maps

Application Note:

Guidelines for proper mailing list management

1737 North First Street
San Jose, CA 95112
www.mail-abuse.com

Table of Contents

Introduction

Mailing lists have a long and venerable history on the Internet. Mailing lists are an excellent vehicle for distributing focused, targeted information to an interested, receptive audience. Consequently, mailing lists have been used successfully as a highly effective direct marketing tool. Unfortunately, mailing lists are also vulnerable to misuse through a variety of means. An all-too-common example is where an individual is forge subscribed to a high number of mailing lists and must take extraordinary measures to be removed. Also, some marketers misuse mailing lists, often through a lack of knowledge about longstanding Internet customs and rules, or because they attempt to apply direct paper mail methodology to the electronic realm.

The guidelines below are intended to assist list administrators in establishing basic list management procedures that should help them avoid the most common pitfalls. Good list management also pays off in other ways such as maintaining a high response rate and reducing costs associated with managing complaints.

MAPS Principles

- All communications must be consensual.
- No one should ever have to unsubscribe from a list they did not intentionally subscribe to.

Internet Fundamentals

Those who desire to establish responsible list management practices must be aware that there are certain fundamentals inherent to the structure of the Internet, and to how the email system functions across the Internet. Among those that are pertinent to these guidelines are the following:

Traffic on the Internet flows by mutual agreement.

This is not a taxpayer-funded highway system. The Internet is a *network of networks*, interconnected in a myriad of ways. Most of the networks that compose the Internet are privately owned. When an entity connects its system to the Internet it immediately becomes dependent on others to see to it that its traffic reaches its destination. Those others in turn have a responsibility to their owners or shareholders to maintain their networks and keep traffic flowing smoothly. This fact gives network and system owners and operators considerable say over the traffic they allow to pass over their networks.

Internet entities are responsible for their own actions.

Traffic flows from one network to another because of such things as *peering agreements*, where two networks agree to carry one another's traffic. The Internet is made up of many interconnected peers; it is not only expected, but necessary that those peers, and all those systems connecting to them, act responsibly. The larger the system, and the more traffic it desires to transit the network, the greater the expectations and responsibilities incumbent upon it.

The recipient subsidizes the cost of delivery.

This is not a postal mail or parcel system, where the sender pays the full cost of delivery. Every email box belongs to an individual, a group, an organization, perhaps a corporation; in any event, its existence is most often paid for by someone besides the sender of a message. This fact gives the recipient considerable say over what will be accepted for delivery, and it is why MAPS emphasizes that *all communications must be consensual*.

Guidelines

The following guidelines are offered as a statement of Internet standards and best current practices for proper mailing list management.

There must be a simple method to terminate a subscription.

Mailing list administrators must provide a simple method for subscribers to terminate their subscriptions, and administrators should provide clear and effective instructions for unsubscribing from a mailing list. Mailings from a list must cease promptly once a subscription is terminated.

There should be alternative methods for terminating a subscription.

Mailing list administrators should make an "out of band" procedure (e.g., an email address to which messages may be sent for further contact via email or telephone) available for those who wish to terminate their mailing list subscriptions but are unable or unwilling to follow standard automated procedures.

Undeliverable addresses must be removed from future mailings.

Mailing list administrators must ensure that the impact of their mailings on the networks and hosts of others is minimized. One of the ways this is accomplished is through pruning invalid or undeliverable addresses.

Mail volume must take recipient systems into account.

List administrators must take steps to ensure that mailings do not overwhelm less robust hosts or networks. For example, if the mailing list has a great number of addresses within a particular domain, the list administrator should contact the administrator for that domain to discuss mail volume issues.

Steps must be taken to prevent use of a mailing list for abusive purposes.

The sad fact is that mailing lists are used by third parties as tools of revenge and malice. Mailing list administrators must take adequate steps to ensure that their lists cannot be used for these purposes. Administrators must maintain a "suppression list" of email addresses from which all subscription requests are rejected. The purpose of the suppression list would be to prevent forged subscription of addresses by unauthorized third parties. Such suppression lists should also give properly authorized domain administrators the option to suppress all mailings to the domains for which they are responsible.

The nature and frequency of mailings should be fully disclosed.

List administrators should make adequate disclosures about the nature of their mailing lists, including the subject matter of the lists and anticipated frequency of messages. A substantive change in the frequency of mailings, or in the size of each message, may constitute a new and separate mailing list requiring a separate subscription.

Unconfirmed Mailing Lists

The following explanations and examples are offered as information regarding mailing lists and confirmation of email addresses to be added to mailing lists.

New subscriber's email addresses must be fully verified before mailings commence.

