OUTBLAZE

Response to OFTA Consultation Paper:

"Proposals to contain the problem of unsolicited electronic messages"

October 2004

Prepared and submitted by Outblaze ltd.
Unit 1106-08, Cyberport 2
100 Cyberport Road
Hong Kong

http://www.outblaze.com

Approved and endorsed by APCAUCE

APCAUCE
Asia Pacific

The Asia Pacific Coalition Against Unsolicited Commercial Email
http://www.apcauce.org
http://apcauce.mail.daum.net

Table of Contents

Introductory note: the "transfer of cost" problem

A fundamental objection to spam is the transfer of messaging cost from marketers to service providers and end-users, and the possibility for abuse this entails. In traditional off-line junk mail, marketers must organize and pay for the distribution of their materials, usually by paying for postage; on the Internet, owing to a design legacy of operation on a trusted network, it is simple for anyone to market products and services for free by spamming very large numbers of users.

Marketers pay nothing to send out email solicitations, other than basic Internet connectivity; however, further downstream, email must be handled, sorted, and stored, which in the case of a high volume of spam substantially raises costs for bandwidth, disk space, and technical support. ISPs must meet these extra costs and therefore charge their users higher fees in order to avoid operational deficits. In the present situation, *end-users are unintentionally paying higher Internet fees so that they can receive spam.*

As long as this unfair transfer of cost from spammer to consumer is possible, there is no such thing as legitimate unsolicited commercial email. Spam is not simply email with pornographic or fraudulent content, as the Direct Marketing Association (DMA) has strongly insisted in discussions in the U.S.; spam includes <u>all</u> *unsolicited* junk mail *regardless* of content, because the operational problems and costs caused by spam of differing contents remain exactly the same.

We therefore believe the best possible solution to the spam problem is to require that commercial email be **solicited**, either directly between a consumer and a marketer, or via an **opt-in** process (in which an end-user explicitly signs up to receive email offers and announcements).

Opt-out (in which end-users are only entitled to send a request for removal from a distribution list once they are already on it) is merely a half-measure. One of the golden rules when receiving spam is to avoid responding to the spam message, because the response can alert (by email or by URL to a purported "unsubscribe" page) the spammer that the email account is "live" and "active". Professional spammers turned the opt-out process into a system to confirm email addresses several years ago, before any country made it a legal requirement to provide opt-out options on each marketing message. More recently, the opt-out mechanism was co-opted by writers of malicious code as a way to spread viruses, trojans, etc. As one of the world's largest email and anti-spam operators, we emphasize that opt-out is not a viable solution to the problem of spam, and we strongly suggest that an opt-in approach be enforced.

NATURE OF THE PROBLEM

15-26

In addition to the problems listed in the consultation paper, we would like to emphasize the increased potential for deceptive practices enabled by spam. For example, "phishing", also known as *carding* or *brand spoofing*, is the sending of emails that appear to come from a legitimate web site (CitiBank, AOL, etc.) in an attempt to obtain personal details such as passwords or credit card information from the message recipient.

Special attention has to be paid to phishing and all forms of identity theft that use spam to trick people into revealing their personal information. This problem is likely to require an international initiative that brings lawmakers, ISPs, online merchants, and credit card providers together, such as www.antiphishing.org.

EXISTING MEASURES AND THEIR EFFECTIVENESS

35-46

While there are several ordinances and laws that may be suitable to target specific categories of spam, including laws on false advertising, fraud, the sale of illegitimate products, etc., none are able to address the spam problem in its entirety, which is often a cocktail of several basic elements. Relying solely on separate existing laws will result in piecemeal solution for those who wish to take legal action against spammers.

It is also important to take a stern approach towards unsolicited email that advertises so-called "legitimate" products and services, such as those coming from otherwise respected companies; the reason, again, is that spam drives up ISP and end-user costs *regardless of content and sender.* Although a marketer advertising newspaper subscriptions or discounted software may be satisfied he is doing nothing wrong, at the email destination the technical problems his/her unsolicited bulk email causes are exactly the same as those caused by bulk email sent by marketers trying to sell objectionable products (e.g., child pornography or pyramid schemes).

