



MAAWG Sender Best Communications Practices - Version 1.1

(Subject to Revision)

Introduction:

In an effort to facilitate MAAWG's mission of reducing messaging abuse, the MAAWG Senders Subcommittee offers these best communications practices for high volume SMTP-based email senders¹. The goal of these practices is to enhance the transparency of legitimate messages and enable receiving operators to maximize their resources in the fight against messaging abuse.

In addition to the principles stated below, communications practices for email interchange must begin with a baseline of regulatory compliance requirements inherent within the industry's acceptable use policies and regional government's regulations². Senders must adhere to these requirements to avoid possible industry and law enforcement actions. In addition, senders should consider joining and adhering to relevant self-regulatory initiatives such as those prescribed by industry trade associations and email accreditation providers.

While this document outlines industry Best Communications Practices, it is also understood that not all receiving networks and senders will implement all of these practices due to the complexity of the network infrastructures, public policy considerations and the scalability of network platforms.

I. Obtain Clear and Conspicuous Consent

- a. In establishing consent, senders should provide clear and conspicuous notice to users at the point of email address collection, so that reasonable users can easily and readily understand exactly to what they are consenting upon providing their email address, and make that consent notice obvious and readily available for online reference at any time by any party.
- b. The notice should clearly state the specific type of list(s) in which users are subscribing and consider noting the potential frequency of communications. If email addresses are to be used for secondary purposes, then that purpose should also be disclosed as part of the consent process.
 - i. Whenever a sender collects an email address, it should follow up with a message sent to that address in order to determine the validity³ of the supplied address as well as address within the content of the message the recipient's granting of consent to receive messages from the sender.

¹ This does not refer to person-to-person traffic initiated by ISP's.

² See Appendix.

³ Validity can be determined by identifying email address syntax errors, domain errors, and message-attempt errors.

1. Confirmation messages should be sent using a dedicated IP address.
 2. Confirmation messages should be sent from the same 'From' address as other messaging.
- c. Senders are encouraged to work with industry partners to develop trusted subscription mechanisms which may more easily verify user consent.

II. Enable Clear, Conspicuous, and Easy to Use Unsubscription Options

- a. Senders should make the unsubscription process as clear and easy to use as reasonably possible.
- b. Senders should process unsubscription requests as quickly as reasonably possible and with the recipient in mind. Senders are reminded that unsubscription requests may be regulated and subject to laws of varying jurisdictions..
- c. Senders are encouraged to set expectations during the unsubscribe process as to the specific time-frame in which a sender may process that unsubscribe request and from what list(s) the user has unsubscribed from.
- d. Senders should adopt the List-Unsubscribe mechanism within the header of each message as described in [RFC 2369](#).
- e. Senders should use text descriptions (instead of images) to accompany hyperlinks to a one-click online unsubscribe web page.
 - i. Senders should be able to process an email-based unsubscribe request. Senders should also consider making offline unsubscribe mechanisms available. The 'From' or 'Reply-to' email address should also be able to receive unsubscribe requests, unless otherwise indicated.
 - ii. When new subscribers are presented with hyperlinked online subscription preference centers with multiple subscription options, the specific list-unsubscribe option should be pre-checked by default for those lists in which users are subscribed. When a provider makes new subscription offers available, returning subscribers should be presented with these selections unsubscribed by default.
- f. Senders that receive a recipient abuse-related complaint should:
 - i. Immediately honor any and all abuse-related complaint received regarding an email list subscription as if it were an unsubscribe request.
 - ii. Accept abuse-related complaints at role account email addresses including `abuse@sender-domain` and `postmaster@sender-domain` as well as monitor complaints sent to the WHOIS or other domain directory service contact email address for that particular sending domain name.
 - iii. Monitor and minimize the amount of abuse-related complaints received as they could result in a violation of a senders' outbound or receivers inbound Internet or Email Access Provider acceptable use policy.
- g. Senders are encouraged to work in conjunction with industry participants to develop trusted unsubscribe mechanisms which may more easily facilitate subscriber choice.
- h. Senders should identify the recipient email address in the message body in order to remind recipients as to which email address they are subscribed.

