ZOHO

Zoho Campaigns

Email Deliverability 101

Table of contents

Chapter I
What is email deliverability?

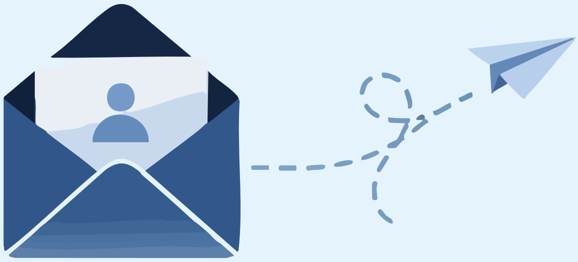
As a marketer, you're well aware it takes an immense amount of time to meticulously design and craft email campaigns full of easy-to-grasp content. Once everything's done, you hit the send button and heave a huge sigh of relief. One day passes, then a couple more days; a week passes; and even by the time a fortnight has passed, you've only received a single reply. To your disappointment, you learn that the vast majority of the emails you sent have landed in spam or never reached your intended audience. You don't know why this has happened or what went wrong. The principles of email deliverability we'll discuss here exist precisely to prevent such incidents from occurring.

So, what is email deliverability? The term refers to your ability as a sender to deliver emails that land in your recipients' primary inboxes. You could consider any email that doesn't land in a recipient's primary inbox as having low or no email deliverability.

When emails land in spam folders or aren't delivered at all, it can be devastating for businesses who rely primarily on brand promotion via email campaigns.

What should you do when this happens? You must—with a big emphasis on must—ensure you're following the best email deliverability practices. In fact, if you're a business just starting out, take the time to understand email deliverability and start tracking it—before you even send a single test email. That's how crucial it is.

Now that you understand what email deliverability is, let's discuss whether it's something you need to consider or not.



Chapter II

Is email deliverability important?

Ah, the all-important question. In short: yes—it's not only important, but something you should actively seek to achieve. Email deliverability is important for every business that sends emails from their own domain irrespective of their purpose.

To avoid landing in spam folders—that is, to make sure your emails get delivered to your audience's primary inboxes—it's essential that you understand the principles of email deliverability. Imagine it to be this magical portal behind which exists a whole new world. To pass through this portal, you must meet some conditions, and once those are satisfied, your email traverses to the primary inbox. This opens up an opportunity for engagement, business growth, creating relationships with your audience, and gaining traction.

So, what if you don't need it? As a business, you'll lose out on opportunities to attract clients, leading to stagnancy and potentially even losses. Moreover, the big players like Google, Yahoo, and Microsoft Outlook will like you if you follow email deliverability practices because they've strict measures in place to prevent spam and unauthorized senders – you needn't get on the wrong side of them.

If your email deliverability is low or poor, your emails have pretty high chances of landing in spam. Emails landing in spam means it's not reaching your audience, which in turn leads to you losing out on actual opportunities to do your business – which is why you would've spent an eternity creating beautiful campaigns in the first place. You've got to act now to prevent this from happening further.

You'll learn in detail about the various practices involved in email deliverability as you traverse through this book.

Chapter III

Deliverability Rate

You may have noticed that we mentioned email deliverability being low or poor in the last chapter. Yes, we understand what's on your mind. So, yes, you can quantify (to some extent) email deliverability using a concept called **Deliverability Rate**. It's the percentage of emails that are landing in your recipients' inbox compared to the total number of mails sent. It's useful for helping you recalibrate your email sending habits. It is calculated as:

$$\text{Deliverability Rate (\%)} = \left(\frac{\text{No. of Emails Delivered to Inbox}}{\text{Total No. of Emails Sent}}\right) \times 100$$

If you send 100 emails out of which 95 emails land in your recipients' primary inbox, then your delivery rate is 95%. Deliverability rate is calculated using online tools like **Google Postmaster**, **MXToolbox**, and many more. A 2024 study by EmailToolTester calculated the average deliverability rate across major Email Service Providers (ESPs) as 83.1%. Below table shows a general classification based on the rate % collated from studies by different tools:

Deliverability Rate (%)	Classification
≥ 95%	Ideal
90-95%	Good
85-89%	Review Needed
70-84%	Problem
<70%	Poor

While you can't solely rely on this metric alone, it is considered one of the crucial aspects of email deliverability along with other factors. In the next chapter, you'll find out about the responsibility factor.

