

[Editor's Note: This paper was reviewed and updated in August 2010. Since 2006, the NCC (National Communications Commission) of Taiwan has been proactive in its fight against Spam. For up to date information please visit: the NCC Anti-Spam website: http://220.132.125.162/antispam/english/Spam_zone.html Relevant legislation was updated and other items were amended in order to ensure the accuracy and time relevance of this document.

Shay & Partners can provide valuable assistance in implementing this proposal. For more information on this subject matter, please contact Shay & Partners directly.]

SHAY & PARTNERS

Summary of 2nd OECD Workshop on Spam: Busan, Korea, September 8-9, 2004 And Recommendations for Further Action by the Government of Taiwan

TABLE OF CONTENTS

I. OVERVIEW OF THE 2nd OECD WORKSHOP ON SPAM	3
II. KEY POINTS FROM THE WORKSHOP	6
Spam Volume Continues to Grow Due to Improved Distribution Methods	6
Spam is Increasingly Used to Spread Viruses and Other Malicious Software	6
Spam is Increasingly Used for Fraudulent Criminal Purposes	7
Reducing the Damages Caused by Spam will Take a Multi-Faceted Approach.....	7
III. RECOMMENDATIONS FOR THE GOVERNMENT OF TAIWAN	8
1. Analyze the Nature of Taiwan’s Spam Problem	9
2. Enact Effective Legislation Regulating Spam	9
3. Assist ISPs to Adopt Effective Self-Regulatory Measures.....	11
4. Implement an Effective Public Awareness Campaign.....	12
outdated membership records	12
5. Improve Taiwan’s Level of International Cooperation.....	14
IV. CONCLUSION	15

For almost two years, the Taipei law firm of Shay & Partners has performed extensive research concerning unsolicited commercial e-mail, commonly known as spam. They have investigated the methods by which spam is distributed, the damages caused by it and possible solutions to reduce its impact on business and the general public. They have researched international legislation, consulted with global authorities (governments, industry and academia) and participated in international conferences. Shay & Partners has prepared an extensive report for Taiwan's Council on Economic Planning and Development.

On February 2-3, 2004, Shay & Partners attorneys Arthur Shay and Christopher Neumeyer attended the Organization for Economic Cooperation and Development (OECD)'s Workshop on Spam in Brussels, Belgium. As a follow-up, the OECD conducted a 2nd Workshop on Spam in Busan, Republic of Korea, hosted by Korea's Ministry of Information and Communication.

On September 8-9, 2004, both Arthur Shay and Christopher Neumeyer attended the OECD's 2nd Workshop on Spam, where they attended presentations by the world's leading spam thought leaders. They both had the unique opportunity to discuss various spam related issues with these experts. Mr. Shay was invited and spoke as a panelist concerning the development of an OECD "anti-spam toolkit." The workshop was a great success. Participants agreed that spam is a very serious and growing problem perpetrated by gangs of clever criminals whose tactics are constantly evolving in order to evade laws and technology, for the purpose of committing fraud and earning vast sums of money.

Consequently, developing and implementing effective measures to counter such tactics is an extremely difficult task. The 2nd OECD Workshop brought together a diverse group of thought leaders from a wide-variety of backgrounds all working together to develop solutions to problems caused by spam.

This report is intended to summarize the information presented in the 2nd OECD Workshop and provide recommendations for Taiwan's government to consider implementing to reduce the damages that spam causes to its citizens, businesses, Internet Service Providers (ISP's), and government.

I. OVERVIEW OF THE 2nd OECD WORKSHOP ON SPAM

The workshop opened with a speech by the Vice-Minister of Korea's Ministry of Information and Communication, Dr. Chang-Kon Kim, who noted with pride that his country has developed one of the world's highest rates of broadband Internet penetration, but they later discovered that such technology also serves as a perfect vehicle for the distribution of spam and to the shame of the Korean government, criminals around the world have taken advantage of Korea's broadband infrastructure to make the country one of the world's leading sources of spam.

As a result, Dr. Kim, explained, the Korean government is deeply committed to helping solve the problems caused by spam. Dr. Kim's speech was moving and obviously sincere: the government of Korea has been extremely proactive in its fight against spam by hosting the 2nd OECD workshop, sending a large number of representatives to attend both workshops and enacting anti-spam legislation. This legislation imposes strict penalties for spam offenders. The Korean government also executed an agreement with the government of Australia for international cooperation in the fight against spam.

