Bounce Handling Process, Email Delivery Rejection, and Receiving System Policies

Presented to the Email Deliverability Summit II
September 16, 2003

V1.0
Steve Koenig, VP Client Services, Yesmail
Mark Herrick, Operations Security Director, Road Runner

Bounce Handling Process, Email Delivery Rejection, and Receiving System Policies

This document describes recommendations to email senders and receivers that will enable more efficient operations, greater deliverability, and an improved user experience. These recommendations carry obligations for both senders and receivers. Nevertheless, each sender should adopt the recommendations, regardless of whether adopted by a particular receiver, and vice versa. The recommendations are a result of conversations within a working group of industry participants representing various points of view.

Definitions

List hygiene is used in this context to describe how a sequence of delivery failures to a single address results in the address being removed from the delivery list.

Delivery rejection refers to a returned or bounced email. The more specific an ISP is with error messages (e.g. specific RFC and DSN-compliant codes), the better senders will be able to manage list hygiene. Delivery rejection events may be a subset of, or equivalent to, all types of delivery failure events, depending upon the working definitions used by sending and receiving parties. For example, certain parties may wish to exclude delivery failures that can reasonably be thought to be transient (e.g. mailbox full, ISP capacity issues, or temporary SMTP failures), versus persistent (e.g. recurring over multiple delivery attempts). An agreement upon an explicit definition of delivery rejection represents a further opportunity for the working group to develop industry norms.

Recommendations

1. List Hygiene Policy: senders should mark an address as “dead”, meaning the sender should remove the address from the delivery list and not attempt to deliver to the address until the sender has reason to believe that delivery rejection would not occur, if the following two conditions are both met:

    A. 3 consecutive delivery rejections have occurred; AND
    B. The time between the most recent consecutive delivery rejection and the initial consecutive delivery rejection is greater than fifteen days.

A sender should have the capability to manage delivery rejections differently between ISPs, whether based on previous agreements or explicit requests from these ISPs.

2. Reply Coding Standards: receiving systems should comply with RFC and DSN codes. RFC 821, DSN or RFC 1894 are relevant standards. For example, ISPs can use RFC 550 5.7.1 “Go Away” to indicate that the ISP is intentionally rejecting the delivery of an email that is thought to be in violation of the list hygiene policies indicated herein.

3. Receiving Systems Policies: receiving systems should publish their policies and standards regarding requirements for delivering incoming

email in an easy to find section of their public website, and should apply the policies consistently across legitimate senders.

4. Senders and Receivers Cooperation: senders and receivers should participate in an inter-industry communications facilitation program such as ISIPP's Email Deliverability Database (EDDB) or other such mechanism, to help ensure that they can communicate effectively and in a timely manner when an email delivery problem occurs.

Comments

There are numerous ways to tailor these recommendations to specific needs of senders and receivers. For example, senders and receivers may decide that an email bounced with a RFC 550 5.7.1 code should be immediately "sidelined" and not mailed to, provided the ISP provides a notification of the issue and how many addresses are impacted. In addition, the industry participants may wish to define how the various RFC and DSN codes should be used by ISPs to indicate the cause or intent (if intentional) of the delivery rejection. In general, ISPs should practice consistent, standardized use of specific reply codes and delivery status notifications to indicate that delivery rejection has occurred. For example, a delivery rejection may be defined as a result of any one of the following events:

A. The receipt of a 553 return code from SendMail or a 501 return code from IronPorts. 553 is a SendMail specific SMTP response code whereas 501 is the generic SMTP error code for malformed SMTP requests.
B. If the bounced message contains a Delivery Status Notification that definitively indicates that the delivery failed. DSN is specified by RFC 1894.
C. If the message matches neither case 1 nor 2, then the message is a delivery failure if the subject of the reply contains any of a number of well known subject lines, e.g. "RETURNED MAIL," "MAIL DELIVERY FAILED," etc.

In addition, industry participants may wish to determine whether it is practical and desirable to recommend that senders remove, or recommend their clients remove, "dead" addresses from all mailing lists or simply from the list that resulted in 3 consecutive delivery rejections over 15 days or more (recommendation #1). In general, the working group agreed that the list hygiene policy should apply on a list-by-list basis, due to the demands of practical implementation by senders, although this could be a fruitful subject for further discussion.