III. Enhancing Sender Accountability and Messaging Reputation

- a. Senders should be aware of and adhere to inbound messaging acceptable use policies (AUP's) of each Internet or Email Access Provider, where available, to which messages are sent. Senders should also be aware of, and comply with, the usage policies of their own sending Internet access providers, IP services partner, and domain name registrars.
- b. Senders should adopt email authentication for all types of messaging, such as through path-based and cryptographic methodologies.⁴
 - i. Senders should consider utilizing varying authentication mechanisms and identifiers based on various types of messaging.
 - ii. Senders should also recognize that email authentication does not secure the transport of messaging, so senders with private content are encouraged to adopt secure messaging technologies in conjunction with email authentication methodologies to ensure the protection and integrity of messaging content.
- c. Senders should adopt these messaging identification practices:
 - i. Ensure accuracy and accountability for outbound messaging domain name record identification within the WHOIS database.
 - ii. Ensure that reverse domain name system (rDNS) records are established for outbound and inbound messaging domains.
 - iii. Dedicate and maintain consistency with outbound Internet Protocol (IP) address(es) per sender and with their corresponding domain names, i.e.: forward and reverse DNS should match.
 - iv. Senders should use consistent domain names for each (but not necessarily across) HELO/EHLO, rDNS, MAIL-FROM and body 'From' for each campaign or list consistently, and not use different domain names for the same campaign.
 - v. Ensure the HELO/EHLO presented by the SMTP client is the valid fully-qualified domain name (FQDN) of the sending host, rather than a literal IP address.
 1. This hostname should also resolve a DNS address resource-record-set used by the host.
 2. The HELO/EHLO should match the reverse DNS of the sending IP even if it is from an IP address shared between multiple campaigns and/or domains. In environments where multiple email servers are behind a router, the HELO/EHLOs of each server should be in the same domain.
 - vi. The three components of the RFC 822/RFC 2822 'From' mailbox address(es) (display-name, local part, and domain) should all be equally identifiable and accountable and should be consonant with each other. That is, a human reader of all three values should be able to interpret them as referring to the same organization or entity, and the addresses should be appropriate to the content of the message.
 - vii. In cases of multiple senders on a shared IP network, messaging administrators should ensure:

⁴ Path-based methodologies include the Sender Policy Framework (SPF) and Sender-ID, and cryptographic methodologies include DomainKeys Identified Mail (DKIM).

1. Common identification of shared email server-level domain names identifying the messaging provider with an option to include identification of the sender in conjunction with the messaging provider.
 2. If messaging provider uses its own domain name for visible and/or envelope identification, then it is also encouraged to allocate a sender-level subdomain in conjunction with that messaging provider's domain, such as news@sender-domain.messaging-provider.com or provide a sub-domain for the HELO/EHLO and rDNS which will identify the sender.
 3. Consistency and similarity of outbound IP addresses for senders, such as being within the same /24 IP range.
 4. Dedication of IP ranges for certain types of senders and/or content, such as differentiation of transactional messaging from commercial messaging or content that is highly likely to fall under corporate policy restrictions.
- viii. Messaging domains should reference the sender's website.
- d. Sender content should be transparent and accountable by following these principles:
- i. When requesting users to add a sender's 'From' address to a recipients' addressbook, senders should point out to recipients that an entry in the addressbook does not ensure message receipt, but rather, may improve the likelihood of delivery to the recipients' Inboxes and/or delivery of images.
 - ii. Refrain from use of multiple and various domain name redirect links within the body of a message. (This is not to be confused with dynamic domain name-specific tracking links which are acceptable.)
 - iii. Minimize the use of large image files and messages composed of a single image.
 - iv. Refrain from uses of special coding scripts and embedded forms.
 - v. Refrain from attaching files to messages.
 - vi. Senders should use anti-spam filter tools to evaluate potential content delivery issues and distinguish their content from that of commonly used text and content-structures used by non-permission based emailers.
 - vii. Use of cookies and tracking pixels (i.e.; web bugs or beacons) should be clearly and conspicuously disclosed in conjunction with a sender's privacy and P3P policies.
- e. Senders should identify themselves and enable accountability through designated Internet or Email Access Provider whitelist and/or abuse feedback loop request web pages or other postmaster-specific communications.
- viii. Messaging from Internet or Email Access Providers to abuse or related role accounts should be scalable to the proportion of mail sent by that sender or messaging provider.
 - ix. Senders should actively monitor and minimize abuse-related complaints received from an individual or network provider. Senders should also recognize that there is no parity in the percentage of abuse-related complaints sent from one Internet or Email Access Provider to another and that each provider sets their own thresholds for acceptable numbers of complaints.
- f. Senders should adopt their own anti-spam techniques or obtain services by third-parties that employ their own techniques to characterize lists offered by potentially abusive accounts. For

example, when a sender identifies an account or data segment that appears to have triggered a decoy-based anti-spam filter, use of the account or data segment should be suspended and investigated.

- g. Senders should actively attempt to identify and account for any addresses that have not received email for a lengthy period of time. When identified, senders are encouraged to ensure the maintained accuracy and behavioral response interest-level with these legacy addresses as some Internet Access or Email Providers may re-use these addresses for other customers or with their anti-spam recognition efforts.