Chapter IV

Responsibility factor

We've covered the what and why aspects of email deliverability. It's time to cover the who now. Who's responsible for maintaining optimum email deliverability? It's a two-way street. Both you (the user) and the Email Service Provider (ESP) you use are equally responsible.

User

If you're using an email marketing software like Zoho Campaigns to deliver your marketing campaigns, you play an important role. You need to be as thorough as possible in ensuring the upkeep of email deliverability. Below are some aspects in which you can do this:

- Remember that how your subscribers interact with your emails (opening, clicking, or even marking them as spam) reflects directly on you.
- Build and maintain a clean, permission-based list of people who actually want your emails.

- Make sure your domain is properly set up with authentication protocols like SPF, DKIM, and DMARC.
- Keep the content you send relevant; if it feels like spam, people will treat it like spam.
- Finally, be mindful of how you send emails—how often, how much, and how consistently.

Email service providers

An ESP is a software tool you use to send emails to large audiences of people. It not only enables you to send emails in bulk, but also provides vital functions like building and designing campaigns. Zoho Campaigns is an example of an ESP.

- Doing the heavy lifting in the background with technical aspects
- Managing the reputation of shared IP addresses (unless you're using a dedicated IP address)
- Equipping you with tools, insights, and best practices so you can monitor your performance and improve deliverability
- Providing and maintaining the technical infrastructure that sends your emails

Chapter V

Proper list management

Just as you manage contacts on your mobile phone, you should also spend some time managing your mailing list in any ESP you use. This is one of the most important aspects of improving email deliverability.

If you ignore your contacts, they can pile up, and it'll be difficult to know which contacts want to receive your campaigns. You might inadvertently send campaigns to contacts who don't wish to receive them at all—which means they might mark your campaigns as spam and thereby damage your domain reputation. If your reputation keeps tanking, it'll be blacklisted—and that's a serious concern.

Here are some list management practices to follow:

- **No shortcuts:** Don't purchase mailing lists—ever. Don't opt for short-term success by purchasing mailing lists and ignore the long-term loyalty you'll be rewarded with if you grow

- **Go the extra mile:** Use double opt-in instead of single opt-in. This will really tell you which contacts are interested in your marketing campaigns.

- **Segment to increment:** Sending a specific type of campaign to a particular group of contacts will promote growth for your business, as contacts who aren't interested won't receive that campaign.

- **Keep in touch:** Keep your contacts engaged by sending them campaigns periodically. Don't spam them with multiple emails per week.

- **Don't lose hope:** Identify inactive contacts and win them back by enticing them with irresistible offers.

- **Spring cleaning:** Treat cleaning your mailing lists similar to spring cleaning your house; clean them once every six months by removing inactive and unneeded contacts.

Chapter VI

Should you authenticate your domain?

A couple chapters back, you read that one of your responsibilities is to authenticate your domain. Before you ask, **yes**, you **must** authenticate your sender domain. Even before you send an email campaign to your contacts, we strongly advise you to authenticate your domain.

In this busy world, nobody who's running a business has the time to learn the technical aspects of how emails are sent. That's why the ESPs these businesses use have to provide visibility and make it easy for them to authenticate their domains.

What is domain authentication?

Let's say you're the owner of Zylker Inc., you have a website whose address is zylker.com, and your customers can reach you at support@zylker.com. Here, the domain is whatever that appears after "@"—in this case, **zylker.com**. This is the domain you need to authenticate. Generally, you'll host your domain via a domain provider like GoDaddy or WordPress.

But what does it mean to "authenticate" your domain? Domain authentication is a process by which email senders are verified as legitimate so that their emails are delivered, and it involves multiple validation mechanisms.

Without domain authentication, your domain would be susceptible to attacks from spammers or spoofers, which could cause your domain to have a poor sender reputation.

Side note: Spoofing is a cybercrime where someone disguises themselves as a trusted contact or brand to deceive victims and gain access to sensitive personal information.

To simplify, it's like adding your signature and stamp of approval to every email you send. When you send a physical letter, you include a return address to show the recipient that it's really from you. Domain authentication serves the same purpose for emails; it informs inbox providers (such as Gmail, Outlook, and Yahoo) that "Yes, this email is truly from me, and I can verify it."

