# Messaging, Malware and Mobile Anti-Abuse Working Group

# M3AAWG Email Forwarding Best Common Practices

**Version 2.0**
Originally Published 2008
Updated March 2014

## I. Executive Summary

This M3AAWG best practices document presents measures that can be adopted by email volume forwarders and the receivers of forwarded email. These practices are projected to ease interaction between the above two parties and help ensure that email is delivered while avoiding issues resulting from the forwarding of spam and abusive mail.

## II. Forwarding Email

The following practices are designed to reduce misdirected blocks by helping identify forwarded email and the service it passes through.

### A. Dedicated IP Space

- Forwarders should separate servers by function so that no one server performs both sending and forwarding tasks. Configuring servers in this fashion will greatly aid in resolving any delivery issues that may arise.

### B. Clear DNS Format

- Clearly identify any IPs responsible for forwarding in the rDNS for that IP. By doing this, it becomes possible for receivers to treat those servers with appropriate policies and sending limits without having to guess.

### C. Resent From Header

- Make use of the <Resent-From> header[1] in all forwarded messages. This will allow receivers to apply policies based on where email is being routed through.

### D. Filtering

- All forwarded traffic should have some level of spam filtering by default. Opt-out can be an option but at least the most rudimentary filtering should be enabled.

### E. Tagging

- Tagging allows all email to pass through while forwarded spam is identified for the receiver to filter. The tag is placed in the header of the email. Tagging should be used with some level of filtering.

### F. Avoid wildcard forwarding

- Wildcard forwarding is the forwarding of all possible email addresses in a domain to a single destination email address; i.e., *@example.org is forwarded to example@example.com. This practice is not recommended, as mail to even nonexistent recipients on a domain - such as spam sent using a dictionary attack trying random names from a-z at a domain - will be delivered. Also, wildcard forwarding will cause the amount of forwarded spam to increase to very high levels and risks causing serious IP reputation problems for the forwarder at recipient ISPs.

### G. Avoid breaking existing DKIM signatures[2]

- Existing message headers of an incoming DKIM (DomainKeys Identified Mail) signed email that is to be forwarded should not be modified; i.e., edited, removed, order shuffled. The message recipient - if expanded from a user directory like LDAP (Lightweight Directory Access Protocol) – should not be inserted into a modified To: or Cc: header.

- The message body (including MIME boundaries) should remain unmodified as well. This includes antivirus/anti-spam scanning routines inserting or removing content from the message.

## III. Receiving Forwarded Emails

The following practices help receivers identify forwarded email and deliver the email to its intended recipient.

### A. Postmaster Page for Forwarders

- Provide criteria a forwarder should know through a public postmaster page that speaks to which policies the receiver is enforcing.

### B. Feedback using DMARC reports[3]

- IP-based feedback loop reports are of limited utility because a forwarding mailbox provider is not the originator of the spam and will not be able to suspend the spammer's account. At the most, forwarding email service providers will be able to tune their filters to block spam based on feedback loop reports. It is recommended that feedback, where possible, primarily be provided based on the originating email provider, using the provider's published DMARC (Domain-based Message Authentication, Reporting & Conformance) policies where available.

### C. Recognize Forwarders IP Space and rDNS

- Acknowledge IP space that is designated for forwarding. Apply anti-abuse policies relevant to forwarding services such as a higher blocking threshold and enhanced feedback loop reporting.

## IV. Conclusion

Forwarding is quite popular among users who have multiple email accounts that they prefer to manage centrally. University alumni, members of professional organizations and others often have an address that they wish to retain across changes of email address due to job changes, moving to a new ISP or other reasons.

However, email forwarding is a significant challenge to support. Because forwarded accounts tend to pass on all inbound spam that is missed by the accounts' spam filters, they are causing significant IP reputation damage and false positive issues when legitimate forwarded mail ends up getting blocked along with forwarded spam.

The best practice measures described above are a selection of those that have been found, in practice, to mitigate spam related concerns specific to forwarding email addresses.

## V. References

[1] See Internet Message Format**,** RFC 5322 Section 3.6.6, http://tools.ietf.org/html/rfc5322#section-3.6.6

[2] See DomainKeys Identified Mail (DKIM), http://dkim.org/

[3] The IETF DMARC working group is active in characterizing forwarding behavior that can lead to breaking DKIM. More information can be found at http://datatracker.ietf.org/wg/dmarc/charter

## VI. Authors

Todd Herr
Jay Opperman
Suresh Ramasubramanian
Jordan Rosenwald
Severin Walker
Terry Zink


M³AAWG0092