pubconcierge

The Complete Guide for Boosting Email Deliverability

Table of Contents

Introduction

There is a difference between sending emails and potential customers actually receiving them in their inbox. However, emails arriving in spam or junk folders are still considered to be delivered. This is one of the toughest challenges companies often struggle with in their quest of expanding and improving their business. Therefore, the true goal of email deliverability is to get good inbox placement.

In this guide, you will learn tips and get advice on how to increase the open rate of your emails. We'll begin with the basics and move on to advanced methods to cover everything you need to know about boosting email deliverability.

SECTION ONE

First steps for improving email deliverability

1 Use a specific IP address for a transactional email to keep it separate from marketing emails.

Newsletters, transactional emails, reminders, and especially email marketing campaigns, should be treated as separate types of emails. Therefore, it would be wiser to use a dedicated IP and domain name for each one. For example, use the domain “your-company-name.com” for regular corporate transactional emails. For all other emails, use a slightly different domain, such as “your-company-namenews.com”. Segmenting email types into different IP addresses is an important method of maintaining separate reputations.

2 Use dedicated IPs for each domain you send your emails from.

Each domain type must operate on a specific, separate and dedicated IP address. This helps reduce the chance of email providers, such as Gmail or Yahoo, grouping your emails under the “Promotional” and “Other” tabs. Dedicated IP addresses should be something to be considered if you want to better organize and improve your email deliverability.

3 Consider leasing dedicated, reputable IP addresses if you want to ensure your emails are actually received and opened.

If you plan on separating your email types and sending them via specific, dedicated IPv4 or IPv6 addresses, you need to make sure the addresses are not blacklisted and have a well-kept reputation. Therefore, it would be a good idea to reach out to an experienced IP broker and discuss what actual types of IP addresses you need. You can benefit from professional counsel and get to pre-test the IPs to check if they match your needs before leasing them.

4 Make sure the IP addresses you want to use are suitable for the domains you are sending your emails from.

Depending on your mailing strategy and resources, you might end up using more reputable TLDs (Top Layer Domains) such as .com or .org. It is advised to check if the IPv4 and IPv6 addresses you are planning on leasing are suitable for your needs. IP brokers like Pubconcierge offer consulting services and pre-testing sessions for clients who want to make an informed decision and lease the right IP address pool.

5 Send mails only to the users who agreed to double opt-in.

Otherwise, you risk hurting not only your inbox rate, but also the reputation of your IPs and domains. On top of that, your domain might get blacklisted. Nobody wants to clutter their inbox with messages they are not interested in.