Without domain authentication, inboxes can't be certain if an email is genuinely from your domain or if a spammer is attempting to impersonate you.

Domain authentication builds trust.

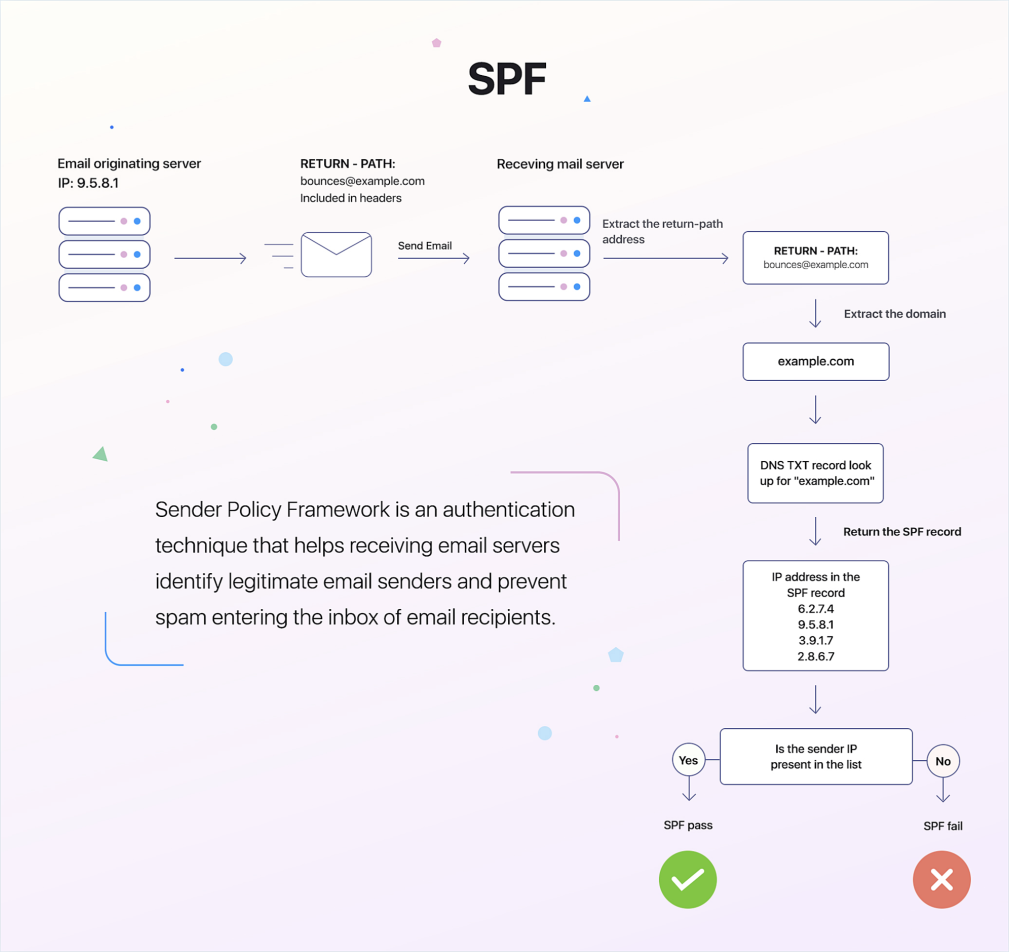
Aspects of domain authentication

There are protocols you should be aware when it comes to authenticating your domain: SPF, DKIM, and DMARC. We'll also learn about BIMI, which is not completely related, but still a topic to learn for marketing your brand.

SPF: A framework for your emails to rely on.

Sender Policy Framework (SPF) is not at all related to sunscreen, but there's an analogy we can make to help you understand SPF.

Think of SPF as sunscreen for your email domain. Just as sunscreen protects your skin from harmful UV rays, SPF protects your reputation by blocking fake emails. When you send an email, the recipient's email server checks your domain's SPF record to see if the sending server is approved. If the server isn't on that list, the email is treated as suspicious, because a spammer might be pretending to be you.



Sender Policy Framework is an authentication technique that helps receiving email servers identify legitimate email senders and prevent spam entering the inbox of email recipients.

