MEDIABUZZ PTE LTD

2ND QUARTER 2005

Empowering AsianeMarketing
Asia's Electronic Marketers

APRIL 2005

WHAT TO DO TO ENSURE YOUR E-MAILS ARE NOT CLASSIFIED AS SPAM

INSIDE THIS ISSUE:

SPECIAL POINTS OF INTEREST:

- **Four APAC countries in top spam producing countries' list, Page 5**
- **E-mail Lifecycle Management (ELM) is becoming the key component of organizations' IT strategy, Page 7**
- **Confidence in the Internet will result in greater faith in e-marketing, Page 9**
- **Securing the Infocomm environment: A national priority, Page 11**
- **A rundown on Singapore's soon-to-be revealed anti-spam law, Page 13**

Commercial e-mails have in general a sales focus - but that's exactly very often the criteria spam filter manufacturers make use of to identify spam. Attached you will find some tips which are quite easy to implement, so that your own mailing is not declared as spam.

The race of the spam producers versus the anti-spam software solution providers is in full swing. While professional spammers vehemently try to outsmart the always improving filter solutions, unaware e-marketers often only stand on the sidelines and wonder why their e-mails apparently do not reach their customers. Yet, it is not so difficult to ensure that your e-mails aren't thrown out by spam filters.

Write the name of the addressee correctly

Next to the intrinsic e-mail address, the complete name belongs in the " To: " line of every e-mail. Accompanied with a personal salutation in the body of the mail, the risk of being blocked by spam filters already sinks significantly. Among the millions of spam mails which are dispatched daily, only a few e-mails can be found which correspond to this exemplary pattern. Spam filters are aware of this and therefore are more likely to bend the rules with properly addressed e-mails.

continues on Page 2

IS YOUR OPT-IN PROCESS A TURN-OFF?

An e-marketer's job is already an all-consuming role, what with ensuring that one's message is not considered as spam, does not get blocked by spam filters, reaches the right target audience, and importantly, is read and so on.

In view of this, are you ensuring that your opt-in process in not scaring off your would-be readers and subscribers?

Take a moment to think about it: how much information do you really need to know NOW to move forward? It is crucial to remember that the less data you need to initiate a response, the better. So be economical.

Ask yourself the question:

Do you really need a physical address and postal code?

continues on Page 2

TIPS FOR AVOIDING SPAM

Spam is seen as a minor annoyance by some users, while others are so overwhelmed with spam that they are forced to switch e-mail addresses. But just how did spammers get your e-mail address in the first place? The answer usually boils down to the individual's online behaviour.

Research shows that e-mail addresses posted on websites or in newsgroups attract the most spam. Spammers use software harvesting programs such as robots or spiders to record e-mail addresses listed on websites, including both personal and institutional web pages.

Some spam is generated through attacks on mail servers, methods that don't rely on the collection of e-mail addresses at all. In "brute force" attacks and "dictionary" attacks, spam programs send spam to every possible combination of letters at a domain, or to common names and words. While these attacks can be blocked, some spam is still likely to get through. Currently, there is no foolproof way to prevent spam, but educating users is still the crucial factor in fighting the nuisance.

continues on Page 3

From Page 1 — What to do to ensure your e-mails are not classified as spam

Use a genuine sender's address

Not only the address of the addressee, but also the one of the sender states a lot about the quality to be expected of the e-mail contents. E-mail marketing activities, which for organizational reasons aren't sent by a personal sender's address, are more likely delivered, if the sender's address consists of entire word or name combinations like for example newsletter@company.com.sg or John.Smith@company.com.sg.

Do not use cryptic characters, slogans, or abbreviations in the reference line

Spam filters are sensitive to certain buzz words, cryptic characters, slogans, abbreviations or even empty subject fields. Reference lines like, *WIN NOW* or *200% IN ONLY ONE WEEK* are classified and rightly eliminated as spam.

Don't use "non-words" in the mail body

The active wordlists of spam filters provide an immediate confiscation of the mail, if fishy words are detected.

Advanced solutions even permit a weighing of single words, so that if a defined threshold value is exceeded, the whole mail quickly gets moved into quarantine. That's why flowery phrases in the body of the e-mail should be avoided, besides the already mentioned slogans in the reference line, as for example "Super-Extraordinary-Special-Offer " and abbreviations like XXL, XXX, or similar. The best approach is to set the benchmark with common word and style elements of a classical professional letter.

Choose your e-mail appendix or attachment carefully

Appendices in JPG or DOC format are also often used by spammers. The Adobe Portable Document format, shortly named PDF on the other hand, has not yet been discovered as an appendix of a spam mail. So, if you dispatch your newsletter with an appendix, it is best to use the PDF format.

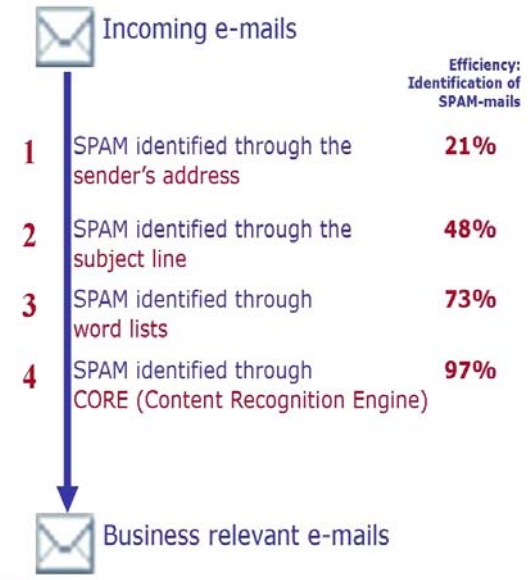
Avoid HTML versions

Graphics lovers will not like this tip, yet: It's proven that spammers have a preference for HTML formatted e-mails. Those of you who avoid this and stick to formulating e-mails as " plain text ", perhaps with hyperlinks to adequate, nicely formed web pages, endears himself to filters.

The inner workings of modern anti-spam filters

The following table shows the modus operandi of advanced anti-spam software. Steps 1-3 have already been explained.

Step 4 shows the latest statistical process technology which automatically categorizes e-mails with high accuracy as SPAM or NOT SPAM, after individual setup by the receiver.



CORE is a statistical process that analyzes and classifies e-mails according to their content. Based on the resulting classification, messages can be delivered to designated recipients, moved to specific folders, sent into quarantine or routed for archival.

No chance anymore?!

Many programs also use individual based Anti-SPAM lists. Once your e-mails have landed in such a personal exclusion list of a receiver, further contact with this addressee will be impossible.♦

By Daniela La Marca

Based on " So werden E-Mails nicht als Spam klassifiziert" by Markus Goss, Vice President Marketing, GROUP Technologies AG, Germany

From Page 1 — Is your Opt-in Process A Turn-Off

This can usually be relegated to a second page, after sign-up has been accomplished up front, via email submission.

When you do create questions, make them relevant to both your audience and your offerings. One of the most common mistakes is that very often, organizations make their opt-in pages marketing research projects. Only ask questions you have a use for in your segmentation strategy. It is also worth trying out the "tiered" opt-in process - that is, setting up over multiple pages.