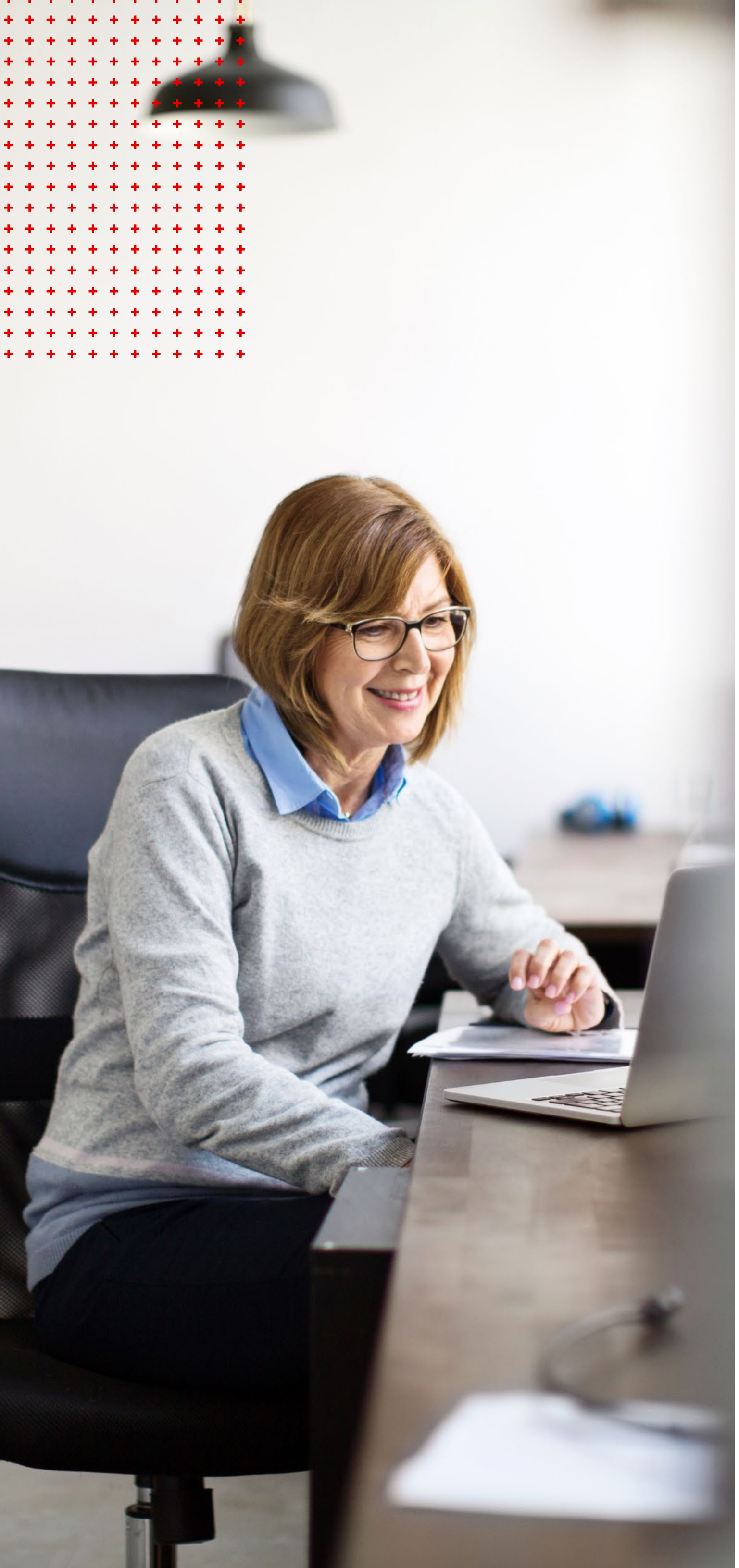
Therefore, make sure you integrate double opt-in confirmation for all of your emails. When a user registers on your site or subscribes to your emails, you need to send them a response. That email contains a link the users must click in order to validate their own email address and confirm they agreed to receive your newsletter.

This will ensure a more careful sorting of your mailing lists and will help avoid damaging the reputation of your IP addresses by sending mails to users who might consider them as spam or junk. Ideally, this will also keep the sign-up logs. Taking the time to make sure you send emails to clients who actually confirmed they are interested in receiving them will boost your success rate exponentially and will build trust between you and your clients.

> “Taking the time to make sure you send emails to clients who actually confirmed they are interested in receiving them will **boost your success rate** exponentially and will build trust between you and your clients.

6 Keep your eyes on your email sending volume and clean your list of any hard bounces.

Most of the emails you are sending should be successfully delivered. The emails that have not been successfully sent were either soft bounced or hard bounced. When an email gets hard bounced, it means you tried to send it to an invalid address. If you get a lot of hard bounces, it’s a signal to mailbox providers that your mailing list isn’t very clean. To avoid this risk, you can do an email validation with the help of platforms like ZeroBounce, which offers a free trial. A soft bounce can occur if the user’s inbox is over quota, if you suddenly increase the volume of your delivered emails or if you email your clients too often for the sake of engagement. Nowadays, most soft bounces happen when there is a sudden increase in email sending volume. If you constantly send, let’s say, 100,000 mails per day and you suddenly send 300,000 mails instead, those extra 200,000 might get throttled. Mailbox providers are sensitive to sudden changes in consistency, so you should carefully manage your volume while keeping in mind these factors.



7 Constantly monitor your sender score.

Domains generally use Sender Score to determine whether or not to allow emails from certain IPs. There are many reasons why your sender score is at risk of decreasing. The most prominent include:

- Content
- Quality of contacts
- Engagement level
- Abuse level
- Sending volume trends

If your Sender Score is below 90, you diminish your deliverability success rate. The average sender score directly influences your average delivery rate.

- Sender score between 91% and 100% → 91%
- Sender score between 81% and 90% → 79%
- Sender score between 71% and 80% → 56%

You can measure your sending reputation by going to SenderScore.org. In this way, you'll get access to detailed reputation reports and other useful information.

