

Spamhaus Deliverability 101

A guide to improving and maintaining email deliverability





Foreword

Written by Annalivia Ford



There's no denying that deliverability has changed – I've seen it all. From the early AOL days way back in 2002 (that makes me feel old) when blocking and allowing were manual (and perpetual), to being part of the team that established the first “reputation engine”. Suddenly, all kinds of events, actions, and considerations came into the mix, other than keeping complaints under 1%!

Deliverability is now about the quality of the mail stream rather than an Email Service Provider's (ESP) ability to sweet talk an Internet Software Provider (ISP) into allowing their IP. Over the years, big data has enabled ISP and filter vendors to measure more things about email than we can imagine; literally, thousands of heuristics are taken into account for each decision made.

Many aspects go into calculating IP and domain reputation, and each ISP and filter vendor does it their way.

Technologies like DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting & Conformance (DMARC) make it possible to trust more data than the connecting IP address. Trusted data is used for reputation decisions and thus used for spam filtering.

I've worked on both sides of the fence, both receiver and sender – I spent years at IBM, where the sender's struggle became mine. I learned what implementing the advice I had been giving from my ISP desk looked like in real life.

It was challenging in many ways, and one of the biggest challenges was getting my customers to trust that what I was saying was true.

“ A lot of deliverability advice sounds counter-intuitive, especially to businesses coming from the direct marketing world and those driven by their C-suite demanding increases in marketing contacts, marketing campaigns, click-rates, and ultimately the bottom line. ”

I've taken all these experiences and sat down with my team to produce this guide. It contains the essential “do's” and “don't's” of getting email to the inbox. I give you... Deliverability 101.

Happy reading.

Annalivia Ford
Senior Threat Analyst

General deliverability knowhow

Here are some of the essential elements of deliverability you should understand before you consider sending marketing emails.



How do you ensure email deliverability?

Page 6-8



How does email reputation work?

Page 9-12



Address acquisition and the legalities

Page 13-15

Program set-up and configuration

Considerations and actions when setting up an email marketing program.



How to avoid looking like a spammer when setting up marketing emails

Page 16-18



Authentication and encryption for email

Page 19-22



Confirmed Opt-in or Opt-out?

Page 23-27

Day to day operations

Discover the best practices when it comes to the day to day running of an email program.



How to avoid looking like a spammer when sending marketing emails

Page 28-29



Address acquisition for mailing lists - the basics

Page 30-33

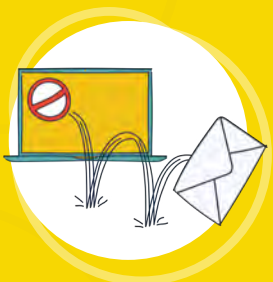


Email frequency and engagement

Page 34-36

Identifying and resolving issues

Here are three major issues you are likely to encounter in your marketing email campaign, along with advice on how to handle them.



How to handle bounced emails

Page 37-41



How to manage email complaints

Page 42-45



Spamtraps - fix the problem, not the symptom

Page 46-48



How do you ensure email deliverability?

How do you ensure email deliverability?



There is no shortcut to successful email deliverability. No matter what services you see advertised in the marketplace, offering that “special deliverability elixir”... don’t be scammed. In a nutshell, you need to **consistently send correctly authenticated, carefully targeted emails to an engaged audience.**

Meticulously adhering to email best practices will lead to excellent IP address and domain reputation, and consequently excellent email reputation. Consider this to be your ultimate goal. Marketers should repeat this as a mantra:

“Excellent reputation is key to successful delivery.”

What is email reputation?

Reputation is defined as “The general opinion or judgment of the public about a person or thing”. In email, reputation is a shorthand way of saying “how recipients reacted to mail you’ve sent in the past predicts how they will react to mail you send in the future”. Good reputation means that recipients like your mail. Many email filters use “reputation” as one piece of their decision making process.

Top 8 ways to improve your email reputation

1 Authentication and encryption

This includes ensuring your emails have Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) correctly set up. These protocols help receivers “trust” your emails.

2 Engagement

Ensuring the email you send is wanted by the recipient.

3 Not doing what spammers do

Sounds obvious, but make sure that you’re not sending bulk email the way a spammer would send it.

4 Address acquisition and data hygiene

Use confirmed opt-in and keep those mailing lists clean. **DON’T PURCHASE EMAIL LISTS** – consent is not transferable.

How do you ensure email deliverability? (continued)

5 Frequency and predictability

Find the sweet spot for how often you send email, set the expectation for frequency, stick to it, and ensure those receiving your emails are engaging with the content.

6 Complaint management

Monitor email campaigns carefully, make it exceptionally easy for recipients to opt out, and honor unsubscribe requests immediately.

7 Spamtraps

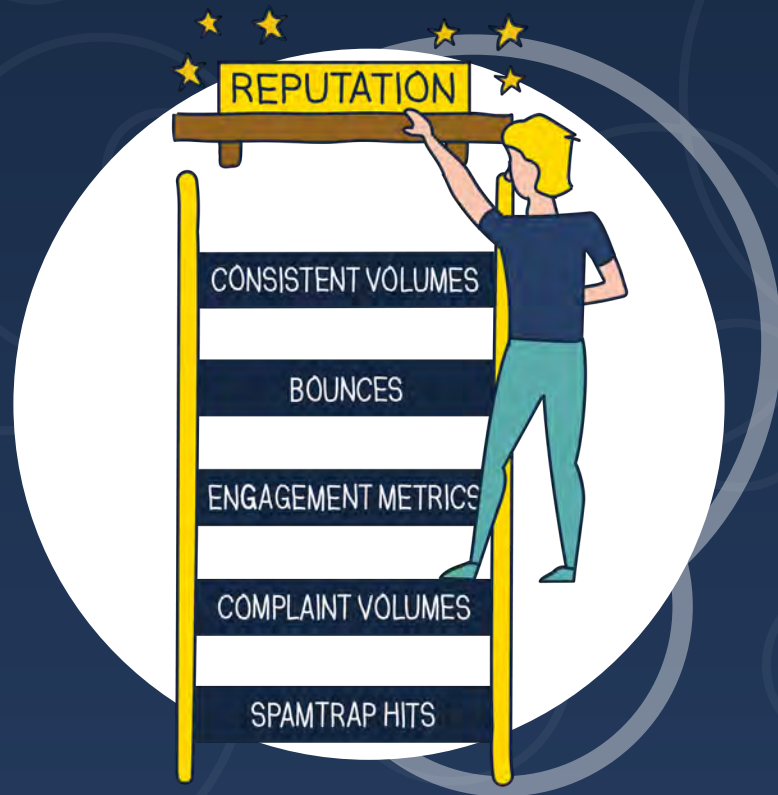
Hitting a spamtrap is a sign of poor data hygiene or issues with your marketing sign-up process. Put your efforts into fixing the data collection, retention and hygiene problem, and not into trying to locate the spamtrap.

8 Bounce handling

Careful management of hard and soft bounces all helps to improve your email reputation.

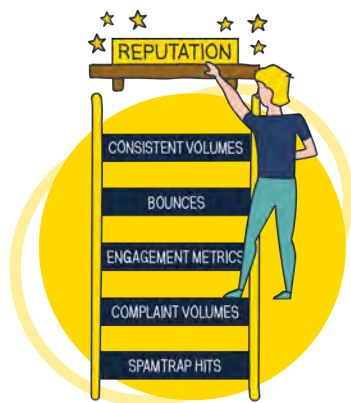
Through this guide we'll be taking a deep dive into each of these areas, arming you with the knowledge to pave your way to successful email delivery.