For example:

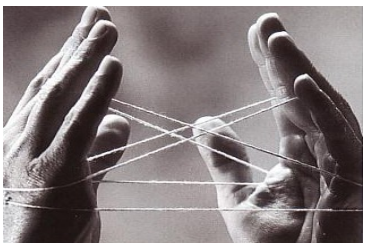
1. Lead with just an email address solicitation on the home page

2. That leads the user to the next page for basic information

3. Further segmentation as necessary

The benefit: you gain your reader's trust, and you reduce his or her anxiety and fear.

In addition, remember to ensure that your opt-in page showcases high-quality graphics and clean design. Doing so adds credibility, elevates reader comfort level, and smoothes the way for continued communication.♦



From Page 1 — Tips for Avoiding Spam

Check out the following methods to prevent spam:

Disguise e-mail addresses posted in a public electronic place: Opt out of member directories that may place your e-mail address online. If your employer places your e-mail address online, ask your webmaster to make sure it is disguised in some way.

Be on guard when filling out online forms requesting your e-mail address: If you don't want to receive e-mail from a website operator, don't give them your e-mail address unless they offer the option of declining to receive e-mail. If you are asked for your e-mail address in an online setting such as a form, make sure you pay attention to any options discussing how the address will be used. Pay attention to check boxes that request the right to send you e-mails or share your e-mail address with partners. Read the privacy policies of websites.

Avoid using short e-mail addresses: They are easy to guess, and may receive more spam.

Use multiple e-mail addresses: When posting to newsgroups or using unfamiliar websites, we recommend creating a particular e-mail address for that specific purpose. An online search for "disposable e-mail addresses" provides you immediately with a list of e-mail providers designed for one-time use e-mails.

Use a filter: Many ISPs and free e-mail services now provide spam filtering. You may also consider simply buying the appropriate software. Although filters are not perfect, they can certainly cut down the amount of spam a user receives.

Pay attention to stripping specific non-essential attachment type files

It's proven that files that end with .bat, .exe, .pif, .scr, .vbs, or .crd often contain worms and viruses.♦

By Daniela La Marca

IS YOUR E-NEWSLETTER BEING DELIVERED AT THE RIGHT TIME?

The options of e-mail programs allows us to recall only in seconds a topical report about the success of transmissions and to measure the success rate with previous actions. Therefore, especially in a detailed examination, it's possible to compare clearly the opening rates, return rates, number of log-ins and log-outs, recommendation rates and responses.

So shouldn't these evaluation opportunities be used for the optimization of further campaigns? Let me show how it helps to determine for instance the optimum dispatch time for your mailing.

There are three aspects that play an important role:

- The opening rate: how many receivers have generally opened the newsletter;
- The click rate: how many receivers have clicked on one or several offers;
- The click presumption: (Click rate x 100) divided by opening rate.

The dispatch time is by no means trivial: whether the readers click rather in the morning or in the evening, on Mondays or during the weekend, depends completely on the target group and on the offer and can influence the success decisively. Besides, opening rates and click rates state quite different things.

So, with an employed target group you will observe high opening rates often in the morning with at the same time low click rates: indeed the mails are opened in the eagerness of work, but the message only glanced at instead of clicked on for further information. On the other hand, in the evening you reach only a few from the same target group at work, but these in general take more time to look through the messages. The result: low opening rates, but high click rates.

A high click chance often arises in the late morning and early afternoon. However, here every company must find out on its own, maybe by tests, which time is the most favorable one. In addition, companies could either change the dispatch time more often, or send them out in groups at different times to improve the effectiveness of the broadcast. In this way, the dispatch time with the highest click rates will be more likely achieved.♦

By Daniela La Marca

GUARANTEE A CLEAR AND EASY WAY TO OPT OUT

Next month, Singapore will most likely enact its Anti-SPAM law. The island-nation is adopting the opt-out regime to fight spam, like Japan, South Korea and Australia. Benchmarking the CAN-SPAM Act, these four countries demand as well "clear and conspicuous" e-mail opt-out mechanisms.

Here are some important notes to bear in mind when planning and sending out your messages via e-mail:

- Don't ask for unnecessary information – it costs only time;
- Don't be meticulous regarding mis-spellings – nobody's perfect;
- Don't require users to log in to your site to unsubscribe - it isn't that important;
- Don't make your reader say it twice when he wants to be removed from your list – the customer is king;
- Handle it in real time, so remove the email address as soon as possible;
- If an error occurs while removing an address, don't just display a cryptic error message - instead send e.g. a friendly message telling how the address can still be removed.
- Send a confirmation notice with a link that invites to re-subscribe.

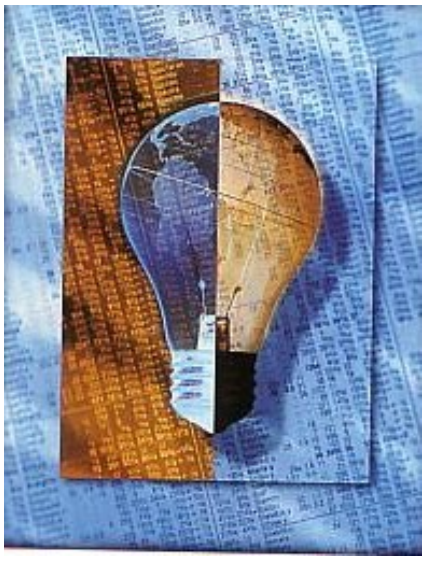
This is useful when someone unsubscribes by accident, or if someone else unsubscribed the person without permission.

The recipient decides what e-mail he accepts and especially how often – and it's his choice!

Of course none of us want to see our circulation lists shrink, but nevertheless the unsubscribe process shouldn't be difficult or tricky for those who want to be removed.♦

By Daniela La Marca

TIP: HOW TO GET GOOD IDEAS FOR MAILINGS



As a person in charge of e-mail broadcasts, you may know the problem: each new mailing activity requires the right touch (ideas, creativity) in order to ensure success. But what happens, if absolutely no ideas cross your mind? Then give the following tips a try– at least once.

In any case, it's important to write down even crazy ideas as every thought may help. Laughing at someone is strictly forbidden!

Brainstorming – several persons of a group give their ideas full scope: Everybody specifies ideas which just occurred to him on the subject. The purpose is to generate as many ideas as possible in a very short time. Take down all results and discuss them more in detail with the team.

Important: this activity shouldn't last longer than 20 minutes and if possible should include, in addition some new and uninvolved people – for fresh ideas.

Aspects game - it can help to look at a problem from a different point of view: Each individual team-member accepts an identity which just occurs to him – a public or fictitious person. Then, the task of the team is to investigate what the imaginary person would expect from the mailing you intend to create. How would you sell e.g. Superman a life assurance or Lee Kuan Yew legal costs insurance?

Industry play – this can open up new perspectives and will boost your ideas: Consider what kind of ideas other industries and enterprises would use for creating and sending out your mailing. What could be considered e.g. by an IT association, an architect or a trader?