In Asia, the government of Korea is clearly taking the lead in the battle against spam. Following Dr. Kim's opening remarks, the two-day workshop followed the schedule below.

Session 1: Developing an OECD Anti-Spam Toolkit

The OECD is presently working on developing an anti-spam toolkit comprising booklets, documents and other materials intended to assist interested parties in fighting spam through various approaches. This includes the enactment of regulation, self-regulation, technical measures, international enforcement and co-operation, public-private partnerships and increased awareness through education. Several speakers discussed the status of various activities, key elements of the toolkit and areas where the toolkit could be especially helpful in reducing spam. It is unclear when any elements of the toolkit will be available to the public, but the OECD welcomes public comments at the following address: spam.project@oecd.org.

Session 2: Network Management Solutions to Reduce Spam

This session highlighted "best practices" in network management solutions that can be used to reduce spam. This includes the necessity for national and international facility managers and providers to work collectively and co-operate with each other. Initiatives in this respect include global efforts to close open-relays and open-proxies, which allow spammers to distribute messages through other people's computers as well as acceptable-use policies that ensure network providers can take effective action against spammers.

Session 3: The Role of Authentication in Reducing Spam

Due to the anonymous nature of spam and the extreme difficulty in tracing its origin, authentication has come to be seen as one of the most promising technological tools in the fight against spam. So far, authentication is only a concept and experts differ on when it will be implemented, with estimates ranging from one year to a number of years.

There are two possible types of authentication: domain-level authentication (which would identify only that an e-mail came from a specific domain name and sender-level authentication, which would identify that, it came from a specific person at a specified domain name.

Domain-level authentication would likely entail the use of a pair of keys and cryptography to authenticate messages, whereas sender-level authentication would require those sending an e-mail to a person for the first time to pass a challenge/response test. (Note – please provide an example of a challenge/response test that I can incorporate into this document).

Some of the issues discussed in this session included the following: Effect of an authentication standard on consumers, including the possibility that it may delay email transmission times, burden computer mechanisms, or produce other adverse effects. The likelihood that authentication will reduce global spam or prevent "phishing."

An overview of authentication proposals, explanation of domain-level authentication vs. sender authentication and summary of authentication proposals currently underway (e.g., Sender ID and Domain Keys). Discussion of the criteria to be used in evaluating authentication standards. Costs of implementing the authentication proposals and who would pay these costs. Challenges that might be faced by ISPs that do not participate in an authentication standard were also discussed.

Session 4: New Technologies and Mobile Spam

This session highlighted new and emerging future technologies and the role they may play in helping to reduce spam and mobile spam, including discussion by government and industry representatives with regard to filtering and other technical solutions for spam and the problem of zombie drones.

Session 5: Developments in APEC and Other Non-OECD Economies

Spam is a global problem that knows no geographic boundaries, so it is commonly said that effective solutions will require cooperation among different countries. Therefore, this session was intended to permit some non-OECD countries to share information on efforts being made in their respective countries. Shay & Partners had applied in advance for the opportunity to present the current issues facing Taiwan in this session, but unfortunately the speakers for the session had already been selected. A consumer representative from Hong Kong, a government official from Peru, and an official from the International Telecommunication Union discussed regulatory and self-regulatory measures in their respective countries as well as further steps that can be taken to improve co-operation between OECD and non-OECD economies and ensure that different regions employ coherent strategies in the fight against spam.

Session 6: Ensuring Coherence and Follow-Up

The Busan Workshop on Spam was a productive follow-up to the Brussels workshop. During this session, speakers from government, business and civil agencies discussed recommendations that can be drawn from the various presentations stressing, in particular, how a coherent and effective framework could be developed for future actions, while limiting the costs to users, access providers and service providers respectively.

II. KEY POINTS FROM THE WORKSHOP

As with the 1st workshop, the 2nd OECD workshop on spam brought together numerous talented experts from a wide-variety of backgrounds who provided compelling presentations on the damages caused by spam and potential solutions.

