

Managing “permission marketing” lists – “a solved problem”

The e-marketing world is full of offers to supply targeted “permission” lists for promotional and marketing messages. Here, an IT professional with long experience in information systems and Internet transactions climbs on his soapbox to explain why you should handle this internally. The task is a “solved problem,” he points out – off-the-shelf software – some of it free – will manage the entire process, automatically. He outlines the standard process for building lists of people who truly choose to receive your e-mail. Public relations practitioners will find knowing the steps valuable, for discussion with Information Technology people and to be able to assure management that your e-mailings will not invite a barrage of unfriendly fire in chat rooms and Usenet groups.

IT IS a long-established practice to buy/sell/rent mailing lists of postal mail addresses for marketing purposes.

What would seem to be the same thing with regard to e-mail addresses is actually an entirely different situation. Virtually every seller of lists of e-mail addresses is a fraudulent operator in one way or another.

- 1) Claims about ‘demographics’ – e.g. ‘pet owners’ are usually fictitious.
- 2) The size of the list is wildly inflated, in terms of possible contacts. Many lists being sold have 75% or more ‘undeliverables’. Some run as high as 90+%.
- 3) Claims that the people have ‘consented’ to receive marketing mails on various subjects are almost universally an out-and-out falsehood.*

If you are going to have any sort of external e-mail lists – those where the mail goes to people outside of the organization – you must totally control the process of how names get onto that list, from the very beginning. One cannot trust a third party to do it for you. You must – yourself – verify that the “actual owner” of any e-mail address that is submitted for inclusion on the list does, in fact, desire to receive the mailings. You must be sure that the e-mail address was not supplied by “someone else” – i.e., a ‘forgery’ – for the purpose of causing you to clutter up the forgery victim’s mailbox.

This ‘verification’ is a simple process, and can be handled on a totally automated basis. It just has to be done with some care. The methodology employed is called **“closed-loop confirmed opt-in.”** It works as follows:

- 1) The ‘initial request’ to be added to the mailing-list comes from “somewhere.” Typical sources are a ‘fill in the blanks’ form on a Web-page, or an e-mailed request.
- 2) Note: You don’t know who generated that ‘request’. It might be the person who owns that e-mail address, or it might not. Thus, **“trust, but verify”** applies.

- 3) Therefore, a brief e-mail is sent to the address that was supplied. The ‘rules’ for this type of message are fairly strict:
- a) It does not contain any advertising/marketing materials.
 - b) If the recipient of the message does not respond, then NO FURTHER mails are sent to that address. They are **not** added to the mailing list.
 - c) The recipient must perform some ‘explicit action’ – usually replying to the message – to confirm that he or she **does** want to be added to the list. This confirmation can be trusted as coming from the mailbox owner, because it is a response to a message sent to that mailbox. (The significant difference between this and the ‘unknown origin’ of the original request, is the entire reason for the process)
 - d) The ‘confirmation request’ message must contain a ‘unique identifier’ that is returned in the confirmation response. This identifier must not be ‘predictable’ or ‘guessable’ from information an outsider might know about the recipient. A simple random number works like a charm. The purpose of this unique identifier or ‘token’, as it is sometimes called, is to prevent a malicious or over-enterprising party from forging the confirmation e-mail as well as the original request.
 - e) The ‘confirmation request’ message should provide whatever information is known about where the original request came from. For example, if it is from a Web-page, one should provide the URL of the Web-page, the date and time that the form was submitted, and the IP address of the machine from which the form was submitted. If the source is an e-mail, providing a copy of the entire e-mail, including all the ‘header’ lines, is indicated. The reason for doing this is that if the request did not originate with the mailbox owner, this provides the owner with the necessary information to start tracking down who is doing the forged subscriptions.
 - f) The more-or-less standard “boilerplate” language for a typical confirmation request message goes like this:

“Someone, possibly you, has submitted this e-mail address for inclusion in the {list name} mailing-list. A short description of this list is provided below, as is the identifying information about where the request came from.

If you DO NOT wish to be on this list, simply DO NOTHING, and we will take no further action.

If you DO wish to be on this list, please reply to this e-mail, including this message in the body, or with the Subject line reading: “Confirm: {unique identifier}”.

We must receive this confirmation within one week of (today’s date). After that point, you will need to start over with a new request.

The purpose of this list is: {one sentence description}

This subscription request, for e-mail address {address}, was made via the Web-page at: <http://www.example.com/form.html> on {date} at {time}. and was submitted from IP address {IPaddress}.”
 - g) One needs ‘smarts’ in the system to silently discard any repeated subscription requests for the same e-mail address within the one-week response period, while there is a ‘confirmation request’ outstanding to that address.

If you operate multiple lists, the process should allow only one request ‘system wide’ to be “outstanding” – i.e. waiting for a response from mailbox owners – at any given time. Duplicate requests for the same list should be silently discarded, as above; while

requests for different lists should be held 'pending' the return of the currently 'outstanding' confirmation request. In this scenario, the confirmation request and reply needs to be able to handle multiple list subscriptions in a single message.

h) FINALLY, when the 'confirmation response' mail is received, then, and ONLY then, is that e-mail address actually added to the mailing list, for actual message sending. This assumes that the 'unique identifier' returned with the confirmation matches the one that was sent to that e-mail address. In the event of a mismatch, or if the time-limit has expired, an 'error' e-mail is sent back, telling them that the subscribe attempt failed, and they need to 'try again'. IF the address is added to the live mailing list, then you send them a 'welcome' e-mail.

i) Be sure to save all the "confirmation response" messages. That way, when someone accuses you of sending 'spam' (unsolicited mass e-mail), you can prove that they did ask for it, and thus it is not 'unsolicited'. This **will happen**; count on it. If the volume of messages on the list is small, people will forget that they signed up for the list. Or perhaps it's a shared e-mail address – husband and wife, for example. She signs up, doesn't tell him. He sees the mail, knows he didn't sign up for it – it must be spam.

OR it's an account at an ISP. The customer who was using that mailbox quits. A different customer is given the same e-mail address. Oops! There's mail incoming that he didn't sign up for. It's obviously spam.

These things are 'no big deal', if you're prepared for 'em.

ALL THIS is a 'solved problem'. Lots of 'off the shelf' software exists that will manage the entire process, entirely automatically – sending the confirmation requests, receiving and processing the responses, and adding them to the actual list.

There's no excuse not to do 'things right'. A lot of this software is free.

For UNIX systems free solutions include MajorDomo, Smartlist, and Mailman. Most of these will work on WindowsNT-based (and successor) platforms too. For IBM mainframes (MVS and cousins), there is LISTSRV. It is likely to be a big-ticket item; price it and compare the advantages.

Lots of other choices are in the market. Picking the right one is a job for the IT people. As is 'making it work the way you require it to'.

Source:

Robert D. Bonomi

*A Network Administrator and Internet Services Consultant,
with 20+ years experience operating mail-systems and e-mail lists.*

Chicago, Illinois

July 1, 2003

* A handful of legitimate marketing lists do exist, where people can sign up specifically to receive marketing information on particular kinds of things. They subscribe to mailings via a Web-page with lots of 'category' choices, where users can add/change/delete their selection of categories at any time. People use these lists when, for example, they are considering purchase of some major expense item, and want to see "what's out there". Once they make a decision, they unsubscribe, because they're no longer interested in such material. The biggest of these operators has a subscriber base in the low-middle six figures. The most popular categories have 'subscriber' counts in the low four figures.