EMAIL DELIVERABILITY GUIDE

Secrets for Better Inbox Placement

Contents

Definitions

What is spam?

Spam (the unofficial name for unsolicited bulk email (UBE)) refers to bulk emails or advertisement emails that are disseminated throughout the Internet. They land unsolicited in millions of electronic inboxes. Most spam emails are commercially motivated and are categorized as follows:

- Commercial email spam
- Chain letters, virus warnings, hoaxes
- Emails sent by viruses
- Phishing emails

Delivery (delivery rate)

The delivery rate is the percentage of successfully sent emails (defined as receipt of the email in the inbox of the recipient) compared to the total number of emails sent. Bounces, meaning undeliverable emails, are not included. The delivery rate is, among other things, an indicator of the quality of the distribution list. To keep the delivery rate consistently high, a process known as bounce handling is needed. This process is also integrated in Retarus' global suppression solution. Email addresses that cannot be delivered to are automatically removed from the distribution list.

Reputation/sender score

Scores are calculated as a moving average over a period of 30 days and represent the ranking of an IP address compared to other IP addresses. It is similar to a percentile rank. The closer to 0 the score is, the worse it is. The closer to 100 the score is, the more effective the sender.

Complaints: This is calculated by dividing the number of complaints by the number of received emails. It also takes into account the number of complaints the IP address receives compared to other IPs.

Volume: The dispatch volume alone is not an indicator of whether a sender has a good or bad reputation. However, it is an important part of the general algorithm. For example, an IP address that sends 100 emails and receives 99 complaints is ranked as questionable. In contrast, an IP address that sends 100,000 emails and receives 99 complaints is ranked as having a good reputation. Thus, the volume always depends on other index values.

External reputation: This number indicates how a sender's IP address compares with other IP addresses also listed on numerous external blacklists and whitelists.

Unknown contacts
The ratio of an IP address' unknown contacts to other addresses is taken directly from the incoming SMTP logins of the involved ISPs. It measures how often an IP address attempts to send an email to a recipient that does not exist.

Rejected emails
This measures how often sent emails result in a soft or hard bounce as compared to other IP addresses.

Accepted emails
This number represents how many emails are accepted by the ISPs and forwarded to the recipients. The number is comprised of all sent emails minus the number of rejected emails.

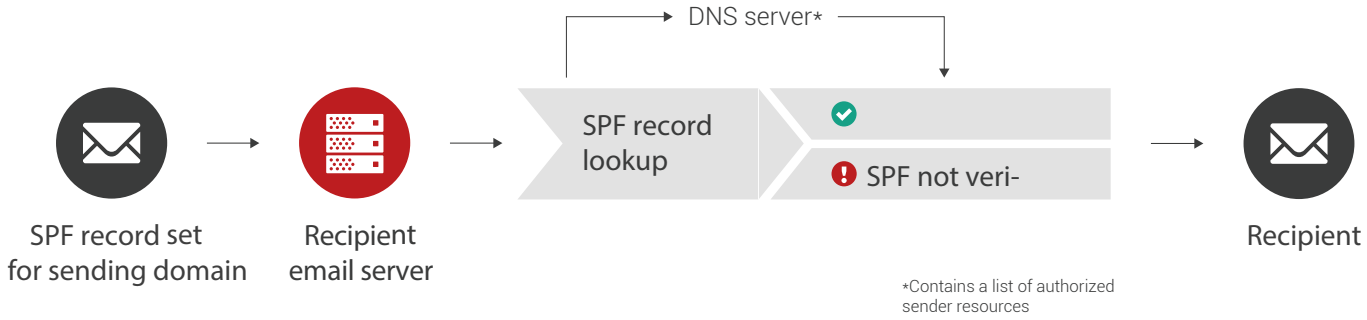
Ratio of accepted emails
The number of accepted emails compared to the total number of sent emails. To obtain this ratio, the number of read emails is divided by number of sent emails.

Ratio of unknown contacts
The number of unknown contacts or invalid email addresses is compared to the number of sent emails.