Ultimately, managing your sender score is closely related to how efficiently you avoid hard and soft bouncing, and staying away from spam traps (honeypots) while maintaining a clean and up to date database.

8 Warm up your IPs!

This means you have to gradually increase the volume of emails sent with a dedicated IP address according to a predetermined schedule. This gradual process helps to establish a reputation with the mailbox provider as a legitimate email sender and prevent the mailbox provider from labeling your emails as spam. It is recommended that you begin sending a low to moderate volume. After a while, you can start working your way up to larger volumes.

This gives the receiving email providers a chance to closely observe your sending habits and the way your customers treat the emails they receive from you. **There are two ways of warming up an IP address: manually and automatically.** If your dedicated IP is relatively new, you have to warm it up manually. If you are adding new dedicated IPs to existing warm IPs, you can automatically warm up your IP through APIs and platforms by using the second, already warmed up IP address as an overflow for any emails that exceed the hourly limit. This method automatically throttles traffic sent through your new IP according to the platform's own suggested warm-up schedule.

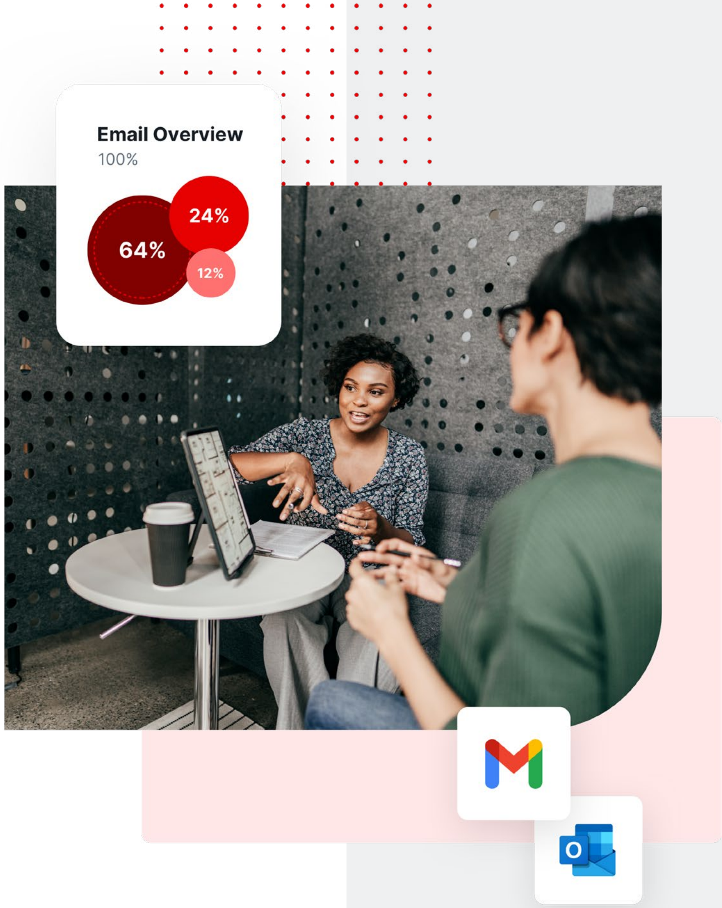
Chances are you opted for a fresh range of dedicated IPv4 or IPv6 addresses, in which case we recommend you warm them up manually. First, you should segment and allocate your IPs accordingly. Then, it is recommended you increase the volume in a slow and careful manner. It is suggested that you should start sending a moderate amount of messages per day from each IP address to each mailbox provider. Afterwards, this volume can be increased by 50% each week, as long as you do not encounter any pushback from the mailbox providers. To get off on the right foot on a new IP , you should consider sending email addresses that have recently clicked or opened an email from you. Email providers are notoriously suspicious of emails sent from new IP addresses, so you might want to be mindful of that.

If the number of recent clickers and openers don't support sending your initial amount of messages per day or the

desired amount of messages per day per mailbox provider on each new IP, then you should consider reducing the number of IP addresses to keep a good volume of email per IP address. In addition, pay attention to the inbox rate. Not progressing past 70% inbox placement at most mailbox providers can lead to your inbox placement stagnating once the warm up process is completed.