Voluntary Codes of Practice (46-52)

Thus far, voluntary efforts have had only minimal impact on combating spam. Such efforts may still be considered worthwhile exercises, but it is clear, as paragraph 52 of the consultation paper states, that **anti-spam measures must be compulsory and backed by punitive provisions in order to have the necessary impact**.

Voluntary efforts must entail serious commitments to provide swift responses to spam complaints, as well as swift removal of verified spammers or hacked/infected systems from the network. A slow response rate makes the problem worse and has been known to attract more spammers, who think they may be able to enjoy a few profitable spam runs before getting kicked off by the ISP.

Paragraph 48 sets out the four preventive measures recommended by the Code; in our opinion these measures are insufficient. We include a caveat that blanket restriction of the use of port 25 requires end-users to use solely their ISP's SMTP server and prevents them from using third-party email servers such as those of their web-hosting provider, office, or alternative ISP. Authenticated mail submission via port 587 is a safe, effective, and standardized alternative to port 25 for allowing the use of third-party mail servers; we therefore encourage the use of port 587 in parallel with port 25 blocking. ISPs should not block port 587 except in circumstances involving clearly insecure servers.

Regarding port 25, we see three possibilities the feasibility of which must be assessed:

1. Access to port 25 restricted by filtering technologies (a potentially expensive approach)
2. Allowing "trusted" users access to port 25 outbound
3. Real-time monitoring of port 25 outbound bandwidth for sudden spikes; disabling of port 25 outbound connectivity for end-user IP numbers that show sudden and abnormally high volumes of port 25 traffic.

The remaining three measures listed in paragraph 48, particularly the prohibition of relay email, are useful but offer an incomplete solution.

> **Open Relays and Proxies**
> Open relays, although still significant sources of spam, are being replaced by open proxies, which are proxy servers that can be tricked into proxying SMTP commands and thus sending email. Open proxies are often truly anonymous in that the ISP at the receiving end of open proxy spam is able to see only the IP address of the proxy, not the IP address of the actual spammer. Furthermore, open proxies are in plentiful enough supply that spammers can rapidly switch between proxies and even distribute their spam runs between several hundred to a few thousand proxies at a time. Note: open proxies are now being supplanted by a growing number of "zombie armies" (please see the discussion section that follows this section).

Paragraph 50 details some possible solutions involving the Real-time Blackhole List. The HKISPA recommended the drawing up of a local list of email servers that are reasonably suspected to have transmitted spam (the M-List), so that ISPs may recognize and handle emails from such servers. We see a number of challenges to this approach:

1. The formation and maintenance of the M-List would seem to require significant global cooperation, because the majority of professional spammers are overseas.

2. The HKISPA recommended that the M-List be operated by a neutral entity such as HKCERT; we feel the idea is good in principle, but the question remains: who will provide the necessary funding, and might that funding be put to better use in other anti-spam programmes?

3. As described in our letter to IBC members dated 3rd of May, 2004, we believe that Hong Kong has a problem with outbound spam as well as inbound spam. According to the Spamhaus Project (www.spamhaus.org) and their Spamhaus Block List (SBL):

   i) Hong Kong was ranked ninth in August among the world's top ten spam producing countries and territories (see www.spamhaus.org)
   ii) There are nine Hong Kong ISPs each hosting at least four or more recognized spammers at the time of writing, including several spammers on the ROKSO list (the 200-strong ROKSO list represents the entities responsible for 90% of global spam)

   (see http://www.spamhaus.org/sbl/isp_list.lasso?country=Hong%20Kong)

   We therefore suggest that HKISPA members should deal with known spammers on their servers in a responsible, comprehensive, and expeditious manner before extending their efforts to initiatives such as the M-List, which may cause additional problems including conflicts of interest.

4. The M-List is a duplication of existing and well-established efforts such as professionally-run block lists like Spamhaus's SBL.

Based on these reasons, we do not believe that a localized spam list will prove effective, or will justify the resources required.

Administrators deploying mail filters of any variety must actively monitor them and be attentive to feedback from their users and any other users adversely affected. This requires the deployment and maintenance of *postmaster* and a*buse* mailboxes at each ISP; these two email addresses have become industry standard "role accounts" as defined in RFC 2142 (http://www.faqs.org/rfcs/rfc2142.html). Administrators actively engaged in the deployment, maintenance, and support of spam filters are also strongly advised to cooperate and coordinate with their peers at other ISPs and network providers. Note: postmaster and abuse accounts should be filtered as little as possible, and mail to them should be handled promptly.

