



*Summary of 2<sup>nd</sup> OECD Workshop on Spam:  
Busan, Korea, September 8-9, 2004  
and  
Recommendations for Further Action by  
the Government of Taiwan*

SHAY & PARTNERS

## **CONTENTS**

	<b><u>Page</u></b>
<b>I. <u>OVERVIEW OF THE 2nd OECD WORKSHOP ON SPAM</u></b>	2
<b>II. <u>KEY POINTS FROM THE WORKSHOP</u></b>	5
Spam Volume Continues to Grow Due to Improved Sending Methods	5
Spam is Increasingly Used to Spread Viruses and Other Malicious Software	6
Spam is Increasingly Used for Fraudulent Criminal Purposes	6
Reducing the Damages Caused by Spam Will Take a Multi-Faceted Approach	8
<b>III. <u>RECOMMENDATIONS FOR THE GOVERNMENT OF TAIWAN</u></b>	8
Analyze the Nature of Taiwan’s Spam Problem	9
Enact Effective Legislation Regulating Spam	10
Assist ISPs to Adopt Effective Self-Regulatory Measures	12
Implement an Effective Public Awareness Campaign	14
Improve Taiwan’s Level of International Cooperation	15
<b>IV. <u>CONCLUSION</u></b>	16
<b><u>APPENDIX I</u></b> : List of Speakers and Presentations from OECD Workshop	18
<b><u>APPENDIX II</u></b> : Sample Anti-Spam Public Awareness Campaign Material	21

For almost two years, the Taipei law firm of Shay & Partners has performed extensive research concerning unsolicited commercial e-mails, or spam, investigating the methods by which it is sent, damages caused by it and possible responses, researching international legislation, consulting with global authorities from governments, industry and academia, participating in international conferences and preparing reports 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, attorneys Shay and Neumeyer attended the OECD's 2nd Workshop on Spam, where they observed presentations by the world's leading spam authorities, discussed the issues with such experts, and Mr. Shay spoke as a panelist concerning the development of an OECD "anti-spam toolkit." The 2nd 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 defeat such criminal tactics is an extremely difficult task, but the 2nd OECD workshop, like the first one, brought together a diverse gathering of talented experts from a wide-variety of backgrounds and locations who are working together to develop solutions to the 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 in order to reduce the damages that spam causes to its citizens, businesses, Internet service providers, government and international reputation.

## **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 sending 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 problem of spam.

Dr. Kim's admission was moving and obviously sincere: the government of Korea has been extremely active in the fight against spam, hosting the 2nd OECD workshop, sending a large number of representatives to attend both workshops, enacting anti-spam legislation, imposing strict penalties, executing an agreement with the government of Australia for international cooperation in the fight against spam, and other measures. 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 below schedule (the speakers' names and many of their presentations are attached as Appendix I to this report):

#### Session 1: Developing an OECD Anti-Spam Toolkit

The OECD is presently working on developing an "anti-spam toolkit" comprising booklets, documents and materials intended to assist interested parties in fighting spam through various approaches, including the enactment of regulation, self-regulation, technical measures, international enforcement and co-operation, public-private partnerships and increased awareness and education. Several speakers discussed the status of such plans, key elements of the toolkit, areas where the toolkit could be especially helpful, where rapid progress can be made, and related issues. 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](mailto:spam.project@oecd.org).

#### Session 2: Network Management Solutions to Reduce Spam

The discussion in this session concerned "best practice" network management solutions that can be used to reduce spam and the necessity, and means, of improving co-operation nationally and internationally among facility managers and providers. Initiatives in this respect have included global efforts to close open-relays and open-proxies, which allow spammers to send messages through other persons' machines, acceptable-use policies that ensure network providers can take effective actions against spammers, and industry self-regulation.

#### Session 3: The Role of Authentication in Reducing Spam

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

there are two possible types of authentication: domain-level authentication (which would identify only that an e-mail came from [www.moea.gov.tw](http://www.moea.gov.tw), for example) and sender-level authentication (which would identify that it came from [certainperson@moea.gov.tw](mailto:certainperson@moea.gov.tw)). The former system would likely entail the use of a pair of keys and cryptography to authenticate messages, while the latter system would require those sending e-mail to a person for the first time to pass a challenge/response test or similar system.