How does email reputation work?

How does email reputation work?



“ You can’t buy a good reputation; you must earn it. ”

These are wise words indeed from the American businessman Harvey Mackay. Whether it’s personal, business, or email, reputation must be earned. Here’s a look at why reputation matters when it comes to email and what you need to be doing to improve it.

A little bit of email reputation history

Since reputation systems became the de-facto method of spam filtering in about 2010, the focus was mainly on IP reputation, with domain reputation lagging. However, this has changed significantly in the last few years; IP reputation is less important than the reputation of domains and content for inbox placement.

One of the reasons IP reputation is falling behind is the advent of IPv6. It’s HUGE. It has over 340 undecillion IP addresses available, or more precisely: **340,282,366,920,938,463,463,374,607,431,768,211,456** - enough IP addresses for every single device in the world to have its own, and there would still be IPs left over.

This glut of IPs means that cybercriminals can afford to burn IPs like paper (and they do), and therefore we cannot solely rely on blocking by IP to protect users. IPv4 is still the default for email, but it’s running out very quickly, and spam filters need to be ahead of the game.

Today’s email reputation reality

In the modern email ecosystem, IP and domain reputation and recipient engagement are the elements that drive email reputation. The days of “whitelisting” are long gone; we are unaware of any ISP that offers allow listing in any form today.

Reputation systems are designed to automate spam filtering and enable ISPs to react to reputational changes in a rapid and agile manner. Another point to note is that they are agnostic:



They do not care about business models.



They do care about end-user engagement.



They do care whether or not mail is authenticated correctly.

How does email reputation work? (continued)

What affects email reputation?

Reputation is composed of an unknown number of variables that ISPs or reputation providers like Spamhaus do not reveal. But some general components are known, and you can manage them with appropriate address acquisition and data hygiene.

Spamtrap hits

A spamtrap is an email address traditionally used to expose illegitimate senders who add email addresses to their lists without permission. Still, spamtraps are also very effective in identifying email marketers with poor data collection and list management practices. Find out more on page 46.



Complaint volumes

Monitoring complaints is an essential part of the reputational pie, so keeping them as low as possible should be every marketer's goal. To do this, you must consider several things. Find out more on page 42.



Engagement metrics

Engagement is useful for measuring how a marketing program is performing, and has typically been measured by recording clicks, opens*, and purchases. Find out more on page 34.



* In the advent of Apple's Email Privacy Protection, measuring "clicks" is now a less accurate measurement to rely on.

Management of bounces/invalid addresses

Bounce management needs to be handled quickly to ensure that you are taking the necessary actions to ensure your mailing list is clean. Find out more on page 37.



Consistent mail stream volumes

Some ISPs are more reactive to this than others. ISPs are far more concerned about botnet spam than marketing mail. Sudden changes in mail volume are typical of infected hosts, and ISPs react accordingly. "Bursty" email streams will degrade even well-established reputation with the major freemail ISPs. Find out more on page 34.



How does email reputation work? (continued)

What drives inbox placement?

Today, inbox placement is dynamic and almost entirely dependent on IP and domain reputation, which is re-calculated exceptionally quickly in response to end-user reactions and thousands of other heuristics, so the way an email stream is treated can change by the moment.

Spam-folder placement is **also** driven by reputation and user-defined mailbox preferences.

Preparing for the launch of a new IP or domain

Reputation is established during the IP or domain warmup/ramp-up phase – this makes the preparation for the warmup process critical.

It is very much like going on a first date: first impressions matter a great deal and linger for a long time.

1 Plan & select: To prepare for the launch of a new IP or domain, you need to plan the deployment, carefully selecting a set of highly engaged recipients for the initial mailings. These should then be sent in a thoughtful and measured fashion until you reach production volume.

2 Continual improvement: This is a crucial period during which every iteration needs to be meticulously studied, adjustments made, and issues corrected – no matter how painful those corrections may be, i.e., how many potential recipients you need to remove from your segmentation.

Increasing rates of volume and speed should depend on the results of each previous deployment. This means that today's email marketers should be focusing on engagement as much (or more!) than on IP reputation.

The days of “batch and blast” are over, but the good news is that **the more engagement an email receives, the better deliverability gets, and this has a positive knock-on effect on a sender's ROI.** It is not instant and can be very frustrating, but it is worth it.

Critical learning when it comes to email reputation

It is much, *much* easier to drive reputation down than it is to fix a damaged one – this behavior was created by design, and there is no override!

“ Don't try and short-cut building good reputation; otherwise, you'll be spending a lot of time, effort, and potentially money rebuilding it. ”

Next, we'll be looking at the legalities around address acquisition.



Address acquisition and the legalities

Address acquisition and the legalities



Here's a quick review of the legalities involved with collecting Personally Identifiable Information (PII). At one time, having solid records of informed consent to send commercial email to people was not required by law. However, in many cases, it is now.

There are email and data protection regulations across at least 77 different countries, and they are all different. **We strongly recommend consulting legal counsel before undertaking any data collection.** The following 3 data protection laws are the best known at this time.



CAN-SPAM, United States

Marketers **MUST** comply with this federal regulation to legally send marketing email: violators can and have been successfully sued by the FTC. For more information about CAN-SPAM, see these links:

- US Federal Law CAN-SPAM¹ information
- The legal text² of CAN-SPAM



Canada's Anti-Spam Legislation (CASL), Canada

See the CASL Guide³ for more information or read the text of the law⁴. Senders **MUST** comply with CASL if you send email to:

- a Canadian domain
- a Canadian user
- or is transmitted through Canada

(1) <https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business>

(2) <https://www.govinfo.gov/content/pkg/PLAW-108publ187/pdf/PLAW-108publ187.pdf>

(3) <https://crtc.gc.ca/eng/com500/guide.htm>

(4) www.fightspam.gc.ca/eic/site/030.nsf/eng/home

Address acquisition and the legalities (continued)



General Data Protection Regulation (GDPR), Europe

GDPR 2016/679 is a regulation in EU law regarding data protection and privacy for all individual citizens of the European Union and the European Economic Area.

It also addresses the transfer of personal data outside the EU and EEA areas. Enacted on May 25, 2018, it is a very complex regulation; violations of this regulation can carry some severe fines. When building an email marketing campaign involving anyone residing in the EU, you should always consider it. For more information, please consult:

- Qualified legal counsel
- The Wikipedia article¹ about GDPR
- The EU legal lexicon²

(1) https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
(2) <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
(3) <https://www.oag.ca.gov/privacy/ccpa>



The California Consumer Privacy Act (CCPA), California, USA

This was enacted in 2018 and took effect on January 1, 2020, and applied to Californian consumers. This legislation gives CA consumers the following rights:

- The right to know what personal information is collected, used, shared, or sold, both as to the categories and specific pieces of personal information;
- The right to delete personal information held by businesses and by extension, a business's service provider;
- The right to opt-out of the sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt-in consent, with a parent or guardian consenting for children under 13;
- The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

For more in-depth information please visit California Consumer Privacy Act (CCPA)³.



The final word on laws around PII: CONSULT A QUALIFIED LAWYER.