Please refer to RFC 2635 (http://www.faqs.org/rfcs/rfc2635.html) for sets of recommendations on how ISPs can handle inbound and outbound spam on their systems.

Discussion of voluntary measures

A problem of increasing severity is the emergence of "zombie armies" of personal computers infected with viruses and trojans designed to send out spam. These forms of malware effectively turn unsuspecting end-users' personal computers into

spamming machines. The multiple sources of zombie spam present a rapidly changing target that spam filters must recognize quickly and block. Zombies should be a priority for ISPs and any educational initiatives: ISPs must run virus filters on incoming and outgoing mail servers, keep a watch for unusual spamming behaviour, and educate end-users on how to protect their computers and identify malware.

We suggest that ISPs consider free distribution of anti-spam, anti-virus, and anti-spyware software on setup CDs and on their websites, to serve as a second line of defence for spam and malware email that manages to slip past mail filters and into users' mailboxes. ISPs ought also to consider educational pamphlets to advise users on how to use freeware or shareware software and services to keep their PCs safe at little or no extra cost. ISPs should also work with Microsoft and other operating system vendors to facilitate the availability and delivery of regular security updates.

Broadband ISPs ought to consider the necessity of measures such as port 25 blocking and periodic network sweeps to detect and disable open relays, open proxies and infected PCs in real-time. These measures contain and mitigate the problem of vulnerabilities resulting from outdated and/or insecure software running on end-users' PCs and servers, and will help to reduce the sending of spam from their networks.

However, it should be noted that blocking port 25 is an approach of limited efficacy when used on its own, since it restricts end-user options and does not necessarily prevent spam sending. The port 25 block prevents ordinary users' access to third-party hosting providers or mail servers, forcing them to use exclusively their ISP's SMTP server. A workaround to this is to popularize the use of port 587 to send email. Port 587 for outgoing email is a standard that has been in place for over a decade, and is widely supported by several mail servers. Users should be educated on the availability of this port for sending outgoing email, and ISPs and mail server software manufacturers must be encouraged to provide support for port 587 in their mail systems (please also see analysis of paragraphs 46-52).

There is a growing lobby that advocates support for certain new anti-spam techniques and trumpets them as effective remedies against spam. As several sources have routinely pointed out, technical solutions cannot *on their own* be considered sufficiently effective answers to spam.

Some classes of anti-spam solutions seek to change the "recipient pays" email model by instituting "e-postage", "online stamp", or other schemes designed to make senders pay for email they send. We do not recommend voluntary participation in these solutions for the following reasons:

- Lack of scalability. There may be several million transactions per hour of payment transfers between senders and recipients, especially when a third party broker or payment gateway is involved. The largest online payment processing systems operated by companies such as Mastercard and Visa would be unable to keep up with more than a fraction of the potential number of transactions for a "sender pays" system of significant size.

- These systems are vulnerable to "gaming" on the part of spammers, who attempt to fool the recipient system into thinking that it has already accepted payment for the emails received when in fact it has not.

- Poorly suited to the global nature of the Internet and the vast differentials in economic status. For example, a fee of one US dollar for 20 emails per day may sound reasonable in North America, but in Vietnam it would feed a family of four for a whole day.

- Universal implementation of "sender pays" email schemes would in our opinion result in a significant drop in the popularity and appeal of email; since email is expected to be both convenient and inexpensive, we believe such a course of action would be destructive for the medium.

A more popular and more promising set of technical solutions may be found in a wide range of authentication schemes such as SPF (Meng Weng Wong et al), Sender ID (Microsoft), Identified Internet Mail (Cisco), and DomainKeys (Yahoo). Most of these schemes serve the primary function of preventing forgery or spoofing of email, and do not directly target spam. A substantial percentage of spam, however, is sent with forged credentials to hide the origin and sender, which means that sender authentication schemes can serve an anti-spam purpose by making it difficult for spammers to mask their identity or fraudulently assume another identity; sender authentication is also particularly useful in preventing phishing and ID theft. It must be noted that there are still several problems with such schemes, but those interested may find the latest information on the various mailing lists maintained by the Internet Engineering Task Force (IETF), as well as at the IETF meetings that are held regularly around the world.