The most important pre-warming tips you might want to know:

- Ensure the IP has a pointer (PTR) record set up in your DNS.
- Sign up the IP with all available mailbox provider complaint feedback loops.
- Add the IP address to a Microsoft Smart Network Data Services (SNDS) account so you can monitor the reputation data the service provides.
- Add the List-Unsubscribe header to your email headers. This is an optional header that you can include in your email messages which is designed to help reduce complaints by providing subscribers with an alternative method to safely unsubscribe without negatively impacting your sending reputation.
- Confirm that all email you send from the new IP is authenticated with DomainKeys Identified Mail (DKIM).
- Update your Sender Policy Framework (SPF) record with the new IP.
- Check the IP address to make sure it is not set up as an open relay. Ask your mailbox provider or email administrator to confirm this.
- Make sure your bounce processing is set up and tested, and that unknown users are removed after one bounce.
- Create a new monitoring profile for the new IP in Everest.
- Confirm that you are sending to the seed list from this IP.
- Identify your engaged subscribers, which are those who open, click, and buy, in the following buckets:



- Less than 30 days
- 30-60 days
- 60-90 days
- 90-180 days
- Over 180 days

- Clean up your list by removing malformed domains, unknown users, and unengaged subscribers.

Advice to follow if you are also changing domains:

- If you are using a new d= domain in the DKIM signature, add the new domain to the Yahoo! complaint feedback loop.
- Create a new SPF record, if possible.
- Update the Whois record for each domain with the correct information. Do not use a domain privacy service.
- Create an *abuse@* and *postmaster@* role account for each domain and ensure they are monitored.
- Add the *abuse@* and *postmaster@* role accounts to abuse.net for each domain.
- Create a Domain-based Message Authentication, Reporting and Conformance (DMARC) record for each new domain and set the policy to monitor (p=none).

Here's what you could try in order to streamline the process of email deliverability:

- Start with a low sending volume of 5,000 total subscribers across all mailbox providers.
- Send to your most engaged subscribers first and gradually introduce other segments of your list with less engaged subscribers.
- Double your sending volume every three to four days until you reach your maximum daily volume.
- Don't force through volume just to hit the volume threshold for that day. For example, if you are sending to 10,000 subscribers on day five, but your delivered volume target for that day is for 8,500 subscribers, it's useless to come up with another 1,500 subscribers to make up the difference. Allow for natural daily fluctuations and just cap the volume for the day.

Here is a common warm up schedule you can follow. You can take into consideration warming up your IP addresses depending on the mailbox provider you are sending to. **The following table and guidelines show some generally recommended limits for mailbox providers**, that you should follow in the first 30 days:

- Yahoo: 200 emails/day/IP (for a minimum of 5 days), afterwards you can double every day.
- Gmail: 200 emails/day/IP (for a minimum of 5 days), afterwards you can double every day.
- Hotmail: 200 emails/day/IP (for a minimum of 5 days), afterwards you can double every day.
- AOL: 200 emails/day/IP (for a minimum of 5 days), afterwards you can double every day.
- Cloudmark (all domains): 50 emails/day/IP
- Time Warner: 100 emails/hour/IP
- Cox: 100 emails per connection per IP, up to 5 IPs

IP Warm-up Schedule (Yahoo, Gmail, Hotmail, AOL)

Day	Suggested Daily Volume per IP
1	50
2	100
3	200
4	200
5	200
6	200
7	200
8	400
9	800
10	1,600
11	3,200
12	6,400
13	12,800
14	25,600
15	51,200
16	102,400
17	204,800
18	Double Sending Volume Daily

9 Use health monitors for deliveries, domains and IPs to ensure a proper email deliverability.

Some of the largest mailbox providers offer tools (more on that in the Resources section) that help you monitor many aspects of your email deliverability. These are primarily used to study factors such as:

- Spam Rate
- IP Reputation
- Domain Reputation
- Registering for mailbox provider Feedback Loop
- Authentication (DKIM/SPF/DMARC) rates
- Encryption (if you send emails using TLS - Transport Layer Security) rates
- Delivery Errors (for example: retry sending too fast)

Implement these technical aspects in your plan

1 Use a CAPTCHA to keep automated bots at bay.

Google's reCAPTCHA, for example, is used to prevent such bots from signing up or registering on your site, subscribing to your newsletters and so on. You put your metrics in jeopardy if you send emails to bot registrations or to people that already got registered by a bot. If a great deal of the emails you send are not opened and/or clicked through, the mailbox provider might throw them into the Junk/Spam pile.