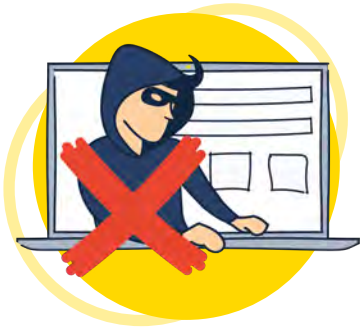
Now it's time to take a look at how to set up and configure your email program, starting with the necessary steps to take to avoid looking like a spammer!





How to avoid looking like a spammer when setting up marketing emails

How to avoid looking like a spammer when setting up marketing emails



In the world of sending email and spam filtering, intentions matter far less than behavior. The spammers set the bar. Even if you are sending authenticated, confirmed opt-in (COI) email, if your email program does not at least meet the basics, no spam filter will understand the difference.

“ Legitimate mailers work hard to build brand reputation based on a real business address, a known domain, and a small, permanent, well-identified range of sending IPs. ”

What steps to take to ensure you look legitimate.

It is critical to follow best practices to distinguish yourself from miscreants who spam. Always keep the following in mind:

- **Authentication:**
 - All emails should be correctly authenticated with DKIM & SPF at a minimum.
 - The SPF record should be as narrow and specific as possible. If you designate the entire internet as “permitted sender,” this is not useful and opens the domain to abuse by spammers.

- **WHOIS:** Do not use anonymized or unidentifiable WHOIS records. Legitimate businesses should have no reason to hide their online identity using WhoisGuard or other such privacy services. Since the advent of General Data Protection Regulation (GDPR) in 2018, many registrars have defaulted to publishing anonymized WHOIS records, but most will remove it upon request.
- **Limit domain usage:** With the increased number of unique domains used to send the same emails, you increase the number of flags raised; use the primary business domain – or a subdomain of it – whenever possible.
- **Use clear and consistent naming schemes in DNS:** keep it simple.

How to avoid looking like a spammer when setting up marketing emails (continued)

1 The best option is delegating a subdomain of the brand's primary domain to the Email Service Provider (ESP): e.g. email.customerbrand.com.

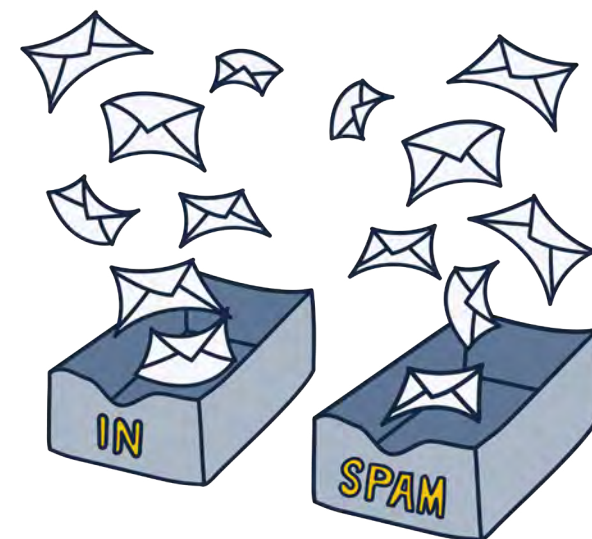
2 The second best would be: "customerbrand.espdomain.com"

3 Last resort (and to be avoided if at all possible): customerbrand-email.com. If this is necessary, it is crucial to use a cousin domain that **clearly relates** to the primary brand name.

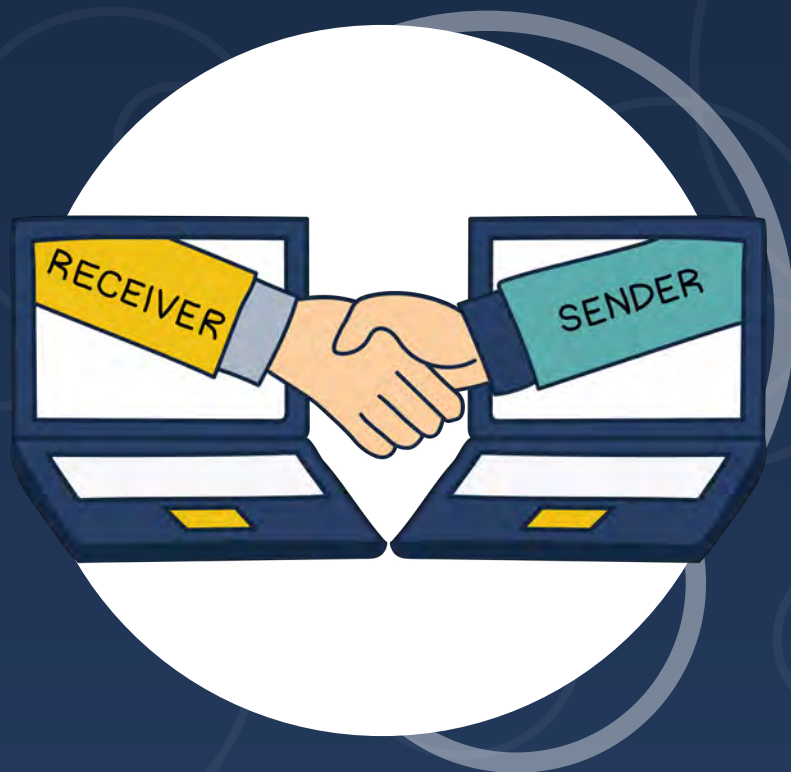
Phishing has made people very wary of look-alikes. Having a clear brand relationship allows receivers to easily distinguish the ESP and customer and reduces the chances of blocks or reputation damage due to unclear identification.

- **Use properly registered domains with working mail AND web addresses.** There should be a website for every domain/brand email domain address used, and not having one looks shady. This is something that spammers do all the time. Link and tracking domains should have a redirect to the primary business website.
- **Every domain that sends email should have functional abuse@ & postmaster@ addresses.**
- **Use contiguous IPs if possible. Use the same network.**
 - If not possible, do not use more IPs than needed.
 - Most brands do not need 100s of IPs scattered across multiple networks – this is the definition of snowshoeing¹.
- **ESPs: Publish an Acceptable Use Policy (AUP)/Terms Of Service (TOS) that is easy to find, read, and enforce.**

Now we've explained how not to appear like someone who's sending spam, we'll be looking at what authentication and encryption is necessary to set up for marketing emails.



(1) <https://www.spamhaus.org/faq/section/Glossary#233>



Authentication and encryption for email

Authentication and encryption for email



One of the first steps to ensuring good domain and IP reputation, and consequently successful email deliverability, is authentication and encryption.

This is going to get a little technical for some marketers reading this. Our advice is that if you don't have a deliverability team to lean on, work together with your IT team to check and ensure your authentication is appropriately set up.

Why are authentication and encryption necessary?

Correctly deployed authentication allows an email receiver to verify that an email's sender is whom they say they are. Why is this necessary? **Everything** in an email header except the IP address that connects to the recipient's server can be forged.

“ Authentication makes it possible for an email receiver to increase their trust in the domains used in headers and the “Friendly From” field. ”

The “Friendly From” name and address are user-defined fields that identify the sender to the recipient and are visible in an email client, i.e., what the end-user sees. If you'd like to take a deeper dive into understanding the various elements of an email header, take a read of our blog: “Understanding the source code of a malicious email”⁽¹⁾.