Why do you need it? Without SPF, malicious users could impersonate your domain and send harmful emails, which leads to trust issues, spam filters, or blacklisting. Setting up SPF correctly shows which servers are allowed to send emails from your domain, which helps protect your brand, subscribers, and email deliverability.

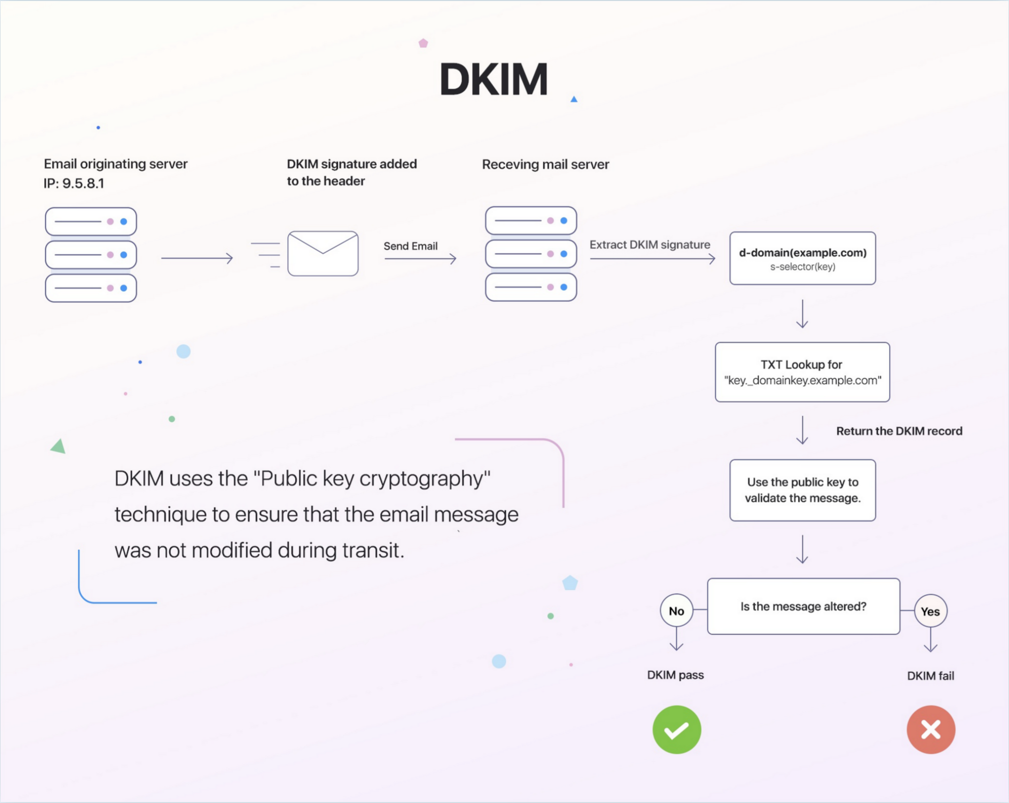
SPF isn't the only aspect of domain authentication; it works in tandem with DKIM and DMARC. You can learn about SPF and its inner workings in greater detail via our useful help resource here.

DKIM: The hidden hero

DomainKeys Identified Mail (DKIM) is another authentication technique. Deploying DKIM prevents emails from being accessed and tampered during transit from sending server to receiving server. It also prevents phishing and spoofing attacks.

Side note: Phishing is a cybercrime that uses fake emails, websites, or messages to trick people into sharing personal or financial data.

Here's another helpful analogy: DKIM is akin to signing your letter with a wax seal. During olden days, a wax seal was a strong indicator that a letter genuinely originated from the sender and hadn't been tampered with during transit.


