NISER REPORT **NISER-SPA-8020-3401**

ANTI-SPAM FRAMEWORK OF BEST PRACTICES AND TECHNICAL GUIDELINES

Issue 2.00
11 April 2005

National ICT Security and Emergency Response Centre
MIMOS Berhad □ Technology Park Malaysia □ 57000 Kuala Lumpur
Tel: +60 (0)3 8996 1901 □ Fax: +60 (0)3 8996 0827 □
http://www.niser.org.my

NISER REPORT **NISER-SPA-8020-3401**

ANTI-SPAM FRAMEWORK OF BEST PRACTICES AND TECHNICAL GUIDELINES

Issue 2.00
11 April 2005

National ICT Security and Emergency Response Centre
MIMOS Berhad Technology Park Malaysia 57000 Kuala Lumpur
Tel: +60 (0)3 8996 1901 Fax: +60 (0)3 8996 0827
http://www.niser.org.my

DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The National ICT Security and Emergency Response Centre (NISER) and the Working Committee shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

This document is not a legally binding document. Readers and organisations are encouraged to copy this document freely.

[This page is intentionally left blank]

1 INTRODUCTION

1.1 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 email 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 email communication was considered spam messages [2]. According to MessageLabs, spam has grown to represent almost 80% of the total email 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 email as a trusted communication tool. For example, some message contents could be misleading or even fraudulent, such as an attempt to steal a credit card 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]

- 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

1.2 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 the Government agencies, Internet Service Providers, Internet Data Centres, Anti-Virus Solutions Providers, Anti-Spam Solutions Providers and Email 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*.

1.3 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

a) Internet Service Providers

b) Web Hosting Service Providers

c) Mailing List Management Service Providers

d) Marketers

e) Organisations

f) 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.

2 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

3 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 email 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 email campaigns on behalf on the client, storing the list, removing dead emails, managing subscriptions, removing emails of those who un-subscribe, and removing duplicate emails. All lists are hosted and kept by the service provider.

d) Marketers - These are organisations that provide marketing services via email 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 email 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 email 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 anti-spam laws in Malaysia, these compiled best practices together with enforcement at all levels are viewed as the best approach to minimise spam.

3.1 Internet Service Providers (ISPs)

3.1.1 Awareness

3.1.1.1 Increase Awareness to Subscribers [6] [7]

ISPs should inform subscribers:

a) how to minimise the receiving of spam

b) that if they breach the contract by engaging in spam practices, their accounts 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

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.

3.1.2 Technology

3.1.2.1 Ensure Proper Server Configuration [8]

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

3.1.2.2 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.

3.1.2.3 Utilise Filters [8] [9]

ISPs should not knowingly distribute to their users unsolicited emails or emails 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.

3.1.2.4 Implement Rate Limits on Outbound Email 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 email addresses of recipients in an ethical manner.

3.1.2.5 Limit the Volume of Emails 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 emails an account may receive in any given time period.

3.1.2.6 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.

3.1.2.7 Destroy All Outbound Emails 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 emails which the sender is attempting to relay through any unsecured/open server.

3.1.2.8 Do Not Permit Mail Server to Relay Email from Third Parties [7] [10] [38]

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

3.1.2.9 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.

3.1.2.10 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 emails sent to real mailboxes.

3.1.2.11 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

f) URL analysis

3.1.2.12 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.

3.1.2.13 Configure Proxies for Internal Network Use Only [7]

Open proxies allow third parties to anonymously send email 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.

3.1.2.14 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.

3.1.2.15 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.

3.1.2.16 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.

3.1.2.17 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.

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

ISPs should use blacklisting or whitelisting techniques that rely on the identification of email 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 email 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 emails from legitimate senders.

Accepting email 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.

3.1.2.19 Checksum [11]

ISPs should provide a mechanism for the destination email server to determine if an incoming email is bulk in nature by comparing the incoming email against all the emails previously received by the destination email server. An email 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 email body rather than the full email with headers.

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

ISPs should apply the reverse DNS lookup technique to determine if the sending email 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.

3.1.3 Procedures

3.1.3.1 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.

3.1.3.2 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.

3.1.3.3 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.

3.1.3.4 Use of Business Registered Names for Bulk Advertisement Email Senders

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

3.1.4 Compliance and Enforcement

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

ISPs should include in their Terms of Services/Acceptable Use Policy a stronglyworded 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 email, receiving responses by any means from unsolicited bulk/commercial email sent via any other provider.

c) Others necessary for preventing spam mail.

3.1.4.2 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.

3.1.4.3 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.

3.1.4.4 Pursue Legal Remedies [8]

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

3.1.4.5 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.

3.1.4.6 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.

3.2 Web Hosting Service Providers

3.2.1 Awareness

3.2.1.1 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.

3.2.1.2 Increase Awareness to Subscribers

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

3.2.2 Technology

3.2.2.1 Proper Server Configuration

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

3.2.2.2 Utilise Filters

WHSs should not knowingly distribute to their users unsolicited emails, or emails 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.

3.2.2.3 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 email 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.

3.2.3 Procedures

3.2.3.1 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

3.2.3.2 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.

3.2.4 Compliance and Enforcement

3.2.4.1 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.

3.2.4.2 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.

3.2.4.3 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 email; receiving responses by any means from unsolicited bulk/commercial email sent via any other provider, being linked to from a "spamvertised" website;

promoting spamming services or distributing or encouraging spamming services or lists of email addresses; linking to "spamware" or sites promoting "spamware".