2 Try using SPF authentication.

Short for "Sender Policy Framework", this is an authentication protocol that checks whether an IP is authorized or not to send emails for a domain. ZeroBounce offers a useful SPF tester for companies that want to make sure everything runs smoothly. Additionally, you can have a go at Scott Kitterman's SPF Validator.

3 DKIM authentication is a great security tool.

“DomainKeys Identified Mail” allows other mail servers to check the integrity and reliability of the email you sent. In other words, it verifies whether the email received from a specific domain was indeed authorized by the owner of that domain. In addition, DKIM generators can be a notable help in creating a DKIM Record.

4 DMARC authentication prevents phishing attacks and reduces spam rate.

DMARC means “Domain-based Message Authentication, Reporting & Conformance”. It is an authentication tool that helps mailbox providers deal with emails supposedly sent from your company that had failed either SPF or DKIM protocols.

5 A reputable DNS Provider cannot be overlooked.

Email delivery depends a lot on being able to retrieve records from DNS. On top of that, mailbox providers also check the reputation of your nameservers. If you are looking for a good DNS Provider, services like Cloudflare provide DNS Management and a suite of optimization tools, while DYN Managed DNS provides a lot of tools and options to properly secure your DNS. It should go without saying that you absolutely need to get a domain that not only has a good reputation, but one that also has a verified and listed history.

A good practice is avoiding using your domains as soon as you register them, or else they risk getting blacklisted. For this, it is recommended you wait at least 15 to 30 days before using your domain.

> “It should go without saying that you absolutely need to get a domain that not only has a good reputation, but one that also has a verified and listed history.

Therefore, a careful balance between domain management and transparency will prevent you from ending up on Spamhaus DBL (Domain BlockList). You can use this tool to check the status of your domain e.g if it's listed and/or blacklisted.

6 Consider using a reputable CDN.

Also known as "Content Delivery Network", it brings you four main advantages, despite the process of warming-up IPs via links being a bit difficult:

A. Faster load times for images included in the emails you send.
B. Trusted by mailbox providers.
C. DDOS protection.
D. Traditional attacks and exploits are repelled by an advanced firewall.

Among popular CDN providers are Cloudflare, Microsoft Azure CDN and Amazon Cloudfront.

7 Set up Reverse DNS for your sending IPs.

Most mailbox providers require FCrDNS (Forward Confirmed Reverse DNS), which is an rDNS configuration that defines strong relationship between IP and domain. To find out if the FCrDNS is properly set up, you must check if the rDNS of the IP points back to the same IP. Here's how you can find the rDNS manually:

- For Windows machines: Use the nslookup command while specifying the desired IP address → open Command Prompt and type as follows: *nslookup [ip_address]*
- For Linux machines: Use the following syntax: *dig -x [ip_address]*
  Another command for reverse DNS lookup in Linux is: *host [ip_address]*

In either case, the output should display the domain name for the specified IP address. Alternatively, you can use rDNS lookup tools. Some suggestions can be found in the Resources section of this guide.

8 Complaint feedback loops help you keep a clean list.

This is an advantage for both parties, in the sense that feedback loops also prevent unsubscribers from getting unwanted mail. This is a service offered by some mailbox providers that reports back complaints (when a subscriber hits the spam or junk button in their inbox) to the sender. You should register to as many FBLs as possible in order to keep track of your lists and adjust your sending volume accordingly. A list of the most commonly used feedback loops can be found in the **Resources** section of this guide.

For optimal results, it is recommended that you keep user complaints below the indicated rates.

Hotmail < 0.1%	**AOL <= 0.3%**
Yahoo < 0.2%	**Comcast <= 0.5%**

9 Clean your list of bounces, traps, and complainers while verifying if the email is properly set up and configured.

Taking care of these aspects drastically improves your email lists. Furthermore you will increase your list quality, your Sender Score, your domain and IP reputation. All these factors increase your delivery and inbox rates.

10 Don't use too many connections per IP when sending your emails.

The number of connections per IP is limited by each and every mailbox provider. In the chart to the right, you can find some values generally considered safe for the most important mailbox providers.