SPF record

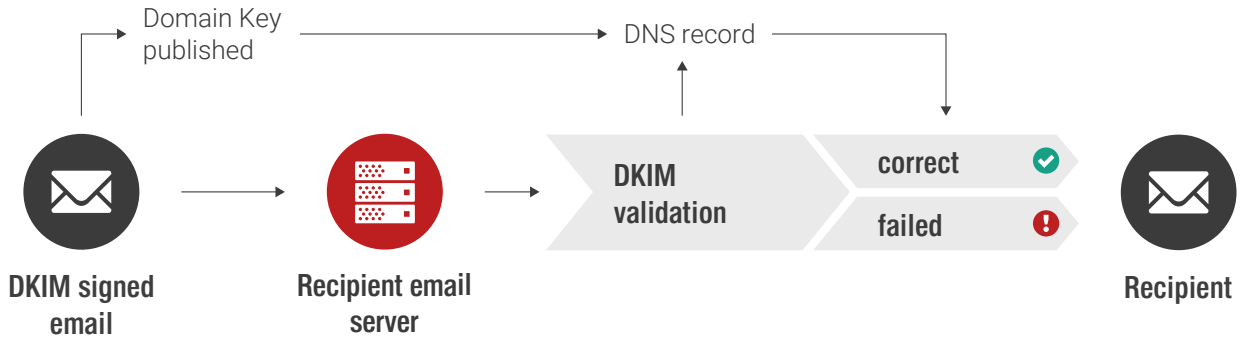
The Sender Policy Framework (SPF), formerly known as Sender Permitted From, is a method designed to prevent the falsification of email sender addresses. It was created as a way to prevent spam. SPF is a record in which the owner of a domain listed in the Domain Name System specifies which computers are allowed to send emails for this domain.

The administrator of a domain saves a TXT resource record (RFC 7208 has rendered the SPF resource record obsolete) in the DNS zone. These resource records contain the IP addresses of the mail transfer agents (MTA) that are permitted to send emails for that particular domain. Using the domain specified in the MAIL FROM and HELO fields, the recipient verifies whether the sender is authorized to send the email. The recipient calls up the SPF information via the Domain Name System for the specified domain and compares the IP address of the sending MTA with the permitted addresses. If the IP addresses match, the sender is authentic. If not, the email can be discarded.



DKIM

DomainKeys is an identification protocol that verifies the authenticity of email senders. It was designed to help prevent and stop unwanted emails such as spam or phishing emails. DomainKeys are based on asymmetric encryption. The email is given a digital signature that the recipient server can verify using the public key, which is available in the Domain Name System (DNS) of the domain. If verification fails, the recipient mail transfer agent (MTA) or the recipient application program can refuse the email or sort it out from the others.



Other definitions in the transactional world of email

Inbox placement rate
Deliverability rate minus the number of emails that landed in a spam or junk email folder

Soft bounce
Emails sent to existing addresses that could not be initially delivered

Hard bounce
Emails that could never be delivered

Opening rate
Number of openings divided by the number of delivered emails

Unique click rate
Number of single clicks in an email by a user (no repeated clicks) divided by the number of delivered emails

Total click rate
Number of all clicks in an email divided by the number of delivered emails

Click to open rate
Unique click rate divided by the opening rate

Conversion rate
The number of targeted actions divided by the effective click rate

Bounce rate
The number of bounces divided by the number of delivered emails

Risks and pitfalls

A current study conducted by Return Path, an email intelligence company, determined that 20 percent of sent and desired emails do not reach their intended recipients. Undelivered emails hurt a company in two ways:

- There is a correlation between a marketing campaign with a smaller reach and a loss of revenue. The revenue potential that lands in spam folders each year in Germany is estimated to equal approximately 3 billion euros.
- Yet companies incur more than just financial loss when emails are mistakenly classified as spam. The reputation of the company and the brand also suffers when sender addresses appear on blacklists and the company receives a negative rating as an email sender.

Causes of spam classification

There are many reasons an email is classified as spam: spam traps, cold IPs, the design of the email, and reputation scores. It is natural that users want to use security software to protect their email inboxes and computers from attacks that are sent through the Internet. It is advisable to consider a customer's security needs when planning email marketing activities.

BLACKLIST

Definition

- Directory of IP addresses and domains that are classified as negative because they send unwanted emails
- Emails sent via these IP addresses are intercepted and blocked
- Large email providers typically have multiple blacklists

Advantages

- Protects the user from undesired communications

Disadvantages

- Desired emails are placed on the blacklist, e.g. if a blacklist blocks an entire domain even though only one subdomain is sending spam emails
- The sender suffers loss of revenue and damage to the company's image; campaigns that are sent via this IP address are no longer delivered
- Time-consuming delisting. It is possible to be deleted from a blacklist. However, if the sender commits multiple offenses, he will eventually be placed permanently on the blacklist
- Unfair business practices

GREYLIST

Definition

- Rejection of an unknown email address and/or IP address on the first attempt at delivery
- A subsequent second attempt is usually successful

Advantages

- Effective spam prevention: many spammers give up after the first try. Real email servers typically try to deliver a second time
- After successful email delivery, the combination of sender, recipient, and email server is entered in the whitelist and subsequent emails are delivered
- Greylisting impacts the quality of the email. Thus, there is no automatic opt out

Disadvantages

- With greylisting, an unwanted email can be delivered a few minutes or even a few hours later
- As soon as the first attempt is made, some email server programs generate a temporary delivery report for the sender, which can be interpreted as failed delivery in some cases
- Using IP tools could negatively impact the success of email delivery

Guidelines for good deliverability

Deliverability is one of the most important keys to professional email marketing. The quality of the systems used by companies to send email campaigns is important. They must be able to maintain high deliverability rates and be expandable.