Visualization – when brought to paper or presented on a flipchart, a problem often seems easier to manage and solve. So, every team member should illustrate the task from his point-of-view and the others comment.♦

By Daniela La Marca

FOUR APAC COUNTRIES IN TOP SPAM PRODUCING COUNTRIES' LIST

The US continues to lead the pack in network security player Sophos' latest "Dirty Dozen" report, exporting an average of 35.70% of all spam from January to March 2005. Four countries from the Asia Pacific region have also made the list, with South Korea and China taking the 2nd and 3rd places respectively, Japan holding the 7th position and Australia 11th on the list.

However, Graham Cluley, senior security analyst at Sophos notes, "Even though the United States is still responsible for producing more than one-third of the world's total volume of spam, the percentage has decreased by 12% since January, compared to other countries."

He adds, "This trend is likely because many ISPs are enforcing policies to ensure that they do not knowingly provide network services to spammers. Some may speculate that the US CAN-SPAM Act has also helped to thwart spam, but at this point we haven't seen any evidence that would correlate the drop off to the Act – time will tell."

In March, Sophos estimated that more than 50% of the world's spam came from zombie computers, which are PCs that have been compromised by hackers or virus writers, who use them to transmit vast quantities of spam. These spam messages tend to contain a link to a website where the tiny minority who respond can complete a transaction. For example, Cluley says that much of the spam sent from Korea's computers was attributed to innocent PCs, which had been turned into compromised zombies by spammers from other countries such as China, Russia and the US.

♦ *By Shanti Anne Morais*

Position	Country	% of Global Spam
1	United States	35.70%
2	South Korea	24.98%
3	China (incl Hong Kong)	9.71%
4	France	3.19%
5	Spain	2.74%
6	Canada	2.68%
7	Japan	2.10%
8	Brazil	1.95%
9	United Kingdom	1.57%
10	Germany	1.23%
11	Australia	1.22%
12	Poland	1.20%
	Others	11.73%

Table: Top Spam Producing Countries

STUDY: INTEGRATED DIALOG MARKETING IS 2005'S HOT TREND

Integrated dialog marketing in the combination of web, e-mail, print, mobile and call center, presents the most important marketing trend of 2005 according to a survey of experts by the communication agency 21 Torr.

82% of the contacted marketing experts believe that this year especially will see the importance of on-line marketing increasing further. The most important communication instrument for the majority of the interviewees (88%) is their own website as a kind of business card. In addition, the study reveals that:

- about 65% strongly advise online public relations;
- about 50% are convinced that e-mail advertisements make an impact in spite of spam;
- 44% recommend search engine adverts;
- 38% send out e-mail-newsletters;
- only 12% still recommend banner advertising

Interestingly, "The Internet is not everything ", say 81% of the experts.

In fact they recommend a combination of on-line marketing and off-line marketing. For three quarters of the respondents, the connection to distribution channels is especially of high importance. More than two thirds hold the bridging to the product and service world of an enterprise as eminently important.

They all totally agree about the fact that online activities have to be geared strictly to branding and brand management. More than 80% consider the spam problems which are related to online marketing as a difficult challenge. 31% are convinced that e-mail-newsletters are the royal road for overcoming the spam hurdles.

Further marketing trends are:

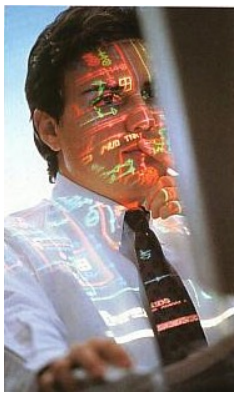
- Integrated direct marketing (57%),
- Pure on-line marketing (44%),
- Mobile marketing (31%),
- Classical direct marketing (18%),
- TV Advertising (13%),
- Classical advertisement (12%),
- Telemarketing (11%) and
- Radio Advertising (8%)

♦ *By Daniela La Marca*

SPAM-FILTER TESTING FLAWED, SAYS META GROUP

Researchers from the META Group (recently acquired by the Gartner Group), have advised IT departments to adopt better-informed criteria when short-listing spam-blocking products and services.

The analysts say many independent information sources such as publications, use limited and flawed methods for testing, categorizing and ranking the effectiveness on anti-spam solutions. Instead of relying on these sources, IT organizations really should base their decisions on tests and criteria that better simulate the real world, say the analysts.



"At root, the issue with many of the most common testing techniques is that they do not simulate real-world conditions or replicate real-time anti-spam abilities," says Matt Cain, senior vice president with META Group's Content & Collaboration Strategies service.

"To put it simply, current testing techniques do not allow organizations to accurately evaluate product capabilities. Invalid testing can, and will, lead to inappropriate vendor selection, an unhappy CIO, and more spam than anticipated," he adds.

In particular, he warns about testing performed on forwarded mail; specifically discrediting evaluations that forward a large quantity of mail to a specific destination for filtering purposes. The reason: Such testing methods ignore the sophistication of header information and IP address manipulation, among other aspects. In addition, these methods also do not allow for real-time message checks, including sender Internet Protocol (IP) validation tests. Also, when using this approach, anti-spam filters cannot glean intelligence from the SMTP transaction – a critical data point for many detection techniques, including traffic-shaping technologies, sender reputation services, and e-mail authentication protocols.

"Spam-filter evaluations based on a mail-forwarding scenario will not provide testers with the information they seek about the accuracy of an anti-spam tool at the workplace," Cain notes. "Equally as ineffective as the forwarding approach are evaluations that focus exclusively on spam capture rates and false-positive generation. Testers must learn to look beyond the easy statistics and measure end-user satisfaction, ease of use, and operational control."

However, META Group analyst stress that a best-practice approach to evaluating e-mails hygiene solutions goes beyond these broader metrics. . They say that smart testers will segment the vendor landscape into three major delivery models (hosted, appliances, and traditional software load) and compare accordingly. They must also recognize that like many technologies, spam-filter products will not provide optimal performance in a plug-and-play situation. Instead, testers need to do the appropriate tuning, thereby enabling recipients to set up blocks and allow lists to attain a more accurate picture of blocking effectiveness.

♦ *By Shanti Anne Morais*

CHINA'S ONLINE SEARCH SERVICES SOARING

An industry report released recently in Xiamen has revealed that China's online search engine market witnessed robust growth last year.

The report released at a meeting on the development of China's search engine industry held in Xiamen City, eastern Fujian Province, showed that the country's online services market hit US$151 million in 2004, rising 81% from the previous year.

The report also predicted that the online searching engine market in China would reach US$278 million this year, and might rocket to US$680 million by 2007.

A total of 50 million Internet users in China used online searching services every day in 2004, and in December there were 188.4 million clicks for online searches.

Huang Chengqing, chairman of the Internet Society of China, said that with the development of information technology and the popularization of computers, online searches have become a major way to access information for Chinese citizens.

Representatives of big name online service companies and investors, including IDG, Yahoo China and IBM, attended the two- day meeting.♦

By Shanti Anne Morais

A total of 50 million Internet users in China used online searching services every day in 2004.