Number of Connections per IP

Internet Service Provider	Connections per IP address
AOL	150
AT&T	5
Comcast	35
Charter	150
Earthlink	150
Gmail	150
Hotmail	150
Italia Online	1
Lycos	150
Mac.com	150
Orange	3
RoadRunner	150
Swiss.com	5
TDC	10
Telefonica	5
Telenor	5
United	5
USA.net	150
Yahoo	150
Verizon	150

“Knowing when to retry sending your mails will greatly help you keep the emails going and maintain a good relationship with the mailbox provider.

11 Stick to a specific schedule when retrying temporary errors.

Mailbox providers almost always use Greylisting to reduce spam. This technique is also known as Temporary Errors, or SMTP 451. When these conditions occur, the mailbox provider expects your mail server to retry sending a specific email at a later time. When attempting to send the email again, you must use the same IP, as rotating the IP will just get the email greylisted again.

It is generally considered that retry times should be configured as follows:

- For the 1st retry: wait 15 minutes
- For the 2nd retry: wait 45 minutes
- For the 3rd retry: wait 2 hours
- For the 4th retry: wait 6 hours
- For the 5th retry: wait 12 hours

Pay attention to such processes, as some errors can significantly hinder your progress. Knowing when to retry sending your mails will greatly help you keep the emails going and maintain a good relationship with the mailbox provider.

For a better understanding of SMTP Error Codes, it’s useful to know what they mean. SMTP (Simple mail transfer protocol) is used to send emails across the network via an MTA (Mail Transfer Agent). It is possible sometimes that the response from the client’s server SMTP server will return a specific error code. Therefore, it would help you to refer to these common classifications and codes in order to better understand what you might be dealing with.

Status codes are generally classified into five different groups. Let’s take a look at them and then examine the most common Basic Status Codes.

Status Code	What does it return?	What does it actually mean?
1xx	informational code	Your request is received successfully and sent for further processing
2xx	success code	Your request is understood and accepted
3xx	redirection code	Your request needs few actions to be taken so that request is completely accepted
4xx	clients error code	Your request is incorrect. It might be a syntax issue or it has an issue that can't be resolved.
5xx	server error code	Your request was valid but the server failed to process due to an internal error on the server

Each status code has a registry, so let's break them into all their respective descriptions:

Status Code	Code	Description
2xx	214	A response to the HELP command
2xx	220	The server is ready
2xx	221	The mail communication channel is getting closed
2xx	250	Requested mail action okay completed
2xx	251	Email will be forwarded because the server was not able to find the user locally.
2xx	252	Cannot verify the user, but it will try to deliver the message anyway
3xx	354	Start mail input
4xx	420	Time out connection problem
4xx	421	Service is unavailable
4xx	422	This error happens when the size of the email exceeds the limits of the recipient's mailbox. The connection will drop during transmission when the email server starts to deliver the email.

Status Code	Code	Description
4xx	447	Maximum number of recipients per email exceeded.
4xx	450	User mailbox is unavailable
4xx	451	Requested action aborted: local error in processing
4xx	452	Too many emails sent / too many recipients
5xx	500	Syntax error, command unrecognized
5xx	501	Syntax error in parameters or arguments
5xx	502	Command not implemented
5xx	503	Bad sequence of commands
5xx	504	Command parameter is not implemented
5xx	521	Server does not accept mail
5xx	523	Size of your mail exceeds the server limits
5xx	530	Authentication required
5xx	541	The recipient’s server rejected your message
5xx	550	Mailbox unavailable
5xx	551	User not local or invalid address
5xx	552	Exceeded storage allocation
5xx	553	Mailbox name invalid
5xx	554	Transaction has failed

*This table indicates the most important Basic Status Codes. These are often followed by Enhanced Status Codes. For an in-depth look at Enhanced Status Codes, head to IANA’s Simple Mail Transfer Protocol (SMTP) Enhanced Status Codes Registry

Ensure your domain/IPs are not on any blacklists!

Many companies use the same blacklist providers, so being listed on a single blacklist can unfortunately affect your delivery to many different mailbox providers. Some of them use multiple blacklists, so it's very important to monitor all aspects of your sending. For this, blacklist checkers are your best friends.

Let's have a look at the most common types of blacklists:

- Public - These are publicly available so any mailbox provider can use them. They are the easiest ones to monitor using automated tools.
- Private - The only way to actively monitor these is to use inbox testing tools to verify your delivery.
- Internal - They can be monitored using inbox testing tools. However, they are maintained by mailbox providers directly.