57 – 67

We are in general agreement with the assessment of OFTA regarding technical tools, users' arrangements, blocking devices, and efforts by ISPs, with the main exception that we would consider somewhat less emphasis on port 25 blocks for reasons stated in the discussion and recommendation section above (see commentary on paragraphs 46-52 and the following discussion).

POSSIBLE SOLUTIONS

Industry cooperation (68 – 70)

We recommend use of the term "block list" rather than the term "blacklist".

It is extremely important to select adequate and professional block lists, and to avoid the increasing number of poorly maintained block lists that have emerged as the substantial market for anti-spam solutions attracts greater numbers of competitors with the lure of easy revenue and market share. Professionally-managed block lists widely used by reputable ISPs, universities, Fortune 500 companies, etc., include

Spamhaus's SBL and XBL, as well as the Mail Abuse Prevention System's RBL (the first such block list).

We do not recommend that ISPs compile a common block list and use it to the exclusion of other block lists; this would represent a needless duplication of existing efforts, without the guarantee of effectiveness and the operational record earned by established block lists.

We emphasize that block lists – especially those run in a competent manner – are not to be considered hostile to ISPs, nor do they gain anything by keeping ISPs blocked. Block lists and ISPs both have one common enemy: spammers. When an ISP is placed on a block list, it is usually to block the spam originating from that ISP's network, and provides an incentive for the ISP to take prompt action.

ISPs should work directly with **responsible** block list operators to receive early warnings about spam on their networks; this will allow a rapid response and the chance to stop spam runs before they are completed.

In our estimate, these initiatives could safely be industry-driven rather than mandatory, since the removal and blocking of spammers has clear economic incentives for service providers.

75

We remain uncertain as to the value of having local ISPs mount the proposed anti-spam campaign. In addition to inbound spam, spammer hosting and outbound spam are significant problems in Hong Kong, although we have yet to see concrete action taken promptly to correct these local issues; this suggests that at least some ISPs are unable or unwilling to deal promptly and effectively with the problem.

Regardless of the agencies responsible, an anti-spam campaign could be extremely effective, particularly if it included a dedicated government website, radio, newspaper, television, and other medium. The campaign should educate users concerning the following categories of information:

- Methods to reduce the amount of spam one receives, such as using long email addresses that incorporate letters and numbers; not posting e-mail addresses online; using different 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, block lists and white lists.

- 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 turning off the preview function on Outlook and other email clients.

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

- ▪ Methods to determine the IP address from which an email was sent, and how to lodge an effective complaint with the sender's ISP.

Despite the technical subject matter, the campaign must not be boring. The primary purpose of the campaign is to get Internet users to notice, understand and observe the messages of the campaign, and it is therefore imperative that it appeal to as many Internet users as possible in order to be effective. 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 (please see Appendix for extracts).

Legislation (79 – 85)

As noted in paragraph 79, a number of countries have introduced or are considering introducing anti-spam legislation. In addition to European Union and Australian opt-in anti-spam laws, a number of other countries are declaring support for such legislation.

Switzerland is considering the matter and Mr. Thomas Grob of Swiss regulator BAKOM presented cogent arguments describing the Swiss rationale for the proposal to introduce opt-in legislation. Mr. Grob's presentation, which may be downloaded at www.oecd.org/dataoecd/34/8/33713634.pdf, details some legal and regulatory aspects of spam blocking. It states that, while access to the internet is guaranteed, there is no similar guarantee for particular Internet services such as SMTP; regulators and governments therefore have little jurisdiction to require companies to accept spam, and the right of companies and ISPs to block spam must be respected.

New Zealand is also preparing an opt-in anti-spam law. Strong support has been expressed by the IT ministry, InternetNZ (which administers the .nz and .cc top level domains and represents New Zealand ISPs), and from the New Zealand Direct Marketing Association. This law is reportedly modeled on the Australian anti-spam law.

