to keep information shared in the context of this Action Plan confidential when requested to do so, to the extent consistent with their respective laws. Similarly, the participating Agencies retain the right to determine the information they share under this Action Plan.

B. The participating private sector representatives (whether as a group or through its members) intend to use their best efforts to develop public-private partnerships against spam and to:

1. Designate a single spam enforcement contact within each organization, who would coordinate with spam enforcement agencies on requests for enforcement-related assistance

2. Work with other private sector representatives to establish a resource list of individuals within particular sectors (e.g., Internet service providers, registrars, etc.) working on spam enforcement.

3. Participate as requested and appropriate in segments of the periodic conference calls described in paragraph A.3 above for the purpose of assisting law enforcement agencies in bringing spam cases. (Because some calls will be focused solely on law enforcement matters, private sector representatives will participate only in selected calls.) In these conference calls, the participating private sector representatives intend to use their best efforts to:

   (a) Report about:

      (i) Cases involving spam or related matters.
      (ii) New technology and trends in e-mail and spam.
      (iii) New ways of cooperating with Agencies.
      (iv) Obstacles to cooperation with Agencies and within the private sector.
      (v) General data on spam and on-line fraud as an early warning mechanism for Agencies.

   (b) Assist as appropriate in training sessions on subjects such as the latest spam investigation techniques to help Agencies in investigating and bringing spam cases.

   In order to prevent inappropriate access to information, a private sector representative may be excluded from participating in all or a portion of the periodic conference calls described above if a participating Agency objects.

4. Work cooperatively with Agencies to develop the most efficient and effective ways to frame requests for information. For this purpose, each participating private sector representative intends to use best efforts to compile written responses to the following questions:

    (a) What kind of information do you provide about potential spammers to domestic law enforcement agencies and under what circumstances?

    (b) What kind of information would you provide about potential spammers to foreign law enforcement agencies and under what circumstances?

    (c) How do you recommend that spam enforcement agencies submit requests for assistance to you?

C. In order to begin work pursuant to this Action Plan, the U.K. Office of Fair Trading and the U.S. Federal Trade Commission intend to use best efforts to:

1. Collect and disseminate information provided pursuant to this Action Plan, including points of contact, notifications from new Participants of their willingness to endorse this Action Plan, and responses to questionnaires, in cooperation with the OECD.

2. Set up the conference calls mentioned in paragraph A.3.

3. Provide a contact for further communications under this Action Plan.

The participating Agencies expect that this procedure may be modified at any time.

D. This Action Plan reflects the mutual interest of the Participants in the fight against illegal spam. It is not intended to create any new legally binding obligations by or amongst the Participants, and/or require continuing participation.

Participants to this Action Plan recognize that cooperation pursuant to this Action Plan is subject to their laws and their international obligations, and that nothing in this Action Plan requires the Participants to provide confidential or commercially sensitive information.

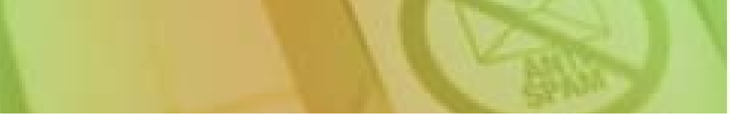
Participants in this Action Plan intend to use best efforts to share relevant findings of this group with the OECD Spam Task Force and other appropriate international groups.

This Action Plan is meant to be a simple, flexible document facilitating concrete steps to start working on international spam enforcement cooperation. It is expected that the collective work program under this Action Plan may be refined, and if necessary changed by the participants, as new issues arise.

Additional Agencies, and private sector representatives as defined below, may endorse and take part in this Action Plan as long as no Agency that has endorsed this Action Plan objects.

"Private sector representatives" invited to participate in this Action Plan include financial institutions, Internet service providers, telecommunications companies, information security software providers, mobile operators, courier services, commercial mail receiving agencies, industry membership organizations, consumer organizations, payment system providers, credit reporting agencies, domain name registrars and registries, and providers of alternative dispute resolution services.

ANTI-SPAM FRAMEWORK OF BEST PRACTICES AND TECHNICAL GUIDLINES



ANTI-SPAM FRAMEWORK OF BEST PRACTICES AND TECHNICAL GUIDELINES

PREAMBLE

Establishment of NISER Working Committee on Anti-spam Framework of Best Practices and Technical Guidelines

Owing to the growth in spamming activities, several initiatives have been taken to combat spam. On its part, NISER has taken the initiative to form a working committee, comprising representatives from the government and private sectors, to deliberate on this matter. This working committee was formed on July 27, 2004. The product was a recommended framework of best practices and technical guidelines for organisations and users to take preventive and precautionary measures against spamming. In producing this framework, 38 documents were reviewed. The list of documents reviewed is listed in the References section.

This document represents the collaborative effort among many organisations in Malaysia. They were representatives from government agencies, Internet Service Providers, Internet Data Centres, Anti-Virus Solutions Providers, Anti-Spam Solutions Providers and E-mail Marketing Organisations. Three brainstorming sessions were held in July, September and October 2004. A list of participating members who have contributed to the development of this framework is listed in Appendix 1.

Scope

This document consists of recommendations for best practices and technical guidelines that have been analysed and compiled from many references. The framework is divided into six categories, namely

1. Internet Service Providers
2. Web Hosting Service Provider
3. Mailing List Management Service Providers
4. Marketers
5. Organisations
6. Home Users

It is impossible to completely eradicate spam. However, it can be minimised if best practices and guidelines are followed. The recommendations made are based on our understanding and knowledge of each area. We are fully aware that this document does not provide a total solution for combating spam. However, if implemented appropriately, it can successfully contribute to improving the current issues on spam in general. This document is a “live” document, and thus it is necessary to update this document from time to time.

GUIDING PRINCIPLES FOR ANTI-SPAM BEST PRACTICES AND TECHNICAL GUIDELINES

This document was developed following a set of guiding principles to address the qualities that should characterise best practices for anti-spam. The following are the guiding principles:

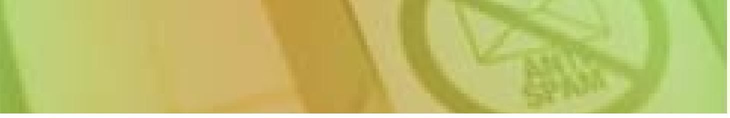
a) **Respecting privacy** - Organisations and individuals shall adopt anti-spam best practices, bearing in mind the need to respect the privacy of individuals and organisations as well as to reduce, if not to avoid, technology and business risks arising from spamming

b) **Striving for the highest anti-spam standards** - Organisations and individuals shall develop, implement and monitor policies and procedures that seek to eradicate spam and shall constantly endeavour to achieve the highest standards in anti-spam best practices

c) **Utilising the latest anti-spam technology** - Organisations and individuals shall, wherever possible and practical, adopt and deploy technology that incorporates the latest anti-spam features

d) **Complying with existing legislation** - Organisations and individuals shall comply with prevailing laws and regulations on anti-spam that are part of their internal corporate policies as well as with national laws and the laws of other countries

e) **Providing lawful outlets for marketers** - Legitimate promoters and advertisers of goods and services shall be provided lawful outlets to promote their businesses in the spirit of not restraining commerce



INTRODUCTION

The Growth and Risk of Spam

In recent years, the Internet has become an increasingly important tool for the world’s socio-economic development. As Internet usage gains more popularity, Malaysia is increasingly being confronted with an increase in incidents of cyber crime such as intrusion, denial-of-service and spam. The emergence of spam threatens the effectiveness of electronic communications and legitimate online business.

This phenomenon hampers the development of the information society by undermining user confidence and trust in online activities. An analysis of the current statistics on unsolicited messages provides an overview of the problems we are facing - the risks and their impact.

Spam, or unsolicited messages, remains one of the most frequent security problems. A total of 14,371 e-mail spamming cases were reported to the Malaysia Computer Emergency Response Team (MyCERT), a unit under the National ICT Security and Emergency Response Centre (NISER), from January to December 2004, compared with a total of 3,383 cases reported in 2003 [1].

NISER has been conducting the ICT Security Survey for Malaysia over the past 3 years and has reported mail spamming being one of the top security breaches experienced by Malaysian users.

The summary of the online survey on spam conducted in 2003 shows that:

- 66% of the organisations saw spam as a serious issue
- Only 12% had taken steps to prevent spam
- 82% felt the need for spam laws
- 74% wanted the government to take action against the culprits
- 61% wanted punishment against the culprits
- 52% received about 10 – 50 spam e-mails a day

The impact of spam on the Internet community is great, causing significant financial costs and losses in productivity. A paper prepared by the ITU World Summit on the Information Society indicated that more than half of all e-mail communication was considered spam messages [2].

According to MessageLabs, spam has grown to represent almost 80% of the total e-mail traffic. The estimated costs to the global economy are approximately USD 25 billion [3]. This is due to the material cost of the time spent identifying and deleting unsolicited messages. It is therefore costly in terms of productivity loss and the need for technical support and software solutions.

Also at stake are the integrity and reliability of e-mail as a trusted communication tool. For example, some message contents could be misleading or even fraudulent, such as an attempt to steal credit cards numbers or install spyware.

This phenomenon threatens the security of an organisation's computer network since a spam’s file attachment may harbour a malicious code. Often, such illegal spyware is also used as a vehicle to promote pornography, get-rich-quick schemes and other deceptive content such as spoofing and phishing.

For Internet Service Providers (ISPs) having to deal with spam, they are forced to consume a larger amount of bandwidth as well as storage and processing capacity. Bandwidth and storage capacity are wasted when the servers become congested with large volumes of unsolicited messages. Not surprisingly, the costs of increasing such capacity are then passed on to end users in the form of extra fee payment. This will tend to discourage Internet utilisation as a whole.