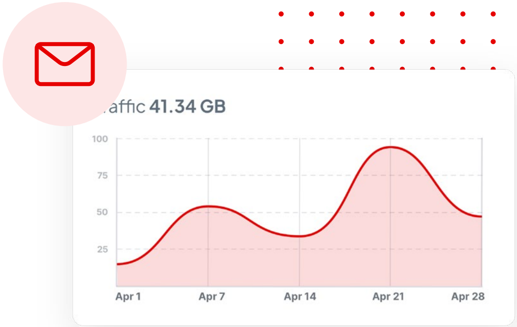
Head to our Resources section to see a comprehensive list of places where you can check if your domain/IP address is on a public blacklist.

Additionally, whitelisting services can help mitigate this "damage". There are many high-quality online services that help you with whitelisting, but most of the time you will need to wait around 90 days for the process to complete, mostly because whitelisting services need to check your sending history. Our **Resources** chapter provides a list of free and paid whitelisting services that you can try.

Ultimately, compliance and respecting the laws will make whitelisting much easier. It is important to promptly comply with the law: CASL for CA (Canada), CAN-SPAM for US, DPEC for EU and other local anti-spam laws. In addition, you should honor all the unsubscribe requests. As fast as possible. Whether it's an automatic unsubscribe link or manually requested, seeing to these matters not only means adhering to a good and ethical business practice, but it will also help your lists stay clean and keep a good email score.

It should go without saying that you must avoid spam traps (also called honeypots) at all costs! These are email addresses owned by mailbox providers. If you send an email to that address, it will severely damage your sender reputation. Hitting a lot of spam traps is one of the worst things you can do to your sender reputation.

To sum up: devise a well thought out improvement plan!



Email marketing is one of the most complex aspects of modern businesses. Therefore, companies have to carefully adapt their strategy to both comply with the law and improve their email deliverability rate.

There are enough deliverability factors that you can control well enough in order to achieve an optimal delivery rate and even boost it significantly. However, you do need to be mindful about several other concepts as well.

Sending high volumes of emails while keeping a good sender score and adhering to good business practices is an art and should be treated accordingly. Treat technical aspects with equal conscientiousness. In the end, here are some of the most important aspects that need to be considered.

1. Use a dedicated IP address and domain for each type of email you send.
2. Carefully and constantly keep track of the frequency and relevancy of your emails. Be careful with your email sending volume to avoid soft bounces.
3. Warm up your IPs! Never send too many emails at once. For the first 30 days respect the limits mailbox providers usually have.
4. It is much easier to avoid winding up on a blacklist than to try and remove yourself from one.
5. Keep your mailing lists squeaky clean, your creatives on point and your mailing method carefully managed.
6. Avoid spam traps!
7. Build a strong and trustworthy relationship with the mailbox provider.

Glossary

CDN - Short for “Content Delivery Network”. It is a group of geographically distributed and interconnected servers. They provide cached internet content from a network location closest to a user to speed up its delivery.

DBL - Short for “Domain BlockList”. It is a list (such as Spamhaus DBL) of domain names with poor reputation.

DKIM authentication - Short for “DomainKeys Identified Mail”. It allows you to sign your email so that other mail servers can check the authenticity of your email.

DMARC authentication - Short for “Domain-based Message Authentication, Reporting & Conformance”. It is an authentication tool that helps mailbox providers deal with emails supposedly sent from your company that had failed either SPF or DKIM protocols.

DNS - Short for “Domain Name System”, it is the naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks.

Email Domain - The part that comes after @ symbol in an email address (such as @yahoo.com, @gmail.com, @hotmail.com).

Mailbox provider - An email hosting provider which implements email servers to send, receive, accept, and store email for other organizations or end users, on their behalf . The most popular examples include Yahoo, Gmail, or Hotmail.

FCrDNS - Forward Confirmed Reverse DNS is a DNS technical configuration that shows a relationship exists between an IP address and a hostname. An FCrDNS proves that an IP address is using a sending domain that has the same owner. This relationship provides a form of authentication that some mailbox providers prefer in their spam filter methodology.

FBL - Short for “Feedback Loop”, also known as “Complaint Feedback Loop”, it enables a mailbox provider to inform a sending organization about spam complaints submitted by recipients of their messages.

ISP - Short for Internet Service Provider, an organization that provides services for accessing, using, or participating in the Internet.