Some of the issues discussed in this session were as follows. 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. Likelihood that authentication will reduce global spam or prevent “phishing.” 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 criteria to be used in evaluating authentication standards. Costs of implementing the authentication proposals and who would bear those costs. Challenges that might be faced by ISPs that do not participate in an authentication standard.

#### Session 4: New Technologies and Mobile Spam

This session concerned new and emerging 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, the problem of zombie drones and mobile spam.

#### 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 from all countries. Therefore, this session was intended to permit some non-OECD entities to share information on efforts being made in their countries. Shay & Partners had applied in advance for the opportunity to make a presentation regarding 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 regions and further steps that can be taken to improve co-operation between OECD and non-OECD economies and ensure that different regions employ coherent strategies.

## 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 representing government, business and civil society discussed conclusions that could be drawn from the presentations stressing, in particular, how a coherent and effective framework could be developed for future actions, while limiting costs to users, access providers and service providers.

## **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 made powerful presentations on the damages caused by spam and potential solutions. Twenty-eight of those powerpoint presentations are attached at Appendix I to this report, however a brief summary of some of the key points is set forth below.

### **Spam Volume Continues to Grow Due to Improved Sending Methods**

Participants unanimously agreed that despite the enactment of legislation in various countries and improvements in filters and other technology, the volume of spam continues to grow at an alarming rate, as spammers constantly develop new and better tactics for pumping out massive volumes of unwanted 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. Another spam-filtering company, 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, almost all spam today is sent indirectly through the machines of users who are unaware that their computers are being used to send spam. 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 locate and take advantage of. Open relays and open proxies are still problematic, but now the major problem 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 harder 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, sometimes recording all keystrokes on the computer (including passwords and other sensitive information) and relaying that information back to the sender of the malware, or permitting the sender to delete or manipulate files or send millions of spam e-mails.

Not only have the above 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, resources and expertise are usually required in order to trace the source of spam and locate and identify the sender, if it is possible at all.

### **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, such as Sobig, MyDoom, Bagel and Netsky, to name just a few. Such programs may be used to steal sensitive data, convert other people's computers into spam-sending drones or solely for the purpose of crashing computers for kicks, but regardless of its purpose, the volume of such malware is rapidly growing.

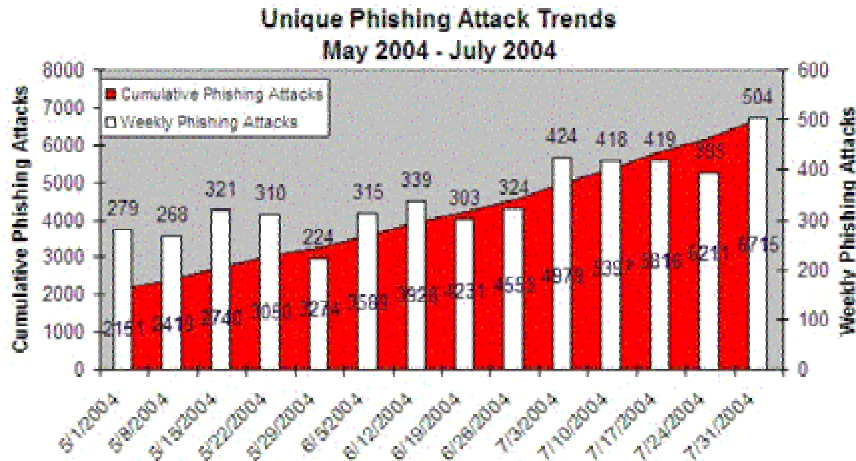
One leading anti-spam company, Sophos, detected 4,677 new viruses in the first 6 months of 2004, a 21% increase over the same period a year earlier. Mark Sunner, CTO of MessageLabs, another major anti-spam company, reported that one out of 11 e-mails scanned by his company during the past four months was carrying 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 leads to the creation of 50,000 new zombies per week.