The People's Republic of China is moving towards opt-in legislation based on high-level discussions with representatives from the Ministry of Information Industry (MII), the Internet Society of China, and Outblaze, among others. This was substantiated in the presentation by Dr. FU Jingguang of MII at the recent ITU/WSIS thematic meeting on spam in Geneva, Switzerland (download the presentation at www.itu.int/osg/spu/spam/presentations/FU_Session%208.pdf). Dr. FU explained that marketers should be strongly encouraged to adopt an opt-in approach to email

marketing, and advocated exclusion of such methods as email header forgery, breaking into or otherwise abusing servers, etc. These proposals contain a key differentiator from the ineffective American CAN-SPAM law, the similar Korean law, and the proposed Chinese Taipei law, in that they explicitly recommend the opt-in approach rather than the spammer-friendly opt-out approach successfully obtained elsewhere by the Direct Marketing Association (DMA).

Australia and the European Union have already passed opt-in anti-spam laws. We strongly recommend that opt-in legislation be implemented in Hong Kong.

Discussion of issues of a legislative anti-spam approach – opt-in vs. opt-out, compliance costs, etc. (85)

We see a number of problems with the guidelines proposed by the Asia Digital Marketing Association (or ADMA, not affiliated with the DMA; ADMA recommendations were cited in paragraph 11 of the consultation paper). The ADMA states support for permission based marketing, yet the term "permission" is loosely defined and remains a grey area. The ADMA's list of recommendations advocates primarily an opt-out approach, which entails some significant problems. In an opt-out approach, email recipients must bear the burden of unsubscribing from each marketing campaign or email, with the added complication that the "unsubscribe" link mandated in a marketing email is frequently co-opted by spammers into an email verification check, which confirms to spammers whether there is a person actually reading email behind an email address (and thus results in more spam). Additionally, the unsubscribe link can serve to spread malicious code, as explained in this article:

> **Click here to become infected**
> *The Register*, 22 September 2004
>
> Users should be wary of pressing the 'click here to remove' link on spam messages because it serves to confirm to spammers that junk mail messages are being read. Such email addresses can be sold at a premium to other spammers.
>
> That's reason enough to simply delete spam messages, but a junk mail message doing the rounds today provides an even more compelling reason. Selecting the 'click here to remove' link on messages blocked by MessageLabs today triggers an attempt to load malicious code onto potentially vulnerable Windows PC.
>
> (Entire article at www.theregister.co.uk/2004/09/22/opt-out_exploit/)

There is no reason that users should be subjected to such hazards and tedium merely for the convenience and profit of marketers, nor will users put up with opt-out standards once they become more aware of the serious risks involved.

The opt-out approach is deeply flawed. Unless a more restrictive approach is taken, we predict increased probabilities that "permission" will become a standard transferable commodity between email marketing firms, with email addresses traded

by means of "co-registration" or shared mailing lists (i.e., an email address trading system that will result in *more* spam).

When a user grants permission to receive marketing emails, that **permission must be explicit, specific, and non-transferable**. Furthermore, the rapidly growing number of email addresses exacerbates simple typing or transcription errors when entering email addresses into marketing databases; such errors can result in recipients receiving marketing email intended for someone else, and saddle the new recipients with the burden of opting out of such email (with the associated risks). Such a lack of due diligence on the marketers' side and a blanket assumption of permission are harmful from a privacy and data protection standpoint.

Unsolicited bulk email is sometimes considered the Internet's equivalent of cold-calling (which is unsolicited advertising material sent using the postal service, or unsolicited telemarketing). Traditional cold-calling, however, is more acceptable than unsolicited email because the sender must bear the full cost of advertising and transmission, whereas through the email medium the cost is ultimately transferred to recipients (via their ISPs or other service providers).

In a "recipient pays" model such as email, marketers' campaigns are effectively subsidized by an enormous number of unwilling and largely unknowing third parties: the recipients of spam. The adoption of a stringent compulsory code of practice for email marketing should remove such problems.

There is a counter-argument stating that the cost of complying with an opt-in anti-spam law will be unacceptably high for email marketers, and that free enterprise will suffer as a result; many marketers claim that the active promotion of e-commerce as a means to grow the Internet economy must not be fettered by unnecessary restrictions. In our view this is a strong argument in favour of self-regulation, and in favour of a *laissez-faire*, hands-off policy from the government, but we are not optimistic that trusting marketers to regulate their activities will address the spam problem, nor do we see any significant incentive to keep marketers from lapsing into spamming techniques to maximize message exposure.