Warming-up unknown IPs

The reputation of IP addresses is primarily based on historical sending patterns and volumes. An IP address that sends consistent volumes of emails over a long period of time typically means it is a highly reputable address. Companies that use dedicated IP addresses maintain their reputation as a sender by sending consistent and predictable volumes of emails. Therefore, Retarus recommends the following when warming-up a dedicated and unknown IP address:

- Duration of warm-up process: 6–8 weeks
- Start by sending a low volume of emails:
  - » Max. 1,000 emails on day 1
  - » Double the volume based on the previous day
  - » Start with controlled dispatch speed
  - » Slowly increase the volume, number of recipients, dispatch speed
- Cleanup the user list in parallel
- Use all available IPs and domains regularly so they remain known and are considered trustworthy
- Do not implement a sudden and extreme ramp-up
- Keep the risk of blacklisting to a minimum (beware of spam traps and affiliate campaigns)
- During the warm-up, dispatch attractive campaigns, not strategically important ones
- Focus the initial dispatch on particularly active and interested customers

Delivery rate

Subscription using the double opt-in method improves the quality of the group of recipients. This means that only those recipients who have chosen to register themselves and whose emails address actually exists receive emails.

To increase the delivery rate even further, the recipient of the newsletter can be asked to add the sender to his personal address book

or personal whitelist after registering for the newsletter. This is because desired emails and newsletters are often flagged as spam in the inbox of the subscriber (false positives). Membership in the Certified Senders Alliance (CSA), a central whitelist database that requests additional security measures, can also have a positive impact on the delivery rate.

Reputation

Awareness is always the first step to improvement. Since it takes a while to improve a poor sender score, senders should be aware of their reputations with the first email they send. There are multiple ways in email marketing to verify companies and make adjustments so that senders can improve their sender scores. The following have the greatest impact on the deliverability of emails:

Irregular sending volumes
Sending the same volume of emails consistently is crucial to a company's reputation. Peaks and other irregularities can have a negative impact on its reputation.

Frequency of sent emails
Sending emails consistently has a positive effect on a company's reputation. It does not matter if the company sends emails daily, every other day, or every week. The frequency is based on a company's marketing requirements. It is only important to ensure that emails are sent at regular intervals. If a company's email marketing strategy is well designed and stable, tests can be used to determine the optimal frequency for each target group.

Being blacklisted
There are approximately 50 known blacklists that record which IPs belong to spammers. Retarus has added the largest and most well-known blacklist operators to customer service active monitoring and monitors them. If users of Retarus Transactional Email appear on one of these blacklists despite a warm-up and other measures designed to improve reputation, Retarus Customer Service will support the customer in delisting and will research why the company appears on the list. Users of Transactional Email can use the results to improve their email marketing methods.

Spam traps
One such case is an email address that was once valid but is no longer valid and is therefore shown to the sender as a hard bounce. However, if a mail server registers that a sender regularly sends emails to an invalid address, this email address can become a spam case. This means that senders no longer receive a hard bounce message. Instead they are notified that the emails have been accepted and the corresponding senders have been flagged as spammers. It is advisable to keep an eye on hard bounces and check distribution lists regularly.

Spam reports
Recipients that categorize a sender as a spammer can use spam reports to report them. This damages the reputation of the sender. Therefore, you should regularly check how high your spam quota is. Here's an indicator: there is no need to worry if one email per 1,000 is flagged as spam.

Quality of the user list

Including a subscribe and unsubscribe function is now commonplace for customer-friendly, reputable email senders. One reason for this are the regulatory frameworks that apply to the sending of emails. Compliance with them is required. Sending newsletters is legal only if the recipient has given consent. Whitelist participants must give their consent with source and timestamp.

The unsubscribe function also plays an important role. Each newsletter must contain this option. A customer who can quickly and freely cancel his subscription will not report the email as spam. This is important, otherwise the sender's reputation can be damaged or the sender can be registered in the blacklist. If a customer unsubscribes, his address should be removed as quickly as possible from the distribution list and no more emails may be sent to his address.