Workshop participants unanimously agreed that such malicious programs pose a tremendous threat and any solution to spam 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 legitimate-looking 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, usually by spoofing 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.<sup>1</sup> 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 make 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, Yahoo and others and over the past couple of years the Internet crime squad has received complaints of similar crimes in Taiwan.<sup>2</sup>

While it is difficult to calculate the amount of damages caused by spam, including lost time, productivity, filters and other anti-spam technology and personnel, lost or delayed e-mails, and so forth, the Radicati Group, a California research firm, found that spam costs businesses globally US\$20.5 billion a year. Similarly, a recent EU study placed the worldwide cost to businesses at \$17 billion a year.<sup>3</sup> Gartner Research estimates that

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

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

<sup>3</sup> See [http://www.theaustralian.news.com.au/common/story\\_page/0,5744,10561978%255E15306,00.html](http://www.theaustralian.news.com.au/common/story_page/0,5744,10561978%255E15306,00.html).

phishing attacks alone have cost banks \$1.3 billion in damages.<sup>4</sup>

### **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 made that same 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 will find other means of sending messages, defrauding consumers and evading detection and prosecution. Consequently, experts unanimously agree that effective relief will be possible only through concerted actions in a variety of areas: legislation; self-regulation by Internet service providers; technical solutions; education and public awareness; and international cooperation.

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 hoped that the government of Taiwan will carefully review the following proposals and seriously consider implementing them in order to make real progress against spam.

### **III. RECOMMENDATIONS FOR THE GOVERNMENT OF TAIWAN**

When compared to other countries, Taiwan has done almost nothing to fight 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.<sup>5</sup> 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's about it.

By contrast, dozens of countries have enacted legislation regulating or prohibiting spam, a few have executed multinational agreements, and numerous spammers have been prosecuted in the U.S. and other countries, resulting in prison sentences and multi-million

---

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

<sup>5</sup> And, frankly, the authors of this report feel that both drafts could benefit from a few amendments.

dollar judgments.<sup>6</sup> 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.<sup>7</sup> Additionally, in other countries ISPs take an active role in scanning for security problems, terminating accounts of spammers and filing legal actions against them. By comparison, Taiwan's largest ISP, HiNet, has earned a terrible 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).<sup>8</sup>

The above is not intended as criticism of the government of Taiwan, but hopefully as motivation to try to do better. 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 commitment by the government. By applying the same wisdom and dedication to spam, Taiwan's government can reduce spam volume, save its citizens, businesses and government vast sums of money and resources, improve the usefulness of the Internet and elevate Taiwan's international reputation. In order to do so, Shay & Partners recommends that the government take the following actions.

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

By learning answers to the above, Taiwan will be better equipped to take meaningful actions; until then, any proposed solutions will not be tailored to Taiwan's specific problems. While there may be persons 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,<sup>9</sup> an Australian company, made an impressive

---

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

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

<sup>8</sup> See <http://www.spamhaus.org/>.

<sup>9</sup> See [http://www.oecd.org/document/46/0,2340,en\\_2649\\_22555297\\_33684718\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/46/0,2340,en_2649_22555297_33684718_1_1_1_1,00.html).

presentation on how his company performs such investigations and provides detailed reports for government agencies and corporations explaining the nature of their spam problems.<sup>10</sup> Shay & Partners would be happy to assist in obtaining further information from SpamMATTERS or other organizations that provide similar services. Regardless of who performs such analysis, that seems to be an important first step in implementing effective responses to spam.

## **2. Enact Effective Legislation Regulating Spam**

The enactment and enforcement of effective spam legislation is the next step. Spam is not legitimate advertising or a minor nuisance: it is a criminal activity that causes billions of dollars in damages and lost productivity. 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 phone spam will be increasingly problematic in the future.<sup>11</sup> Legislation alone won't be sufficient to solve these problems, but it is an essential component of any comprehensive anti-spam strategy.