DKIM

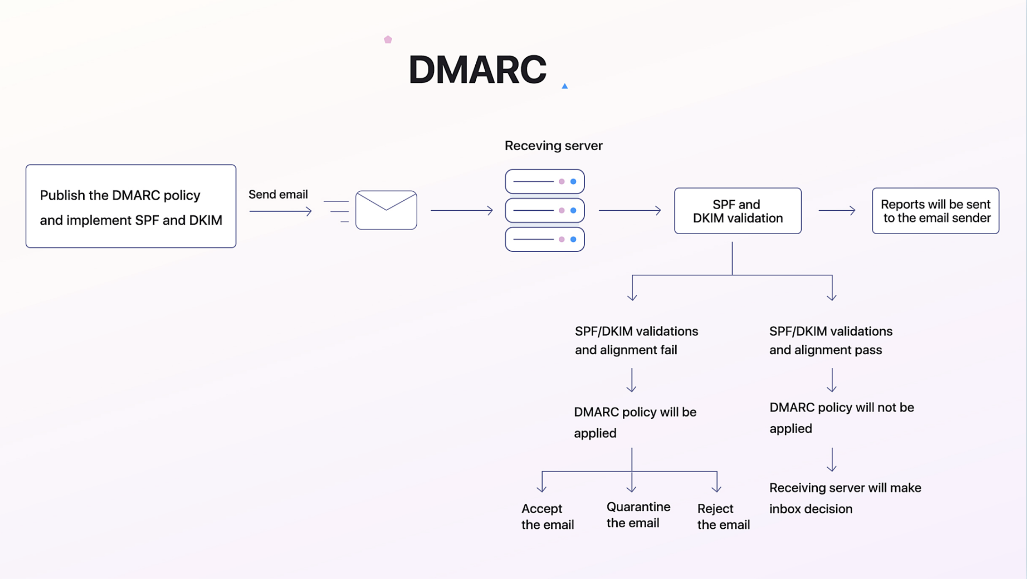
DKIM uses the "Public key cryptography" technique to ensure that the email message was not modified during transit.

DKIM does the same for your emails. When you send an email, your domain "signs" it with a hidden digital signature. The recipient server checks that signature against your domain's public record. If the seal matches, the email is authentic; if not, it may have been altered in transit.

For a more in-depth understanding of DKIM, this help resource is a good starting point.

DMARC: Disruptor of disrepute

Domain-based Message Authentication Reporting and Conformance (DMARC) is a domain authentication technique that improves email deliverability and prevents spoofing. DMARC requires SPF and DKIM to be present, so you first need to authenticate your domain by publishing SPF and DKIM records.


DMARC
Publish the DMARC policy and implement SPF and DKIM
Send email
Receving server
SPF and DKIM validation
Reports will be sent to the email sender
SPF/DKIM validations and alignment fail
SPF/DKIM validations and alignment pass
DMARC policy will be applied
DMARC policy will not be applied
Accept the email
Quarantine the email
Reject the email
Receiving server will make inbox decision

You (the sending server) will be required to publish a DMARC record for your domain. Use any online tool recommended by DMARC.org to generate this record. Publish that DMARC as a TXT record in your domain's domain name system (DNS). Without DMARC, an email that fails SPF or DKIM might still sneak through. With DMARC, that isn't possible; it prevents any disrepute to you or your domain. And as we've established, your domain's reputation is paramount when it comes to having good email deliverability rates.

Side note: High-volume senders (> 5,000 emails/day) are required to implement DMARC policy and conform to DMARC alignment.

Refer to our [detailed help document]() on DMARC for further reading.

How to authenticate your domain

This is the most important question, as the domain authentication needs to be done by the user who's using the ESP to send email campaigns. The process is generally quite simple, but we can't provide a universal how-to guide, as different ESPs have different navigation steps.

Still, the basic steps will involve you going into your ESP's domain settings to copy their SPF and paste it as a TXT record in your domain's DNS. You'll do the same for DKIM. After that, you'll wait some time (probably around 24 hours) for the records to get populated, upon which time you'll return to your ESP to authenticate the domain.

Side note: If you're sending 5,000 emails per day to Gmail and/or Outlook users, both Google and Microsoft have mandated that your sender domain be authenticated (i.e., your SPF, DKIM, DMARC are published), avoid sending unwanted emails, provide a one-click unsubscribe option, and maintain list hygiene.