E-MAIL LIFECYCLE MANAGEMENT (ELM) IS BECOMING THE KEY COMPONENT OF ORGANIZATIONS' IT STRATEGY

Creating and managing an automated e-mail business process that simultaneously addresses issues of security and compliance is becoming a key component of almost every organization's IT strategy. This is confirmed by the German GROUP Technologies AG, a leading provider of e-mail lifecycle management.

In Asia, the company recently signed licensing agreements with Singapore Airlines and has convinced several new customers around the globe with their products and concepts.

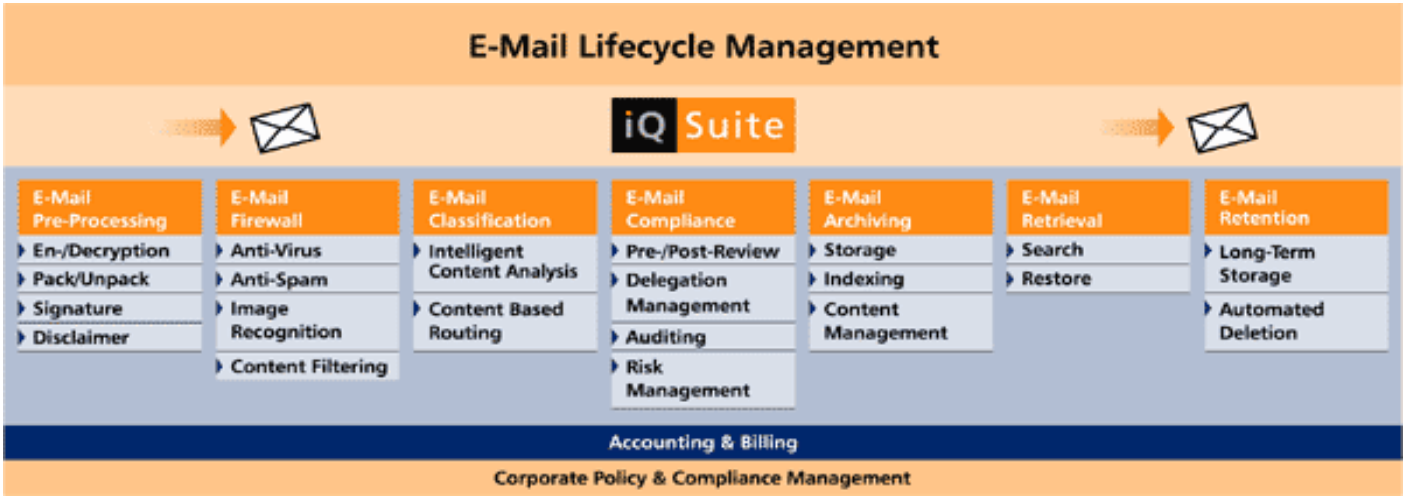
According to them, E-mail Lifecycle Management (ELM) consists of strategies and methods for processing, storing, and managing e-mail, from creation to deletion, in accordance with company-specific business processes and legal regulations. It's essential for companies that want to make e-mail an integrated business process for efficient electronic communication. It includes e-mail encryption, virus and spam protection, automatic e-mail classification, and secure archival. "When it comes to business requirements for e-mail security and organization, an ELM solution is the right choice. ELM centralizes and automates all e-mail-related processes, allowing messages to be managed throughout their entire lifecycle," explains Jürgen Wege, Chairman and CEO of GROUP Technologies.

"The fact that GROUP Technologies can score successes not only in Germany, but also throughout Europe and in the highly competitive US and Asian markets, shows how great the need for a truly integrated e-mail solution really is."

The ELM software platform *iQ.Suite,* developed by GROUP Technologies AG, is a solution for implementing secure and efficient business processes. It provides e-mail administration tools, reporting and statistic function, archiving solutions and compliance systems to the e-mail process. Its concept includes all necessary monitoring and organizational steps as the following graphic shows:

Photo: Juergen Wege

> "When it comes to business requirements for e-mail security and organization, an ELM solution is the right choice."



E-mail Pre-Processing: This step prepares e-mail for additional processing and transmission. Pre-processing ensures that all incoming e-mails are decrypted and unpacked prior to filtering. Outgoing e-mails can be encrypted, packed, signed, and furnished with a disclaimer as required.

E-mail Firewall: Protects against dangerous and undesirable e-mail, and prevents the loss of confidential information. Filtering directly follows pre-processing. In the firewall, e-mail is filtered to remove spam and viruses, as well as prohibited images and text content.

continues on Page 8

The iQ.Suite uses CORE (Content Recognition Engine) technology to filter out spam. CORE analyzes e-mail with maximum accuracy, and prevents the accidental deletion of legitimate e-mail.

E-mail Classification: CORE analyzes, categorizes, and forwards incoming e-mail to the appropriate recipient addresses as needed, depending upon internal company policies. Classification also serves as a basis for additional e-mail processing, e.g. for archiving purposes.

E-mail Compliance: E-mail can be checked for legal compliance and adherence to internal company regulations, and can be blocked prior to delivery if necessary. After it is released, e-mail can then be delivered, placed into quarantine, forwarded to a third party, or deleted.

E-mail Archiving: Filtered e-mails are securely archived. External archiving systems can be seamlessly combined with the iQ.Suite to ensure audit-proof archiving. Archiving precedes delivery, and thus prevents user manipulation (deletion or alteration of e-mail).

E-mail Retrieval: The iQ.Suite automatically supplies the archiving system with important metadata (e-mail headers, processing details, categories) for index generation. E-mail correspondence can be retrieved and restored later through keyword searches.

E-mail Retention: This component provides long-term storage in storage systems and automatic deletion of e-mails after the appropriate time periods.

Considering that more than one third of critical business information is found in e-mails justifies all efforts of protection against corruption, destruction and unauthorized access.♦

By Daniela La Marca

JAPANESE E-MAIL ANTI-ABUSE GROUP ESTABLISHED

Around 30 Japanese companies including the country's major Internet services providers (ISPs) and mobile telecommunications carriers have set up the Japan E-mail Anti-Abuse Group (JEAG) to examine and implement technological countermeasures to fight spam.

According to the Group, Japan is lagging in the race against spam in areas such as research, the implementation of sender authorization and other technologies that stop spam at its source. Prior to the Group's formation, there were only small groups in the country trying to address the problem from a legal aspect and none that were focusing on a comprehensive technological solution that encompasses communications providers, software and hardware makers, and others in the industry.

Through discussion and joint operations, the Group plan a unified approach to counter spam, with the primary objective being the implementation of agreed-upon policies and technologies. Furthermore, JEAG members will share operational experience and expertise in mail systems to further enhance Japan's messaging environment.

Companies involved in the initiative include technology players IBM Japan, NEC Corporation, major Internet service providers such as Yahoo, Japan, Nifty and Softbank BB, as well as Japan's four largest mobile phone service providers.♦

By Shanti Anne Morais

MORE SINGAPOREANS SHOPPING ONLINE

Good news for marketers in Singapore, the Infocomm Development Authority of Singapore's (IDA) annual survey of infocomm usage in households and by individuals has revealed that almost 30% o Singaporeans shopped online in 2004.