Spam is a significant and growing problem that requires a global solution. There is no easy or fixed solution. Therefore, a multi-pronged and cooperative approach is necessary. Appropriate actions in solving the problem of spam require cooperation at national and international levels.

In order to respond to the issues created by spam, a diverse and effective strategy must be employed consisting of a five-layered approach [4] [5]

- Strong and effective legislation
- Development of technical measures
- Establishment of industry partnerships, especially with ISPs, mobile carriers and direct marketing associations
- Education of consumers and industry players on anti-spam measures and Internet security practices
- International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem

ANTI-SPAM BEST PRACTICES AND TECHNICAL GUIDELINES

To facilitate the flow of this document, the recommended best practices are structured into the following areas:

a) Internet Service Providers (ISPs) - These are companies that provide individuals and organisations access to the Internet via high-speed transmission lines and other related services. An ISP has the necessary equipment and telecommunication line access to achieve a point-of-presence on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their customers.

b) Web Hosting Service Providers - These are businesses that provide storage space for the hosting of web pages by individuals or organisations. A web hosting service provider provides the technologies and services needed for Web sites to be viewed on the Web. It allows users to disseminate their own information resources to any Internet user that is interested in accessing them. Web hosting utilizes the server/client model to distribute content. A Web hosting service provider offers its clients access to a Web server that will push that client's content to recipients on request. They also provide SMTP e-mail connectivity.

c) Mailing List Management Service Providers - These are businesses engaged in managing mailing lists of other organisations. Management of the mailing lists includes, but is not limited to, managing e-mail campaigns on behalf of the client, storing the list, removing dead e-mails, managing subscriptions, removing e-mails of those who un-subscribe and removing duplicate e-mails. All lists are hosted and kept by the service provider.

d) Marketers - These are organisations that provide marketing services via e-mail to lists of users that have subscribed to a particular service on the Internet or other means. The list may have been obtained by themselves or through other organisations who have obtained it through any legitimate means. Unlike Mailing List Management Service Providers, Marketers do not carry out list processing for their clients. All lists belong to the Marketers themselves or their affiliates.

e) Organisations - These are any registered businesses that provide their employees with Internet access and e-mail facilities via a dial-up or leased line connectivity.

f) Home Users - A home user is any individual who has Internet connectivity at home and possesses one or more e-mail accounts. Internet connectivity is by means of dial-up or a leased line via any registered ISP locally or internationally.

For each of the affected areas, best practices are further classified into four categories: awareness, technology, procedures, and compliance and enforcement.

a) Awareness - Awareness is an essential element in the combat against spam as it provides users with fundamental knowledge on how to deal with spam. The idea is that as users learn to deal effectively with spam, spamming will become a less attractive activity.

b) Technology - Technological responses are always required to battle spammers who have the flexibility to change their tactics as quickly as the development of new defensive techniques. Such responses should include the development or improvement of filters and other technologies. This document provides best practices on the technical aspects for each affected area.

c) Procedures - Procedures on cutting down spam should be developed at all levels of the organisation. The best practices on procedures should outline the necessary processes and important steps to control spam effectively.

d) Compliance and Enforcement - Regardless of how ideal policies and procedures on spam are, they will be useless unless they are enforced or complied with. Despite the unavailability of specific anti-spam laws in Malaysia, these compiled best practices together with enforcement at all levels are viewed as the best approach to minimise spam.

Internet Service Providers (ISPs)

Awareness

Increase Awareness to Subscribers [6] [7]
ISPs should inform subscribers:

(a) how to minimize the receiving of spam;

(b) that if they breach the contract by engaging in spam practices, their account will be terminated;

(c) that spam filters are available through the ISPs' homepage. They can also be obtained through third party websites, that provides a means for end users to have access or to acquire spam filter;

(d) about costs associated with the above spam filters; and

(e) about the availability of tools to fight spam and messaging abuse.

In addition, ISPs should devote a comprehensive part of their websites to inform customers how to fight spam.

Technology

Ensure Proper Server Configuration [8]

ISPs should ensure that all e-mail servers under their control or management are properly configured to prevent unauthorised relaying of e-mail.

Provide Information About Spammer [8]

IP numbers associated with an ISP should be resolved in such a way as to provide meaningful information to the complainant who is tracing the IP number of not only the immediate provider of the spammer/abuser, but also the geographical location of the server.

Utilise Filters [8] [9]

ISPs should not knowingly distribute to their users unsolicited e-mails or e-mails reasonably suspected of being unsolicited, and in addition should institute multiple forms of filters to prevent such distribution. Filters should at least be a combination of "known phrases" or similar, Open Relay Filters, and Known Rogue IP Filters.

Implement Rate Limits on Outbound E-mail Traffic [7] [8] [10] [11] [38]

ISPs should place a cap on the volume of outgoing mail which may be sent from an IP in any given time period. Clients may apply to raise the limit with legitimate reasons provided they have acquired the e-mail addresses of recipients in an ethical manner.

Limit the Volume of E-mails Received (Rate Limiting at Destination Server) [8] [11]

ISPs should prevent their accounts from being used as "drop boxes" for spam replies by placing a strict limit on the number of e-mails an account may receive in any given time period.

Log the Calling Number Identification (CNI) Via Dialup [8] [12]

Every connection via Dialup provided by the ISP should log the Calling Number Identification (CNI). This will assist in identifying those responsible for spam-related offences.

Destroy All Outbound E-mails Relayed Through Open Server [8]

ISPs should be proactive in auditing their networks and alerting customers who have open relay. Subject to the current legislation, ISPs should take all available measures to intercept and destroy all outbound e-mails which the sender is attempting to relay through any unsecured/open server.

Do Not Permit Mail Server to Relay E-mail from Third Parties [7] [10] [38]

"Open relays" are mail servers that allow third parties (unrelated to the owners of the servers) to relay e-mail through them without any formal authentication. Open relays should be reconfigured as secure relays.

Deny outgoing TCP access to the Internet on Port 25 (SMTP) [7] [10] [11] [13] [14] [38]

All clients using switched access shall not have outgoing TCP access to the internet on port 25 (SMTP). An SMTP server shall be provided by such accounts; if possible the users' outgoing SMTP connection will automatically be redirected to such server.

Create Honey Pot Signatures [15]

ISPs should create honey pot signatures to act as spam catchers or traps. Honey pots are used to provide the basis for generating signatures or patterns of spam received for testing e-mails sent to real mailboxes.

Perform Content Analysis [9] [15]

Subject to the current legislation, ISPs should perform content analysis on inbound e-mails by relying on the suspicious characteristics of legitimate and illegitimate information requests that spammers try to hide from spam filters. Several techniques to be considered are as follows:

(a) Keyword analysis;

(b) Lexical analysis;

(c) Bayesian analysis;

(d) Heuristics analysis;

(e) Header analysis; and

(f) URL analysis.

Monitor formmail.pl and Other CGI Applications [7]

ISPs should regularly scan for misconfigured or outdated programs that can be used to create e-mail. Note that while formmail.pl and other CGI script have been exploited recently, there is potential for other programs to be targeted by spammers on a larger scale. Rate limiting on an ISP's outbound system can help prevent the amount of damage a single insecure script can cause.

Configure Proxies for Internal Network Use Only [7]

Open proxies allow third parties to anonymously send e-mail through them, thus inadvertently opening themselves to abuse by spammers who can conceal the origin of outgoing spam. Tracking down open proxy abusers has been an uphill task considering that proxies usually do not come configured with a logging feature. Therefore:

a) proxy software should be configured to allow only users on internal networks to use it, and

b) ISPs should reserve the right to test customers' proxies at the ISPs' premises to determine any misconfiguration that could allow for third party abuse.

Detect and Quarantine Compromised Computers [7]

Hackers and spammers have intentionally deposited many "back door" open relays or proxies by using viruses, worms and malicious software on the personal computers of unsuspecting users.

ISPs should develop methods for discovering compromised computers. Computers that show signs of infection should be removed from the network or quarantined until virus or worms can be removed.

Implement Authenticated E-mail Submissions [7] [11]

a) ISPs should implement solutions that require authentication from users before mail is sent. Verifying the identity of the sender gives the recipient the confidence that the e-mail is valid.

b) A strong form of an authentication method should be implemented, such as encryption of the password.

c) SMTP authentication should be implemented on the standard Mail Submission Port, port 587, and ISPs should encourage their customers to switch from client software to this port. This port provides seamless connectivity that does not depend on whether a network allows port 25 traffic.

Control Automated Registration of Accounts [7] [38]

Spammers and hackers have found methods to register automatically millions of accounts with ISPs. These accounts can be used for sending spam and mounting Denial of Service (DoS) attacks. ISPs should develop and implement methods to block such automated generation of accounts.

Close web-based redirector services susceptible to abuse [6]

ISPs should secure all web-based redirectors that can be used by third parties without permission.

Blacklisting/Whitelisting [15] [16] [17] [18] [38]

ISPs should use blacklisting or whitelisting techniques that rely on the identification of e-mail senders to determine whether messages are spam. Most **blacklisting** relies on Realtime Blackhole Lists (RBLs), which serve to block known spammers. RBLs contain IP addresses, domain names or e-mail addresses of known spammers, maintained by anti-spam Web sites, service providers, and the IT department itself.

Whitelisting relies on similarly maintained lists that allow e-mails from legitimate senders.

Accepting e-mail sent from whitelisted servers without further filtering can be effective in reducing false positives arising from aggressive blocklists and pattern matching filters. Whitelisting also reduces load on the mail server and speed the mail delivery.

Whitelists and blacklists should come from authorised or reliable sources such as MCMC.