An overview of key authentication and encryption

Here are the critical factors associated with email authentication and encryption:

- **Sender Policy Framework (SPF)** – allows a sender to specify to a receiver where mail should be coming from. Single IPs, IP ranges, or hostnames can be used.
- **DomainKeys Identified Mail (DKIM)** – uses a cryptographic signature to verify that the sender has permission to use the domain in the “from” field and that the content hasn't been tampered with.
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** – tells the recipient what to do with unauthenticated mail.
- **Transport Layer Security (TLS)** – encrypts the transmission phase of sending email.

(1) <https://www.spamhaus.com/resource-center/malicious-email-source-code/>

Authentication and encryption for email (continued)

Overview continued

SPF and DKIM authentication protocols should be considered a must – and are required in any modern email marketing infrastructure. The lack of SPF and DKIM authentication will damage reputation and affect deliverability and inbox placement. DMARC uses SPF and DKIM protocols and is rapidly increasing in importance, particularly within the financial industry.

SPF

- SPF allows the authoritative owner of a given domain to specify to a receiver which networks or ISPs are authorized to send mail using that domain as a 'from' address.
- Single IPs, IP ranges, or hostnames can be used.
- An SPF TXT record should be as narrow as possible for the greatest security.
- This TXT record lives in the DNS zone file for the sending domain.

DKIM

- DKIM uses a cryptographic signature of a designated portion of the email header and the email body.
- It validates the authority of the sending domain.
- It validates that designated headers and content have not been modified in transit.
- It makes use of a public/private key pair.
- It has become a crucial part of deliverability, and email should never be sent without it. Failure to include a valid DKIM signature will negatively affect deliverability and inbox placement at many ISPs.

DMARC

- DMARC is an authentication policy published through a short entry in DNS. It enables senders to specify to receivers how to respond when email fails SPF or DKIM checks.
- It allows senders to request aggregated and anonymized reports from recipients regarding unauthenticated email that claims to be from their domains.
- It creates a way for ISPs to supply this data in a standardized format. In turn, this allows domain owners to monitor possible spoofing of their domains, which is especially useful for commonly abused businesses such as banks, online payment systems, various social media, etc.

Authentication and encryption for email (continued)

DMARC cont.

- It does **not** allow senders to bypass spam filters.
- Some ISPs consider whether or not DMARC “passes” in their filtering decisions. For DMARC to pass, there must be alignment.
- In DMARC alignment: a message must pass ‘SPF authentication’ and ‘SPF alignment’ and/or ‘DKIM authentication’ and ‘DKIM alignment.’
- DKIM alignment: ‘d=’ must match FRIENDLY FROM
- SPF alignment: RETURN-PATH must match the FRIENDLY FROM domain

TLS

- Transport Layer Security (TLS) is an encryption method used to encrypt the communication channel between two computers. It is the successor to Secure Sockets Layer (SSL), and the two terms are often used interchangeably. SSL/TLS are widely used to encrypt connections over the internet. For example, whenever a lock appears in the browser bar, the browser encrypts communication between you and the website you are connected to.
- TLS can be used to encrypt email during the transmission stages. Some recipients require it and refuse mail that is not TLS encrypted, but that is not very common (yet). Many MTAs have the option to request TLS if it is available and will failover to an unencrypted connection if it is not.

With all the previous correctly configured, you will have built the foundations for increasing your email reputation and having good inbox placement.

Having taken a closer look at the world of email authentication and encryption, we’ll review what kind of opt-in method you chose to use when building your mailing lists.

Further resources:

Additional reading

The official websites for:

- SPF – the Sender Policy Framework is defined in RFC 7208¹
- DKIM – DomainKeys Identified Mail’s official website²
- DMARC – Domain-based Message Authentication, Reporting & Conformance’s official website³
- Wiki page for TLS⁴

Useful tools:

- Kitterman’s SPF checker⁵ tool
- DKIM Core Key checker⁶
- DMARC validation⁷ tool

(1) <https://datatracker.ietf.org/doc/html/rfc7208>
(2) <http://dkim.org>
(3) <https://dmarc.org>
(4) https://en.wikipedia.org/wiki/Transport_Layer_Security
(5) <https://www.kitterman.com/spf/validate.html>
(6) <https://dkimcore.org/tools/keycheck.html>
(7) <https://dmarcian.com/dmarc-inspector/>



Confirmed Opt-in or Opt-out?

Confirmed Opt-in or Opt-out?



There are various methods used today to build mailing lists and contact databases. Confirmed Opt-In (COI) is the gold standard. It is a simple and powerful method of building and maintaining a clean, high-quality database of marketing contacts. This, in turn, will help build and maintain your email program's reputation and subsequently ensure and maintain good deliverability.

1. Confirmed Opt-In/Double Opt-in

Here is an outline of the process for confirmed opt-in (COI).



Confirmed Opt-in or Opt-out? (continued)

Benefits of Confirmed Opt-In

While this method requires more work and investment than others, the payoff in list quality more than offsets it.

- ✓ It increases the **integrity and reputation** of the sender in the eyes of the recipient.
- ✓ **Happy recipients are more engaged** – if you treat a recipient's inbox and time with respect, they are less likely to report that email as spam and less likely to unsubscribe (and happy customers tend to make more purchases).
- ✓ **You won't regularly hit spamtraps** – see page 46. They significantly reduce the likelihood of poisoning a contact list with a trap.
- ✓ **You won't risk all your emails being blocked** – ISPs often block whole email streams that generate a lot of spam complaints or hit their traps, resulting in a loss of inbox delivery, reputation, and revenue.

- ✓ **It makes investigations easier to resolve.** When an ISP, filter vendor or reputation provider refuses a sender's email, they often require proof of consent as part of the investigation. You can't provide this if you haven't sought permission and had it granted via COI. They also can require a 're-permissioning' pass and demand that you offer all your subscribers the chance to opt-out or remain subscribed and that those choices must be honored.

“ Confirmed opt-in provides a low-risk, high ROI method of reaching contacts. ”



Confirmed Opt-in or Opt-out? (continued)

2. Opt-in/Single opt-in

This is a widely used method that involves no confirmation of consent:




Issues with single opt-in


While it is possible to run a successful email marketing campaign using this method, it can cause these problems:

- ❗ **Uncertainty.** It is impossible to know if the recipient truly wants to be added to your marketing list without the recipient verifying this is the case.
- ❗ **Increased risk of spam complaints.** If the contact didn't realize they were subscribing to your marketing emails and suddenly started to receive them, they may mark them as spam or make a direct complaint.
- ❗ **Hitting spamtraps.** If someone uses a spamtrap email address for a signup, it will poison your mailing list. Malicious submissions of spamtraps can cause tremendous difficulties, which can be very time-consuming and expensive to resolve.
- ❗ **Potential to be listed on blocklists.** The consequences of hitting spamtraps could be a listing on a blocklist, leading to bounces for all your emails.

Confirmed Opt-in or Opt-out? (continued)

 **Risk of typos, bot submissions, or throw-away emails.** Unconfirmed email addresses can be maliciously submitted. People often use throw-away, typed, expired, or imaginary email addresses to get what they want from a website without accepting more marketing emails.

All of these factors can poison a mailing list since user engagement is the most critical factor in determining the fate of an email today. Unexpected marketing mail causes people to report it as spam, driving down reputation and deliverability.

