

ISOC-AU Submission on SPAM to NOIE 2 May 2002

Introduction

This submission responds to an invitation dated 10 April for input into an issues paper for consideration at the 2 May round table discussions. These round table discussions are toward investigations into the extent of spam (unsolicited bulk e-mail) problems in Australia and to assess the effectiveness of current counter measures for controlling illegal or inappropriate practices, as requested by the Minister for Communications, Information Technology and the Arts, Senator Richard Alston.

The Internet Society of Australia, ISOC-AU, is a non-profit, user-focused organisation that promotes development of the Internet in Australia to benefit the whole community, including business, academic, professional and individual Internet users.

ISOC-AU is committed to the positive evolution of the Internet. It is the Australian chapter of the worldwide Internet Society, ISOC - the parent body of the Internet Engineering Task Force: a large, open community of network designers, operators, vendors, and researchers which actually creates the protocols and standards that are fundamental to Internet operation. Further information about ISOC-AU is available at <http://www.isoc-au.org.au/>.

Spam or Unsolicited Bulk Email (UBE) is email sent to large numbers of recipients without their explicit prior consent.

Spam is a growing problem, already known in many negative guises to Australian homes and businesses.

Spam is a problematic, retarding, dissuasive and costly influence on email communication.

Careful and informed consideration must be given to mechanisms to prevent Australian spam and strengthen international restrictions to an international problem.

Problems

Spam pushes content, sometimes inappropriate and illegal in nature to recipients. Common email client applications auto-preview email, exposing illegal, adult, and inappropriate content to children. Common spam content subjects include pornography, online gambling, credit offers, online pharmaceuticals, get rich quick schemes, and other generally irrelevant content totally disregarding of the individual, their interests and geographic location. The extent of the problem and the content of some spam may be so upsetting it moves recipients to emotionally charged action and retaliation.

Spam is so problematic and unwanted that spam senders (spammers) resort to fraudulent practices. Knowing full well the negative reactions they cause spammers actively and fraudulently avoid the consequences of their actions, hiding behind faked or uncertain identities.

Spam requires the recipient to at least read the subject, and for unclear subjects, open the email to assess its content. It is not easily deleted or avoided.

The above add to the cost of spam to the recipient, in terms of time, energy and resources. For many individuals Internet access is charged either by time spent online or volume of data received. In either case, spam adds to the cost of receiving email and for accessing unclear and referred online content referred to by spam.

Businesses and Internet Service Providers (ISPs) incur additional costs of unknowingly transmitting and receiving spam, and of having to respond to problems and answer questions resulting from spam. Any Internet provider whose mail server is not correctly secured is also at risk that the server will be used by spammers without authorisation to relay spam around the world. Relaying shifts Internet usage costs from the spammer to innocent third parties whilst hiding the identity of spammers.

The cost for spam senders is relatively insignificant. Access to the Internet to send spam is kept to a minimum through bulk emailing software. Powers of ISPs to terminate accounts upon becoming aware of spam activities result in the extent of financial costs to spammers being limited to the pre-paid or monthly access fees lost.

Costs for spam are shifted from the sender to the recipient. Unlike offline marketing methods, costs are not proportional to the level of advertising and other information transmitted. Natural limits do not exist for spammers. Disincentives in costs and social terms are far outweighed by the returns for spammers. Further, incentives exist to spam more from inversely proportional costs providing economies of scale.

When aggregated, these time, money, energy and social costs are significant.

Email addresses used in spam are obtained from sources generated by the natural and common use of the Internet. Worse yet, many such addresses increase in value when recipients naturally respond to spam to opt-out. Many spammers take advantage of real world social protocols by harvesting opt-out responses and using these now confirmed active email addresses to spam more. Email addresses, sometimes collated in the millions are commonly resold.

The above is a common example of how opt-out actions are used against the intended wishes of the 'spam victim'. Opt-out is inconsistently implemented across the Internet, resulting in little or no trust and reliability by informed and experienced individuals. Those uninformed and inexperienced are simply taken advantage of and are subjected to further spam, as above.

Even if all opt-out requests to a given spammer were received and honoured, spam is now such a widespread phenomenon that the removal of one's address from a single spammer's list will scarcely make a dent in the volume of spam email received. Opt-out is not an acceptable option.