Some may feel that Taiwan already has adequate legislation. 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 insecurities in 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."<sup>12</sup> But even if the above laws apply as stated, they are completely inadequate as a response to spam.

Taiwan needs specific legislation regulating spam because the above laws do not define illegal spam;<sup>13</sup> do not require accurate routing information or advertising labels;<sup>14</sup> do not prohibit harvesting e-mail addresses from Websites or sending bulk e-mails to

---

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

<sup>11</sup> 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>.

<sup>12</sup> 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.

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

<sup>14</sup> 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.

auto-generated addresses;<sup>15</sup> do not impose liability on merchants who knowingly profit from illegal spam;<sup>16</sup> 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 promulgate strong legislation designed specifically 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 promulgated in the near future and that may be just as well. The two versions are very different and it is unclear whether Taiwan's lawmakers understand the crucial differences between the two. Most notably, SOSA's draft bill is an "opt-in" version, whereas the NCC's is "opt-out."<sup>17</sup> 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.<sup>18</sup> 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 for increased bandwidth, disk space, filters, technical support and 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.
- One of the most basic rules for reducing ones volume of spam is to never respond to spam, 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

---

<sup>15</sup> 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.

<sup>16</sup> 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.

<sup>17</sup> 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.

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

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.

- As noted above, one of the most troubling aspects of spam is its frequent use to spread viruses and other malware. Already, 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.<sup>19</sup>

Not only does 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. And, while it requires spam to include a feature for opting out of further e-mails, it does not require that feature to actually work.<sup>20</sup> While the SOSA draft is better, it too has flaws, such as the fact that it permits 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.

Shay & Partners would welcome the opportunity to share with Taiwan’s lawmakers orally or in writing what it has learned from its research concerning the prevailing global views on essential provisions in spam legislation, in particular regarding opt-in and opt-out. Shay & Partners would also gladly assist in revising or drafting appropriate legislation, upon request. Whether the government accepts such offers or not, it is essential that Taiwan enact effective legislation regulating spam and use its best efforts to enforce it.

### **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 the harms that it causes. Unfortunately, Taiwan’s ISPs, have earned a reputation for not taking such actions.<sup>21</sup> 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, but HiNet’s expenditures

---

<sup>19</sup> See [http://www.theregister.co.uk/2004/09/22/opt-out\\_exploit/](http://www.theregister.co.uk/2004/09/22/opt-out_exploit/).

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

<sup>21</sup> 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.”)

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 insecurities 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 and identify malware. 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 catch malware that slips past ISPs filters.
- ISPs should perform periodic network sweeps to detect open-relays, open-proxies and infected PCs, notify users of such problems and assist in closing such insecurities and curing the problems.
- ISPs should work closely with one of the widely-used, reputable professional block-lists, such as the Spamhaus SBL<sup>22</sup> or Mail Abuse Prevention System's RBL,<sup>23</sup> 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 the common enemy. By taking such an 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;<sup>24</sup> the ISP has inverse address records that permit users to look up a particular IP address in order to find the domain

---

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

<sup>23</sup> See [http://www.mail-abuse.com/services/mds\\_rbl.html](http://www.mail-abuse.com/services/mds_rbl.html).

<sup>24</sup> 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

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. But as noted above, their efforts thus far have been totally ineffective. By taking the above actions they will likely see a significant reduction in spam and corresponding savings in resources. Upon request, Shay & Partners will gladly provide recommended Terms of Use, detailed instructions on implementing the above measures, and introductions to leading technical experts who will be happy to assist.

Finally, based on past performance, it seems unlikely that Taiwan's ISPs can be counted on to take actions such as the above 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:

- 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.
- Methods to reduce the threat of malware, such as 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 an effective complaint with the sender's ISP.

Despite the technical subject matter, the campaign should not be boring. After all, 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 medium.<sup>25</sup> Shay & Partners lacks such artistic skills, but would be happy to assist in writing the text of messages to be used in such an educational campaign.

## **5. Improve Taiwan's Level of International Cooperation**

It is often said that 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 greatly pleased that Taiwan's government recognizes this and has taken active steps to cooperate with other nations in finding solutions to spam.