This is up 20% from 2003 and is the biggest jump year-on-year since 2000.

Popular online purchases were for tickets (39%), books and magazines (31%) and travel-related items (30%).

Some findings that marketers may find interesting:

	2003	2004
Average number of online purchases made*	2.3	2.8
Average online dollar-spend in*	$336	$539
Usage of government-related transactions	42.2%	55.5%
Online Banking*	32.60%	39.50%
Proportion of total population using Internet	51%	57%

*Internet users aged 15 and above

CONFIDENCE IN THE INTERNET WILL RESULT IN GREATER FAITH IN E-MARKETING

Infocomm technology has been a tremendous gift to many of us, yet, it faces many challenges – key issues being cyber security and fraud. Bearing this in mind, a group of enterprising organizations in Singapore recently joined forces and set up the Internet Industry Association of Singapore (IIAS), a non-profit and independent Association that intends to be the voice of the Internet industry in the island nation.

Officially launched in March 2005, the IIAS will provide counsel and advice on a range of business and market issues, and in addition, aims to enhance access, equity, reliability and growth of the Internet medium here and in the region.

Photo: J. A. Ravindran

J. Anton Ravindran, the founding chairman of IIAS reveals that the idea to form a local Internet-related organization occurred during the visit of Peter Coroneos of the Internet Industry Association of Australia, in September 2004.Representatives from like-minded enterprises in Singapore, including the current founding members, met-up with him and discussed the idea of setting up a similar association here.

Elaborating on what drove the founding of IIAS, Ravindran notes, "Nowadays, it is almost impossible to find any company that operates completely offline in Singapore. However, while infocomm technology continues to evolve and enrich our lives, the Internet industry faces its own set of pressing concerns such as cyber security, open source standards, offensive online content, and frauds, which could inexorably hinder the growth of the industry and encumber consumer confidence. The IIAS aims to be a driving force for those within the industry who seek to address these issues."

In an interview with Asian e-Marketing, Ravindran gives insights into where he thinks e-marketing and e-commerce in Singapore are heading.

What more needs to be done for e-marketing in Singapore, especially to make it more accepted?

To implement e-marketing, its lifecycle should be firstly understood. Companies with an online presence should be enlightened about how to acquire more visitors, increase retention and loyalty, and drive revenue. Whether one is looking to implement a targeted email marketing campaign to promote a web site, or is willing to improve its search engine rankings, the need is to research, develop and execute a strategic Internet marketing plan.

What is your take on Singapore e-marketers especially with regards to the issue of spam?

Appropriate e-mail marketing requires marketers to target their messages and to provide recipients with genuine contact information as well as a genuine opportunity to have their names removed from future mailings. In this respect, the Direct Marketing Association of Singapore (DMAS) has drawn up a set of rules to guide marketers who seek to use the e-mail marketing channel responsibly. This step will solve the problem of spam and will result in better e-marketing.

Do you think the IIAS efforts will help Singapore e-marketers? How?

One of our objectives is to build confidence in using the Internet for both businesses and non-commercial purposes. With this, we are not just dealing with users but also service providers and marketers that utilize the Internet extensively for their business.

The latter group would require education, guidelines and standards in ensuring that they comply with legislations concerning the proper and ethical use of computers and the Internet. e-marketers could face some serious issues, especially when it comes to spam.

What is the IIAS take on spam?

Spam in simple terms is any form of unwanted email. In Singapore, one out of every 3 e-mails received is spam. It is causing more than S$20 million in lost productivity each year.

Many of the activities associated with the more serious forms of spamming are already illegal in Singapore. It is a criminal offence to engage in e-mail fraud or to obstruct the use of a computer through spamming. Sending spam that contains false or misleading advertising or product claims, or that contains pornography is also unlawful.

On the other hand, spamming per se is currently legal in Singapore. To close this gap, the Singapore government is proposing to enact an anti-spam law.

This proposed law will balance the interests of businesses seeking to advertise via e-mails legitimately with the interest of e-mail users, protecting them from being deluged by unwanted e-mail solicitations. It will deter local spammers and clarify the rules for local marketers. It will also give ISPs, who are the main victims of spam, a right of legal recourse against spammers. At the moment, the major ISPs in Singapore already have procedures in place to investigate spam reports and take appropriate action against spammers.

What is the Association doing specifically with regards to the spam problem?

One of the initiatives that the Association will take is to educate the general public in Singapore about the ways and means of fighting spam.

continues on Page 10

PROTECTING CYBERSPACE IS CIPHERTRUST'S NAME OF THE GAME

Asian eMarketing recently caught up with CipherTrust, a leader in messaging security. Trusted by more than 30% of Fortune 100 companies, and with more than 2000 customers worldwide, more than anyone in the same space and in addition, having more enterprise e-mail users than any other solution – over 7.5 million and growing – CipherTrust delivers e-mail security and spam protection.

According to Paul Serrano, CipherTrust's marketing director for the Asia Pacific, the company's IronMail appliance sets the bar for e-mail security solutions. IronMail addresses issues including:

- Spam and fraud (phishing and spoofing) protection
- Virus and malicious code control
- Policy and regulatory compliance enforcement
- E-mail privacy
- E-mail gateway security

The company also has Threat Response Updates (TRU) which leverages the expertise of CipherTrust's e-mail security specialists and data from their network of customers to offer what Serrano refers to as "optimal configurations for IronMail".

Photo: Paul Serrano

CipherTrust currently has seven patents pending in e-mail security and anti-spam technology. Amongst its long list of achievements – the company introduced the first secure e-mail gateway, offered the first e-mail anomaly detection technology, developed the first anti-spam "cocktail", combining multiple anti-spam tools and also created the first anti-spam correlation.

Solely focused on messaging security, Serrano is optimistic that spam will become manageable due to the combination of technology, policy education and policy enforcement.

continues on Page 11

From Page 9—Confidence in the Internet will result in greater faith in e-marketing

We will be holding a Security Conference in the month of June, which will-solely focus on the spam situation in Singapore and the security aspects related to it. Issues related to cyber-security will also be addressed in the seminar.

What activities will the IIAS undertake this year to achieve the objectives of its Security and Anti-piracy Interest Group?

The Security and Anti-piracy Interest Group is spearheaded by our founding members – SurfControl, Microsoft, Genovate and Zara Technology – to reinstate confidence in using the Internet for e-commerce, leisure and non-commercial purposes. The Interest Group is planning for forums and discussion platforms where the exchange of ideas can be facilitated. More details will be available and announced in due course.

The IIAS is also currently working with the Media Development Authority of Singapore (MDA), Parents Advisory Group for the Internet (PAGi) and the NAICCC on addressing the issues relating to undesirable content on the Web and in ensuring that the Internet is secure for consumers and businesses alike.

One of the purposes of the IIAS' Security and Anti-piracy Interest Group is to boost confidence in using the Internet for e-commerce. What is your take on the current e-commerce scenario in Singapore, and how can greater user confidence be built?