 **Increased bounce rates.** Incorrect addresses cause high bounce rates, which can (and do) provoke adverse reactions from ISPs, resulting in spam foldering, rate-limiting, or blocking.

3. Opt-out

Opt-out is the least useful, messiest, and riskiest of all acquisition methods, and you should avoid it at all costs. It has been proven to negatively affect IP and domain reputation, causing severe problems with successful email delivery.

Opt-out employs the assumption that you can acquire permission after the event; that's not how permission works. It cannot be granted retrospectively; you must get it upon initial contact. Opt-out methods also include the use of purchased or rented mailing lists, addresses scraped or harvested from the web, etc.

Issues with opt-out

Opt-out places the burden of permission on the recipients, which rarely goes well for the marketer. Use of this method is guaranteed to cause:

-  **High bounce rates.**
-  **Spam complaints.**
-  **Hitting Spam traps.**
-  **ISP blocks.**
-  **Listing on blocklists by reputation and filter vendors.**

Next stop... let's move onto the day-to-day operations of running a marketing email program starting with how to avoid looking like a spammer when you're sending emails.



How to avoid looking like a spammer when sending marketing emails

How to avoid looking like a spammer when sending marketing emails



The day-to-day running of an email program opens up as many pitfalls of appearing like a spammer as the program's set-up does. Here are a few key elements to abide by to ensure an ISP or blocklist provider doesn't view your marketing emails as malicious:

1 Spammers often send email erratically

Therefore, a steady sending pattern is essential. Bursty mailings or sudden and significant changes in volume are things that infected hosts do. Remember that an ISP's filtering systems do not know or care that your company is trying to make money on Mother's Day retail activity - if your sending patterns mimic an infected host, your email will not get through!

2 Never send to a suppression list by accident

The phrase "we sent the wrong segment by accident" has been used by spammers to the point that it has created a knee-jerk response in ISP abuse-desk workers. Do NOT let this mistake happen: render such an event completely impossible!

3 Questionable ways that miscreants acquire mailing lists

Given the various questionable ways that miscreants acquire mailing lists for their malicious campaigns, their unknown user rate per send is likely to be high. Hence it's vital to ensure a low rate of unknown users in any given send.

4 A spammer's care factor is almost 0% regarding reputation

They burn through IP addresses and domains. Your reputation does matter, so keep an eye on all of your sending metrics, including unexpected bounces, temporary failures, and anything that could indicate abnormalities in the mail stream. If you're an Email Service Provider (ESP), keep an eye on your SMTP logs.

5 A cybercriminal's engagement rate doesn't need to be high

Sometimes, a spammer is just looking for a few victims per email campaign. This is why your engagement rate does need to be high. Where possible, use a "preference center" to let people choose what content they're interested in receiving from you to maximize engagement rates.

6 Don't send attachments with emails

One fundamental way a cybercriminal delivers their malware payload is via an attachment.

With these elements covered, we will be delving into the fundamentals of address acquisition to ensure you're building your mailing lists appropriately without potentially damaging your email reputation.



Address acquisition for mailing lists - the basics

Address acquisition for mailing lists - the basics



There are various ways to acquire contacts when building email marketing lists; however, these approaches won't always benefit your deliverability and email reputation. Here we examine the data marketers should be recording, considerations when using online forms, and address acquisition methods to avoid at all costs.

“ The methods utilized to build mailing lists or contact databases are critical to creating and maintaining good list hygiene. ”

What data should you be collecting?

In today's world, where laws regarding Personally Identifiable Information (PII) are prevalent (see page 13), you must accurately record data during the acquisition process, preserve it and update it as necessary.

We recommend keeping the following information for every contact:

- The date & time of the sign-up in UTC.
- The channel that was used to obtain the email address.
- The IP address that submitted the email address.

If one of your IPs or domains is blocklisted and manual intervention is required to resolve the issue, ISPs and/or reputation providers often demand proof of consent.

Without good records, such proof is impossible to provide, and therefore any resolution to a block will take longer.

In the event of a GDPR or similar data removal request, having these records could save your company a great deal of money in fines.

Recommendations for website and online forms

Make “opting-in” voluntary – If you collect contact email addresses via a website or online form, we recommend utilizing a checkbox that the user **must voluntarily select** before being added to a marketing program.

Using a pre-checked box is generally viewed as dishonest and is actively illegal in some countries. People can fail to notice the checkbox and then get an unpleasant surprise when they receive marketing emails they did not ask for or expect. Consequently, they report the mail as spam, causing you reputational and brand degradation. Be transparent in your sign-up process!

Address acquisition for mailing lists - the basics (continued)

Protect your forms – Due to an ongoing and widespread problem that began in August of 2016 that has been escalating ever since, we recommend that you secure web forms against abuse by adding a CAPTCHA¹ or reCAPTCHA² to the form (both are free tools).

Bots use unsecured forms to sign up an uncountable number of bad email addresses, resulting in database poisoning. This can also create what amounts to a denial of service attack (DoS).

Confirmed opt-in – Once a contact has completed a form, we strongly recommend using the confirmed opt-in (COI) method, obtaining active consent via email from the user. See page 24 for an in-depth look at opt-in options.

Ways NOT to increase your marketing contact lists

When it comes to increasing the number of marketing contacts in your lists, we strongly advise against any of the following methods:

- 1 Buying a list
- 2 Harvesting email addresses
- 3 Using append

Best practice states that contacts should confirm that they consent for you to send them communications (COI). **Consent is not transferable**, and violating it makes recipients angry. In the days of GDPR (and other laws), breaking that consent can be an exceptionally costly thing to do.

Continue reading for a detailed explanation of why you shouldn't ever consider using one of the above three approaches to expand your marketing lists.

Purchased or Rented Mailing Lists

The damage that a purchased list can do is incalculable.

Spamhaus has clear views about purchasing and selling mailing lists: because consent is not transferable, this practice is, by definition, impossible and therefore fraudulent. Buying and selling lists do not allow the purchaser to obtain consent to send email to the recipients in that list.

“ Permission is not transferrable. ”

As a result of complaints, bounces, and potential spamtrap hits, using such lists can:

- Result in IPs or domains being put on blocklists.
- Reduce overall deliverability and inbox placement for a long time – reputation is much harder to rebuild than to destroy!
- Cause severe damage to brand reputation.

(1) <http://www.captcha.net>

(2) <https://www.google.com/recaptcha/about/>

Address acquisition for mailing lists (continued)

The Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) has published a statement⁽¹⁾ about the sale of email address lists, which Spamhaus fully supports – ***“The practice of selling, buying or sending to lists of purchased email addresses – whether business to business (B2B), business to consumers (B2C) or other categories, is in direct violation of M3AAWG core values.”***

Harvesting

Harvesting is a data collection practice in which emails are obtained by scraping websites, forums, etc. Some less than scrupulous operators also try random combinations of email addresses at specific ISPs to find active email addresses.

This method provides no avenue for opt-in or any kind of permission or consent and typically causes serious blocking and delivery issues for any sender that employs it.

Permission is not transferrable

- As a result of complaints and spamtrap hits, using such lists can:
 - > Cause severe, long-lasting damage to brand reputation.
 - > Degrade inbox placement in the short term.
 - > Reduce deliverability in the long term.

Epending/Appending

In marketing terms, “epending” or “appending” is the practice of taking demographic information known (or assumed) to be related to a particular customer and matching it with other data. The terms are interchangeable in use.