So far, such cooperation has taken several forms for Taiwan, 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 means of keeping up with technological developments in a rapidly changing field, sharing information and strategies, and making valuable connections with governmental and industry authorities from around the world. 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 made a big step in this direction in January 2004, when the Directorate General of Telecommunications (DGT) was one of 36 agencies in 26 countries that signed the US

---

<sup>25</sup> See Appendix II. While the comic is written in Dutch and may not be understandable to most readers of this report, it is included to demonstrate how the messages can be communicated in a clear and entertaining manner.

FTC's "Operation Secure Your Server," a global campaign to identify open relays and open proxies and take actions to close them. It is unclear whether the DGT has followed through on that agreement by taking appropriate actions – if it hasn't done so it should be encouraged to do so. In any event, Taiwan's government is to be commended for signing on to the above 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,<sup>26</sup> 2004 Joint Statement between Australia and Thailand,<sup>27</sup> and 2004 MOU between Australia, the US and the UK.<sup>28</sup> 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. Shay & Partners could provide extremely valuable assistance in implementing the above proposal. Not only are the attorneys at Shay & Partners thoroughly familiar with the above agreements, but they have close relationships with governmental officials who were responsible for drafting, negotiating and executing the above agreements, having communicated extensively with them by e-mail and at various spam seminars. Taiwan's government is strongly encouraged to further investigate, negotiate and ultimately execute such a multi-national agreement and Shay & Partners would be happy to assist.

#### **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 brag about 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 has 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.

---

<sup>26</sup> See [http://www.aca.gov.au/consumer\\_info/frequently\\_asked\\_questions/spam\\_MOU.rtf](http://www.aca.gov.au/consumer_info/frequently_asked_questions/spam_MOU.rtf).

<sup>27</sup> See [http://www.aca.gov.au/consumer\\_info/spam/Aust\\_Thailand\\_Joint\\_Statement.rtf](http://www.aca.gov.au/consumer_info/spam/Aust_Thailand_Joint_Statement.rtf).

<sup>28</sup> See <http://www.ftc.gov/os/2004/07/040630spammoutext.pdf>.

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, largely, as a practical guide to assist Taiwan's government in implementing such solutions. By taking appropriate actions in all of the above 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.

---

Shay & Partners is a Taipei law firm that handles matters involving telecommunications, broadcasting, technology, intellectual property, international commercial and corporate matters and the Internet. For further information or assistance, please contact attorneys Arthur Shay ([arthur@elitelaw.com](mailto:arthur@elitelaw.com)) or Christopher Neumeyer ([Christopher@elitelaw](mailto:Christopher@elitelaw)).

## APPENDIX I

### Chairpersons, Speakers and Presentation Materials From the 2nd OECD Workshop on Spam<sup>29</sup>

#### SESSION 1: DEVELOPING AN OECD ANTI-SPAM TOOLKIT

Chair: [Tom Dale](#) (Chair of the OECD Task Force on Spam and Department of Communications, Information Technology and the Arts, Australia)

[Lindsay Barton](#) (Department of Communications, Information Technology and the Arts, Australia)



The Spam "Toolkit": A mini-armoury against spam!

[Jean-Jacques Sahel](#) (Vice-chair of the OECD Task Force on Spam and Department of Trade and Industry, UK) Working internationally against spam through the OECD spam toolkit: Strengthening Global Confidence in the Information Society



[Peter Coroneos](#) (Internet Industry Association, Australia) Anti Spam Initiatives in Australia - A Case Study of a Toolkit Approach



[Philippe Gérard](#) (Vice-chair of the OECD Task Force on Spam and Directorate General, Information Society, European Commission ) The contribution of regulation and self regulation to the fight against spam



[Eung-Lyeol Koh](#) (Korea Information Security Agency) Existing and Emerging Technical Measures against spam



[Kenji Totoki](#) (Ministry of Economy, Trade and Industry, Japan) Strategic Awareness and Education in Japan