With the higher penetration of the Internet in Singapore, and the e-commerce industry on the upsurge, the Singapore Government is studying the feasibility of implementing a National Authentication Infrastructure (NAI), which will enable the government and businesses to offer more secure e-services by leveraging on a common, trusted identification and authentication framework.

The NAI initiative was highlighted during the recent announcement of the Infocomm Security Masterplan. Developed under the guidance of the high-level multi-agency National Infocomm Security Committee, the Infocomm Security Masterplan is a strategic roadmap that charts Singapore's national efforts to build and develop capabilities to prevent cyber security incidents, protect its critical infrastructure from cyber threats and to respond swiftly to recover from actual attacks. The government intends to invest about S$38 million over three years – from 2005-2007 – to implement the plan.

The IIAS offers annual corporate membership to organizations that utilize and actively engage the Internet for the day-to-day running of their businesses. Membership is open to companies from various sectors, with annual fees of S$1,000 and S$500 for small and medium enterprises with 1,000 employees or less.

Founding corporate members of the Association include eBay Singapore, Yahoo! Southeast Asia, Genovate Solutions, Macromedia South Asia, McCorkell & Associates, MediaConnect Asia, Microsoft Singapore, Network for Electronic Transfers Singapore (NETS), SurfControl, Zara Technology and ZUJI.♦

By Shanti Anne Morais

SECURING THE INFOCOMM ENVIRONMENT: A NATIONAL PRIORITY

Singapore is recognized today as a global leader in the adoption and use of infocomm technology. In terms of network readiness, the country was ranked second in the world in 2004, after the United States. It has also recently been short-listed as one of the world's top seven Intelligent Communities by the Intelligent Community Forum.

In Singapore businesses, four out of five companies have adopted some form of infocomm technology and three out of four have Internet access. Moreover, the overall use of electronic commerce has increased steadily over the years, with about half of all companies engaging in some form of online trade.

Given the pervasive use of infocomm technology in Singapore society, the government unveiled a three-year strategic Infocomm Security Masterplan in late February, which will be the backbone of a national effort to maintain a secure infocomm environment for the government, businesses and individuals. It also encompasses the defense of the nation's critical infrastructure from cyber threats such as hacking, virus attacks and cyber terrorism.

To support this initiative, the Singapore government will pump S$38 million over the next three years to build capabilities to manage cyber threats and to enhance cyberspace security.

When coming up with the Masterplan, the government took into account feedback and input given by companies and government agencies through surveys and focus group discussions. One major concern that was voiced out – the country's lack of experienced professionals in infocomm security. As a result of this, businesses have difficulty formulating and complying with IT security policies and best practices as they lack the necessary expertise and experience. Another worry, the general level of poor awareness among employees on the importance of infocomm security and the measures that are required.

"Infocomm security is just as important in protecting Singapore as physical security at our borders. The Infocomm Security Masterplan is a major step forward in the never-ending effort to make cyberspace a safer place for all of us. I encourage the industry, critical infocomm infrastructure owners and operators to participate and support the Masterplan. Everyone needs to play a part in order to achieve our vision for a safe cyberspace for all – one in which e-government, e-commerce and e-society can flourish," notes Deputy Prime Minister, Dr. Tony Tan.

The Infocomm Security Masterplan will augment current capabilities and develop new capabilities in three core areas:

Information protection assurance and risk mitigation measures

This includes risk assessment, vulnerability analysis and reduction, authentication and technology assessment.

Enhanced situational awareness and contingency planning assurance

This includes round-the-clock vigilance and business continuity preparedness.

Human and intellectual capital development

This includes cyber security awareness of Internet users, the development of professional skills and the promotion of research & development in infocomm security.

continues on Page 12

From Page 10—Protecting cyberspace is CipherTrust's name of the game

He also believes that anti-spam legislation is an effective deterrent saying, "Spam legislation criminalizes spam and thus the enforcement of these laws leads to penalties, thereby decreasing the profit model for spammers. With effective anti-spam legislation, it is no longer a lucrative and low-risk activity to send spam." He adds, "While spam may become manageable due to effective deployment of technology such as CipherTrust IronMail, there are always new threats, and IronMail is positioned at the gateway to manage any threats to enterprise messaging systems – now and in the future."

Serrano also has positive views regarding the often panned US Can-Spam Act, noting, "It has been a solid first step.

Firstly, because it drew public attention to messaging security – for example, enabling both the public as well as private individuals to better protect our own piece of cyberspace as per the national strategy to secure cyberspace (a Y2000 US document from the White House). Secondly, the Act has criminalized the act of spamming."

CipherTrust is actively pushing for anti-spam awareness and legislation in this region. Serrano says the company is doing this especially through its research team that provides sanitized messaging security trend data and statistics on current as well as emerging threats to law enforcement agencies and various governments. "This type of information can help legislators make wiser decisions in crafting legislation based on current atmosphere. It also helps to locate the phishers and spammers. In fact, law enforcement and governments have included CipherTrust among their trusted resources for help in these areas," elaborates Serrano.♦

By Shanti Anne Morais

From Page 11—Securing the infocomm environment: A national priority

Initiatives to be rolled out by Singapore's Infocomm Development Authority (iDA) include:

- The National Cyber-threat Monitoring Centre, which will be a central facility for 24 by 7 vigilance and analysis of cyber threats, proactively monitoring and detecting real-time attacks.

- A National Authentication Infrastructure, to develop reliable and robust authentication means to curb identity theft and encourage more secure e-services.

- The National Infocomm Security Awareness Program, where a series of public outreach and awareness campaigns will reach out to educate home users on best computing security practices.

- An Infocomm Vulnerability Study for National Critical Infrastructure, to assess the infocomm protection defenses of critical infrastructures such as finance, energy, water, telecoms, healthcare and transport.

- Business Continuity Readiness Assessment Framework, to measure the effectiveness of business continuity plans of government agencies.

- A Common Criteria Certification Scheme, to build the capability to certify infocomm products in accordance to the Common Criteria, a set of international standards on security.

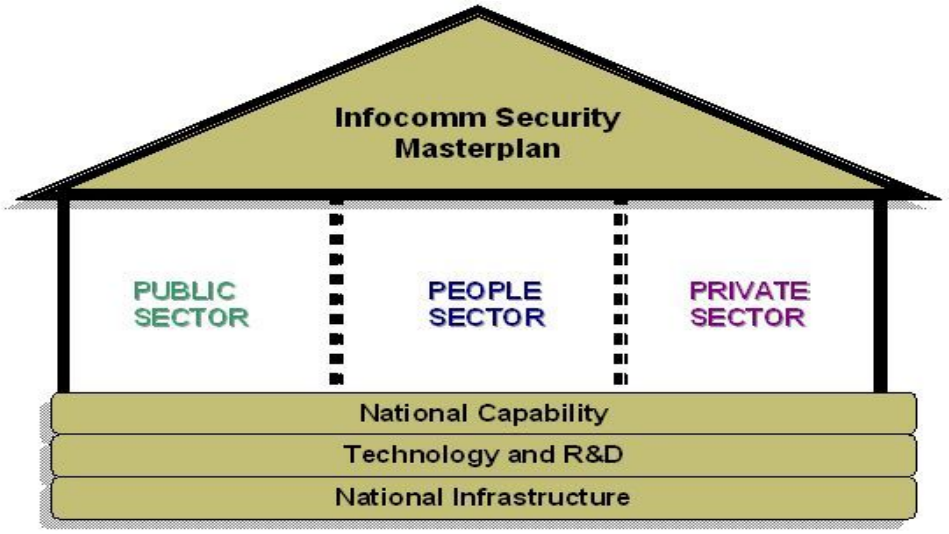
The six critical areas of the framework form the six strategies of the Infocomm Security Masterplan:

- **Securing the People Sector**
- **Securing the Private Sector**
- **Securing the Public Sector**
- **Developing National Capability**
- **Cultivating Technology and R&D**
- **Securing National Infrastructure**

The Masterplan will build on the current best practices in cyber security adopted by the government and businesses for infocomm security. The iDA emphasizes that it is a major step in the journey of enhancing the nation's infocomm security, resilience and preparedness.