There is also a strong argument by the email marketing community that the "spam" spam (meaning especially objectionable items such as Nigerian scams, pyramid schemes, ads for virility drugs, etc.) should be suppressed in order to reclaim email marketing as a legitimate, useful method for direct advertising and sales. It is true that in the correct, responsible hands, email is an efficient and cost-effective method of advertising, able to reach the largest number of targets at an extremely low cost. The low cost, however, is currently illusory, since in the present situation recipients are indirectly subsidizing spammers and legitimate marketers both.

An important argument against self-regulation is exemplified by the famous rhetorical question posed by the Roman writer Juvenal: "Sed quis custodiet ipsos custodes?" ("But who will watch the watchmen themselves?" *Satires*, VI.347-8). To be competitive, bulk marketers transmit their message to the maximum number of people

in the most cost-effective way. This competitive approach works in a manner fair to all parties in "sender pays" models such as telemarketing, postal direct mail, etc., but does not apply to the "recipient pays" structure of email, as previously argued.

Methods of self-regulation that would be quite acceptable in direct sales on other channels are therefore not acceptable in today's email medium, because there is no economic incentive to restrict marketers' activities or targets; there are no postage charges, no telephone bills, and no wages to pay to bill-stickers and telephone salespersons.

The costs of compliance with a well-designed opt-in anti-spam law, and the costs of maintaining the integrity and permission levels of an email database are minimal when compared to the real and virtual costs that are unwillingly paid by recipients around the world as a result of unsolicited bulk email.

We stress that marketers must comply with opt-in laws and other aspects of responsible mailing list management, including due diligence and prompt processing of any bounces received in order to remove "stale" email addresses (addresses that have been cancelled by the user or are otherwise deactivated and undeliverable).

We believe such compliance will confer a positive reputation on responsible email marketers who send emails to end-users that have explicitly solicited such communication, and on marketers who respect the resources of ISPs and email operators by not overloading mail servers with deliveries to large numbers of non-existent users. This compliance will also ensure that marketers can concentrate their energies on acquiring and retaining customers who are already interested in their products, rather than trying to broadcast to a huge, mostly uninterested general audience.

In our view, such compliance and reputation would attract *more* legitimate business for marketers, not less, so it would seem a desirable development for all parties.

INTERNATIONAL COOPERATION

86 – 87 and others

The spam situation in Hong Kong must be studied in the context of the larger spam problem faced by ISPs in mainland China, where in recent years numerous spammers have set up operations. Some relevant points concerning this situation were made by Outblaze Postmaster Suresh Ramasubramanian at the China International Antispam Summit 2004 (please see http://www.hserus.net/spam-srs-isc-china revised04.ppt).

ISPs must work together to improve acceptable use policies that prohibit spam, and must build and maintain contacts with other ISPs and email server operators around the world to detect and address spam runs in real-time.   Some suggestions on how this can be accomplished were presented by Outblaze at the recent OECD Antispam Workshop in Pusan (presentation at http://www.oecd.org/dataoecd/7/44/33696482.pdf).

Chiefly, the two primary recommendations are international cooperation among mail administrators and the promotion of facilitating policies.

International cooperation among mail administrators

1. Attend anti-spam conferences for mail systems and anti-spam administrators (APCAUCE, InboxEvent, etc.)

2. Participate in anti-spam mailing lists, such as spam-l@peach.ease.lsoft.com and (for the Asia-pacific region) discuss@apcauce.org

3. Use the INOC-DBA telephone system (www.pch.net/inoc-dba/), a closed voice-over-IP (VOIP) phone system that allows systems, network, and anti-spam administrators direct person-to-person access.

Facilitating policies

4. Have active *postmaster* and *abuse* mailboxes for handling complaints

5. Staff a rapid response "tiger team" to promptly address serious abuse issues (death threats, fraud, Denial of Service attacks, etc.)