Checksum [11]

ISPs should provide a mechanism for the destination e-mail server to determine if an incoming e-mail is bulk in nature by comparing the incoming e-mail against all the e-mails previously received by the destination e-mail server. An e-mail that is sent to a large number of recipients has a high likelihood of being spam. However, to avoid inaccuracies, the checksum should come from the e-mail body rather than the full e-mail with headers.

Reverse DNS Lookup [15] [16] [19]

ISPs should apply the reverse DNS lookup technique to determine if the sending e-mail is legitimate and has a valid host name. This will eliminate the majority of spam sent by mail servers connected to the Internet (by using a dial-up, ADSL or cable connection) should any of those servers not be registered in any domain name server (DNS) as a qualified host. ISPs should add a new process in domain registration to encourage corporate networks to register and validate their reverse DNS.

Procedures

Maintain an Abuse Desk [8] [10] [37]

ISPs should maintain an adequately and competently staffed abuse desk during working hours, with additional resources after working hours if the situation warrants it. There shall be an 'abuse account'. Mail sent to this account shall be routed to a responsible person or team that has the ability to investigate and act on such complaints. All complaints to 'abuse' shall be replied to.

Initiate Prompt Investigation and Action [8] [10]

Upon receipt of an evidence-based abuse report, the abuse desk of the ISP should investigate the complaint and act within 2 working hours. If valid, the account should be terminated immediately. If the complaint cannot be properly investigated within 2 working hours, the account should be temporarily suspended while investigation continues.

Complaints shall be investigated and action must be taken against any user flouting the Terms and Conditions concerning spam.

Remove Remote Access to Consumer Premises Equipment (CPE) [7]

All ISPs should ensure that remote access to CPE is turned off, or that at least the CPE does not respond to a known default password, for example, a blank password for the admin user.

Use of Business Registered Names for Bulk Advertisement E-mail Senders

All ISPs should require bulk e-mail advertisement senders using their services to use their business registered names when registering IP addresses and e-mail addresses. Those who do not comply with this Policy shall be banned from sending and receiving e-mails and block the addresses of the violators. These should be stated in the Terms of Services/Acceptable Use Policy.

Compliance and Enforcement

Include an Anti-Spamming Policy Provision [8] [10] [37] [38]

ISPs should include in their Terms of Services/Acceptable Use Policy a strongly worded anti-spamming provision on their own websites or other related documents:

a) Stating that spamming is an act against the law and regulations;

b) Prohibition against any involvement in spamming including sending unsolicited e-mail, receiving responses by any means from unsolicited bulk/commercial e-mail sent via any other provider; and

c) Others necessary for preventing spam mail.

Termination of Account [8] [10]

ISPs should ensure that violation of the anti-spamming policy as per the Terms of Service/ Acceptable Use Policy will result in immediate suspension and warning, to be followed by termination of the account if the violation is repeated. The offender will be blacklisted.

A "clean up fee" may be imposed on the offender or deposit collected during registration may be forfeited.

Assure Protection of Personal Information [8]

ISPs should include in the Privacy Statement strong privacy provisions stating that: personal information acquired through the ISP in the course of their business will never be sold, rented, swapped or in any other way provided to third parties; the ISP itself will never use personal information for any purpose for which the ISP has not received clear, prior, optional and voluntary consent of the person about whom the personal information contains.

Pursue Legal Remedies [8]

If an ISP has been fraudulently associated with a spam, the ISP should identify the perpetrators and initiate legal action.

Report Spam [6] [7]

ISPs should take reasonable steps:

a) to make formal report to respective authorities about complaints of spam.
b) to advise subscribers of their rights to complain about spam. Thus, ISPs need to have a code of practice to handle these complaints.
c) to develop a system for subscribers and external parties to report spam sent by subscribers from the same ISP or from other sources.
d) to enlighten subscribers the means by which ISPs deal with complaint reports.

Compliance [10]

ISPs that conform to the framework of best practices will be allowed to advertise that they are conforming to the said framework. However, if they have flouted the conditions under the framework without reasonable excuse, the authority should remove any ISPs' right to advertise.

Web Hosting Service Providers

Awareness

Share Information on Offenders [20]

Web Hosting Service Providers (WHSs) should reserve the right to pass on all information regarding breaches of their Terms of Service to any other service provider known or believed to be used by the offender.

Increase Awareness to Subscribers

WHSs should work together with the relevant parties to develop awareness programs to advise subscribers on ways to minimise spam.

Technology

Proper Server Configuration

WHSs should ensure that all e-mail servers under their control or management are secure and are properly configured to prevent the unauthorised relaying of e-mail.

Utilise Filters

WHSs should not knowingly distribute to their users unsolicited e-mails, or e-mails reasonably suspected of being unsolicited, and in addition should institute a multiple form of filters to prevent such distribution. Filters should be, at the minimum, a combination of "known phrases" or similar, Open Relay Filters, and Known Rogue IP Filters.

Configure Proxies for Internal Network Use Only

WHSs should configure proxy software to allow only users in the internal networks to use the proxy.

Open proxies allow third parties to anonymously send e-mail through them, thus in advertently opening themselves to abuse by spammers who can conceal the origin of outgoing spam. Tracking down open proxy abusers has been an uphill task considering that proxies usually do not come configured with a logging feature.

Procedures

Maintain an Abuse Desk [20]

WHSs should maintain an adequately and competently staffed abuse desk. Contact details of the abuse desk should be not only easily accessible on the WHS's website but also listed with all the Network Abuse Clearinghouses such as abuse.net

Handling Complaints [20]

Upon receipt of the evidence-based abuse report, the abuse desk of the WHSs should investigate the complaint and act on it. An auto-responder should be sent to the complainant informing that the complaint has been recorded and will be looked into. If the complaint is valid, the account of the perpetrator should be terminated immediately, the offender barred from future use of the service, and the violation and termination reported to other service providers known or believed to be used by the offender. All complainants should be sent a reply stating the outcome of the investigation and the action taken.

Compliance and Enforcement

Opt-in [20]

WHSs should, as part of their Terms of Service, require that any mailing hosted on their service be subscribed to only via a confirmed-opt-in or a paid subscription procedure.

Ensure “Resellers” Abide by the Principle of Best Practices [20]

Where the WHS markets its services through "resellers" the WHS must ensure such "resellers" abide by this set of Best Practices.

Insert an Anti-Spamming Policy Provision [20]

Web Hosting Service providers should include in their Terms of Service / Acceptable Use Policy a strongly worded anti-spamming provision, covering prohibitions against any involvement in spamming - including but not limited to: sending unsolicited bulk/commercial e-mail; receiving responses by any means from unsolicited bulk/commercial e-mail sent via any other provider, being linked to from a "spamvertised" website; promoting spamming services or distributing or encouraging spamming services or lists of e-mail addresses; linking to "spamware" or sites promoting "spamware".

Mailing List Management Service Providers

Awareness

Increase Awareness to Subscribers

Mailing List Management Service Providers (MLMSPs) should work together with the relevant parties to develop awareness programs to advise subscribers on ways to minimise spam.

Technology

Avoid harvesting technology

MLMSPs should refrain from using harvesting technology to update or compile their lists.

Procedures

Conduct Due Diligence [21]

Before accepting a new client with a pre-existing mailing list, the MLMSPs should make all possible enquiries and conduct a "due diligence" to ensure that the existing list being transferred has been acquired via either: confirmed-opt-in or paid subscription processes.

Abuse Desk [21]

MLMSPs should maintain an adequately and competently staffed abuse desk. The communication details of the abuse desk should be easily accessible on the website of all MLMSPs such as abuse.net.

Compliance and Enforcement

Insert a Clear un-subscription Procedure [21]

MLMSPs should ensure that all lists hosted possess, use and publicise a clear and easy-to-use un-subscription procedure. Clients who use the MLMSPs services must agree to have this option available and implemented.

Include a Strong Anti-Spam Policy [21]

MLMSPs should ensure that their Terms of Service / Acceptable Use Policy include a strongly-worded anti-spam clause, prohibiting the sending of unsolicited e-mail, whether directly or indirectly.

Termination of Accounts [21]

In the event of a clear-cut violation of Terms of Service / Acceptable Use Policy, the list hosting Service should terminate all accounts associated with the offender, after receiving the evidence-based abuse report.

Marketers

Awareness

Do Not Disclose E-mail List Without Permission [22]

Marketers should not provide to unrelated third parties any e-mail list without the consent of its owner. Even so, the owner has the ability to remove any e-mail address on the list.

Technology

Do Not Hide True Origin of the E-mail [7]

Marketers should not attempt to obscure any information that reveals the true origin or the transmission path of bulk e-mail.

Do Not Harvest E-mail Addresses Without the Owners' Affirmative Consent [7] [22] [37]

Marketers should not acquire e-mail addresses by any means, including through any automated mechanism without the consumer's consent.

Do Not Use “Dictionary Attacks” [23]

Marketers should refrain from using "dictionary attacks" as an e-mail solicitation method. Programs that use “dictionary attacks” utilise technologies to predict the existence of e-mail addresses in order to blast e-mail to those addresses. These programs are automated and consumer consent was never obtained.

Procedures

Use Valid Headers and Domain Names [7]

Marketers should not use or send e-mails that contain invalid or forged headers, as well as invalid or non-existent domain names in the From and Reply-To headers.

Provide Clear Return E-mail and Physical Address [22]

Marketers should provide a clear valid return e-mail and a physical address. Marketers are encouraged to use their company or brand names in their domain address prominently throughout the message.

Clearly Identify the Sender and Subject Matter [22] [23] [24]

Marketers should clearly identify themselves and the subject matter at the beginning of each e-mail. Doing so reduces consumer confusion, adds legitimacy to the message, and contributes to long-term trust in the medium.