Following published industry best practices, we firmly recommend not using this address acquisition method.

M3AAWG has published a clear statement about e-pending, which Spamhaus fully supports: ***“The practice of email appending is in direct violation of core MAAWG values.”***

Co-reg/Affiliate Marketing

Co registration (co-reg) is when a third-party is used to handle the permission collection for you. Affiliate marketing is where you incentivize or pay a third party to advertise your services (via email).

Managing your data collection methods brings peace of mind

When you buy, rent, endpend/append, or use co-reg/affiliate lists, you have no quality assurance on the integrity of this data. You cannot purchase consent, and such lists significantly increase the risk of long-term damage to your email campaigns because permission is not transferrable. As we said at the beginning – please avoid at all costs.

With a robust sign-up policy in place, it's time to think about how frequently you should be sending emails and the importance of engagement.

(1) <https://www.m3aawg.org/sites/default/files/m3aawg-selling-email-lists-2019-06.pdf>



Email frequency and engagement

Email frequency and engagement



Setting recipient expectations during your confirmation/welcome message is a helpful strategy; sticking to that expectation is invaluable. Sending email too frequently can cause “email exhaustion”; people who have a clear expectation that is met will feel respected and are much less likely to report as spam, delete the emails unread, or unsubscribe.

How often should you send to your mailing list?

Marketers should tailor the “correct” frequency to the individual marketing campaign, but having a sunset strategy - asking people to confirm if they wish to continue getting marketing emails from you - is vital to maintaining a healthy and engaged mailing list. Here is an example:

- If more than a week passes without the recipient opening an email, change them from weekly to monthly.
- If more than a month passes without the recipient opening an email, send them an email asking, “Do you wish to continue your subscription?” This should contain a link that the contact can click if they wish to continue.
- If they don’t respond, add them to your suppression list and stop sending them emails!
- Sending email in bulk to addresses that have never given consent to receive those messages is spam. Continually sending to email addresses that have never successfully been delivered is also spam.

Considering changing the frequency of your marketing emails?

Intended changes in frequency should be very carefully considered, especially around the holidays.

Many marketers believe that ISPs, reputation, and filter vendors such as Spamhaus “tighten the rules” around the holidays, which is not the case. Nothing changes on the recipient or vendor side - what causes the perceived “tightening” is created by changes in sender behavior.

The holidays are when senders tend to reach deeply into their subscriber lists (or even buy lists!), taking chances on sending to unengaged or even unsubscribed customers in the hopes of making some extra money during the lucrative holiday sales season. What usually happens is that using those older, unused segments triggers the domino effect of a decline in reputation.

Then inbox placement is affected, leading to adverse outcomes, including tempfails, deferrals, blocks, and sometimes even inclusion on reputation lists, such as Spamhaus produces.

Email frequency and engagement (continued)

The value of email engagement

Engagement is valuable for measuring how your marketing program is performing and is typically measured by recording clicks, opens, purchases, and interaction with social media. If engagement is too low, it is time to look at the age, content, mailing frequency, and segmentation of the program lists.

Please note - Spamhaus reserves the right to engage with the spam we receive, and even to follow non-subscription links. There are also many anti-spam appliances that now do this. The fact that an email is opened or a link is clicked does not mean consent has been given.

How often should you review email engagement?

We strongly recommend that you carry out continuous iterative work to segment out anyone that has not actively engaged with a given mail stream in X amount of time. The usual starting place is one year, then moving to six months, three months, etc., depending on results.

The importance of good email data hygiene

Remember – keep it clean! The regular practice of data hygiene is crucial: flawed address collection processes and bad sending practices can result in you adding spamtraps to your mailing lists (see page 46). The presence of spamtraps confirms the underlying data problems; focusing on finding and removing traps treats the symptom, not the problem. Spamtrap hunting is a short-term solution with limited benefits, as traps are only one part of the reputational mix that is in use today.

Here are other mistakes that can be exceptionally costly in both time and money.

- ❗ Sending to the “wrong” segment of a database, including failing to use your suppression list.
- ❗ Making sudden sizeable changes to the volume or frequency of email streams.
- ❗ Sending to older lists that may contain spamtraps or many invalid addresses.
- ❗ Using a purchased list.

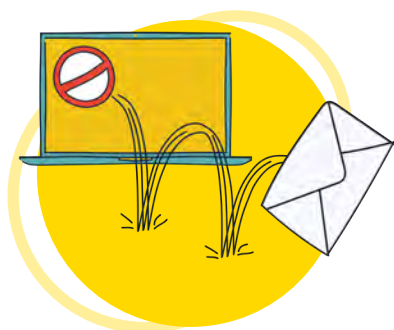
Keeping recipients engaged and active is the single most important thing a marketer can do to ensure the success of an email marketing program. Reputation is much harder to rebuild than ruin.

Part of keeping that good reputation intact is effectively managing bounced emails and we'll be explaining how to do this next.



How to handle bounced emails

How to handle bounced emails



Managing hard bounces, soft bounces, and blocks is another crucial element of maintaining a successful email marketing program. Here's an explanation of the difference between hard and soft bounces, ISP hard blocks, and what you should be doing when you encounter them during an email campaign.

Hard bounce

Definition of a hard bounce – Fatal Error: No retry will occur

A hard bounce occurs when the email server rejects the email due to permanent conditions. This typically results when 'user unknown' or 'domain not found' errors occur. However, there are also other, less common reasons.

The SMTP response code for all hard bounces begins with 5xx. Below are some of the most frequently seen by marketers:

550 **“Non-existent email address”:** This usually defines a non-existent email address on the remote side. The great majority of errors 550 mean that the recipient's email address doesn't exist.

512 **A DNS error:** The host server for the recipient's domain name cannot be found. The domain does not exist in DNS.

551 **“User not local or invalid address – Relay denied”:** Meaning if both your address and the recipient's are not locally hosted by the server, a relay can be interrupted.

552 **“Requested mail actions aborted – Exceeded storage allocation”:** Simply put, the recipient's mailbox is full.

553 **“Requested action not taken – Mailbox name invalid”:** There is an invalid email address in the “recipient” field.

In relation to an email marketing campaign, most of these errors are the direct result of poor data hygiene. As there is a considerable amount of churn in email addresses, sending to outdated lists increases the chances of sending to non-existent domains. This can be dangerous as non-existent domains can be spamtraps (see page 46).

If you encounter a hard bounce, ensure you don't send to the contact again - delete them, or at the very least, add them to a suppression list.

How to handle bounced emails (continued)

Soft Bounces



Definition of a soft bounce: **Temporary Failure: retry will occur**

A soft bounce occurs when the email server rejects the email due to a normally temporary condition, such as a connection problem or too many complaints. When that happens, the system tries to send the email again until it is either accepted or times out. The time-out is set on the sending side and varies by network.

421 The service is unavailable due to a connection problem: It may refer to an exceeded limit of simultaneous connections, a lack of resources on the receiver side, or a more general temporary problem such as a reduction in reputation.

450 “Requested action not taken – The user’s mailbox is unavailable”: The mailbox has been corrupted or placed on an offline server, or the email hasn’t been accepted due to reputation or blocklisting.

451 “Requested action aborted – Local error in processing”: The ISP’s server or the server that got the first relay has encountered a connection problem.