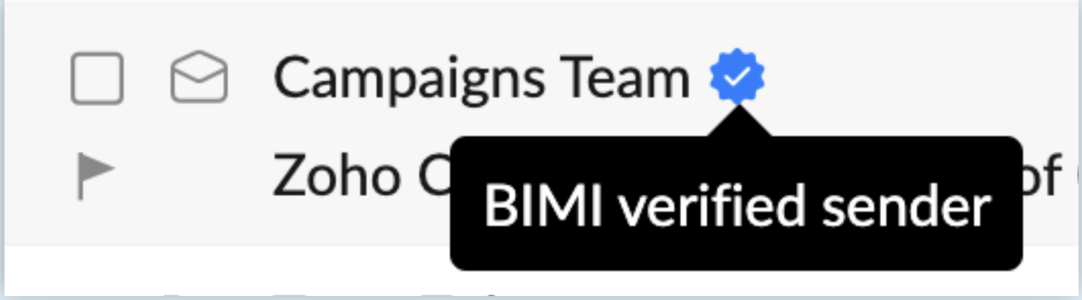
For Zoho Campaigns, you'll first add the sender domain and verify it. Next, you'll copy the SPF record and paste it in your domain's DNS, and then do the same for DKIM. After waiting for some time, you can authenticate your domain in Zoho Campaigns. You can find the detailed steps to authenticate your domain here.

There are many domain providers, and each of them have their own steps for pasting SPF and DKIM records. We've documented some of the most widely used domain providers and their navigation steps here for your reference.

BIMI: A badge for your brands

While Brand Indicators for Message Identification (BIMI) doesn't constitute an authentication technique per se, it's worth mentioning because it does add a layer of authentication to your emails. BIMI displays your brand's logo in the emails you send, which acts as a visual layer on top of domain authentication.
To implement BIMI, you must already have implemented SPF, DKIM, and DMARC. You know those check marks you see on social media pages next to account names? That mark signals authenticity. BIMI does the same for your brand's name and email address.

Check out the image below from Zoho Mail, which is one of the few email clients that supports BIMI. When you click the email, the brand's logo will be displayed as well.



BIMI isn't mandatory, but it's an added advantage for your brand. The benefits of BIMI include:

- **Instant brand recognition:** Your logo shows up beside your emails, making it easier for subscribers to spot you in a crowded inbox.
- **Strong trust:** A verified logo reassures recipients that the email is really from you—reducing the chances of phishing or impersonation.
- **High engagement:** Familiar branding can increase open rates because people are more likely to click on emails they recognize.
- **Professional image:** Displaying your official logo makes your emails look professional and credible.
- **Competitive advantage:** Not all senders use BIMI yet, so early adoption helps your emails stand out.

For further reading on BIMI, check out this help document.

Chapter VII

Zoho Campaigns' role in email deliverability

For the uninitiated, Zoho Campaigns is a powerful all-in-one email and SMS marketing solution. You can create campaigns and send them to your contacts—from scratch or using templates you can build using Zoho Campaigns' intuitive drag-and-drop builder.

- **Lists and segments:** Easily send campaigns to multiple mailing lists that consist of thousands of contacts. Segment your contacts based on location, demography, psychographic traits, or company type.
- **Analytics and reporting:** With just a few clicks, you can find detailed reports on key performance metrics such as bounce rates, clicks, and opens. These are helpful in understanding where you can improve.
- **Backend infra:** Zoho Campaigns uses robust infrastructure and servers to send campaigns—from its own servers.
- **Your own IP:** You can have your own dedicated IP address to send campaigns instead of using a shared IP address.
- **Unsubscribing:** Zoho Campaigns mandates that users enable recipients to opt out of emails.
- **Organic contacts:** You can collect contacts organically via signup forms and a double opt-in method so that you have only contacts who are interested in your emails.
- **Stringent compliance:** Zoho doesn't allow anything violations of its terms or privacy policy.

Chapter VIII

Shape your content

The way you present the content matters a lot, because if you overdo it, you might catch the attention of spam filters.

If people find your content boring, uninteresting, or useless, they won't hesitate for even a second to mark your campaigns as spam.

Regardless of how fantastic your email's design looks, if its content doesn't resonate with your audience, you can't expect to reap the rewards of your hard work. If you try too hard to impress your contacts with unnecessary and spammy content, you'll get

- You should provide a proper introduction in your emails.
- Your subject line should be short, simple, and feel personalized. Include a pre-header as well.
- Avoid catchy and attention-seeking words; don't overuse punctuation marks and emojis.
- Always include the option to unsubscribe from your emails.