IV. **Managing Delivery Errors and List Maintenance**

- a. In addition to monitoring Delivery Status Notifications (DSNs), senders should ensure relevant SMTP session logs are also reported and examined. SMTP delivery errors are defined in RFC2821 and in RFC3463. RFC3464 defines DSN message format extensions to aid with the parsing for error codes. Senders should note that error code examples given in the RFC documents may not accurately reflect the actual cause for an error, and the text accompanying the error describing the cause may need to be examined.
- b. Senders should strategically incorporate RFC 2821 section 4.5.4.1 into their sending retry attempts.
 - i. Too many connections to the same host may result in the host rejecting subsequent connections from the same client for a period of time.
 - ii. When connection timeouts occur or temporary errors are received, the number of simultaneous connections being attempted should be reduced.
- c. Senders should vary retry attempts in conjunction with network operator response codes indicating a temporary status failure such as 4xx error code. The duration or the number of a sender's overall retries may vary depending upon the nature of the message content.
 - i. A sender's retry process should not continue beyond four (4) days, which allows server recovery following a weekend outage. On occasion, the DSN will offer information on how to retry transient failures.
 - ii. Should senders encounter multiple sequential temporary status failures, then they should investigate whether their SMTP infrastructure is in conflict with a receiving network policy.
- d. When senders encounter permanent delivery failure error codes which may include text or other descriptive elements, then they should assess some of the following conditions prior to extraction of the failed addresses:
 - i. Errors indicative of resource-related delivery failure codes might require an extended assessment period to accommodate such as a vacation-related overflow condition.
 - ii. Errors including a 55x_5.7.1 (Delivery not authorized, message refused) error code are considered to be violations of ISP acceptable use policies and should be investigated prior to engaging in subsequent messaging.
- e. Senders should not consider subsequent mailing attempt history when delivering to an address with a persistent permanent DSN failure (hard bounce) and remove such addresses unless subsequent additional information indicates there has been a change in its status.

Editorial Note: MAAWG is committed to increasing accountability and transparency for SMTP error messaging and is conducting in-depth discussions to identify areas of SMTP error messaging improvement.

V. Mitigating and Resolving Messaging Disruption Issues

- a. Senders should be aware of, and recognize all relevant Internet access or email providers' inbound messaging acceptable use policies (AUPs). In most cases, the provider's web site will contain links or other navigation to their respective AUPs.
 - iii. Another such method may be to access an SMTP HELP transmission which may refer to the providers' AUP.
 - iv. In the event that the web site or SMTP does not disclose the AUP, then the sender is encouraged to contact the provider directly.
- b. Senders should track accountability metrics for the individual IP addresses and domain/subdomain names for all outbound messaging, including:
 - i. Recipient complaints through ISP feedback loops, directly from recipients, or through third party services.
 - ii. Permanent DSN failure percentages (i.e.; hard bounce)
 - iii. Spamtrap addresses (when available, typically through third parties⁵)
- c. Senders should access and track metrics through Internet or Email Access Provider postmaster data repositories, where available⁶.
- d. Senders should use reasonable means to establish delivery test accounts at relevant Internet or Email Access Providers to provide increased accountability for network-wide deliverability issues as opposed to investigating potentially isolated incidents reported by recipients. Senders are encouraged to use delivery test accounts as evidence in the event that further investigation is warranted with the provider. Senders should be able to provide an actual email message sent to that domain rather than forward a message sent to another provider.
- e. When messaging disruption issues are identified, senders should:
 - i. Investigate and identify the full extent of the disruption to IP addresses, domain names, or potential content-specific causes.
 - ii. Investigate the SMTP error logs to identify the specific return code associated with that disruption. According to RFC 3463, the error code in the text portion of the message designated for an acceptable use policy violation is 5.7.1.
 - iii. Identify the most applicable email address or web page to contact the messaged-to entity in question.
 1. In many cases this is the postmaster@ISP or abuse@ISP email address.
 2. Senders are encouraged not to contact non-abuse/postmaster related entities such as the advertising, customer service or other corporate communications representatives unless all other options are exhausted.
 - iv. Correspond with the most specific IP addresses and domains in use and include the applicable recipient-specific SMTP error identification.
 - v. Be prepared to identify the specific source and date/time of subscription consent with recipient addresses in question.

⁵ For example, services such as Spamcop offer senders metrics on spamtraps delivered to per day.

⁶ For example, Microsoft offers senders access to its Smart Network Data Services portal detailing messaging metrics sent to MSN/Hotmail.

- f. Senders should be proactive and participate in relevant industry groups as well as list their own abuse-related contact information in any publicly accessible forum in the event that a provider or end-user wishes to contact them.

For technical or policy reasons, senders should recognize that Internet or Email Access Providers may provide little or no explanation for neither the reason why sender messaging is disrupted nor how senders can mitigate future instances of this disruption from occurring. For more details on Internet and Email access provider policies, refer to the MAAWG Code of Conduct.