Spam Volume Continues to Grow Due to Improved Distribution Methods

Participants agreed that despite the enactment of legislation in various countries and improvements in filters and technology, the volume of spam continues to grow at an alarming rate. Spammers constantly develop new and better methods for distributing massive volumes of junk e-mails. According to Brightmail, a leading anti-spam software company, spam volumes in May 2004 accounted for 64% of all e-mail traffic. Postini, reported in September that 75% of the 5.6 billion messages it processed were spam. Another company, FrontBridge Technologies, reported in August that 90% of 3.1 billion messages it processed were spam.

Today, most spam is distributed indirectly through the machines of users who are unaware that their computers are being used to send the unwanted messages. Until recently, this problem consisted mainly of open relays and open proxies – security flaws in the mail servers of innocent parties that spammers have learned to use for their advantage. Open relays and open proxies are still a problem, but the major problem today is zombie-drones, armies of computers that have been hijacked by spammers and turned into spam-sending machines, without the knowledge of the machine's owner. While similar in effect to open-relays and open-proxies, spam zombies are much more difficult to detect and prevent. Zombie drones are typically created when an Internet user opens an attachment or visits a website containing a virus, worm, Trojan-horse or other malicious software ("malware") that enables the spammer to operate the user's computer remotely. They can also record all of the keystrokes on the computer (including passwords and other sensitive information) and relay that information back to the perpetrator of the malware. Not only have tactics led to a dramatic increase in the volume of spam, but they have made it increasingly difficult to trace the source of spam. Considerable time and resources are required in order to trace the source of spam and locate and identify the sender, if at all possible.

Spam is Increasingly Used to Spread Viruses and Other Malicious Software

While spam was initially used primarily as a means of advertising pornography and fraudulent products, it is increasingly used for the delivery of worms, viruses, Trojans and other malware (viruses), such as Sobig, MyDoom, Bagel and Netsky, to name just a few. These programs may be used to steal sensitive data, convert other people's computers into spam-sending drones or for the purpose of crashing computers for amusement, but regardless of its purpose, the volume of such malware is rapidly growing.

One leading anti-spam company, Sophos, detected 4,677 new viruses in the first 6 months of 2004, a 21% increase over the same period a year earlier. Mark Sunner, CTO of MessageLabs, another major anti-spam company, reported that one out of 11 e-mails scanned by his company during the past four months contained a virus or other malware. Such programs often spread with alarming speed, such as the SobigF worm, which generated more than 200 million infected e-mail messages in its first week of activity, and some believe this phenomenon lead to the creation of 50,000 new zombie drones per week. Workshop participants unanimously agreed that such malicious programs pose a significant threat and any solution must address the delivery of such programs.

Spam is Increasingly Used for Fraudulent Criminal Purposes

In addition to the increasing use of spam for sending malicious software, participants noted a dramatic increase in the use of spoofing, phishing and other fraudulent schemes perpetrated through spam by international organized crime networks. Spoofing is the sending of a legitimate-looking e-mail that appears to come from a respected company. Typically, the message contains the spoofed company's logo and is linked to a convincing fake website. Usually spoofing is part of a phishing attack where fraudulent e-mails are used to deceive recipients into releasing personal financial data such as credit card numbers, account names, passwords, and so forth. They usually spoof using well-known banks, online retailers and credit card companies. The Anti-Phishing Working Group, estimates that 5% of those who receive phishing e-mails are deceived into responding, and the number of phishing attacks rose from 116 in December 2003 to 1,422 in June 2004 -- a 12-fold increase in six months.¹ The rise in the number of unique phishing attacks in recent months can be seen below.