Spam increases the older the email address. This provides disincentive to keep older addresses or maintain permanent online identities. Some undertake the burdensome process of changing email addresses and advising new contact details to associates just to avoid spam. This may be akin to feeling forced to change phone numbers due to nuisance calls.

Learned defenseless and its signature apathy has resulted for some from spam being such a pervasive problem with little sign of improving. It is not uncommon for half the email received by frequent Internet users to be spam, and worse, for this to be accepted as the norm.

Spam has the unknown risk of the problems of responsibility and burden of proof for illegal content received by spam. Content may be automatically saved or cached on the recipient's computer and this may well be illegal in nature.

Spam may pose additional privacy-related risks by including hidden images and links ("web bugs") that spammers use to confirm and track each successful receipt of spam, sometimes down to specific recipients.

Disincentives and problems resulting from spam may become so severe individuals minimise or cease to take advantage of the communication benefits of email, and business may restrict or defer its implementation. The effect of spam constrains how the Internet is used and its growth.

Commentary on Current Controls

Opt-out, as stated above is unacceptable, being inconsistently implemented, unreliable and often worsening the problem. It is common for opt-out requests to be misused with premeditated intent to increase the exposure of spam to those following normal social protocols of opt-out actions and replies to spam. The greatest impact is to the uninformed and inexperienced who are unaware of these fraudulent practices.

Global opt-out systems are not supported or widely used, making them ineffective and compounding their disuse. These systems suffer the same opt-out problems with some global opt-out systems resulting in increased spam to those genuinely requesting to opt-out.

Email spam filters are ineffective. Filters are currently not intelligent enough to accurately deal with the nature, complexity and diversity of communication contained in email. Filters based on ban lists suffer similar problems of complexity and changeability of criteria being filtered on. Even with filters human attention is required to sift through filtered email to ensure important and legitimate email has not been incorrectly filtered or discarded. Filters therefore still present a cost in time, as well as the additional risk of losing important messages. Filters try to stop the problem after it's occurred and their use only masks the extent of the problem and reduces action required to address the true nature of spam.

Proposed Considerations

ISOC-AU proposes the following be considered at 2 May round table discussions:

- An agreed definition spam of spam for the purposes of the round table.

- Legislating against spam with the exception of opt-in. Personal details and email addresses used to send spam must be collected in a manner consistent with privacy law.
- Legislation needs to recognise that the benefactors of Spam are not the senders but those who are selling a product or services. Legislation must be aimed at those deriving a benefit and the discouragement of this as an appropriate marketing technique.
- Restricting content of spam to assume any audience, by not permitting adult other content inappropriate for minors. Such content must be linked from the email requiring an explicit action by the reader to review further content. For example, HTML email should not include or call into email images inappropriate for children.
- To be effective, Australian mechanisms need to be aligned with the growing number of countries implementing legislating to ban and restrict spam activities. Spam is an international problem requiring a coordinated international solution.
- Require legitimate and working opt-out processes providing the ability to opt-out at any time after the user has opted in, with recourse/process if an opt-out request is not effectively handled in a timely manner.
- Discussion on confirmed opt-in (double opt-in), its scalability and appropriateness for certain situations. For example, not all small businesses and communities wishing to take advantage of opt-in mailing lists have the money or resources available to implement confirmed opt-in systems.
- Discussion on spam in other online personal communications beyond email, such as instant messaging, eg. ICQ, MSN Messenger, etc.

The Internet Society of Australia (ISOC-AU) believes Internet communications should be accessible and for the benefit of everyone, hence our slogan "The Internet is for everyone!" Email is the most used Internet application for interpersonal communications. Email is increasingly ubiquitous, is critical for current and future online communications, and vital for Australian homes, businesses and e-government.

This submission was prepared by Galen Townson, ISOC-AU Director, with contributions and guidance by the Board and members of ISOC-AU.

ISOC-AU informed its members of NOIE's invitation to the round table and invited input into this submission. ISOC-AU encouraged additional feedback from its Members to NOIE's Spam Questionnaire and the information available from <http://www.noie.gov.au/Projects/consumer/Spam/>. ISOC-AU welcomes the opportunity to contribute in these round table discussions toward clarifying and resolving the problems of spam and will continue to involve its Members in the process.

This Submission may be treated as public information and distributed by NOIE. It will be published on the ISOC-AU website.

Kate Lance
Executive Director
Internet Society of Australia