In addition to spam origination, one of the major difficulties that ISPs in Hong Kong (and around the world) must face is the abuse of their facilities for the purpose of "spam support services". This includes the hosting of web and DNS servers for domains that are advertised in spam, or the spammer's own servers hosted in another country. Spammers quite commonly send out spam of a thoroughly "international" nature; for example, a particular item of spam may do all the following:

- advertise a domain hosted in China
- load images in the email body off a server hosted in India
- be sent through an open proxy in South Africa
- link to a payment gateway (for end-users who want to purchase the advertised product) that is hosted in the Bahamas

The internationally distributed nature of spam is a problem that requires greater attention to acceptable use and anti-spam policies in order to expedite prompt and decisive action against spammers that abuse an ISP's facilities in any manner, *which may or may not include sending out email through that ISP's servers*.

We recommend inter-ISP cooperation in particular, and, in general, other avenues of international cooperation such as regular exchanges with lawmakers and regulators from around the world. We note:

- Organizations such as the OECD provide excellent venues for such efforts at a macro or global level, but this must not stop ISPs from forming small, *ad hoc* groups, and maintaining well-defined contact mechanisms with each other. ISPs will thus be able to receive and transmit early warning on spam related

issues affecting their networks, and to share ideas on dealing effectively with spam.

- Other possible venues and forums for cooperation are APCAUCE (http://www.apcauce.org) anti-spam tutorials and conferences, organized every six months at cities throughout the Asia-Pacific region. The optimum events are large network operator meetings such as APRICOT (http://www.apricot.net) that are already widely attended by ISP and network administrators from Hong Kong and the rest of the region. These conferences bring together ISPs and network administrators with representatives from block lists, peers from large global ISPs, leading experts in email technology such as mail server authors, and developers of anti-spam technologies such as SPF / Domain Keys etc.

Conclusion

Present measures to limit spam, including the opt-out approach, are ineffective. Fighting spam is no simple task, but we believe we have discussed a number of measures that can significantly limit spam's impact and proliferation. These measures include opt-in standards, prompt removal of spammers and hacked or insecure systems, adoption of authenticated email schemes, unequivocal anti-spam legislation, rapid response times at ISPs, and the diffusion of better email marketing management techniques. Individually, these measures are only partial solutions; vigorous adoption of all these measures, however, will greatly diminish the problems and costs currently generated by the growing tide of spam.

Appendix
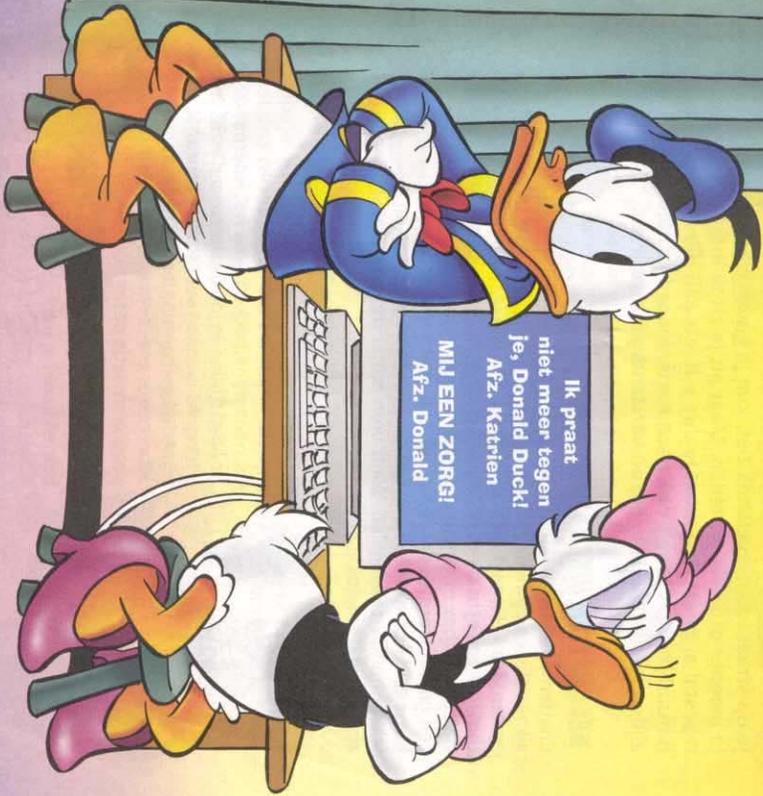
INTERNETREGELS UIT HET HANDBOEK VAN DE JONGE WOUDLOPERS

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 die narigheid doen. En natuurlijk moet je zelf ook geen kattenkwaad uithalen. Op deze bladzijden lees je hoe je veilig en verstandig kunt surfen.