PTR - Short for “Pointer Record”, is the data verifying that the IP address matches the domain name, and it’s the reverse of the “A record,” which provides the IP address associated with the domain.

rDNS (Also known as Reverse DNS) - The querying technique of the Domain Name System (DNS) to determine the domain name associated with an IP address.

Sender Score - Sender Score is a service that rates the reputation of every outgoing mail server IP address on a scale from 0-100. If you want to quickly check your sending reputation head to SenderScore.org.

SNDS - Short for “Smart Network Data Services”. This is a free service offered by Outlook. It is primarily used to gain insight into some important data about a marketer’s sender reputation and email deliverability to Microsoft mailboxes.

SMTP - Short for “Simple Mail Transfer Protocol”. It is used by mail servers to send, receive, and/or relay outgoing mail between email senders and receivers.

Spam Trap (also known as Honeypot) - An email address that is not used for communication but rather to identify and monitor spam email.

SPF authentication - Short for “Sender Policy Framework”, this is an authentication protocol that checks whether an IP is authorized or not to send emails for a domain.

TLD - Top-Level Domain is the final part of domain names (such as .org and .com). Different domain name registrars can register different DNS.

TLS - Short for “Transport Layer Security” is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP).

Resources

- Tools for SPF Testing:
  - ZeroBounce - Mail Tester
  - Scott Kitterman’s SPF Validator
- DKIM generators you can use to create your DKIM Record: EasyDMARC
- DKIM tools that will sign your emails:
  - Exchange DKIM Signer
  - Limilabs Mail.DLL Component
  - Email Architect DKIM For Exchange and IIS SMTP Service
- DMARC Generator: MXTOOLBOX
- Some DNS Providers:
  - DYN Managed DNS
  - Cloudflare
- A few CDN Providers:
  - Cloudflare
  - Microsoft Azure CDN
  - Amazon Cloudfront
- Some popular online reverse DNS tools you can try:
  - DNS.Google
  - MXTOOLBOX
  - WhatIsMyIP
  - Hacker Target
  - WhatIsMyIpAddress
- Some major ESPs that provide FBLs:
  - AOL
  - Bluetie
  - Comcast
  - Cox
  - Earthlink
  - Gmail
  - Hotmail
  - Mail.ru
  - Rackspace
  - Synacor
  - Terra
  - Tucows
  - Yahoo!

- A useful service to monitor your domain's health when working with Gmail: Google Post Master
- Easily check if your IP/domain is blacklisted at multirbl.valli.org. To see if the IP/domain is blacklisted, but not included in a certain automated blacklist check, try the following:
  - Barracuda Central
  - Sophos Threat Center
  - Symantec IP Reputation
  - Cloudmark IP Remediation Portal
  - Proofpoint IP Reputation Lookup
  - Trend Micro IP Lookup
  - GoDaddy's Secure Server
  - Hetzner Online
  - Invaluement
  - Manitu
  - Linux Magic
  - Weighted Private Blacklist
  - SURBL Blacklist
  - HRBL Blacklist
  - Cyren IP Reputation
  - (Cisco) Talos Reputation
  - WIFI4INDIA Blacklist Lookup
  - SonicWall
  - Postmaster.Free.FR

Where can you try whitelisting your IP addresses?

- Free whitelisting services
  - DNS WL
  - inbox.lv
- Paid whitelisting services
  - Return-Path
  - CSA (Certified Senders Alliance)
  - ISIPP
- A free website that helps you check your sending reputation: SenderScore.org
- A comprehensive section that detalis SMTP Enhanced Status Codes can be found on the IANA website

References

1. ZeroBounce - The Guide to Email Deliverability - Email Marketing Done Right
2. Bloomreach - The Ultimate Guide to Mastering Email Deliverability (2022)
3. Cakemail Blog - The Email Deliverability Guide
4. Validity Help Center - How to warm up an IP address
5. Green Arrow Documentation - IP Warm-Up Recommendations
6. Netcore - Everything you need to know about SMTP Error Codes
7. Drip.com - 8 Best Practices to Improve Your Email Deliverability
8. Mailgun - How to improve your email deliverability in 2022
9. Campaign Monitor - 4 Steps To Improve Email Deliverability
10. Concep - Strategies to improve email deliverability in professional services
11. Common Product Notification Errors (and Solutions) - Courier.com