Chapter IX

Domain warm up

If you're just now venturing into the world of email marketing, that means your sender domain is pretty new and hasn't been used that much for sending campaigns. Hence, you need to warm up your sender domain, because you can't send thousands of emails per day from a new sender domain—as that can affect its reputation.

New sender domains, or rarely used old ones, are considered "cold" and need to be "warmed up" before they can be used. Warmed-up domains will have improved email delivery rates.

Before warming up a domain, follow this checklist:

- **Authenticated domain in Zoho Campaigns:** SPF, DKIM, and DMARC records should be published.
- **Proper mailing list management:** Ensure you've added contacts organically and that they're double opted-in.
- **Business domain:** Your domain should be a business domain and not a public sender domain (@gmail.com, @yahoo.com, @hotmail.com).
- **No invalid email addresses:** Remove email addresses of contacts that return errors, contain typos, are expired, or address entire roles/groups.

- **Proper setup:** Set up tools to check your spam complaints, delivery errors, and other important metrics. For example, if your contact base has a lot of Gmail users, use Gmail's Postmaster Tool.

Side note: Gmail and Outlook offer inbox placement mostly for emails that keep their contacts engaged and that are sent from sender domains with positive reputations.

Warming up a domain involves sending a limited number of emails during the starting stage and gradually increasing the count as your delivery rates and domain reputation build. To initiate the warm-up process:

- Start by sending campaigns to contacts who've recently signed up or engaged with you, as they're more likely to show immediate interest.
- Segment your mailing list to focus on contacts genuinely interested in your offerings. Send to them regularly—but not excessively—to maintain engagement without overwhelming them.
- Zoho Campaigns recommends beginning with a daily send rate of 5 to 10% of your total recipients. Avoid sending large volumes initially. As your delivery rates and engagement improve, gradually increase your volume by about 5% per day. For larger lists, start with 50 to 100 contacts and scale up by 50 per day.

- If you notice poor deliverability, high unsubscribes, or spam complaints, roll back your sending volume until these issues stabilize, then increase gradually.

- Continuously monitor key metrics—open and click rates, bounces, unsubscribes, and spam complaints—to decide when to scale up or slow down your campaign volume.

What if you don't warm up your domain? You have to be prepared to face the repercussions, which are:

- **Emails getting rejected:** Many email clients like Gmail, Outlook, and Yahoo have strict anti-spam filters that block emails from domains that lack solid reputations.

- **Emails landing in spam:** Inbox placement depends heavily on your sender domain's reputation. Sending large volumes from a new or untrusted domain will likely cause your emails to end up in the spam folder.

- **Low engagement and growth:** When your emails don't reach the primary inbox, you lose valuable opportunities to engage with your audience, which directly impacts your campaign performance and business growth.

- **Blacklisted domain:** Frequent spam complaints can severely damage your domain reputation and eventually lead to blacklisting—a major setback that can prevent your emails from being delivered at all.

Chapter X

What to know before doing a blast

An email blast is a single email campaign sent in bulk to hundreds or thousands of contacts. This is especially useful if you want the same content to reach your targeted audience. But you must warm up your sender domain before doing an email blast, because if a cold sender domain isn't warmed up, it'll have a low deliverability rate and its chances landing in spam are high. Once the warm-up is complete, you're ready to do an email blast. Here are some precautionary measures you can take before you perform an email blast:

- **Analyze your contacts:** Check your contacts' email addresses. If the majority of them are from a single email client like Gmail or Outlook, segment them to send campaigns only to those contacts.

- **Increase interest:** Once you've identified your contacts' interests via their search patterns, link clicks, or inquiries they make on your website, you can capture that interest further by sending targeted campaigns.

- **Target those who open:** Try sending campaigns mostly to contacts open them; email clients can analyze your sending patterns, and if they detect that most of your campaigns aren't being opened, your domain reputation may take a hit.

- **Split equally:** If you feel you're sending too many campaigns, you can always split them into equal parts and send them at regular intervals in the same day or across multiple days. If 5,000 emails per campaign (one per contact) is high, you can split it so that you send 1,000 campaigns across five time periods.

- **Use a clean list:** Of course, your mailing list shouldn't be shabbily maintained; purge inactive contacts and remove those with invalid email addresses.

- **Provide a way out:** Even though your contacts have opted in to receiving your campaigns, you should still provide them the option to unsubscribe—ideally in a single click.