Phishing is already a problem in Taiwan. In September 2004 the Taipei Times reported that a local teenager was arrested for sending spam containing fake "membership account confirmation" requests, by which he obtained account numbers, user names and passwords, which he used to withdraw money from ATM machines and makes Internet purchases. The suspect also included viruses with his spam to obtain remote access to the recipients' computers. According to the Internet Crime Investigation Squad of Taiwan's Criminal Investigation Bureau, victims included the Hong Kong and Shanghai Banking Corporation, Citibank, Bank of America, and Yahoo. Over the past few years, the Internet crime squad has received complaints of similar crimes in Taiwan.²

While it is difficult to calculate the specific amount of damage caused by spam, the Radicati Group, a California research firm, estimates that spam costs businesses globally around US\$20.5 billion a year. Similarly, a recent EU study placed the worldwide cost to businesses at \$17 billion a year.³ Gartner Research estimates that phishing attacks alone have cost banks \$1.3 billion in damages.⁴

Reducing the Damages Caused by Spam will Take a Multi-Faceted Approach

The world's leading anti-spam authorities, have said countless times that no single solution will ever be effective in resolving the problems caused by spam: virtually every speaker in both OECD workshops agreed with this statement. The business of spam is too profitable, those who send it are too clever, and when one measure is applied to suppress spam, those who send it find other means of distribution, defrauding consumers and evading detection and prosecution. Consequently, experts unanimously agree that effective solutions will be possible only through concerted efforts in a variety of areas such as: legislation; self-regulation by Internet service providers; technical solutions; education and public awareness campaign as well as international cooperation.

1 See <http://www.antiphishing.org/>.

2 See <http://www.taipetimes.com/News/taiwan/archives/2004/09/23/2003203975/print>.

3 See http://www.theaustralian.news.com.au/common/story_page/0,5744,10561978%255E15306,00.html.

4 See <http://www.enterprisepianet.com/security/news/article.php/3412921>.

In the 2nd OECD workshop, authorities spoke of “cutting off the air” to those who send spam by diligently employing all of the above tactics. Anything less, they explained, will be ineffective. The anti-spam toolkit that is being developed by the OECD is intended to assist countries in developing and implementing effective systems in each of those areas. While it is unclear when, or if, the OECD toolkit will actually be completed, the following section of this report is intended to serve the same purpose with regard to Taiwan. It is anticipated that the government of Taiwan will carefully review the following proposals and consider implementing them in order to make real progress against spam.

III. RECOMMENDATIONS FOR THE GOVERNMENT OF TAIWAN

Compared to other countries, Taiwan has done very little to combat spam. The NCC preparatory office and Secure Online Shopping Association (SOSA) have each prepared a draft spam law, although neither draft is anywhere close to being enacted.⁵ The government is looking into the possibility of executing a mutual-cooperation agreement with Australia and has commissioned the law firm of Shay & Partners to provide counsel on spam and attend relevant seminars (for which Shay & Partners is extremely grateful). Taiwan’s ISPs make some efforts to filter out spam but that is the extent of the effort to combat spam. By contrast, dozens of countries have enacted legislation regulating or prohibiting spam. Some have executed multinational agreements, and numerous spammers have been prosecuted in the U.S. and other countries, resulting in prison sentences and multi-million

dollar fines.⁶ While the U.S. only enacted federal spam legislation in the past year, more than 35 states in the U.S. have laws restricting spam that date back to 1997.⁷ Additionally, in other countries ISPs take an active role in scanning for security problems, terminating accounts of spammers and filing legal action against them. By comparison, Taiwan’s largest ISP, HiNet, has a poor global reputation for spam and one of the world’s leading anti-spam organizations, Spamhaus, presently ranks Taiwan as the world’s fourth worst source of spam (after the U.S., China and South Korea).⁸

The above is not criticism of the government of Taiwan, but as motivation to try to find innovative solutions to this ever-growing problem. Taiwan excels in technology in many respects, from its high Internet, broadband and mobile phone penetration rates, to R&D, manufacturing, e-commerce and e-governance. Such accomplishments are largely due to numerous insightful incentive programs and a long-term commitment by the government and industry to excel in technology. By applying the same effort to spam, Taiwan’s government can reduce spam volume, save its citizens, businesses and government vast sums of money and resources and improve the usefulness of the Internet. This will also serve to elevate Taiwan’s international reputation in fighting spam. In order to do so, Shay & Partners recommends that the government take the following actions.

⁵ And, frankly, the authors of this report feel that both drafts could benefit from a few amendments

⁶ See <http://spamlinks.openrbl.org/legal.htm#country>.

⁷ See <http://www.spamlaws.com/state/summary.html>.

⁸ See <http://www.spamhaus.org/>.

1. Analyze the Nature of Taiwan's Spam Problem

As previously noted, Taiwan is presently ranked as the world's fourth worst source of spam. But that figure raises some interesting questions.