452 Too many emails sent or too many recipients: More in general, a server storage limit exceeded.

Some ISPs respond to dips in reputation by issuing “tempfails” preceded by a 4xx code, usually 421. This means they will defer mail for a determined amount of time until either the mail stops coming or reputation re-calculates upward again. That error can look like this: “421 4.7.0 [TS01] Messages from x.x.x.x temporarily deferred due to user complaints.”

Addresses affected by a temp-fail should not necessarily be removed from a mailing list! If the block is due to a poor-quality mailing list, you should review your list hygiene and correct any problems before trying again.

ISP Hard Blocks

In the modern email ecosystem, most receivers base their spam filtering on a reputation-based system, be it purchased, home-grown, or a combination of the two. They all have different ways of accomplishing their goal of protecting their users from unwanted email, but they all have some commonalities. ISPs typically respond to mail that is coming from an IP/domain with poor reputation and/or incorrect or missing authentication in this general pattern:

- Placing mail in the spam folder.
- Increasing levels of rejection, beginning with temp-failing or throttling the problematic mail stream.
- Bouncing/rejecting the problematic mail stream and possibly escalating to hard blocking.

How to handle bounced emails (continued)

If an ISP issues a hard block, they are indicating they will no longer accept mail from the sending IP and that this is not a temporary issue. The most commonly used SMTP code for hard blocks is:

554

This is a permanent error, and the server will not try to send the message again.

This type of bounce occurs when the receiving email server rejects the email for policy reasons, including:

- URL or email body content blocks.
- Lack of correct authentication.
- Poor IP or domain reputation.
- The presence of the sending IP/domain on a blocklist in use by the recipient.

Depending on the ISP, the blocks will often disappear over an arbitrary period (24-72 hours, generally) if the triggering issue ceases.

The error for such a block will usually begin with “554” and contain more specific information or a URL you can consult for more details. For example: “554 The IP address of your mail server (127.0.0.1) was found in the Spamhaus blocklist. See <https://check.spamhaus.org/for details>”.

These blocks can result from a decision made by looking at their own data, data provided by a reputation provider like Spamhaus, a filter vendor such as Cloudmark, or a combination of two or more of these.

If the block does not resolve on its own, but you have resolved the triggering issue, you will need to open a ticket with the network that is issuing the block to fix the problem, if possible. It will be necessary to understand what caused the block and correct it before opening a ticket. Some ISPs, notably Gmail, have no remediation.

“ Correctly managing bounces goes a long way toward keeping mailing lists clean and up to date. ”

Spam Filters and Reputation Providers

As a general rule, it is safe to say that Gmail, Hotmail, and Verizon Media (what used to be Yahoo and AOL) use mostly home-grown spam filtering technology. Due to the nature of their business model as mailbox providers, they have access to a huge amount of data regarding their own users’ email behavior. Generally, these providers prefer to use their data, as it is more accurate in relation to their networks. They may or may not use commercially available data combined with their own: they will not say.

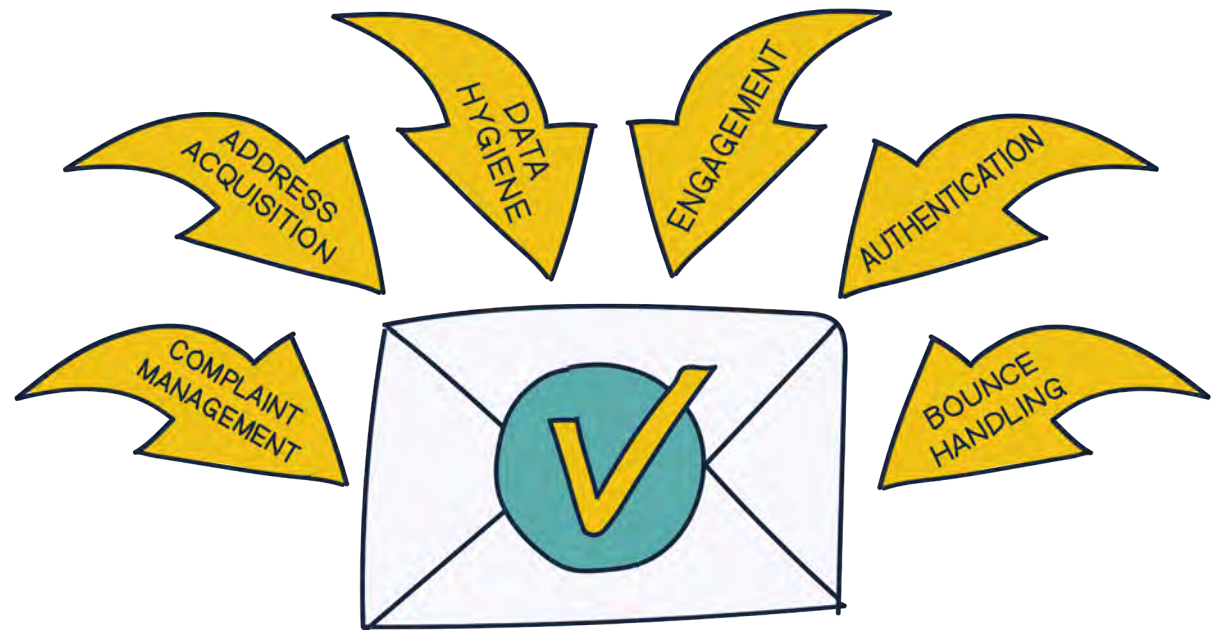
Providers like Comcast, RoadRunner, and Sky use commercial spam filters and reputation providers such as Cloudmark’s and Spamhaus’ offerings.

Modern spam filters have become very sophisticated; they are flexible and fast. Being blocked by any spam filter vendor (such as Cloudmark) or reputation provider (such as Spamhaus) can have time-consuming and costly results.

How to handle bounced emails (continued)

Of course, the impact depends on many factors, including how widespread the adoption of the filter is. There are hundreds of blocklists in the industry, but only a few have a broad impact. Even if you use a comprehensive blocklist checking tool to review your IP or domain (MXToolbox, for example), you will end up on a blocklist somewhere. How seriously to take that depends on who is issuing the block. For example, a listing on the Spamhaus Blocklist (SBL) has enormous reach, whereas you can happily ignore a listing by SPEWS.

Now you know how to handle bounced emails, let's review how to manage complaints.





How to manage email complaints

How to manage email complaints



Monitoring complaints is a vital piece of the reputational “pie,” so keeping them as low as possible should be every marketer’s goal. There are many reasons recipients click “report spam,” some of which are manageable, and some are not.

Manageable email complaints

- **They didn’t sign up to receive the email you’re sending to them.** Don’t send emails to people unless you have, at a minimum, opt-in from them.
- **Failure to correctly set recipient expectations regarding frequency and content.** Be clear in your confirmation opt-in email of what your recipients can expect to receive and how often they will receive it.
- **They get too much email from you, or there has been a notable change in frequency.** Mail that is too frequent can annoy recipients. Conversely, mail that is too infrequent may be unexpected, and recipients will report the mail as spam. Be consistent.
- **The mailing list was purchased.** Management of this issue is simple – don’t purchase lists!
- **The messages your recipients are receiving aren’t relevant.** Content that your recipients don’t like can frustrate them to the point that they report it is as spam. Targeting the correct demographic and audience is crucial.
- **Sending mail after the recipient has unsubscribed.** A recipient should be removed from your mailing list immediately if they unsubscribe, regardless of how long the applicable law says it is permissible to wait.