As technology evolves and develops, the infocomm environment and the threats that it faces are ever-changing. Hence, it is crucial that the government, businesses and individuals join together in this journey to ensure a secure, well-connected society.♦

By Shanti Anne Morais



Pictorial Representation of the Masterplan Framework

AUSTRALIAN AUTHORITIES SEARCHING FOR SPAM FACTORY

Officers of the Australian Communications Authority (ACA) have raided properties belonging to a Perth company which allegedly sent tens of millions of spam emails. The ACA reacted after receiving reports from members of the public claiming that they had received unsolicited spam messages from the company.

The company, which has yet to be named, is suspected of swamping computers around the country with millions of unsolicited commercial emails, breaking Australia's federal anti-spam legislation.

Besides the company's offices, the home of the company's owner in northern Perth was also raided. The contents of computer hard disks and other equipment were seized by investigators and computer forensics experts. The Federal Magistrates Court has ordered the company and its owner to produce documents and other information about their activities.

Australia's anti-spam legislation came into effect in April 2004, and allows for penalties of up to AU$1.1 million a day for companies who repeatedly break the law.♦ *By Shanti Anne Morais*

A RUNDOWN ON SINGAPORE'S SOON-TO-BE REVEALED ANTI-SPAM LAW

From a minor annoyance, spam has evolved into a significant global economic and social problem. Approximately 60% of global e-mail traffic today is spam, up from 8% in mid-2001. However, more than simply being rude and intrusive, spam is also causing a drain on the global economy, with some industry estimates saying that spam could be costing more than US$20 billion in wasted technical resources.

Singapore too has not been spared from the global scourge of spam. According to the Infocomm Development Authority of Singapore (iDA), one in every 3 e-mails received in the country in 2003 was spam. According to their estimates, e-mail spam is causing Singapore end-users more than S$20 million in lost productivity each year. This excludes losses from businesses, for example ISPs.

More and more individuals and businesses are using e-mail as their core medium of communication. Therefore, if left unchecked, spam may erode consumer confidence in e-mail as a medium of communication and commerce. According to Leong Keng Thai, Deputy Chief Executive & Director-General (Telecoms), iDA, spam may even jeopardize the performance of information networks and the national IT business infrastructure. He likens spam to a piece of litter – "It does not ruin the countryside on its own, but once everybody litters, the land is ruined and the cost for cleanup is high."

In view of all this, it is not surprising that Singapore has declared war against spam with its anti-spam legislation due to be announced sometime in May this year. The proposed law seeks to balance the legitimate interests of businesses seeking to advertise via e-mails and the interests of e-mail users who do not want to be deluged by unwanted e-mails. All-in-all it aims to ensure the responsible use of e-mail. It will clarify the rules for local marketers and deter local spammers. It also aims to give ISPs a right of legal recourse against spammers.

In the run-up to its anti-spam legislation, iDA has spent the past year working closely with key stakeholders to develop an appropriate set of measures to curb e-mail spam in the nation. They include:

- Attorney-General's Chambers of Singapore, in the review of Singapore's legislative options against spam;
- The three major local Internet Service Providers - Pacific Internet, SingNet and StarHub. Together, the three major local ISPs serve almost the entire consumer market in Singapore;
- The Consumer Association of Singapore and the Singapore Business Federation, representing the interests of local consumers and businesses respectively;
- The Direct Marketing Association of Singapore, representing the local direct marketing industry; and

The Singapore infocomm Technology Federation, representing the infocomm industry and the anti-spam solution providers.

Singapore will be using a multi-pronged approach in its fight against spam. These include:

- **Public education and technical measures:**

This involves steps that every user should take to minimize the amount of spam received, for example, by installing spam filters. In addition, public education efforts through seminars, workshops and e-newsletters will be stepped up in order to equip users with the necessary knowledge and tools to fight spam.

- **Industry self-regulation:**

It is important to remember that ISPs as well as legitimate marketers are also victims of spam.

The three major ISPs in Singapore – Pacific Internet, SingNet and StarHub have already implemented a set of anti-spam guidelines. It is interesting to note that Singapore Telecommunications has pointed out that legislation alone will not solve the problem of spam in Singapore. In fact, SingTel is not convinced that legislation is necessary, given that most spam received in Singapore is from offshore sources. The company points out that this leaves limited enforcement opportunities under a legislative regime. It also emphasizes that not all commercial e-mails should be considered spam and certain principles should be borne in mind when classifying what exactly constitutes spam (see other story on Page 14). However, the telco giant is supportive of the government's initiatives to address spam and on its part has urged the government to take a balanced and commercial approach, with a significant emphasis on public education, and the use of technology such as anti-spam software.

In addition, the Direct Marketing Association of Singapore (DMAS) has issued a code of practice to guide marketers on the appropriate use of e-mail for advertising purposes. The code is mandatory for its members. DMAS is also setting up a Consumer Communications Preference Program that will allow e-mail users to register their preference not to receive unsolicited commercial e-mail.

continues on Page 14

From Page 13— A rundown on Singapore's soon-to-be revealed anti-spam law

These initiatives represent the efforts of the e-marketing community to safeguard e-mail as a communication tool and channel.

The e-marketing community in Singapore is certainly waiting with bated breath for the actual announcement and implementation of the country's anti-spam laws. As yet, just as the US Can-Spam Act has proved, there is no silver bullet in the war against spam. With the e-commerce industry in Singapore poised to take-off, it is important that the soon-to-be announced law keeps in mind the interest of genuine e-marketers and safe-guards them too. It is already a great help that the government is most likely to go with the "opt-out regime" as an "opt-in" approach will definitely constrain and hinder the still young e-commerce market here.

SingTel's proposal on what should be incorporated into Singapore's anti-spam legislative framework:

The definition of spam should refer to the bulk sending of "unsolicited e-mails" in "bulk";

If "unsolicited commercial e-mails" are sent in bulk, they will need to contain specified information, and the sender will need to meet minimum standards under an "opt-out" regime. If these minimum standards are not met, the sending of such e-mails should be an offence under the proposed legislation.