3.3 Mailing List Management Service Providers

3.3.1 Awareness

3.3.1.1 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.

3.3.2 Technology

3.3.2.1 Avoid harvesting technology

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

3.3.3 Procedures

3.3.3.1 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.

3.3.3.2 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.

3.3.4 Compliance and Enforcement

3.3.4.1 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.

3.3.4.2 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 email, whether directly or indirectly.

3.3.4.3 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.

3.4 Marketers

3.4.1 Awareness

3.4.1.1 Do Not Disclose Email List Without Permission [22]

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

3.4.2 Technology

3.4.2.1 Do Not Hide True Origin of the Email [7]

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

3.4.2.2 Do Not Harvest Email Addresses Without the Owners' Affirmative Consent [7] [22] [37]

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

3.4.2.3 Do Not Use “Dictionary Attacks” [23]

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

3.4.3 Procedures

3.4.3.1 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.

3.4.3.2 Provide Clear Return Email and Physical Address [22]

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

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

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

3.4.3.4 Work With Credible Mailbox Providers [7]

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

3.4.3.5 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).

3.4.3.6 Opt-out – An Unsubscribe Method To Be Presented Noticeably in Every Commercial Email Sent [7] [12] [22] [23] [25]

Marketers should ensure that all commercial email must provide consumers with a clear and conspicuous electronic option to be removed from lists of future email 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 emails 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.

3.4.3.7 Make Available Alternative Subscription Terminating Methods [25]

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

3.4.3.8 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 email addresses.

3.4.3.9 Personalise Mail [25]

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

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

Marketers should refrain from using harvested lists.

3.4.3.11 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 emailing list the buyer intends to operate.

3.4.4 Compliance and Enforcement

3.4.4.1 Compliance with Advertising Ethics [7] [22]

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

3.4.4.2 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 email 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.

3.4.4.3 Provide A Clear Privacy Policy [22]

Marketers should provide their privacy policy in their commercial emails, either within the body of the email or via a link.

3.4.4.4 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.

3.4.4.5 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.

3.4.4.6 All Commercial Email Content Should Not Be Offensive [23]

Marketers should ensure that no commercial email 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.

3.5 Organisations

3.5.1 Awareness

3.5.1.1 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 emails that can be categorised as spam.

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

3.5.2 Technology

3.5.2.1 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

3.5.2.2 Check Sender Authentication [15]

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

3.5.2.3 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.

3.5.2.4 Use Anti Relay Systems [16]

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

3.5.2.5 URL Detection [27]

Organisations should apply the URL detection technique to detect the domain name of spammers. Most incoming emails 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.

3.5.2.6 Implement Rate Limits on Outbound Email 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.

3.5.2.7 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 emails sent to real mailboxes.

3.5.2.8 DNS Lookup [16]

Organisations should apply the DNS lookup technique, which is able to determine if the sending email 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.

3.5.2.9 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.

3.5.2.10 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)

3.5.2.11 Provide Legitimate Outlets for Marketers

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

3.5.3 Procedures

3.5.3.1 Do Not Reply to Email Scam [19]

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

3.5.3.2 Opt Out [30]

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

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

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

3.5.3.4 Ensure Proper Server Configuration

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

3.5.3.5 Utilise Filters [9]

Organisations should not knowingly distribute to their users unsolicited emails, or emails 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.

3.5.3.6 Limit the Volume of Emails 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 emails an account (employee) may receive in any given time period.

3.5.3.7 Destroy All Outbound Emails Relayed Through Open Server

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

3.5.3.8 Do not Allow Mail Server to Relay Email from Third Parties

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

3.5.3.9 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.

3.5.3.10 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.

3.5.3.11 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.

3.5.3.12 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 email 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 email 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 emails from legitimate senders.

3.5.3.13 Create Special Email Addresses for Marketers

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

3.5.4 Compliance and Enforcement

3.5.4.1 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.

3.5.4.2 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.

3.5.4.3 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.

3.6 Home Users

3.6.1 Awareness

3.6.1.1 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.

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

Home users should never make a purchase from an unsolicited email. 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.

3.6.1.3 Delete Email From Unknown Sender [14] [30] [31] [32] [35] [36]

Home users should delete emails from unknown sender of unsolicited emails. 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.

3.6.1.4 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.

3.6.1.5 Ignore chain letters [30]

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

3.6.2 Technology

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

Home users are recommended to use an email spam filtering program.

3.6.3 Procedures

3.6.3.1 Disable preview function of email client software [30] [31] [32]

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

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

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

3.6.3.3 Protect Your Email Address When Online [9] [12] [14] [18] [30] [31] [33] [34]

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

a) Do not provide their email addresses unless absolutely necessary.

b) Do not post their addresses online.

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

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

3.6.3.4 Use an Alternative Email Address [12] [14] [31] [32] [33]

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

3.6.3.5 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.

3.6.3.6 Block a Sender (Spammer) [12]

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

3.6.3.7 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 email server.

3.6.4 Compliance and Enforcement

3.6.4.1 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].

3.6.4.2 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.

3.6.4.3 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 email addresses or other information with any other organisations.

4 CONCLUSION

Our dependence on the Internet will continue to grow in the years ahead, as will our dependence on the email 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%20Cooperation.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 Email Service Providers, Co-regulating in Matters Relating to Spam Email* (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, *Email Marketing Guidelines as Part of DMAS Code of Practice*, May 2004

[23] McAfee, *Best Practices for Small, Medium and Large Business Email 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, *Email 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 Email 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, June 1999 <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

Committee 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

Name	Organisation
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
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

Secretariat

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