## WEL CHATTEN, NIET KATTEN!

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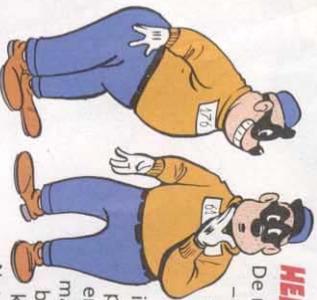
HELP! ZWARE JONGENS!

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

Natuurlijk wil je zelf ook niet voor inbreker worden aangezien. 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 goeie mop of leuke foto naar al je vrienden of vriendinnetjes sturen. Sta er altijd wel even goed bij stil wát je stuurt. Het is bijvoorbeeld kinderachtig om iemand met een vreemde foto of slechte grap voor gek te zetten. Of om nare 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 voor dat je op send of verzenden drukt! Waarschuw altijd direct je ouders als je zelf rare of nare mail krijgt. In ieder geval er nooit op reageren!

KEN IK U?

Net als op straat moet je ook op het internet en bij het chatten vreemden 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 wegklikken dus!

SNIF! MIJN COMPUTER IS ZIEK!

Een computer kan net als jij ziek worden. Meestal komt dat door virussen. Die virussen kunnen overal zitten. Bijvoorbeeld in e-mailtjes 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 tegenhouden. Open in ieder geval nooit mailtjes van mensen die je niet kent. Gelijk deleten, niet openen! Stuur ook geen e-mailtjes door die je niet vertrouwt, want die kunnen de computer van een ander weer besmetten. Zelfs zo erg dat-ie 't helemaal niet meer doet. En daar zou iedereen doodziek van worden!

surf op safe

Verderop...

Ik hou ervan om mensen een plezier te doen! Als juffrouw Katrien haar foto's heeft, dan kan ik de verbinding weer verbreken!

Hé, wat betekent dit? Wat moeten jullie hier?

Wij willen enkel een klein schijfje met een leuk spy-programma erop!

Geen nood! De laatste keer zat ik met Handige Hein de Hacker in de cel!

Zo, dat ding hebben we, maar wat nu? Ik weet niets van computers!

WAAW! Dat ziet er perfect uit! Veel beter dan die illegale programma's die ik zelf schrijf!

Kijk 'ns of je in de bestanden van Dagobert Duck kunt komen, wil je?

Ik ben al binnen! Geld, oliebronnen, aandelen! Zelfs foto's...

Niet te geloven!

Heintje! Ouwe chipsvreter, je moet ons helpen!

HELP! HELP! INBREKERS!

Moet je horen wie het zegt!

Grote griebels! Mijn hele harde schijf is gewist! Die juffrouw Katrien moet een vreselijk *VIRUS* hebben!

NIETS MEER

Zie je dat? Zelfs een zwartwit-foto van die ouwe vrek van die baby!

Geen Flauwekul, Hein! Kijk liever hoeveel geld die vrek heeft!

Makkelijk zat... internetbankieren! Ik zet een kleine overschrijving in zijn administratie! HI! HI!

Ten gunste van de Zware Jongens BV! Geweldig!

En zo...

Wat moeten jullie?

Wat is dat voor een lawaai daar buiten?

Al je contantgeld, ouwe schraper! En we staan volledig in ons recht!

€ 14.321. 456.789. 100.000, enzovoort, 36

Veertien Fantastiljoen en nog wat kleingeld ligt er contant!

En hoe krijgen we dat *MODERN* in handen?

Hier! Ik heb een printje gemaakt van de transactie!

Bedankt, en als jij ooit een *KLUIS* wilt kraken, kom je maar!

Vrachtwagens? De Zware Jongens? Als ze maar weten dat ik ze meteen de politie bel!

Ik hou meer van computers kraken! Ha! Ha!

Klopt! Dus vertel maar op! Wat hebben jullie hier te zoeken, Zware Jongens?

Wat is dat nu weer voor een onzin? Toevallig heb ik de politie al gebeld!