How much spam is sent from Taiwan versus how much is sent to Taiwan? What types of spam are most common in Taiwan: those selling illegal pharmaceutical products, body modification products, financial fraud or phishing attacks? Is spam from Taiwan sent directly, or is it merely routed through Taiwan? What types of technologies are being exploited: open-relays, open-proxies, zombies? What specific ISPs and IP addresses are being used? Who owns the IP addresses being used to distribute vast amount of spam? How many Websites used by spammers are hosted in Taiwan and what ISPs are hosting them?

By learning answers to these questions, Taiwan will be better equipped to take meaningful action in identifying and working to reduce spam. While there may be individuals in Taiwan who could perform some of the above forensic research and analysis, Shay & Partners spoke with experts at the OECD workshops who seem especially qualified to handle such investigation. In particular, David Jones, founder and CEO of SpamMATTERS,⁹ an Australian company, made an impressive presentation on how his company performs such investigations and provides detailed reports for government agencies and corporations explaining the nature of their spam problems.

2. Enact Effective Legislation Regulating Spam

The next step is the enactment and enforcement of effective spam legislation. Spam is not legitimate advertising or a minor nuisance: it is a criminal activity that costs billions of dollars in damages and lost productivity to many individuals and corporations. Well over half of all e-mail is spam and the volume keeps growing. Most spam has false or misleading headers, routing information and subject lines and is used for fraudulent or malicious purposes, such as selling phony products, stealing personal data and spreading harmful viruses. While Internet spam is the main problem now, text-messaging and mobile spam will be increasingly problematic in the future.¹¹ Legislation alone will not be sufficient to solve these problems, but it is an essential component of any comprehensive anti-spam strategy.

Some feel that Taiwan already has adequate legislation in regards to spam. Fraudulent spam should be deemed a violation of civil and criminal code prohibitions against fraud. False or misleading subject lines or routing information may violate the Fair Trade Law. Violation of an ISP's terms of use should amount to breach of contract. Routing spam through others' computers violates the Criminal Code's anti-hacking prohibition that was enacted in 2003. Harvesting or trafficking in e-mail addresses may violate Taiwan's Computer-Processed Personal Data Protection Law, which prohibits most private entities from collecting, processing, transmitting or using "personal data."¹² But even if the above laws apply as stated, they are completely inadequate as a response to spam.

9 See http://www.oecd.org/document/46/0,2340,en_2649_22555297_33684718_1_1_1_1,00.html.

10 SpamMATTERS' Website can be found at the following link: <http://www.spammatters.com/>.

11 In Japan, 90% of spam is sent to mobile phones, not PCs, and the trend is growing in other countries.

See <http://www.oecd.org/dataoecd/33/55/33713690.pdf>.

12 However, it is unclear whether an e-mail address would qualify as personal data. Personal data is defined as information "sufficient to identify a person" and an e-mail address might not meet that definition.

Taiwan needs specific legislation regulating spam because the above laws do not define illegal spam;¹³ do not require accurate routing information or advertising labels;¹⁴ do not prohibit harvesting e-mail addresses from Websites or sending bulk e-mails to auto-generated addresses;¹⁵ do not impose liability on merchants who knowingly profit from illegal spam;¹⁶ do not authorize statutory damages per illegal message; and, most importantly, the general laws described above will not lead to a reduction in the volume of spam. It is clear that Taiwan needs to enact strong legislation specifically designed to regulate spam, backed by strong penalties and vigorous enforcement.

Taiwan's government has started work on such legislation. Shay & Partners is pleased that two draft spam bills were released for public discussion in June 2004, one from the preparatory office for the National Communication Commission (NCC) and the other from the Secure Online Shopping Association (SOSA). Realistically, it seems unlikely that either of the above draft bills will be enacted in the near future and that may be advantageous to Taiwan. The two versions are very different and it is unclear whether Taiwan's lawmakers understand the critical differences between the two. Most notably, SOSA's draft bill is an "opt-in" version, whereas the NCC's is "opt-out."¹⁷ Spam authorities worldwide overwhelmingly favor opt-in laws, such as those adopted by the E.U. and Australia, and believe opt-out laws, such as the U.S. CAN-SPAM Act, will make matters worse.¹⁸ Just a few reasons why Taiwan should enact opt-in legislation rather than opt-out are as follows:

Marketers pay virtually nothing to send millions of bulk e-mails, other than Internet connectivity; however, downstream, e-mail must be handled, sorted, stored, processed, filtered and deleted, causing substantial costs to ISPs, businesses and consumers. This takes the form of increased bandwidth, disk space, filters, technical support and lost time. By forcing ISPs, businesses and consumers to pay these costs, e-mail marketers transfer their costs of doing businesses to others, most of whom do not wish to receive the spam e-mails. Therefore, there is no such thing as legitimate unsolicited bulk e-mail; senders, should pay for such e-mails, not recipients; so all senders of bulk e-mails should be required to obtain the recipients' consent in advance before sending such messages.

One of the basic rules for reducing the volume of spam is to never respond to any Spam message, because a response alerts the sender that it has reached a "live" and "active" e-mail account and the response will usually lead to an increase in spam. However, opt-out legislation asks Internet users to do exactly that – to respond to spam e-mails requesting to be taken off the mailing list. When the majority of spam is fraudulent, it is absurd to expect that spammers will honor opt-out requests instead of using them as a means of verifying addresses where they will send more spam.

¹³ This is essential for the benefit of businesses, marketers, ISPs, consumers, prosecutors and judges.

¹⁴ If all commercial e-mails must include a certain label in the subject line identifying them as advertising, Internet users can set their filters to block all e-mails bearing such a label, if they so desire.

¹⁵ Spam is frequently sent to random, auto-generated addresses, but most such addresses are invalid, so the e-mails bounce back and forth, consuming tremendous resources as ISPs repeatedly try to deliver them.

¹⁶ Many feel that such merchant liability is an essential part of good spam legislation, because such merchants are the fuel that drives the spam industry; without them, no one would be sending spam.

¹⁷ As explained above, an opt-out law allows persons to send unlimited spam to recipients until each recipient expresses a desire to receive no more unsolicited e-mails; an opt-in law prohibits the sending of unsolicited bulk e-mails except to recipients who have already consented to receiving such e-mails or with whom the sender has a pre-existing transactional relationship.

¹⁸ It would have been hard to find a participant at either OECD workshop who favored opt-out legislation.

As noted above, one of the most troubling aspects of spam is its frequent use to spread viruses and other malware. Spammers have started using the “Click to remove name from list” button as a means of spreading such programs. By clicking on such a button, not only do you confirm your address for the spammers, but you have downloaded malicious software onto your machine.¹⁹

Shay & Partners feel strongly that Taiwan should enact opt-in legislation, rather than opt-out, but it has noted a number of changes and additions that it would recommend making to each of Taiwan’s draft bills. For example, the NCC draft law fails to prohibit harvesting of e-mail addresses or sending of bulk e-mails to auto-generated addresses. While it requires spam to include a feature for opting out of further e-mails, it does not require that feature to actually work.²⁰ While the SOSA draft is better, it also has its limitations, such as permitting the sending of unsolicited commercial e-mails only to those with whom the sender had a previous transactional relationship, but it fails to define such a relationship.

3. Assist ISPs to Adopt Effective Self-Regulatory Measures

ISPs play a crucial role in protecting Internet users from spam; they can take numerous actions to effectively reduce spam and its negative effects. Unfortunately, Taiwan’s ISPs, have earned a reputation for not taking action.²¹ Taiwan’s largest ISP, HiNet, has stated that it spends considerable resources dealing with spam and Taiwan’s ISPs vowed years ago that they would work together to tackle spam. To date HiNet’s expenditures have clearly been ineffective and the ISPs have failed to take any meaningful actions.

Consequently, the government should assist Taiwan’s ISPs to take appropriate steps to fight spam. A few actions that Taiwan’s ISPs should take are as follows:

All of Taiwan’s ISPs must adopt Terms of Use strictly prohibiting the sending of spam, and enforce such terms, promptly terminating the account of any person who sends spam or hosts a Website used in connection with spam.

