

ANTI-SPAM PLEDGE BY ISPs

1. This Joint Statement is issued by the undersigned ISPs in response to the growing problem of spam in Mauritius and to outline the anti-spam measures we pledge to take.
2. The use of the Internet to send large volumes of unsolicited e-mail to promote products and services has annoyed many Internet users as well as strained the facilities of Internet Service Providers (ISPs) and businesses. Such e-mail, sent without the recipients' prior request or consent, is commonly referred as 'spam'.
3. Spam e-mail on the Internet is a serious and growing worldwide problem, which accounts for a large percentage of e-mail traffic on the Internet. It affects end-users' Internet experience and their productivity as they have to spend more time accessing, downloading, reviewing and discarding unwanted e-mail. It also wastes the time and resources of businesses and ISPs, and imposes substantial operational costs needed to tackle this problem, such as hardware and manpower requirements. The spammer, on the other hand, bears virtually no cost.
4. As providers of Internet access services, ISPs have no control over the types of content being carried in e-mail. Our experience shows that the vast majority of spam e-mail originates from overseas. We acknowledge this problem and wish to provide assistance to our customers to manage the spam problem.
5. Spam e-mail is, by nature, subjective and it is difficult to find a precise definition agreeable to everyone. Nevertheless, a *working definition* of spam e-mail is necessary for us to co-operate and move towards implementing effective anti-spam measures.
6. We acknowledge that our definition is not comprehensive at this stage and does not cover many other forms of unsolicited e-mail that users may also consider as spam e-mail. However, we have identified the two most serious forms of spam to focus our efforts on, namely:
 - a. Unsolicited bulk e-mail sent to e-mail servers (of ISPs and corporations) by guessing the e-mail addresses of recipients, resulting in substantially increased server-loads and handling of error messages. This is often referred to as "dictionary-attack" spam.
 - b. Unsolicited commercial e-mail with
 - i. fake or invalid sender e-mail address;
 - ii. deceptive subject label (or heading) that does not match the content of the e-mail; and/or
 - iii. no or invalid instruction for recipients to opt-out from receiving future email from the sender.
7. We believe that public education efforts need to be targeted not only at the end-users but also at the e-mail marketers. Some less responsible senders of spam e-

mail may not be aware of the adverse effects of their marketing practices. We would thus like to encourage them to adopt responsible e-mail marketing practices. Such forms of e-mail marketing practices should provide recipients with the opportunity to have their names removed from the marketers' mailing list.

8. We will work together in an effort to:
 - Implement clear policies that strongly discourage subscribers from using the ISPs' facilities for sending spam e-mail.
 - Provide clear feedback procedures for subscribers with regards to spam.
 - Co-operate with each other to address subscriber's feedback, for example, tracing the source of the spam e-mail, warning subscribers who send spam mail and taking appropriate actions against such subscribers.
 - Implement certain technical measures to manage the spam problem.
 - Make available to subscribers, information on managing spam, including information on email filtering tools and options.
 - Educate subscribers to raise awareness and enhance a general understanding of the spam problem, and to encourage them to take preventive actions.