
Expansion and Clarification of the BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators

A publication of the Messaging Anti-Abuse Working Group¹

Background

ISPs and network operators have an important role in the fight against spam.

Given this important role, ISPs, network operators, technical groups and alliances continue to share best practices for preventing/diminishing spam sent from or across their networks.

Although best practices will not, in and of themselves, constitute a comprehensive solution to spam, they are part of a multi-prong strategy for addressing the problem of spam. The larger the number of entities endorsing and applying common practices, the more effective they will be.

In the event that these voluntary Best Practices are taken up by ISPs and Network Operators, their positive impact will be increased if end-users also take necessary steps to protect the security of their computers, software and networks, including the protection of their personal identity on-line.

—BIAC and MAAWG Best Practices for ISPs and Network Operators

Most entities that engage in online activities come in contact with the all-too-familiar messaging abuses commonly referred to as “spam,” “spim,” “hacking,” “phishing,” “pharming,” etcetera. The Messaging Anti-Abuse Working Group (MAAWG) was created to attract the participation of Internet Service Providers (ISPs), Email Service Providers (ESPs), email system managers, device managers and other interested parties towards developing universal policies and procedures to address network abuse.

Messaging abuse is a global problem that costs the industry billions of dollars each year, and therefore it is necessary for industry professionals to unite and collaborate to fight this increasing economic and social burden.

Intent

BIAC and MAAWG Best Practices for ISPs and Network Operators are a set of voluntary principles developed by business aimed at enhancing the security of network infrastructures in the fight against Spam. Industry will continue to collaborate on additional technical and procedural measures to further implement these principles.

BIAC and MAAWG propose the following Best Practices for ISPs and Network Operators as an important tool in combating Spam. These Best Practices and any additional measures are voluntary, and in all cases precedence is given to applicable legal and regulatory frameworks.

¹ The text in aqua boxes is reproduced from the *OECD Anti-Spam Toolkit, Annex II - BIAC-MAAWG Best Practices for Internet Service Providers and Network Operators* (<http://www.oecd-antispam.org/>)

Implementation of these Best Practices and any additional measures will vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. We note that flexibility in the implementation of these Best Practices and any additional measures is the key to achieving their broad and meaningful adoption by service providers of all sizes.

Given the rapid pace of technological change, the Best Practices will be reviewed and updated as necessary.

MAAWG recognizes that an important part of this challenge is to develop and communicate a set of voluntary Best Practices, drawn from the long experience and expertise of the MAAWG membership. MAAWG will continue to expand upon the voluntary principles outlined in the Best Practices developed in conjunction with BIAC, and will describe the technical and procedural measures that MAAWG members have developed to further implement these principles.

BIAC and MAAWG Recommendations

In any given national jurisdiction, each of the Best Practices is understood to be recommended only if it is not in contradiction with existing national legislation.

In the context of these Best Practices “ISPs and network operators” include any entity operating a SMTP server connected to the Internet.

1. Within the boundaries of the appropriate legal framework, ISPs and network operators address the problem of compromised end-user equipment by establishing timely processes to allow such end-user equipment and network elements to be managed and eliminated as sources of Spam;

MAAWG recommends the careful management of port 25 as one of the main measures leading to the elimination of spam emitted by compromised end-user equipment. This is documented in “Managing Port 25 for Residential or Dynamic IP Space,” at <http://www.maawg.org/port25>.

There are three aspects of this problem: infection of end-user equipment, neutralization of spam flow, and finally disinfection of that same equipment. Port 25 management is an effective remedy only for the second goal, of neutralizing or reducing spam and other abusive activity. The best overall course of action, obviously, is to avoid infection in the first place – which requires citizen and customer education.

2. ISPs and network operators utilize industry standard technology to authenticate their email and/or their sources;

It is the sure belief of many MAAWG members and other industry experts that email sender authentication is the most important next step toward regaining control over the messaging infrastructure. Much effort has gone into defining authentication technologies over the past few years, and two leading standards have emerged.

The first of these to be tested widely was the SenderID Framework. Information on the implementation of – along with its predecessor, SPF – can be found at:

<http://www.microsoft.com/mscorp/safety/technologies/senderid/default.msp>

A companion document regarding DomainKeys and its successor, DomainKeys Identified Mail (DKIM), has recently been approved as a standard by the IETF (rfc4871), <http://www.ietf.org/rfc/rfc4871.txt>.