Session 1: Panel Discussion

[Arthur Shay](#) (Shay and Partners law firm)

[Bernard Courtois](#) (Information Technology Association of Canada) Public-Private Partnerships : A Critical Element of Canada's Anti-Spam Toolkit Initiative



[Joseph Alhadeff](#) (Oracle, Chair of the Business and Advisory Committee to the OECD Task Force on Information Security and Privacy)

---

<sup>29</sup> Note: If you are reading this report online, most of the names on this list contain a link to the speaker's bio and a PDF file of the speaker's presentation. Otherwise, such information can be found at [http://www.oecd.org/document/39/0,2340,en\\_2649\\_22555297\\_33680935\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/39/0,2340,en_2649_22555297_33680935_1_1_1_1,00.html).

## SESSION 2: NETWORK MANAGEMENT SOLUTIONS TO REDUCE SPAM

Chair: [Stéphane Marcovitch](#) (EuroSPA)

[Yonnie Kim](#) (Daum Communication Corp.) A Case Study : Solution & Policies



[Suresh Ramasubramanian](#) (Outblaze Limited) Cooperative handling of email and network abuse



[Thomas Grob](#) (Federal office of communications, Switzerland) Legal and social implications of ISP initiatives to block SPAM



[Sanjay Pol](#) (Cisco) Identified Internet Mail



## SESSION 3: THE ROLE OF AUTHENTICATION IN REDUCING SPAM

Chair: [Hugh Stevenson](#) ( Federal Trade Commission, United States)

[Carl Hutzler](#) (Anti-Spam Operations at America Online) Email Authentication Technologies : Effect on Consumers and other "End-Users"



[David Crocker](#) (Brandenburg InternetWorking) How Will Authentication Reduce Global Spam?



[Alan Packer](#) (Microsoft) Email Authentication



[Helmut Haag](#) (Allaboutit) Authentication Standards and Costs



## SESSION 4: NEW TECHNOLOGIES AND MOBILE SPAM

Chair: [Wonki Min](#) (Ministry of Information and Communication, Republic of Korea)

[Enrique Salem](#) (Symantec) The Spam Problem



[James Seng](#) (Infocomm Development Authority of Singapore) Emerging Technologies in Spam



[Mark Sunner](#) (MessageLabs) Turning Email Security Inside Out



Session 4 (continued) Chair: [Eiichi Matsuzawa](#) (NIFTY)



[David Jones](#) (SpamMATTERS) Eliminating the Technical Burden of Regulation Automated Collation, Forensics and spam complaint handling



[Dong-Woon Kim](#) (SK Telecom) Combat against Spam SMS



[Kimihiko Oku](#) (Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan) Joint initiative between public and private sectors against mobile spam



## SESSION 5: DEVELOPMENTS IN APEC AND OTHER NON-OECD ECONOMIES

Session 5 Chair: [Peter Ferguson](#) ( Vice-chair of the OECD Task Force on Spam and Chair of the OECD

Working Party on Information Security and Privacy, Industry Canada)

[Robert Shaw](#) (International Telecommunication Union) Spam: a global challenge in a borderless society



[Carlos Romero Sanjinés](#) (Ministry of Communications, Peru) Spam situation in Peru



[Connie Lau](#) (Hong Kong Consumer Council) A Hong Kong Perspective on Spam



Elizabeth Shelton (Department of State, United States) International Cooperation



## SESSION 6: ENSURING COHERENCE AND FOLLOW- UP

Chair: [Philippe Gérard](#) (Vice-chair of the OECD Task Force on Spam and Directorate General, Information Society, European Commission)

[Martin Westerhof](#) (Ministry of Economic Affairs, Netherlands ) Ensuring Coherence and Follow-Up:



Role of Government

[Joseph H. Alhadeff](#) (Oracle, Chair of the Business and Advisory Committee to the OECD Task Force on Information Security and Privacy) Ensuring Coherence and Follow-Up: A Business View



[Patrick von Braunmühl](#) (Federation of German Consumer Organizations) Ensuring coherence and follow up - a perspective from civil society