The majority of all spam is routed through security breaches on innocent users’ machines. ISPs should make it a top priority to prevent such practices by running virus filters on incoming and outgoing mail servers, restricting the use of port 25, watching for unusual spamming behavior and educating users on how to protect their computers. ISPs should consider free distribution of anti-spam, anti-virus and anti-spyware software on CDs and on the ISP Websites, as a second line of defense, to identify malware that gets past ISPs filters.

¹⁹ See http://www.theregister.co.uk/2004/09/22/opt-out_exploit/.

²⁰ Critics identified the same flaw in an early draft of the CAN-SPAM Act, leading to the Act being revised.

²¹ For example, the Spamhaus Blocklist lists more than 60 IP addresses of spammers that are hosted by Hinet, and criticism of Hinet is common. See e.g., <http://web.greens.org/etc/twmail.shtml> (“The largest Internet Service Provider in Taiwan, Hinet, lets its customers send all the junk email they want . . . Since spammers are now able to use Hinet with relative impunity, spammers have flocked to them. Any message from a Hinet network address is likely to be spam”); <http://www.spamreaper.com/blackhats.html> (“As far as I can tell Hinet has never taken any action against any spammer using their servers and never will.”)

ISPs should perform periodic network sweeps to detect open-relays, open-proxies and infected PCs, notifying users of the problem and assist in closing such security breaches in order to solve the problem.

ISPs should work closely with one of the widely used, reputable professional block-lists, such as the Spamhaus SBL²² or Mail Abuse Prevention System's RBL,²³ and promptly take action against listed addresses. Numerous universities, government agencies and major companies use the above systems, so there is no need for ISPs to compile their own block lists. ISPs should recognize that blocklists are not hostile to them. They have a common enemy – spammers – and should work together in a spirit of cooperation against them. By following this approach, Taiwan's ISPs will discover that operators of blocklists are eager to assist and can be extremely helpful in reducing spam.

Every ISP should ensure that users can lodge complaints about spam by verifying that the ISP's contact information at the Asia Pacific Information Centre (APNIC), one of the world's four regional Internet registries, is correct;²⁴ the ISP has inverse address records that permit users to look up a particular IP address in order to find the domain name of the sender; the ISP has an abuse or postmaster mailbox where complaints can be lodged; and the ISP monitors complaints regularly and acts upon them. Most ISPs receive massive volumes of spam, so it is understandable that ISP administrators may feel they have done all they can to combat the problem. But as noted above, their efforts thus far have been ineffective. By taking these actions recommended in this paper they will likely see a significant reduction in spam and a corresponding savings in resources.

Finally, based on past performance, it seems unlikely that Taiwan's ISPs will take actions such as these on their own. Consequently, it may be appropriate for the government to implement measures to assist through the provision of materials, advice or financial incentives, or even require ISP actions through mandatory legislative provisions or regulatory measures.

4. Implement an Effective Public Awareness Campaign

The government should launch a public awareness campaign to inform Internet users of effective tactics that can be employed to reduce ones volume of spam, risk of being infected by malware, and risk of being victimized by fraudulent spam. When the NCC has been created, it might be ideal for handling such a campaign; until then, the NCC Preparatory Office, Government Information Office or other agency might be appropriate. Regardless of what agency is responsible, such a campaign could be extremely effective, particularly if it included a dedicated government website, radio, newspaper, television and other media.

The campaign should educate users concerning the following types of information:

²² See <http://www.spamhaus.org/sbl/>. As of August 31, 2004, the SBL listed 61 IP addresses hosted by HiNet that was known sources of spam. See <http://www.spamhaus.org/sbl/listings.lasso>.

²³ See http://www.mail-abuse.com/services/mds_rbl.html.

²⁴ While APNIC requires that organizations register valid contact details, it does not verify such details, is not automatically notified if they later cease to be valid and has long been criticized for having incorrect or outdated membership records

Methods to reduce the amount of spam one receives, such as using long e-mail addresses that incorporate letters and numbers; not posting e-mail addresses online; using separate addresses for chatrooms and personal use; and not responding to spam.

Methods to filter out unwanted spam, such as through the use of filtering software, blocklists and whitelists should also be highlighted.

Methods to reduce the threat of malware, including updating Windows regularly; installing anti-virus and anti-spyware programs and updating them regularly; installing a firewall; not opening or downloading suspicious files or attachments; and closing the preview function on Outlook and similar software.