Work With Credible Mailbox Providers [7]

Marketers should consider working with relevant and trusted parties that have the proven ability to help companies’ e-mail meet the highest industry standards.

Monitor SMTP Responses [7] [23] [25]

Marketers should practice thorough list maintenance including timely processing of bounces and removal of hard bounces. Monitor SMTP responses from recipients' mail servers to avoid non-existent users. Promptly remove all e-mail addresses to which the receiving mail server responds, for example, with a 55x SMTP code error (for example user does not exist). Opt-out – An Unsubscribe Method To Be Presented Noticeably in Every Commercial E-mail

Sent [7] [12] [22] [23] [25]

Marketers should ensure that all commercial e-mail must provide consumers with a clear and conspicuous electronic option to be removed from lists of future e-mail messages from the sender. The electronic remove feature must be easy to find and use, reliable, functional, and prompt, and its effect must be to remove the recipient from all future e-mails from the sender. There should be an instruction for opting out in the same language as the content language, and there should be one version in English.

Make Available Alternative Subscription Terminating Methods [25]

Marketers must ensure that an “out of band” procedure (e.g. an e-mail address to which messages may be sent for further contact via e-mail or telephone) is to be made available for those who wish to terminate their e-mailing list subscription but are unable to or unwilling to follow standard automated procedures.

Opt-In [23]

Marketers should use the opt-in method to build their mailing lists. If they do not have a prior business relationship with their intended recipients, they should ask for recipients’ permission before they send. As an added precaution, marketers should also consider asking the recipients to confirm their e-mail addresses.

Personalise Mail [25]

Marketers should deepen personalization and create more personalized e-mail campaigns. Marketers should move beyond basic name and address targeting by going deeper into customer profiles to create relevant content, products and offers.

Refrain from Using "Harvested” Lists [23] [24]

Marketers should refrain from using harvested lists.

Use Legitimately-Acquired Lists for Their Original Purpose [23]

Marketers who acquire a mailing list should determine that all recipients have in fact opted-in to the type of e-mailing list the buyer intends to operate.

Compliance and Enforcement

Compliance with Advertising Ethics [7] [22]

Marketers should adopt the Direct Marketing Association (DMA) guidelines pertaining to advertising ethics.

Prevent Abuse of Mailing Lists [25]
Marketers should take adequate steps to ensure mailing lists are properly protected (via password protect or encryption).

Administrators must maintain a “suppression list” of e-mail addresses from which all subscription requests are rejected. The purpose of the suppression list is to prevent forged subscription of addresses by unauthorised third parties. Such suppression lists should also give properly-authorised domain administrators the option to suppress all mailings to the domains for which they are responsible.

Provide A Clear Privacy Policy [22]
Marketers should provide their privacy policy in their commercial e-mails, either within the body of the e-mail or via a link.

Disclose Data Sharing Practices [23]
Marketers should fully disclose relevant data sharing practices at the point of collection. If marketers would like the option of sharing personally identifiable information with third parties, especially for marketing purposes, they should clearly disclose this when obtaining consent.

Ensure Clarity of Disclaimers and Disclosures to Consumers [23]
Marketers should ensure that consumers are able to notice, read or hear, and understand the information pertaining to all disclaimers and disclosures. A disclaimer or disclosure is not enough to remedy a false or deceptive claim.

All Commercial E-mail Content Should Not Be Offensive [23]
Marketers should ensure that no commercial e-mail will be sent out that contains nudity, profanity and other languages and images of a disturbing and offensive nature, unless content of this nature is specifically solicited.

Organisations

Awareness

Increase Awareness to Employees [6] [7]

Organisations should inform employees:

(a) how to minimise the receiving on spam
(b) the availability of spam filters
(c) not to send e-mails that can be categorised as spam.

In addition, employees should be made aware of the availability of tools to fight spam and messaging abuse.

Technology

Content Analysis [9] [15] [16] [26]

Organisations should perform content analysis of the inbound e-mails by relying on the suspicious characteristics of legitimate and illegitimate information requests that spammers try to hide from spam filters. Several techniques that can be considered are:

(a) Keyword analysis

(b) Lexical analysis

(c) Bayesian analysis

(d) Heuristics analysis

(e) Header analysis

(f) URL analysis

Check Sender Authentication [15]

Organisations should identify spam by checking the identification of named e-mail senders based on either sender e-mail or IP addresses. Organisations should block e-mail with malformed headers. In addition, they should block e-mail according to a configurable list of major known mailers.

OCR Recognition Text [16]

Organisations should use the OCR (Optical Character Recognition) technique, which has the ability to read text even when it appears as a graphic image. Many spam messages arrive as graphic images and not as text. Thus, spam tends to escape identification by many anti-spam systems as they are unable to analyse text that appears in the graphic image.

Use Anti Relay Systems [16]

Organisations should deploy anti-relay systems to protect mailservers from being hijacked and used by spammers to broadcast unsolicited e-mails. This option blocks all e-mails that do not belong to the organisation where they have been directed.

URL Detection [27]

Organisations should apply the URL detection technique to detect the domain name of spammers. Most incoming e-mails will include a link with the hope that the recipient will click on it. However, there are limitations when a URL is contained in images or when there are no links coded into the URL itself.

Implement Rate Limits on Outbound E-mail Traffic

Organisations should place a cap on the volume of outgoing mail which may be sent from one account (employee) in any given time period.

Create Honey Pot Signatures

Organisations should create honey pot signatures to entrap spam. Honey pot signatures are used as the basis for generating signatures or patterns of spam received for testing e-mails sent to real mailboxes.

DNS Lookup [16]

Organisations should apply the DNS lookup technique, which is able to determine if the sending e-mail is legitimate and has a valid host name. This technique will eliminate the majority of spam sent by mail servers connected to the Internet (by using a dial-up, ADSL or cable connection) should any of those servers not be registered in any domain name server (DNS) as a qualified host.

Use Anti-Spam Solutions [28]

Organisations should utilise anti-spam solutions. In selecting the software, organisations need to consider:

(a) The software's ability to detect, effectively and accurately, all or nearly all spam with minimal false positive.

(b) The need for product and spam updates to catch up with the current growth and trend of spam.

(c) The software's ability to block spam regardless of the languages and dialects in use.

(d) Not to install anti-spam solutions via the services of anti-spam providers so as to avoid violation of confidentiality.

(e) Having integrated protection against viruses, worms, Trojan horses and other “pests”.

(f) Using innovative approaches that can quickly detect spam based on characteristics that spammers cannot easily change, such as the RPD technology.

(g) Including the facility to create whitelists automatically.

(h) Using a server-based anti-spam product.

Follow a Layered Approach In Anti-Spamming [6] [7]

Organisations should follow a layered approach in its anti-spamming techniques. There are 3 layers involved:

(a) At Network layer (reverse address lookups, DNS real-time blocklists, local blocklist, maximum recipient limits, TCP/IP connection limits, SMTP anti-relay)

(b) At content layer (explicit and generic spam phrases, profane text and image processing)

(c) At policy layer (define actions to take, whom to check for spam messages, exceptions)

Provide Legitimate Outlets for Marketers

Organisations should have an internal e-mail address to which spam or other inappropriate e-mail can be forwarded and monitored by e-mail administrators.

Procedures

Do Not Reply to E-mail Scam [19]

Organisations should ensure careful use of corporate e-mail addresses. One of the ways is not to reply to an e-mail scam asking to be removed from the list - this will only confirm a valid e-mail address to a spammer.

Opt Out [30]

Organisations should opt out of member directories that place their e-mail addresses on-line. If an organisation places its employees' e-mail addresses on-line, it should ensure that they are concealed in some way.

BCC (Blind Copy) [30] [31] [32]

Organisations should use bcc, when sending e-mail messages to a large number of recipients, to conceal their e-mail addresses. Sending e-mail where all recipient addresses are exposed in the "To" field makes it vulnerable to harvesting by a spammer's trap.

Ensure Proper Server Configuration

Organisations should ensure that all e-mail servers (if they manage any) under their control or management be properly configured to prevent unauthorised relaying of e-mail.

Utilise Filters [9]

Organisations should not knowingly distribute to their users unsolicited e-mails, or e-mails reasonably suspected of being unsolicited, and in addition should institute a multiple form of filters to prevent such distribution. Filters should be, at the minimum, a combination of "known phrases" or similar, Open Relay Filters, and Known Rogue IP Filters.

Limit the Volume of E-mails Received (Rate limiting at Destination Server)

Organisations should prevent their accounts from being used as "drop boxes" for spam replies by placing a strict limit on the number of e-mails an account (employee) may receive in any given time period.

Destroy All Outbound E-mails Relayed Through Open Server

Organisations should take all available measures to intercept and destroy all outbound e-mails which a sender is attempting to relay through any unsecured/open server.

Do not Allow Mail Server to Relay E-mail from Third Parties

Organisations should ensure that mail servers shall not be allowed to relay e-mail from third parties. Mail servers that allow third parties (unrelated to the owner of the server) to relay e-mail through them without any formal authentication are considered open relay. Open relays should be reconfigured as secure relays.

Deny Outgoing TCP Access to the Internet on Port 25 (SMTP)

Organisations should ensure that all clients using switched access shall not have outgoing TCP access to the Internet on port 25 (SMTP). An SMTP server shall be provided by such accounts; if possible the users' outgoing SMTP connection will automatically be redirected to such a server.

Monitor formmail.pl and Other Cgi Applications

Organisations should regularly scan for misconfigured or outdated programs that can be used to create e-mail. Note that while formmail.pl and other CGI script have been exploited most recently, there exists the potential for other programs to be targeted by spammers on a large scale.

Detect and Quarantine Compromised Computers

Organisations should develop methods for discovering compromised computers. Computers that show signs of infection should be removed from the network or quarantined until the virus or worms can be removed.