Chapter XI

What is domain reputation?

Domain reputation is the reputation of a given domain among email clients like Gmail, Yahoo, Outlook, or Hotmail, and is determined based on that domain's online activity and history. Domain reputation also affects how emails are placed in email clients' inboxes.

Think of domain reputation like the reviews your favorite restaurant receives on Google. When customers enjoy the food and leave positive reviews, the restaurant's reputation grows, trust increases, and new visitors follow. But if unhappy customers leave negative reviews, your ratings drop and business slows down. Your domain reputation works the same way: Good email practices build credibility and trust, while poor practices can quickly damage your reputation and hurt deliverability.

Why domain reputation matters

Landing your campaigns in inboxes is vital to marketing your brand. If you can't achieve that, you can't grow your business effectively. Major email clients track your domain's reputation, and if they find abnormalities, they'll alert their users about your domain. This leads to spam complaints and blacklists.

Boosting your presence is crucial for marketing, and a good domain reputation helps you with that. Newly bought sender domains or old domains that are rarely used have low reputations; warming them up is a necessity to boost their reputations.

How to increase domain reputation

Some best practices to improve your domain reputation include the following:

- Authenticate your sender domain by publishing SPF, DKIM, and DMARC records. This is a non-negotiable, just like how you should add contacts organically with double opt-in.
- Ensure that your campaigns' content doesn't contain spam phrases, blacklisted URLs, or shortened URLs that can trigger spam filters.
- Implement hygienic email-sending practices, like identifying your contacts' time zones before sending emails and maintaining a healthy email volume and frequency.
- Offer content that addresses your contacts' needs and interests. Unrelated content can quickly cause your campaigns to be marked as spam.
- Prune your mailing lists every six months and win back contacts who haven't engaged with you for quite some time. Don't use purchased mailing lists—ever.

Checking a domain's reputation

There are online tools you can use to check your domain's reputation. For Gmail contacts, you can use Google's Postmaster Tool. Some other tools include MxToolbox, Spamhaus Project, and Barracuda. There are lots of tools, so choose the one you're comfortable with.

Conclusion

You've reached the end of Email Deliverability 101—and we sincerely thank you for taking the time to read this ebook.
We hope it's helped you gain a clearer understanding of email deliverability and why it's so crucial for your marketing success. We've covered some of the most important fundamentals here, but there's plenty more to explore—and we'll save that for the next edition.

This is just the beginning. More insights are on the way.

Until next time—happy marketing!

Glossary

Below are brief definitions of the commonly occurring terms to help familiarize you with the ebook's topic. The definitions are arranged in alphabetical order instead of order of appearance.

Brand Indicators for Message Identification (BIMI): Helps display the logo of your organization in email inbox to establish trust and improve email deliverability. .

DomainKeys Identified Mail (DKIM): Another domain authentication technique that ensures email deliverability.

Domain-based Message Authentication Reporting and Conformance (DMARC): Also a domain authentication technique.

Domain: A unique name that identifies a website or email address on the internet (like example.com) and serves as its online address.

Domain authentication: The practices and techniques involved in verifying emails' origins to ensure delivery.

Domain reputation: The reputation of a domain among inbox providers like Gmail, Yahoo, and others; an important aspect of email deliverability.

Domain warm-up: The process of sending a small number of emails initially and gradually increasing the volume to build delivery rates and domain reputation.

Double opt-in: The process of signing up whereby contacts confirm their subscriptions through verification emails to ensure genuine consent..

Email deliverability: An email's ability to land in its recipient's primary inbox.

Email Service Provider (ESP): Software like Zoho Campaigns which enables users to send emails in bulk, create attractive templates, and view analytics related to sent emails.

Mailing list: A list of contacts to whom a business can send email campaigns.

Primary inbox: The main inbox or folder in one's email account, in which they see priority and important emails first.

Sender Policy Framework (SPF): A domain authentication technique for ensuring email deliverability.

Zoho Campaigns: A cloud-based email marketing software tool for creating, sending, and managing targeted email campaigns.

Zoho
Campaigns

support@zohocampaigns.com

Talk to our team

Learn with our help docs

Explore Zoho Campaigns

Join Zoho Campaigns Community