Methods to differentiate between phishing attacks and legitimate e-mails from banks or other such entities requesting sensitive personal data.

Methods to determine the IP address from which an e-mail was sent and lodge a complaint with the sender's ISP.

Despite the technical subject matter, the campaign should not be overly technical. The purpose of the campaign is to get Internet users to notice, understand and observe the messages of the campaign, so it is imperative that the messages be clear and accessible. For example, the government of the Netherlands included in its educational anti-spam campaign a Donald Duck comic, communicating a potentially tedious message in a clear, lively, and entertaining manner through an extremely popular Walt Disney character.

5. Improve Taiwan's Level of International Cooperation

Spam is a global problem that will require global solutions. Because e-mails are not confined by national boundaries, enforcement of spam legislation is difficult and international sharing and coordination of information and strategies is essential. Shay & Partners is pleased that Taiwan's government recognizes this and has taken steps to cooperate with other nations in finding solutions to spam.

So far, such cooperation has taken several forms, including hosting and sponsoring the attendance by Shay & Partners and others at seminars, such as the Asia-Pacific Net Abuse Conference, in Taipei in 2003, and others sponsored by the OECD, APEC and Asia-Pacific Coalition Against Unsolicited Commercial E-mails (APCAUCE). Such opportunities are an outstanding opportunity to keep up with technological developments in a rapidly changing field, share information and strategies, and make valuable connections with governmental and industry authorities.

The government should continue to host and sponsor participation at such events. The next step in international cooperation is to execute multi-national agreements regarding sharing of information and cooperation in the battle against spam. Taiwan's government took a big step in this direction in January 2004, when the Directorate General of Telecommunications (DGT) was one of 36 agencies in 25 countries that signed the US FTC's "Operation Secure Your Server," a global campaign to identify open relays and open proxies and take action to close them. It is unclear whether the DGT has followed through on that agreement by taking action against spammers – if it has not done so it should be encouraged to do so. In any event, Taiwan's government is to be commended for becoming part of the global campaign against spam.

Going a step further, the government has expressed interest in several multi-national agreements that other countries have executed regarding spam, such as the 2003 MOU between Australia and Korea,²⁵ 2004 Joint Statement between Australia and Thailand,²⁶ and 2004 MOU between Australia, the US and the UK.²⁷ Taiwan's government is apparently considering the possibility of entering into a similar agreement, possibly with the Government of Australia. that would be an outstanding accomplishment for Taiwan and an effective tool in the battle against spam.

25 See http://www.aca.gov.au/consumer_info/frequently_asked_questions/spam_MOU.rtf.

26 See http://www.aca.gov.au/consumer_info/spam/Aust_Thailand_Joint_Statement.rtf.

27 See <http://www.ftc.gov/os/2004/07/040630spammoutext.pdf>.

IV. CONCLUSION

Taiwan is a highly-developed nation that excels in technology, including R&D, manufacturing, mobile phone penetration, broadband Internet usage, e-commerce, e-government, and so forth. But the country has little to show in the battle against spam. Taiwan's government has been slow enacting legislation, ISPs have done little, and the country is presently ranked as the world's fourth worst source of spam. To be fair, one must recognize that spam poses an enormous, ever-growing, ever-changing problem, once considered just a minor annoyance, but today recognized as an extremely costly criminal threat, and no country in the world have implemented means to effectively control it. Even the US, arguably the world's most technologically advanced nation, has always been the world's leading source of spam and has not yet devised a solution.

The good news is that numerous, extremely bright and talented experts from a wide variety of backgrounds and geographic regions, have been working for years on developing solutions to spam and, while they are unlikely to develop a single solution, they have developed a number of measures that, when used together, should result in a meaningful reduction in the problems caused by spam. These solutions include technology, legislation, education and public awareness, industry self-regulation and international cooperation.

This report is intended as a practical guide to assist Taiwan's government in implementing such solutions. By taking appropriate actions in all of these areas, there is little doubt that Taiwan can reduce its volume of incoming and outgoing spam, save businesses, ISPs, individuals and the government vast sums of time and money, and greatly improve Taiwan's international reputation as a technology leader.