How to manage email complaints (continued)

Less manageable email complaints

- **Recipients don't remember signing up.** You can't control someone's memory; however, if they unsubscribe, ensure you action this immediately. You can control frequency; if someone signs up and you don't send the first email for weeks or months later, they will forget.
- **The address was collected at the point of sale, and human error took over.** Once again – this is out of your control. Just ensure that anyone who unsubscribes never receives another unsolicited email from you because you can guarantee that they will report it as spam next time.
- **Frustrated recipients reporting indiscriminately.** Some recipients get so annoyed with the amount of email they receive that they will select large portions of their email box and report all of it as spam.

Tools to help with email complaint management

Some ISPs offer more in-depth data about what happens to email once they have accepted it. Here's a selection:

- Hotmail Smart Network Data Service¹ (SNDS) provides data about traffic such as mail volume, instances of deferrals or tempfails, complaint rates, and the number of their traps hit.
- Google Postmaster Tools² – provides limited data about complaint volumes and domain reputation via a web interface.
- Participate in all available feedback loops (see across for more details).
- Contract with a reputable Deliverability Consultant or hire a reputable email analytics company. Not all are created equal, so you should research these carefully.

Email feedback loops

A “feedback loop” (FBL) allows Internet Service Providers (ISPs) to report spam complaints submitted by their users to the originating network. This is done using Abuse Reporting Format (ARF), a machine-readable format that redacts Personally Identifiable Information (PII). Some major ISPs offer a feedback loop as a free service.

You should process these reports promptly and immediately remove the complainants upon receipt. The length of time allowed for suppression to occur varies by law and country, so ‘immediately’ is the best practice.

The number of complaints generated by a given IP is given significant weight by receivers, though ISPs will not reveal the threshold as it is part of their spam filtering recipe and will vary from ISP to ISP. A good reputation allows slightly more forgiveness than a poor one. That being the case, keeping complaints as low as possible is the prudent thing to do.

(1) <https://sendersupport.olc.protection.outlook.com/snds/addnetwork.aspx>

(2) <https://gmail.com/postmaster/>

How to manage email complaints (continued)

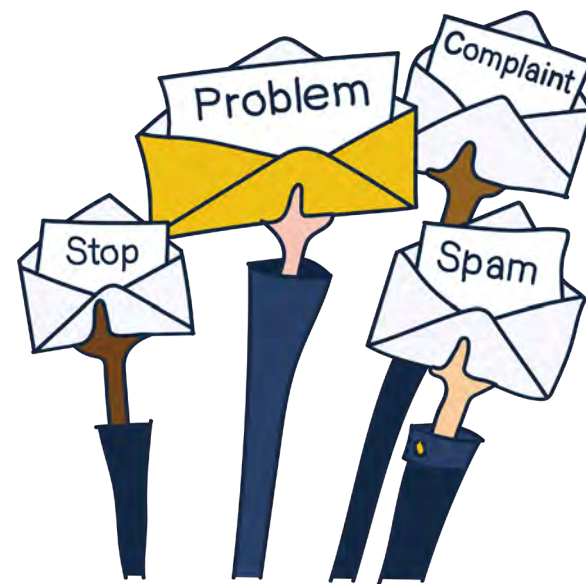
Advice to help marketers avoid email complaints

- When you confirm an opt-in, be clear about what the user will receive and when. Keep that promise.
- Offer different frequency options that recipients can manage via a preference center.
- Don't pre-check subscription boxes.
- DO NOT USE PURCHASED LISTS/LEADS.
- Make unsubscribing super easy. Some laws regarding marketing mail require this, but even if they don't, it's always better to have someone use an unsubscribe link than report spam.
 - > Do **not** require a log-in to unsubscribe. It is illegal in some places and makes subscribers angry everywhere.
 - > Place the unsubscribe so it can be easily found, for example, a link on the top of the email. If receivers can't locate it quickly, they will report it as spam instead.

- Use careful segmentation and A/B testing to ensure that you send email to the most well-targeted and engaged audience possible.

If you sign up recipients via confirmed opt-in, keep your mailing lists clean, and only send relevant content to engaged contacts, you should have minimal complaints to manage. But, if you do receive them, we urge you to deal with them rapidly.

Next in our guide is a detailed look at spamtraps.





**Spamtraps – fix the
problem, not the symptom**

Spamtraps – fix the problem, not the symptom



A spamtrap is an email address traditionally used to expose illegitimate senders who add email addresses to their lists without permission. They effectively identify email marketers with poor permission and list management practices.

“ We strongly urge people to view spamtraps as proof of a data collection or hygiene issue and not be misled into conducting a hunt for spamtraps. Attempting to locate and remove traps only treats the symptom and not the underlying problem. ”

Spamtraps are never revealed by their owners. Partly because they are a component of the secret sauce of their filtering, and partly because if the trap is identified, what usually happens is that the sender simply suppresses the trap address – and they don’t undertake any of the necessary to work to improve their data. Here’s an outline of the various types of spamtraps in use:

Classic or Pristine Spamtraps

Classic spamtraps are email addresses never given to a live user or exposed on a website but have started receiving email anyway. In some cases, these are addresses at domains that accept mail to any local part (wildcard domains: e.g. `*@example.com`).

Seeded Traps

Seeded traps are email addresses that trap owners create and deliberately scatter – seeding around various places online that are not obvious (in webpage source code, for example).

These traps highlight that the sender is either scraping addresses from the web or is buying lists from someone else who is scraping addresses. These traps are good for identifying sources sending mail without permission and those not honoring unsubscribe requests.

Spamtraps – fix the problem, not the symptom (continued)

Typo Domain Traps

These are traps at domains that are similar to common domains: yaaho.com or ynail.com, homail.com, etc. Mail to these traps suggests to the trap owner that the sender is trying to send mail to real people. These are not “pure” spam traps, can contain a lot of real mail, and are generally weighted accordingly. Employing COI at the data collection point is a perfect way to avoid your lists being polluted by these nuisance traps.

Dead Address Traps

“Dead” traps were once-valid email addresses that ISPs have turned off. All mail to these addresses is rejected with a hard bounce for a period of time, often 12 months or more. After consistently rejecting mail for a pre-determined period, the addresses are silently turned back on in the form of spamtraps.

Live Traps

These are email addresses belonging to a real user. Owners use them for real mail, but they use the unsolicited mail coming into those addresses to make blocking decisions. Hitting these can be extremely dangerous if the person who owns them has connections.

Domain registration addresses (a subset of Live Traps)

Registration (or role account) addresses are a special type of live trap. These addresses, published in WHOIS records, are frequently harvested and mailed. These types of addresses should almost NEVER be on a marketing mailing list. Examples include postmaster@ example.com, abuse@example.com, admin@example.com, etc.

At the end of the day, if you follow our best practices paying attention to data collection, hygiene, and sending frequency, you won't need to worry about the various types of spamtraps that exist... Because you won't be hitting any.

A final word

We'll finish where we started at the very beginning of this guide...

“ Sending correctly authenticated, desired, well-targeted email to an engaged and active audience is the key to ongoing successful email delivery. ”



Check your IP and Domain reputation

Use our checker to see if any of your IPs
or domains are listed on Spamhaus' blocklists.



<https://check.spamhaus.org>