This is essential as hackers and spammers have intentionally deposited a lot of "back door" open relays or proxies using viruses, worms and malicious software on the personal computers of unsuspecting users.

Apply Blacklisting/Whitelisting Methods [15] [16] [17] [18] [26]

Organisations should employ whitelisting and blacklisting methods to combat spam. These techniques rely on the identification of e-mail senders to determine whether messages are spam. Most blacklisting relies on Realtime Blackhole Lists (RBLs), which serve to block known spammers. RBL contain IP addresses, domain names or e-mail addresses of known spammers, maintained by anti-spam Web sites, service providers, and the IT department itself. Whitelisting relies on similarly maintained lists that allow e-mails from legitimate senders.

Create Special E-mail Addresses for Marketers

Organisations should create special e-mail addresses for legitimate marketers to promote their products on the Internet.

Compliance and Enforcement

Maintain an Online Site Policy [19] [29]

An organisation should have an on-line site policy for its employees to follow, under which an employee can sign for on-line newsletters, forums, newsgroups and chat-rooms. These, however, should be business-related and stay within company guidelines.

Include an Anti-spamming Policy Provision [17]

Organisations should not only implement a "no spam" policy but should also include in their operational policies on spam a strongly worded anti-spamming provision covering prohibition against any involvement in spamming.

Report Spam [6] [7]

Organisations should take reasonable steps to inform respective authorities about spam complaints.

- ◆ For advisory on handling spam, organisations should report to MyCERT at mycert@mycert.org.my or by telephone at 03-89961901 or fax at 03-89960827.
- ◆ For advisory on legal action, organisations should contact MCMC at 1-800-888-030.

Home Users

Awareness

Avoid Becoming an Accidental Spammer [7] [14] [34]

Home users should take precautionary measures to avoid being accidental spammers. They should:

(a) Install or enable firewalls on their PCs and use up-to-date anti-virus software along with screening tools in order to detect incoming viruses, malware, and harmful or suspicious codes.

(b) Update security patches in the PC.

Refrain from Doing Business With Spammers [14] [18] [30] [32] [33]

Home users should never make a purchase from an unsolicited e-mail. Apart from encouraging spammers, such an action inadvertently delivers identifiable information (name, address, phone numbers, credit card numbers etc) to them. Furthermore, you can be sure to receive more spam.

Delete E-mail From Unknown Sender [14] [30] [31] [32] [35] [36]

Home users should delete e-mails from unknown sender of unsolicited e-mails. While most spam messages are just annoying text, one may actually contain a virus and/or other exploit that could damage the computers of all who open it.

Do Not Respond to Spam [14] [18] [30] [31] [32] [34]

Home users should never respond to any spam messages or click any link in the messages. They should not respond if the source seems dubious.

Ignore chain letters [30]

Ignore chain letters or other spam that encourages you to send, forward or perpetuate the chain e-mail to others. These e-mails typically serve (whether intentionally or otherwise) as valid SMTP address gathering mechanisms.

Technology

Use A Filter [33] [34] [35] [36]

Home users are recommended to use an e-mail spam filtering program.

Procedures

Disable preview function of e-mail client software [30] [31] [32]

Home users should avoid using the preview function of their e-mail client software. Using the preview function essentiality opens an e-mail and tells spammers you are a valid recipient, which can result in even more spam.

Use a Bcc (Blind Copy) [30] [31] [32]

Home users should use the bcc when sending e-mail messages to a large number of recipients to conceal their e-mail addresses. Sending e-mail where all recipient addresses are exposed in the “To” field makes it vulnerable to harvesting by a spammer’s trap.

Protect Your E-mail Address When Online [9] [12] [14] [18] [30] [31] [33] [34]

Home users should protect their e-mail addresses when online. They can do this by taking the following measures:

a) Do not provide their e-mail addresses unless absolutely necessary.

b) Do not post their addresses online.

c) Do not give their primary e-mail to anyone or any site they do not trust.

d) Opt out of member directories that place their e-mail addresses on-line.

Use an Alternative E-mail Address [12] [14] [31] [32] [33]

Home users should use a "public" e-mail address when online for unofficial business. They should have and use one or two secondary e-mail addresses.

Contact the Business Owner Directly to Make a Complaint [34] [36]

Home users should contact the business owner directly, stating that they are receiving unsolicited messages from a particular sender, and requesting that the organisation stop sending the messages.

Block a Sender (Spammer) [12]

Home users should block a particular sender in an e-mail program so that they will not have to view any future e-mail from the sender.

Contact the ISP [12]

Home users should contact the user's ISP if they are unable to stop messages from a particular sender, requesting that the sender be blocked at the e-mail server.

Compliance and Enforcement

Report Spam to the Relevant Authority to Make a Complaint [34]

If the problem still persists, home users should report the spam to the relevant authority [such as MCMC and MyCERT].

Read the Fine Print [14] [30]

When signing up for services or interacting with the companies on the internet, home users should be cognizant of the check boxes/fine print on the HTML forms.

Check Privacy Policy [12] [35]

Home users should check the privacy policy (if any) of the organisation with whom business is conducted on-line. For example, they should check whether the organisation has made a commitment not to share e-mail addresses or other information with any other organisations.

CONCLUSION

Our dependence on the Internet will continue to grow in the years ahead, as will our dependence on the e-mail as a means of communication. Spam will continue to increase in volume because of its attractiveness to marketers and malicious coders alike. Stakeholders - the authorities, ISPs, organisations and home users - should all play their role in combating spam. Legislation alone is hardly enough.

There is a need for a more holistic approach to combat the spam menace. The best practices prescribed in this document should be adopted as one of the ways of improving the online environment.

The framework in this document does not represent the only solution to the spam problem. There is a need for a multi-layered approach through strong and effective legislation, development of technical measures, establishment of industry partnerships, especially among ISPs, mobile carries and direct marketing associations.

There is also a need to educate consumers and industry players on anti-spam measures and Internet security practices. International cooperation at the levels of government, industry, businesses, consumers and anti-spam groups is another key element to enable a more global and coordinated approach to solving the problem.

There are other worldwide initiatives in combating spam which originate from government agencies and industry players such as ISPs, anti-virus and anti-spam solution providers.

This framework is produced as part of the Malaysian contribution to the international efforts in combating spam. It is our aspiration for this framework to be immediately utilised by the Malaysian Internet community in our combined efforts to combat spam.

REFERENCES

[1] www.mycert.org.my

[2] International Telecommunications Union, World Summit on Information Society Thematic Meeting on Countering Spam, Spam in the Information Society: Building Frameworks for International Cooperation <http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20 Cooperation.pdf>

[3] MessageLabs, Spam is still growing, ZdNet, 14 June 2004, online at <http://zdnet.com/2102-1105_2-5233017.html?tag=printthisH>

[4] ITU WSIS Thematic Meeting on Countering Spam, Chairman's Report, CICG, Geneva, 7-9 July 2004 <http://www.itu.int/osg/spu/spam/chairman-report.pdf>

[5] Malaysian Communications and Multimedia Commission (MCMC), A Report On A Public Consultation Exercise, Regulating Unsolicited Commercial Messages, 17 February 2004 <http://www.mcmc.gov.my/Admin/FactsAndFigures/Paper/PC-SPAM-04.pdf>

[6] Internet Industry Association, Internet Industry Spam Code of Practice, A Code for Internet and E-mail Service Providers, Co-regulating in Matters Relating to Spam E-mail (Consistent With The Requirement of the Spam Act 2003 and Consequential Amendments), July 2004, Version 1.0 <http://www.iia.net.au/nospam/Draft_IIA_Spam_Code.pdf>

[7] Anti-Spam Technical Alliance (ASTA), Technology and Policy Proposal, Version 1.0, 22 June 2004 <http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf>

[8] BestPrac.Org, Principles of Best Practice – Internet Service Providers <http://www.bestprac.org/principles/isp.htm>

[9] Jaring Antispam Policy, v1.0

[10] Hong Kong Internet Service Provider Association (HKISPA), Anti-Spam, Implementation Guideline, Version 1.0, 8 February 2000 <http://www.hkispa.org.hk/antispam/guidelines.html>

[11] ITU WSIS Thematic Meeting on Countering Spam, Curbing Spam via Technical Measures, An Overview <http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Curbing%20Spam%20Via%20Technical%20Measures.pdf>

[12] The National Office for the Information Economy (NOIE), Spam, Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered, 2003
<http://www2.dcita.gov.au/__data/assets/file/13050/SPAMreport.pdf>

[13] http://www.broadbandreports.com/shownews/38004

[14] Celcom ISP Internet Security Policy

[15] Mark Levitt and Brian E. Burke, Choosing the Best Technology To Fight Spam, IDC, April 2004
<http://www.commtouch.com/documents/040429_IDC_Choosing%20_the%20_Best%20_AS_Technology.pdf>

[16] Aladdin Knowledge Systems, Anti Spam White Paper, 2003
<www.eAladdin.com>

[17] Lindsay Durbin, Intelligent Spam Detection & Best Practice Spam Management, Clearswift, The MIMEsweeper Company,
<http://www.sitf.org.sg/anti-spam/Intelligent%20Spam%20Detection%20&%20Best%20Practice%20Spam%20Management%20%20Lindsay%20Durbin%20%20ClearSwift%20(Frontline).pdf>

[18] Net Sense – IT Consulting, Spam Solutions White Paper,
<http://www.netsense.info/Spam_Solutions_WP.pdf>

[19] NetIQ, Controlling Spam, White Paper, March 24, 2004

[20] BestPrac.Org, Principles of Best Practices – Web Hosting Services
<http://www.bestprac.org/principles/whs.htm>