Appendix A

Commonly Used Definitions:

[IP Address](#)

An **IP address (Internet Protocol address)** is a unique address that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (**IP**)—in simpler terms, a computer address. Any participating network device—including routers, computers, time-servers, printers, Internet fax machines, and some telephones—can have their own unique address. Also, many people can find personal information through IP addresses.

[/24 Network: A 24 bit IP network with space for 254 hosts. A typical IP allocation set used by broadcast mailers.](#)

[Domain Name System \(DNS\)](#)

The **domain name system (DNS)** stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers accepting e-mail for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use.

[RDNS](#)

Reverse DNS lookup (rDNS) is a process to determine the hostname associated with a given IP address. Typically, the DNS is used to determine what IP address is associated with a given hostname; so to reverse resolve a known IP address is to lookup what the associated hostname for it. A reverse lookup is often referred to simply as **reverse resolving**, or more specifically **reverse DNS lookups**. **RFC 1912** says that all hosts on the Internet should have a valid rDNS entry.

[RFC](#)

In [internetworking](#) and computer network engineering, **Request for Comments (RFC)** documents are a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies. Through the Internet Society, engineers and computer scientists may publish discourse in the

form of an RFC memorandum, either for peer review or simply to convey new concepts, information, or (occasionally) engineering humor. The Internet Engineering Task Force (IETF) adopts some of the proposals published in RFCs as [Internet standards](#).

[WHOIS](#)

WHOIS is a TCP-based query/response protocol which is widely used for querying a database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet. WHOIS lookups were traditionally made using a command line interface, but a number of simplified web-based tools now exist for looking up domain ownership details from different databases. Web-based WHOIS clients still rely on the WHOIS protocol to connect to a WHOIS server and do lookups, and command-line WHOIS clients are still quite widely used by system administrators.

[Simple Mail Transfer Protocol \(SMTP\)](#)

Simple Mail Transfer Protocol (SMTP) is the *de facto* standard for e-mail transmissions across the Internet. Formally SMTP is defined in [RFC 821](#) (STD 10) as amended by [RFC 1123](#) (STD 3) chapter 5. The protocol used today is also known as [ESMTP](#) and defined in [RFC 2821](#).

- EHLO: A client SMTP supporting SMTP service extensions should start an SMTP session by issuing the EHLO command instead of the HELO command. If the SMTP server supports the SMTP service extensions it will give a successful response, a failure response, or an error response.
- HELO: In the HELO command the host sending the command identifies itself; the command may be interpreted as saying "Hello, I am<domain>".

[Fully Qualified Domain Name \(FQDN\)](#)

A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: *somehost.example.com.* An FQDN differs from a regular domain name by its absoluteness; a suffix will not be added.

[MX Record](#)

An **MX record** or **Mail exchanger record** is a type of resource record in the Domain Name System (DNS) specifying how Internet e-mail should be routed. MX records point to the servers to send an e-mail to, and which ones it should be sent to first, by priority.

[Delivery Status Notification/DSN \(aka: Bounce\)](#)

An automated electronic mail message from the receiver's mail system, the message tells the sender that the message could not be delivered. The original message is said to have bounced

Appendix B

Email regulations by various regions:

U.S. CAN-SPAM Act

<http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>

- Among other provisions, this act requires subscription removal within ten business days.
- The act also has provisions for express authorization when collecting wireless email addresses or suppression of [wireless email domains](#).

The Australian Spam Act

<http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/E9920A4E670D0FC8CA25702600124DC5?OpenDocument>

Among other provisions, this act requires a subscription removal within five business days.

EU Electronic Communications Directive

http://europa.eu/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

- [Article 29 Working Party document on marketing communications](#)
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

The Canadian Personal Information Protection and Electronic Documents Act

http://www.privcom.gc.ca/legislation/02_06_01_e.asp

The Canadian Task Force on Spam

http://e-com.ic.gc.ca/epic/internet/inccic-ceac.nsf/en/h_gv00248e.html

David E. Sorkin's - SpamLaws.com

<http://www.spamlaws.com/>

Appendix C

Email Associations or Services with Sender Initiatives:

U.S. Direct Marketing Association

<http://www.the-dma.org/councils/responsibleemailcouncil/>

U.K. Direct Marketing Association

<http://www.email.dma.org.uk/content/home.asp?h=0>

Email Sender & Provider Coalition

<http://www.espcoalition.org/>

<http://www.deliverability.com>

Authentication and Online Trust Alliance

<http://www.emailauthentication.org>

TrustE

<http://www.truste.org/>

Network Abuse Clearinghouse

<http://www.abuse.net/>

Canadian Marketing Association

<http://www.the-cma.org/>

Email Experience Council

<http://www.emailexperience.org/>

Interactive Advertising Bureau

http://www.iab.net/comm/email_comm.asp