## CLOSING REMARKS

[Tom Dale](#), Chair of the OECD Task Force on Spam

## APPENDIX II

### Sample Anti-Spam Public Awareness Campaign

#### Materials from the Netherlands



# INTERNETREGELS UIT HET HANDBOEK VAN DE JONGE WOUDLOPERS



Surfen op internet is net alsof je op straat loopt. Je ziet leuke dingen, maar je kunt ook vervelende dingen meemaken. Als je op straat iets vervelends ziet, kun je gauw weglopen en het thuis aan je moeder of vader vertellen. Maar als je zit te internetten, ben je meestal al thuis! Dan moet je dus zelf iets aan de situatie doen. En natuurlijk moet je zelf ook geen lastenkwad uitdelen. Op deze bladzijden lees je hoe je veilig en verstandig kunt surfen.

## WELCHATTEN, NIET KATTEN!

Chatten of e-mailen kan heel leuk zijn. Je ziet elkaar met en toch kun je makkelijk met elkaar praten. Maar vergeet niet dat digitaal met wie je chat wel een echt mens is! Iemand praten of lachen via een chatbox of e-mail is net zo naar als in het echt. Als je zelf gepost wordt is dat natuurlijk ook heel vervelend. Maar er is één voordeel: je kunt gewoon je pc afzetten en lekker buiten gaan spelen. Want uren achter de computer zitten is immers ook niet gezond!



## HELP! I WARE JONGENS!

De mogelijkheid bestaat dat internetters – zogenaamde hackers – via het internet gaan rotsbuitelen in jouw computer. Deze Zwarte Jongens kunnen veel schade aanrichten. Een goede bescherming tegen computer-inbrekers is een 'viruswalf'. Dit is een programmaatje dat ervoor zorgt dat niemand je computer binnen kan komen.



Natuurlijk wil je zelf ook niet voor internet worden aangezet. Als je op plekken terecht komt waarvan je vermoedt dat je er niet hoort te komen, ga daar dan snel vandaan.



## BRIEF AAN...

Via internet kun je met één druk op de knop een grote map of leuke foto naar al je vrienden of vriendinnen sturen. Sta er altijd wel even goed bij stil wat je stuurt. Het is bijvoorbeeld kinderachtig om iemand met een vreemde foto of slechte grap voor gek te zetten. Of om naar of rare dingen te sturen die je zelf ook niet zou willen ontvangen. Tel dus altijd even tot tien en denk goed na wat de gevolgen kunnen zijn voordat je op send of verzenden drukt! Waarschuw altijd direct je ouders als je zelf naar of rare mail krijgt. In ieder geval er nooit op reageren!

## SNIFI MIJN COMPUTER IS ZIEKI!

Een computer kan net als jij ziek worden. Meestal komt dat door virussen. Die virussen kunnen overal zitten. Bijvoorbeeld in e-mails van een vriend of vriendin. Of in programma's of spelletjes die je downloadt van internet. Vraag dus aan je ouders of er wel een virusscanner op de computer zit. Want die kan virussen begraven. Open in ieder geval nooit mails van mensen die je niet kent. Gelijk deleten, niet openen! Stuur ook geen e-mails door die je niet vertrouwt, want die kunnen de computer van een ander virus bevesten. Zelfs zo erg dat-ie helemaal niet meer doet. En daar zou iedereen doodziek van worden!



## KEN IK U?

Niet als op straat moet je ook op het internet en bij het chatten vrienden niet zonder meer vertrouwen. Mail daarom nooit je echte naam, adres of telefoonnummer naar mensen die je niet kent. Ga ook nooit in op 'aanbiedingen' of koopjes op internet, want die kunnen je ouders een hoop last bezorgen. Direct weeg kijken dus!







## SHAY & PARTNERS

11F, 109 REN AI RD., SEC.4, TAIPEI, 106 TAIWAN

TEL:+886-2-87733600 FAX: +886-2-87733611

<http://www.elitelaw.com>

E-mail: [webmaster@elitelaw.com](mailto:webmaster@elitelaw.com)