[21] BestPrac.Org, Mailing List & Auto-responder Hosting Services
<http://www.bestprac.org/principles/lhs.htm>

[22] Direct Marketing Association of Singapore, E-mail Marketing Guidelines as Part of DMAS Code of Practice, May 2004

[23] McAfee, Best Practices for Small, Medium and Large Business E-mail Marketers, Network Associates Technology, 2004
<http://us.mcafee.com/fightspam/default.asp?id=tipsMarketer>

[24] National Office for the Information Economy (NOIE), Australian Communications Authority, Spam Act 2003: An Overview For Business , February 2004,
<http://www.aca.gov.au/consumer_info/spam/spam_overview_for%20_business.pdf>

[25] NetInfinium, E-mail Marketing and List Management Best Practices

[26] Lawrence Didsbury, Spam Filtering-Building a More Accurate Filter, MCSE, MASE, 2003
<http://www.singlefin.net/resources/white_papers/Singlefin_Spam_Filtering_WhitePaper.pdf>

[27] Commtouch Software Ltd, The Challenges for Anti-Spam Technology,.p.4

[28] GFi White Paper, How To Keep Spam Off Your Network, June 4, 2004
http://www.gfi.com/whitepapers/block-spam-from-your-network.pdf

[29] Clearswift, Whitepaper, Effective Spam Management, January 2003
<http://www.infosec.co.uk/files/White_Paper_2003_clearswift_Spam_Documentation.pdf>

[30] CMS/CWS Customer Relations Section, Anti-SPAM Best Practices Guide, p. 1&2

[31] Sophos, Minimising Exposure, Simple Steps to Combat Spam, 2004,
<http://www.sophos.com/spaminfo/bestpractice/spam.html>

[32] Datanet UK, Combat Spam, Anti-Spam White Paper,
http://www.data.net.uk/pdf/white_paper_spam.pdf

[33] McAfee, Consumer Tips to Prevent E-mail Spam, Network Associates Technology, 2004 <http://us.mcafee.com/fightspam/default.asp?id=tipsConsumer>

[34] Australian Communications Authority (ACA), Fighting Spam in Australia, A Consumer Guide
<http://www.aca.gov.au/consumer_info/spam/consumer_information/spam_consumerguide.pdf>

[35] Beantree, Protect Yourself From Spam, Whitepaper, July 2002

[36] Sally Hambridge and Albert Lunde, Don't Spew, A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam), Network Working Group, Scotland Online, June1999
<http://www.sol.co.uk/sol/abuse/guidelines.htm#Status%20of%20This%20Memo>

[37] Ministry of Information, Republic of Korea, Guide fro Preventing SPAM Mail, presented at The Asia pacific Forum on Telecommunication Policy and Regulation, 17-20 May 2004

[38] Ministry of Information and Communication Republic of Korea and Korea Information Security Agency, Guide to Best Practices for Blocking Spam, version 1.0, September 2004

APPENDIX 1

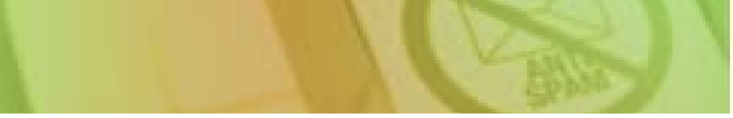
List of Participants

Commitee Members

Name	Organisation
Roslan Ibrahim	Alam Teknokrat Sdn. Bhd.
Mohd Izham Mohammad	Alam Teknokrat Sdn Bhd.
Velautham Sivaraja	AVP (SEA) Sdn. Bhd.
Mohan Kumar	AVP (SEA) Sdn. Bhd.
Abdul Rauf Muhamad Nor	Celcom (Malaysia) Bhd.
Zaini Mujir	Celcom (Malaysia) Bhd.
Ahmad Nizam Ibrahim	Cisco Systems (Malaysia) Sdn. Bhd.
Juharimi Hasan	Cisco Systems (Malaysia) Sdn. Bhd.
Shaun Lim	Computer Associates Sdn. Bhd.
Zainuddin Ali	Computer Associates Sdn. Bhd.
Eddie Hooi	Computer Associates Sdn. Bhd.
Anthony Lim	Computer Associates Sdn. Bhd.
Mark Vyner	Extol Corporation (M) Sdn. Bhd.
Hasannudin Saidin	IBM Malaysia Sdn. Bhd.
Syahrul Sazli Shaharir	Jaring
Rahmat Abu Nong	Malaysian Communications and Multimedia Commission
Azlan Hussain	Maxis Communications Berhad

Jagajeevan Marappan	Maxis Communications Berhad
Jason Yuen Chee Mun	Microsoft (Malaysia) Sdn. Bhd.
Zaid Hamzah	Microsoft (Malaysia) Sdn. Bhd.
Azamin Abu Sujak	MIMOS Berhad
Sy Ahmad Shazali Sy Abdullah	MIMOS Berhad
Shafee Sajat	Ministry of Science, Technology and Innovation
Edwin Tay	NetInfinium Corporation Sdn. Bhd.
Husin Jazri	NISER
Raja Azrina Raja Othman	NISER
Ariffuddin Aizuddin	NISER
Zahri Yunos	NISER
Philip Victor	NISER
Maslina Daud	NISER
Sharifah Sajidah Syed Noor Mohammad	NISER
Siti Suharti Abu Sujak	NISER
Ahmad Nasir Mohd Zin	NISER
Liew Chee Wah	Panda Software (Malaysia)
TS Wong	Panda Software (Malaysia)
Kannan Velayutham	Symantec Corporation (M) Sdn. Bhd.
Mohd Yusri Mahadi	TM Net Sdn. Bhd.
Khairul Naim Zainal Abidin	TM Net Sdn. Bhd.
Santhana Vasan	Trans-Innovation Sdn. Bhd.
Albert Loo	Trans-Innovation Sdn. Bhd.
Ang Ah Sin	Trend Micro (Singapore) Pte. Ltd.

ANTI-SPAM SOLUTIONS



ANTI-SPAM SOLUTIONS

TABLE OF CONTENTS

1. Introduction

Recent analyst indicates that over 60 percent of the world's e-mail is unsolicited e-mail, or "spam". Spam has now become a significant security issue and a massive drain on financial resources.

Today there are a large number of solutions designed to help eliminate the spam problem. These solutions use different techniques for analyzing e-mail and determining if it is indeed spam. Because spam is constantly changing, the most effective spam blocking solutions contain more than one of these techniques to help ensure that all spam, and only spam, is blocked.

This document is divided into two parts:

- Part one gives an overview of the different anti-spam strategies and the different solutions in the market today; and
- Part two describes the criteria used to evaluate anti-spam solutions.

2. Anti-Spam Strategy

The first step in determining how to stop spam is deciding where to put your defenses. Unlike viruses, which can penetrate a network from multiple points (web access, web-mail, floppy disks, SSL, etc.), spammers have only one entryway into the enter prise i.e. through the Internet gateway.

IT departments can then choose where best to lay their defenses: at the e-mail client, on the enterprise e-mail servers, at the perimeter of the network, or outside the network (where outsourced solutions filter e-mail before it hits the corporate firewall).

As organizations gain more experience in fighting spam, the pros and cons associated with fighting spam at each of these points are becoming more clearly understood.

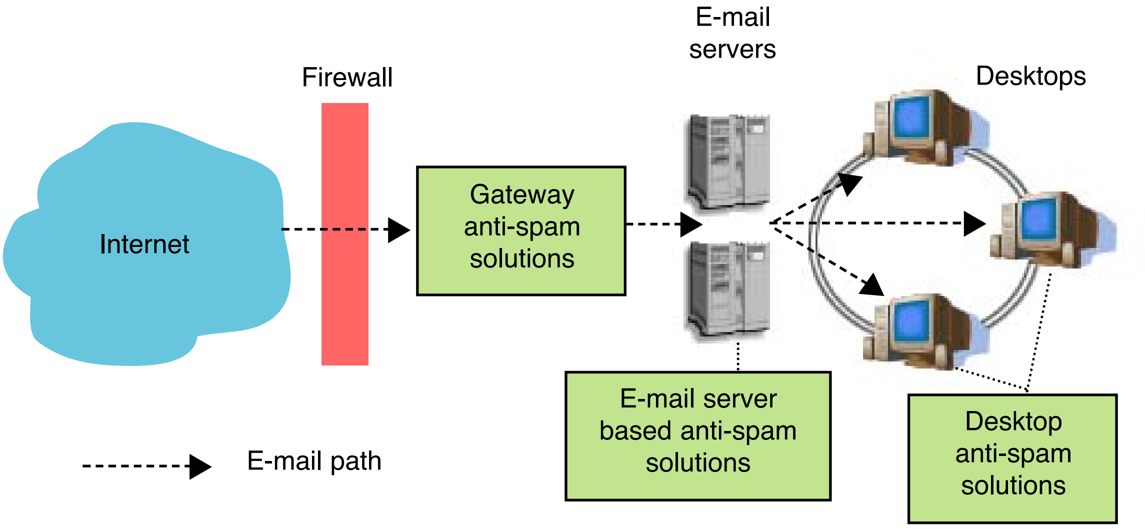

E-mail servers
Firewall
Desktops
Internet
Gateway anti-spam solutions
E-mail server based anti-spam solutions
Desktop anti-spam solutions
E-mail path

Figure 1: Places to implement anti-spam solutions

2.1 Desktop Anti-Spam Solutions

2.1.1 Pros

- A number of client-side anti-spam solutions available today work reasonably well, although they are primarily consumer-focused.

- Most client-side products allow end users to fine-tune spam blocking capabilities to suit their individual needs.

- Some of these solutions can be found free of charge.

- Normally bundled with other desktop security services (firewall, antivirus, antispyware).