Using attachments

ISPs frequently check for typical file types with a high risk potential. These include, in particular, executable files (.exe) or scripts.

.ade	.js	.msh	.ps1xml
.adp	.jse	.msh1	.ps2
.app	.ksh	.msh2	.ps2xml
.asp	.lib	.mshxml	.psc1
.bas	.lnk	.msh1xml	.psc2
.bat	.mad	.msh2xml	.tmp
.cer	.maf	.msi	.url
.chm	.mag	.msp	.vb
.cmd	.mam	.mst	.vbe
.com	.maq	.ops	.vbs
.cpl	.mar	.pcd	.vps
.crt	.mas	.pif	.vsmacros
.csh	.mat	.plg	.vss
.der	.mau	.prf	.vst
.exe	.mav	.prg	.vsw
.fxp	.maw	.reg	.vxd
.gadget	.mda	.scf	.ws
.hlp	.mdb	.scr	.wsc
.hta	.mde	.sct	.wsf
.inf	.mdt	.shb	.wsh
.ins	.mdw	.shs	.xnk
.isp	.mdz	.sys	
.its	.msc	.ps1	

Role-based sender addresses

Role-based addresses are typically company addresses that are not defined by a person but by a job, and are often managed by multiple people or eventually not even used. Some of these types of addresses have high bounce rates and receive spam complaints. Therefore, they are blocked by Retarus upon request. In addition, role-based email addresses may not be used to register for an account.

abuse@	list@	spam@
admin@	noc@	support@
billing@	no-reply@	sysadmin@
compliance@	noreply@	tech@
devnull@	null@	undisclosed-recipients@
dns@	phish@	unsubscribe@
ftp@	phishing@	usenet@
hostmaster@	postmaster@	uucp@
inoc@	privacy@	webmaster@
ispfeedback@	registrar@	www@
ispsupport@	root@	
list-request@	security@	

Strategy and prioritization of campaigns

The right strategy and proper prioritization of campaigns also contribute to maintaining a good reputation. The key to maintaining your reputation includes the following:

Defining the frequency
The time and frequency of sending campaign emails have a significant impact on how recipients categorize the emails. A flood of individual emails within just a few hours will most likely lead to rejection by the recipient. This also has a negative impact on reputation if this feedback impacts the ISP.

Prioritization/addressing targeted groups
It is advisable to send important emails at a time that differs from when less important campaigns are sent. A higher sending volume increases the risk of negatively impacting a company's reputation. Thus, the delivery rate of important campaigns sinks and the defined goal of the campaign is not achieved.

Use differentiated communication channels with clear separation
Separate channels help achieve high delivery rates for campaigns. Campaigns should not be sent from the main domain, but rather from sub-domains. Using dedicated IP addresses is even better.

Email content

The sender may neither disguise nor conceal the commercial nature of emails in the header and subject line of the email. An email is considered disguised or concealed if the header and subject line are presented in such a way that the recipient, before viewing the content of email, is not given any information or is given misleading information about the actual identity of the sender or the commercial nature of the email.

Each email sent must contain an easily recognizable impressum that complies with the applicable statutory requirements.

SUBJECT LINE

- An email should always have a subject
- Keep it short and to the point
- Avoid capital letters and special characters
- Avoid specific words (e.g., SEX, FREE!$, LOAN)
- Ensure there is a correlation between the subject and the content of the email
- Avoid repetitive words

Tips for creating effective emails

Ensure the relevance for the recipient is clear
Focus on a specific topic and make this clear.

Use the above-the-fold space
Place the most important elements of the email at the very top so that they are spotted immediately.

Add appropriate calls to action
Make it clear to the reader what he should do and what he gets for his action.

Give images a file name
Give images a suitable file name so that the reader understands its contents if it does not load.

Avoid spam terms
Do not use terms that have anything to do with money or prizes. This will ensure your newsletters land in the recipient's inbox and are not flagged as spam.

Make social media sharing possible
Include the ability to share the email via social media so that the reader can publish it.

Personalize the email
Recipients feel directly addressed when they read their own names. Therefore, address the recipient by name.

Furthermore, the following applies to the dispatch of emails containing promotional content
The initiator of a promotional email must be clearly recognizable and visible. Each email recipient must be made aware of the option to unsubscribe or opt out from receiving emails at any time. Opting out/unsubscribing from emails must, in general, be easy to do (for example, no access data such as a user name or password should be needed).

Author: Peter Schnäp, Technical Product Manager Transactional Email. Created on 6/5/2018

We would be happy to consult with you on how Transactional Email can help increase your email deliverability:
www.retarus.com/contact