An "opt-out" regime is to be preferred to an "opt-in" approach. There should be a valid return e-mail address, instructions for opting-out in English, a functional opt-out mechanism and compliance with opt-out requests within specified time limits;

Commercial e-mails that are sent by Singaporean businesses to existing clients/customers should not be regarded as spam, and should not fall within the prohibition on spam (even if they do not meet requirements of an "opt-out" regime). The legislation should expressly state that such e-mails do not fall within the definition of spam (as they are not "unsolicited");

The Government agency/agencies that are to be responsible for the enforcement of the legislation should be clearly identified. Of course, such agencies should be able to initiate prosecutions against "spammers" who do not comply with the minimum standards (for example, following the investigation of a common complaint);

Consumers and/or recipients of spam and ISPs should also be given the right to commence their own court actions against "spammers" who do not comply with the minimum standards set out in the legislation. ISPs should not be expected to commence action against spammers on behalf of consumers and/or recipients of spam; and

ISPs should be given the right to cease providing services to those spammers (at the sole discretion of the ISP) as well as to recover damages and/or losses suffered due to spam.

The legislative approach should not impose cost or administrative burdens on ISPs. For example, ISPs should not be expected to assume monitoring functions or to police compliance with the legislation.♦

By Shanti Anne Morais

Empowering Asian eMarketing
Asia's Electronic Marketers

TEAM

Editor
Daniela La Marca

Contributing Editor
Shanti Anne Morais

Circulation Manager
Sean Wong

Graphic Designer
Evelyn Valente

Published quarterly by
MediaBUZZ Pte Ltd
60 Havelock Road, Tower A3
10-08 River Place
Singapore 169658

Tel: +65 6836 1607
Tax: +65 6235 1706

email: info@mediabuzz.com.sg
http://www.mediabuzz.com.sg

BUZZWORD: SPF SENDER POLICY FRAMEWORK

In computing, Sender Policy Framework (SPF) - formerly known as Sender Permitted From - is an extension of Simple Mail Transfer Protocol (SMTP), the standard Internet protocol for transmitting email. SPF makes it easier to counter most forged "From" addresses in email, and thus helps to counter e-mail spam. Normal SMTP allows any computer to send email claiming to be from anyone. So, it's easy for spammers to send e-mail from forged addresses. This makes it much more difficult to trace the true source of the e-mail, and makes it easy for spammers to appear to be senders the receiver would ordinarily trust. Many believe that the ability for anyone to forge "From" addresses is a security flaw in SMTP, and SPF is one of a variety of new methods being proposed which restricts this ability.

SPF allows the owner of an Internet domain to use special Domain Name Systems (DNS) records to specify which machines are authorized to transmit e-mail for that domain. For example, we, as the owner of the mediabuzz.com.sg domain can designate which machines are authorized to send email whose email address ends with "@mediabuzz.com.sg". Receivers that implement SPF then treat as suspect any email that claims to come from that domain but fails to come from locations that domain authorizes.

SPF protects the use of the 'reverse-path', or the address that the mail claims to come from at the SMTP level; the address to which bounces would be sent if the mail is not delivered. It does not have any relation to the visible 'From:' header of the email, which can still be forged when SPF is used. Other schemes attempt to prevent forgery of the visible headers.

SPF makes it more difficult for spammers to send spam, because if they simply forge a reverse-path from a domain that implements SPF with a record containing -all, receivers that implement SPF will know to ignore the message. SPF only keeps spammers from forging the domain names given in the reverse-paths of an email. If a spammer legitimately has an account in that domain, or owns the domain, they can still send email; however, doing so makes the spam much easier to trace and prosecute because they

must reveal more about their location. It also makes it easier for service providers to drop support. The disclosure of the spammer's true domains makes it much easier to automatically "blacklist" domains that send spam. Spammers can also use computer attacks (such as viruses) to force authorized computers to send email, or use computer attacks against Internet infrastructure (such as corrupting DNS or attacking BGP to subvert entire address blocks) to take control over other networks. However, such actions are illegal in most countries and are more likely to initiate serious government investigation. Moreover, the legal penalties for performing such attacks are often more severe than those for spamming alone.

Users whose e-mail addresses are being forged as reverse-paths will also find SPF beneficial. Such users typically receive a large mass of error messages (bounces), making it more difficult to use email normally. If these people use SPF to specify their legitimate senders, the number of error messages may be reduced because receivers implementing SPF will know that the message is forged. SPF also has advantages beyond helping identify unwanted email. In particular, if a sender provides SPF information, and the receiver uses it, the receiver has some justification in believing that the email at least came from the domain that it asserts it came from.

If a domain adopts SPF with a record containing -all, the domain thereby prevents anyone with an address in that domain from sending mail through mailing lists or forwarding schemes that don't change the reverse-path to suit SPF's requirements. Some believe that this breakage of SMTP will pressure these systems to be 'upgraded' to meet the new requirements. Until they are, SPF will cause valid mail to be lost.♦

MediaBUZZ Pte Ltd us currently conducting some market research on a solution against spam, developed by a German technology company, and already available in Europe. We would appreciate if you, our valued readers, take two minutes to complete our simple questionnaire.

Please download it here:

http://www.mediabuzz.com.sg/questionnaire.html

By taking part, you stand to win a BMW Z4 Baby Racer

EDITORIAL

Dear Reader,

E-marketing is a unique mix of skills that calls upon a variety of technological components to market businesses electronically. The components are comprised of traditional marketing concepts and the use of analytical tools to measure ROI, effectiveness, and market saturation.

With our quarterly e-InfoSource Asian e-Marketing, we intend to support and empower you to survive in the ever-changing electronic marketing environment.

Nowadays, both email marketers and email recipients are trying to strike a delicate balance. Marketers want their messages to be delivered reliably and to be read, while recipients want their e-mails to arrive in manageable quantities with relevant content. Asian e-Marketing will explain you the "do's" and "don'ts" that promote that balance and keep you up-dated with relevant changes in legislation.

Be informed by reading our article on the "infocomm Security Masterplan" or about "Singapore's soon-to-be revealed anti-spam law". Furthermore we explain e.g. the term "E-Mail Lifecycle Management" and present you with a lot of tips and tricks to improve the effectiveness of your e-marketing campaign.

If you want to make sure that you receive Asian e-Marketing next time as well, please subscribe now by visiting this link: http://www.mediabuzz.com.sg/subscribe.html

I look forward to receiving your feedback at daniela@mediabuzz.com.sg

Best Regards,

Daniela La Marca
Editor, Asian e-Marketing

Focused on the Asia Pacific region, our mission is to provide e-marketers with insights on news, strategies, tactics, trends and results of studies relevant to survive in the ever-changing e-mail environment. Asian e-Marketing is essential to all types of marketers, but its content pays special attention to business-to-business online marketing.

MediaBUZZ Pte Ltd respects the privacy of its readers.

If you no longer want to receive our e-InfoSource Asian e-Marketing follow this link, enter your email address and write unsubscribe into the subject line.

Privacy Policy: http://www.mediabuzz.com.sg/terms.html

Empowering Asian e-Marketing
Asia's Electronic Marketers