2.1.2 Cons

- Non tech-savvy users sometimes find it difficult to get the most out of these applications.

- Users have to manage an additional desktop application, which incurs a measurable productivity cost, particularly if the software requires training before people can use it effectively.

- Supporting any new desktop application also puts demands on already scarce IT resources. The cost of updating the software, deploying patches, and help desk support count among the key concerns.

- Most desktop anti-spam applications lack enterprise-class features such as centralized management, control and reporting. This makes it troublesome to implement corporate-wide anti-spam policies.

2.2 Server-based Anti-Spam Solutions

2.2.1 Pros

- Sitting at the corporate e-mail servers, end users do not waste time managing an anti-spam application. Spam e-mails are discarded before reaching users mailboxes.

- Since the organization is taking positive action to ensure that end users do not view pornographic or hate-based spam, this approach provides good risk reduction in terms of legal liability.

- In terms of security, these solutions tend to perform fairly well, as they inherit the security features of the e-mail servers on which they reside, and they significantly reduce end-user exposure to spam scams.

2.2.2 Cons

- Since spam still traverses the corporate network, most of the costs of network bandwidth and mail server storage/capacity are still incurred.

- Email server plug-ins, especially ones that do complex processing such as anti-spam filtering; tend to degrade the performance and uptime of mail servers.

- IT management costs are higher for larger organizations (generally over 500 mailboxes), which tend to have multiple e-mail servers. IT staff may need to replicate management tasks for the anti-spam solution at every mail server.

2.3 Gateway-based Anti-spam Solutions

Gateway-based anti-spam solutions reside at the perimeter of the corporate network where the MTA (Mail Transfer Agent), or e-mail relay, routes e-mail to and from the Internet.

2.3.1 Pros

- Gateway-based anti-spam solutions eliminate most spam before it reaches the corporate e-mail servers.

- These solutions also provide good network resource benefits because spam is blocked before it enters the corporate network.

- Centralizing anti-spam efforts at the gateway eliminates the need to manage individual spam applications installed on every e-mail server, or on desktops and laptops typically scattered throughout an enterprise. Centralization also streamlines administration of anti-spam measures, such as updating enterprise-wide spam policies, and managing quarantine queues.

- A gateway antispam solution operating at the perimeter offers the advantage of working outside fragile heterogeneous mailserver operating environments.

- Gateway-based solutions may benefit from access to the SMTP protocol-level and network-level information available at the gateway and thus deliver more effective spam blocking.

2.3.2 Cons

- Running a gateway-based solution requires some amount of time and resources, including software, network resources and IT administration. For smaller organizations that do not currently have an e-mail relay (and expose their corporate mail server directly to the Internet), these costs may be significant.

2.4 Available Solutions

Some tips in getting the right anti-spam solution:

- In general, desktop solutions are most appropriate for small businesses and individuals.

- Server-based solutions are cost effective for smaller organizations that have only a single e-mail server for the entire organization (usually organizations with less than 500 mailboxes). However, this is not a cost-effective approach for organizations with multiple e-mail servers.

- Gateway-based solutions are the best approach for larger organizations (with more than 500 mailboxes), more than one e-mail server.

No.	Product Name	Company	D	S	G	Website reference
1	EmailProtect	Content Watch	•			www.contentwatch.com
2	SpamEater Pro	High Mountain Software	•			www.hms.com
3	Qurb	Qurb	•			www.qurb.com
4	ChoiceMail One	RegNow	•			www.digiportal.com
5	Spam Killer	McAfee	•			www.spamkiller.com
6	Spam Buster	Contact Plus	•			www.contactplus.com
7	Matador	Mail Frontier	•			www.mailfrontier.com
8	SpamNet	CloudMark	•			www.cloudmark.com
9	PureMessage	Sophos		•	•	www.sophos.com
10	proofpoint	proofpoint		•	•	www.proofpoint.com
11	MailFrontier	MailFrontier		•	•	www.mailfrontier.com
12	Barracuda	Barracuda Networks			•	www.barracudanetworks.com
13	Brightmail	Symantec			•	www.symantec.com
14	CipherTrust	CipherTrust			•	www.ciphertrust.com
15	Mxtreme	BorderWare			•	www.borderware.com
16	Postini	Postini			•	www.postini.com

D = Desktop S = Server G = Gateway

Table 1: A Non-Exhaustive List of Anti-Spam Solutions

3. Anti-Spam Evaluation Criteria

3.1 Spam Identification

In terms of identifying spam, there are two key criteria by which the effectiveness of a solution should be measured: capture rate, and false positive rate.

3.1.1 Capture rate

Capture rate is defined as the percentage of messages identified as spam, divided by the actual number of spam messages received.

No enterprise anti-spam technology can deliver a 100% capture rate on real-world spam. The key in evaluating these products is to find a solution that provides a high capture rate (80%-90%) on a continuing basis, even as spam evolves and changes over time.

Most anti-spam products provide an “update” service in order to maintain a high capture rate over time.

3.1.2 False Positives

The other key measure of effectiveness is the “false positive” rate, which measures the percentage of valid messages that were incorrectly identified as spam (in other words, legitimate business messages that were blocked).

This metric is particularly important where e-mail is mission critical, and where organizations cannot afford to lose business messages. No anti-spam technology can provide a zero false positive. Less then one tenth of one percent (0.1%) represents a more realistic goal.

A number of vendors provide a “quarantine queue” mechanism that holds suspected spam for manual review by an IT administrator or end users.

Vendor	False positives	Vendor	Spam caught
BorderWare (MS=S)	0.04%	0Spam.Net	99%
Sophos	0.04%	Netriplex	99%
BorderWare	0.04%	Vircom	98%
Postini	0.08%	Process Software	98%
CipherTrust	0.12%	Postini	97%
Symantec (MS=S)	0.16%	MailFrontier (MS=S)	97%
Symantec	0.16%	Messaging Architects	97%
Advascan	0.19%	NoSpamToday!	97%
Proofpoint	0.20%	SpamStopsHere	97%
CipherTrust (MS=S)	0.23%	BlueCat	97%
MailFrontier	0.25%	Intellireach (MS=S)	97%
Proofpoint (MS=S)	0.29%	Advascan	96%
Barracuda	0.30%	Roaring Penguin	95%
Spamfighter	0.34%	MailWise	95%
Cloudmark	0.35%	Solid Oak	95%
NetCleanse	0.46%	CipherTrust (MS=S)	94%
NetIQ	0.55%	Proofpoint (MS=S)	94%
MailFrontier (MS=S)	0.54%	Barracuda	94%
Mycom	0.89%	Clearswift (MS=S)	94%
Aladdin	0.92%	Symantec (MS=S)	93%

Table 2: Capture Rate and False Positive benchmarking of anti-spam solutions by Network World Fusion 2004 (http://www.nwfusion.com/reviews/2004/122004spamcharts.html#ms)

3.2 Five Layers of Defense

The following framework identifies five basic layers of spam defense that an organization should look for in the anti-spam solutions it evaluates.

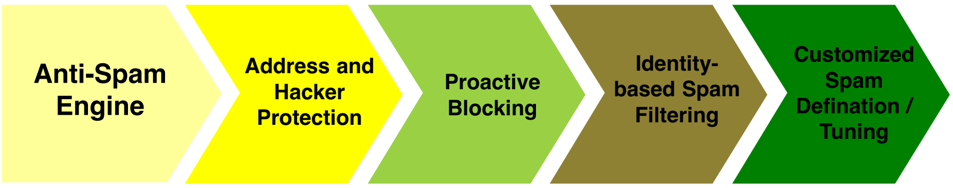

Anti-Spam Engine
Address and Hacker Protection
Proactive Blocking
Identity-based Spam Filtering
Customized Spam Defination / Tuning

Figure 2: Evaluation framework

3.2.1 Anti-Spam Engine

There are a number of different spam engine technologies on the market today, offering varying levels of effectiveness. The table below provides a comparison of the leading anti-spam engine technologies and approaches, including their relative strengths and weaknesses.

Technology	Pros	Cons
Lexical Analysis Applies content filtering to each e-mail message to identify suspected spam, based on word and phrase lists. Note that spam solutions vary in the depth to which they apply lexical analysis – solutions should analyze message subject, body, attachments, and HTML tags, and support some way to identify "disguised" text.	• Proactively identify spam based on common phrases/ words. • Word weightings allow for tuning of spam capture based on word frequency. • Regular expression and pattern matching technology coupled with lexical analysis allows for more precise analysis (for example, "G.a.p.p.y" text can be identified). • Allows an enterprise to tune or customize its definition of spam.	• Some difficulty in detecting bizarre spellings of words (e.g. 'V.I.4.G.R.A'). • Not effective on the increasing amount of HTML based spam that contains no text, just URLs and images. • Is time consuming and error prone if not combined with a dynamic update service, maintenance and testing of word lists. • No understanding of the context of words used in a message (e.g. the word "breast" is an appropriate term in the Healthcare industry).
Heuristics-based Analysis Uses a set of rules to analyze an e-mail message to determine the likelihood that it is spam. Can be combined with lexical analysis to provide improved spam identification.	• Proactively identify spam based on multidimensional attributes. • Equally effective on HTML, graphics based, and text-based spam. • Examples include: - E-mail with two or more embedded images has a higher likelihood of being spam. - Backdated or future-dated e-mail has a higher likelihood of being spam.	• Heuristic rules tend to be complex and difficult to build, test, and maintain. • If not combined with a dynamic update service, maintenance can be time consuming for the IT administrator.
Signature-based Analysis Maintains a database of 'hashes' of previously identified spam messages, and compares each incoming e-mail to this database. Messages that match are identified as spam.	• Fast, effective identification of known spam messages. • Equally effective on HTML, graphics based and text-based spam.	• Catch rates of these methods have degraded as spammers learn to deliberately introduce random variations into their messages. • Must be used in conjunction with a dynamic update service. • Updates must be virtually continuous for maximum spam blocking effectiveness. • Dependent on vendor to maintain spam database.