This is usually accomplished by means of an email message sent to the subscriber's email address to which they must reply, or containing a URL which the subscriber must visit, in order to confirm their desire and permission to have their email address added to the mailing list. However it is implemented, a fundamental requirement of all lists is for full verification of all new subscriptions.

Terms and conditions of address use must be fully disclosed.

Mailing list owners or managers must make adequate disclosures about how subscriber addresses will be used, including whether or not addresses are subject to sale or trade with other parties. Also, conditions of use should be visible and obvious to the potential subscriber. For example, two lines buried deep within a license agreement do not constitute adequate disclosure.

Acquired lists must be used for their original purpose.

Those who are acquiring fully verified mailing lists must examine the terms and conditions under which the addresses were originally compiled and determine that all recipients have in fact confirmed their permission to have their email address added to additional mailing lists of the type that the person acquiring the list intends to operate.

One subscription, one list.

Addresses should not be added to other lists without fully verified consent of the address owner. It should never be assumed that subscribers to a list on one subject want to be added to another list on the same subject, let alone a list on another subject, even if the new list is being operated by the same list owner or manager. A notification about the new mailing list may be appropriate on the existing mailing list, but existing subscribers should never be subscribed automatically to the new list.

Methods of Full Verification

Below are some examples of the many methods by which one can ensure that email addresses are fully verified before they are added to a mailing list.

Please note that there is more then one way to verify email addresses, and MAPS does not endorse any particular method.

Closed Loop Confirmation.

Closed loop confirmation is frequently discussed as a good way to verify email addresses before adding them to a mailing list. Closed loop confirmation (also referred to as "full confirmation", "full verification", and even "double opt-in") refers to the process by which, when a list owner or manager receives a subscription request, they send a confirmation message which requires some affirmative action on the part of the owner of the email address before that email address is added to the mailing list. Confirmations which require the email address owner to take action to remove themselves from a list are opt-out, NOT verified opt-in. While anybody can type any email address into a subscription form, only the true owner of that email address will actually receive email at that email address. Thus, if there is an affirmative reply to the confirming email, the list owner can be certain that the owner of the email address is actually the one who subscribed to their mailing list, and that they truly intended to subscribe for their mailing list.

Closed loop confirmation is not the only way for a mailing list owner to confirm addresses before they are added to their mailing list. In some cases it may be the easiest way for the mailing list owner to perform confirmation, but it is by far not the only solution.

Email Addresses Obtained Via a Webform.

Where email addresses are obtained via a webform, the mailing list owner should create a system to verify those addresses collected. This could include email confirmation, including a specific URL that must be visited by the owner of the email address to unlock the email address and subscribe it to the mailing list. This could also include sending a unique token via email that must be returned by the owner of the email address (such a system must be able to deal with auto-responders and have a way to verify that the returned email does not come from an auto-responder (such as the auto-responder found on most role accounts)).

Email Addresses Obtained Through a Business Transaction or Relationship.

Where addresses are obtained as part of a service or business transaction, the mailing list owner should implement a system to verify those addresses before adding them to the mailing list. This could be done by using the email confirmation technique. It could also be done by contacting the owner of the email address from other information obtained, as long as there are records kept of this confirmation. In the case that a business does sales, and requires an email address to send a confirmation email to before processing the order, as long as it is made clear that the policy is that the email address used to conduct business will be added to their mailing list, and the owner of the email address confirms the order before the address is added to the mailing list, and the business keeps records of these transactions, then the email address is considered to have been confirmed before addition to the mailing list.

Email Addresses Obtained From Another Mailing List.

Where an email address was on a verified mailing list, and the policies and verification for that original mailing list clearly state that by confirming for the original list, the owner of the email address agrees to having their email address given to other list owners or managers, and placed on other mailing lists, then that email address is considered to be confirmed for subsequent mailing lists as well provided those mailings reasonably fall within the parameters disclosed in the original sign-up. If the original mailing list owner or manager has in fact implemented mailing list policies and procedures to include a statement that notifies the owner of an email address that by confirming their email address to be added to the original mailing list they also give consent to the list owner to redistribute their email address to other mailing lists at the list owner's discretion, or the distribution of that email address falls outside the limits of the disclosure, then the owner of the mailing list in question should provide this as proof of verification.

In all cases where a mailing list owner or manager wishes to add email addresses from one list to another, whether the original list is in the list owner's or manager's control, or obtained from a third party, any email addresses on the original list which are not fully confirmed as to the original list must be fully confirmed as to the new list, regardless of any perceived permission granted by the owner of the email address to transfer their email address from one list to another.