3. ISPs and network operators block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be attained from the customer;

The concept of self protecting one's infrastructure for the safeguard of customer service is illustrated by Principle 3 of the MAAWG "Code of Conduct for Messaging System Operators," available at: <http://www.maawg.org/about/CodeofConduct.pdf>.

4. ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately;

Entities from which abuse originates should take reasonable action to address the abuse within a reasonable time. This might include solutions that restrict users from using any other messaging server except for the one provided by the service provider (described further in recommendation #8 below), limiting the number of messages a particular user can send in a period of time, or scanning the messages for spam or viruses before they are sent to the receiving network (described further in recommendation #3 above.)

Some methods to further limit abuse include:

- SMTP user authentication (described further in recommendation #8 below)
- Restricting or otherwise controlling access to port 25, described in the MAAWG publication "Managing Port 25 for Residential or Dynamic IP Space," at <http://www.maawg.org/port25/>
- Limiting high outbound mail volumes
- Performing outbound virus scanning
- Using inbound virus filters for outbound mail (described further in recommendation #3 above.)

This list is not exhaustive and other solutions may be available to manage abuse originating from a network. Additionally, these solutions may not be suitable for all environments.

Principle 2 of the MAAWG "Code of Conduct for Messaging System Operators" addresses the problem of abuse patterns in regard to the relationships with customers and with peer operators. It is available at <http://www.maawg.org/about/CodeofConduct.pdf>.

5. ISPs and network operators establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints.

Good communications between messaging operators can have the result of better practices being adopted and implemented, and a better end user experience.

Operators should make reasonable accommodations for the exchange of information for the purpose of identifying and resolving abuse issues and minimizing user impact. Understandably, the victimized operators should take reasonable precautions to protect its assets and the security and privacy of its users. Proven communication mechanisms include:

- Functional abuse@ and postmaster@ email addresses (as documented by rfc2142), following procedures described under recommendation #1 above
- Feedback loops (sending and receiving)
- Feedback loop implementers will most likely wish to use the draft standard Abuse Reporting Format, <http://mipassoc.org/arf/>
- Published escalation procedures on a publicly available company website

- Transparent error and bounce messaging to indicate the disposition of an email message
- Participation in communication forums such as industry mailing lists and other collaborative venues, including MAAWG events. Join the conversation!

MAAWG members participate in a multi-role contact database, designed to facilitate timely communication between members.

Communication between messaging operators is also addressed by Principle 4 of the MAAWG “Code of Conduct for Messaging System Operators.” It is available at: <http://www.maawg.org/about/CodeofConduct.pdf>.

6. ISPs, network operators and enterprise email providers communicate their security policies and procedures to their subscribers;

Online entities that give other entities access to their network messaging resources should clearly state, make available and enforce their policies concerning the use of those resources. The policy should also state the consequences that will occur if said policy is violated.

This is clearly illustrated by Principle 1 of the MAAWG “Code of Conduct for Messaging System Operators,” available at: <http://www.maawg.org/about/CodeofConduct.pdf>.

7. ISPs and network operators attempt to send non-delivery notices (NDNs) only for messages originated by their own account holders;

A literal interpretation of this best practice might induce the cessation of all non-delivery notices, which is not recommended because these are a useful and expected function of email systems. The objective of this best practice is instead to avoid the sending of NDNs to forged addresses, which can create a substantial share of unwanted email traffic.

MAAWG therefore prefers the following alternative wording:

In order to avoid sending non-delivery notices (NDNs) to forged addresses, ISPs and network operators should configure their gateway mail servers to immediately reject undeliverable email, rather than accepting it and generating NDNs later;

Rejection of undeliverable email by the gateway mail will simply provide equivalent information to the sending mail server, which can apply local policy regarding whether or not to notify the message sender.

- 8. ISPs and network operators take measures to ensure that only their account holders use their email submit servers;**
- 9. ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;**
- 10. ISPs and network operators ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries; that all local area network (LAN) operators are compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets," and that in particular, LANs do not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.**