Advice on delivering email to remote services

Advice on delivering email to remote services

Over the past few months, several Janet organisations have experienced problems with delivery of mail to Yahoo and BT addresses (BT's consumer e-mail service is outsourced to Yahoo).

Both the affected organisations and Janet(UK) have contacted BT and Yahoo to try to determine the cause of this. Although the specific reasons why particular sites have been blacklisted by Yahoo are not always clear, it appears that there are a number of common factors that may have been responsible. Addressing these is, in any case, good practice for e-mail services. So ensuring that your mail system is configured according to the following recommendations should reduce the likelihood of causing problems (or being perceived as causing problems), and perhaps being blacklisted, across a wide range of Internet e-mail services.

- All outbound email servers MUST have a valid sensible reverse PTR record set up. This PTR record should ideally point back to the same IP address.
- You should consider scanning outbound email for viruses.
- Consider rate-capping outbound email from servers/departments/sub-domains so that, if an account or system on your network gets infected, is the victim of a successful phishing exploit, or otherwise compromised the damage it can cause will be limited.
- The rate-capping should also be applied to webmail and authenticated email to limit harm if accounts using them are compromised.
- Any site forwarding email off to an external mail service should consider separating internally (on site) generated email from externally forwarded email. (They should both leave the site using a separate originating IP address.)
- Sites forwarding externally received email on to an external mail service should apply a competent spam and virus filter and reject problem email rather than accepting it. They should not just casually accept external email and then pass it on in the hope that the remote service will accept it. For forwarding on, tagging problem email is not an acceptable option.
- If you are forwarding email on to an external service, you should as far as reasonably possible maintain a complete user list of the addresses you forward to, and ONLY forward addresses you know about. This should be kept up to date and if the remote end starts to reject a user for any length of time (i.e., 7 days) the forwarding for that user should be disabled until the problem at the remote end is resolved.
  Do not simply use wildcard domain-based forwarding unless you have specifically arranged that with the remote provider, i.e.,

  BAD:

forward *@alumni.university.ac.uk

GOOD:

forward user1@alumni.university.ac.uk [1]
forward user2@alumni.university.ac.uk [2]
...
forward usern@alumni.university.ac.uk [3]
reject *@alumni.university.ac.uk

- For lists that will deliver to external mailboxes, categorising the lists into two groups may reduce problems:

  Compulsory/must-read/important
  Informational/social/open

  Ideally these should be sent from different servers. Some criteria for the first may be lists that current staff/students MUST be on and cannot opt out of, or perhaps circulars to staff members who need to be kept informed about current events. That may help to reduce the impact on vital communications caused when inexperienced users hit the spam button because they did not immediately recognise the source of an informational email.

- All optional lists should have a simple, readily accessible, and effective method of enabling users to opt out.
- Sites should resist the temptation to adopt aggressive delivery and retry configurations. Hammering a remote email server with 50 simultaneous connections, and retrying failed connections every 60 seconds for hours on end is a sure way of triggering remote anti-spam and virus defences.
- Sites that generate large email shots that may go out to a remote service should ensure they are using an outbound list server that is friendly to the remote service. Some email list programs work by generating a separate email connection for each remote recipient instead of opening a single connection and passing all the recipients through that. For large email postings these should not be allowed to talk to an external service. Such list programs should be pointed at a competent local smart host which should then relay the email on in a responsible fashion.

Links
[1] mailto:user1@alumni.university.ac.uk
[2] mailto:user2@alumni.university.ac.uk
[3] mailto:usern@alumni.university.ac.uk