Bayesian Analysis Algorithm that can be trained to automatically differentiate aggregate textual attributes of spam and non-spam messages. Applied to identify probability that any given message is spam.	• Potential approach to intelligent, learning algorithm for blocking spam. • Works well at the desktop, as the user can train the algorithm according to his/her needs.	• Not effective on the increasing amount of HTML-based spam that contains no text, just URLs and images. • Not proven at enterprise scale – Bayesian learning algorithm difficult to apply automatically at the gateway.
Natural Language Processing Artificial intelligence technology that combines morphemic, syntactic, and pragmatic analysis to correlate text with categories of meanings.	• Can be effective in identifying subtle, text-rich spam messages. • Can filter messages based on multiword concepts, rather than individual keywords.	• Not effective on the increasing amount of HTML-based spam that contains no text, just URLs and images. • Not designed to handle content that is created with the explicit goal of avoiding automated analysis using lexical or grammatical obfuscation. • Performance has typically been an issue.
Challenge/Response Requires senders to verify their authenticity before the e-mail is received by the recipient. The sender of the message will receive a challenge e-mail in response to their original message.	• Authenticates the sender (although this is not foolproof). • Can work for very occasional consumer e-mail users.	• Sending out a challenge for every spam message received significantly increases outbound e-mail volume by 50% or more. • Fails on all automated e-mails, even if they are valid. • Fails on all mass mailings, even if they are valid. • Can be irritating to valid senders. • Spammers are figuring out ways to automate responses to challenges. • Delays message delivery if sender is not checking e-mail.
Collaborative Filtering End users vote on which messages constitute spam.	• OK for consumers applying spam blocking at the desktop.	• Not tailored for enterprise messaging traffic. • Can lead to high incidence of false positives. • If implemented at the gateway, performance can be an issue. • Enterprises usually prefer to control these types of policies for liability and security reasons.

Cocktail Solution that combines multiple analysis methodologies to produce the highest degree of spam identification accuracy.	• If implemented well, will block a broader range of spam variations with the least number of false positives. • The most effective approach for enterprise e-mail traffic that can vary widely from company to company and industry to industry.	• If done poorly, has the potential to equal the sum of false positives of each individual method. • If the underlying architecture is not sound and scalable the cocktail approach can introduce performance issues that could lead to e-mail delivery problems.

Table 3: Different Anti-Spam Engine Technologies

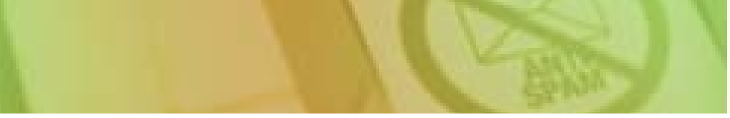
Overall, the most effective solutions tend to incorporate multiple, overlapping anti-spam technologies, and provide a mechanism for dynamically updating the anti-spam engine to maintain effectiveness against evolving spam tactics.

3.2.2 Address and Hacker Protection

In addition to anti-spam engines, an enterprise's first line of defense involves protecting its networks and e-mail infrastructure from attacks and address harvesting.

In particular, spammers often try to harvest e-mail addresses from enterprise e-mail domains by sending an exhaustive set of fabricated; likely e-mail addresses (often tens or hundreds of thousands of e-mail messages). In this so-called Directory Harvest attack, spammers attempt to identify valid e-mail addresses through a process of elimination based on bounce-backs or protocol responses. They then send spam to these addresses, and sell the lists to other spammers over and over again. To make matters worse, entry barriers are extremely low, as novice spammers can easily and cheaply purchase the harvesting tools used to execute these attacks.

Technologies used to defend against these types of attacks often include the e-mail relay, and possibly e-mail policy engines found in e-mail firewall products. In addition to Directory Harvest attacks, these technologies provide protection against Denial-of-Service (DoS) attacks, open relay hijacking, and address re-writing to obscure internal domains. In general, e-mail firewall products provide the strongest defenses in this area since they incorporate a native e-mail relay.



3.2.3 Proactive Blocking

One of the more effective anti-spam defenses involves proactively blocking known spam sources at the Internet gateway. This technique deflects spam before it hits the anti-spam engine, thus eliminating the need for analysis and processing.

Proactive blocking can provide a significant performance improvement in spam processing/message throughput. The key technology that enables these capabilities is the SMTP relay, with possible help from a rules engine/policy engine.

The technologies and techniques used in this type of spam fighting include
- RBLs (real-time black hole lists)
- RDNS (reverse DNS lookup)
- Enterprise/end-user defined blacklists and white lists

Notably, RBLs are starting to wane in popularity because they tend to be so aggressive as to often block non-spam sources.

3.2.4 Identity-based Spam Filtering

One of the reasons that the spam crisis exists today is because it is extremely difficult to accurately identify the sender. The SMTP protocol and the Internet allow people (spammers in particular) to remain anonymous. A number of identity validation / authentication technologies exist today, and this area is just starting to emerge as an effective partial solution to the problem of spam.

By allowing trusted e-mail from known senders to automatically bypass the spam filtering engine and enter the network, IT administrators can create an environment that minimizes loss of business messages and maximizes throughput. E-mail from unknown or non-trusted sources still must pass through the standard spam-filtering process.

The technologies that make it possible to “know” or “trust” the sender of e-mail primarily revolve around digital signatures and encrypted e-mail. For instance, if you can validate the identity of an e-mail sender by looking up his/her digital certificate, the probability decreases that the message is spam.

And if it does turn out to be spam, you have now identified a party against which to pursue legal recourse. Technologies in this area include:

- **S/MIME** - an Internet standard for e-mail encryption for years, supports digital signatures and thus strong authentication. While hard to deploy at the desktop, S/MIME is a viable server-to-server solution and is used today by business partners in finance, healthcare, and government to create ‘trusted networks’.

- **TLS** - based messages - an emerging standard that allows e-mail servers to set up an encrypted channel between them-to the extent the other server can be trusted, the message can be allowed in.

- **Directory integration** (either LDAP or some other internal directory format) - works by confirming that a recipient is valid before passing an e-mail message into the network.

- **Outbound e-mail recipient caching** - makes it possible to identify current or recent correspondents based on outbound message traffic, which is assumed to be valid.

- **Harvesting of digital certificates from inbound e-mail** - used to "remember" trusted senders.

3.2.5 Customized Spam Definition / Tuning

Since every organization will have its own definition of “spam”, the ability to tune and tailor this definition becomes crucial. Some types of technologies lend themselves to customization more than others. Signature-based and heuristic technologies tend to be maintained by an external vendor lab, so some form of override capability must be present in this type of anti-spam engine to support tuning. On the other hand, technologies such as lexical analysis are quite easy to modify.

The best approach for handling this tuning is to support some form of override or exception processing technology as part of the anti-spam engine. These include:

- **White Lists —** allow administrators or end users to identify specific messages or message types that should be allowed to enter the organization, whether or not the message was identified as suspected spam. This is often used to allow in e-mail newsletters for example, which can be hard to distinguish from spam in many cases.

- **Policy Engine-based Exception Lists —** identify specific message attributes that should be granted override access to the network. This type of mechanism is often used to ensure that industry-specific messages/content are not blocked by the anti-spam engine - for example, allowing a message containing words such as “penis” or “breast” to reach its intended recipient in a healthcare organization.

- **Directory-based Anti-spam Policies —** allow IT departments to apply different policies to different individuals/groups/departments in the organization. For example, this approach enables an administrator to allow the marketing department to receive advertising that would normally be blocked as spam.

3.3 Performance: Accept Rate vs. Delivery Rate

Accept rate is the rate at which an anti-spam solution can accept the e-mails before any processing are carried out.

Delivery rate is the rate at which the e-mails can be delivered to the recipient's servers after going through the anti-spam processing.

If a product accepts mail faster than it can deliver it, it has to flow-control the incoming mail at some point. Solutions that don't flow-control are susceptible to a denial-of-service attack because someone can fill up your disks and lock up your server. On the other hand, solutions that accept mail as fast as they can scan or deliver don't deal with mail volume peaks very well.

The best strategy is to accept mail at a faster rate than you can scan it up to some point, then start slowing down senders as resources are consumed.

Vendor	Accept rate (msgs/sec)	Delivery rate (msgs/sec)
Aladdin	21	21
Spamfighter	11.2	11.2
MailFrontier	15.2	10.9
CipherTrust	50.7	7.8
Cloudmark	7.7	7.7
Symantec	15.7	6.4
Sophos	22.3	4.1
Proofpoint	2.8	2.8
BorderWare	10.7	10.6
Barracuda	90	6.7

Table 4: Accept Rate vs. Delivery Rate Performance Benchmark by Network World Fusion

4. Conclusion

Before implementing any anti-spam solution in the enterprise, an administrator has to clearly identify and balance between the anti-spam requirements and the total cost of ownership of such solutions. Finding this right balance requires the understanding of the anti-spam technologies as well as the solutions that are available in the market today.

ENQUIRIES

For further enquiries please contact:-

Information and Network Security Department
Monitoring and Enforcement Division
Malaysian Communications and Multimedia
Commission
63000 Cyberjaya
Selangor Darul Ehsan
Tel : 03 8688 8000
Fax : 03 8688 1000
www.mcmc.gov.my

**Malaysian Communications
and Multimedia Commission**

63000 Cyberjaya, Selangor Darul Ehsan
Tel : 03 8688 8000 Fax : 03 8688 1000
www.mcmc.gov.my