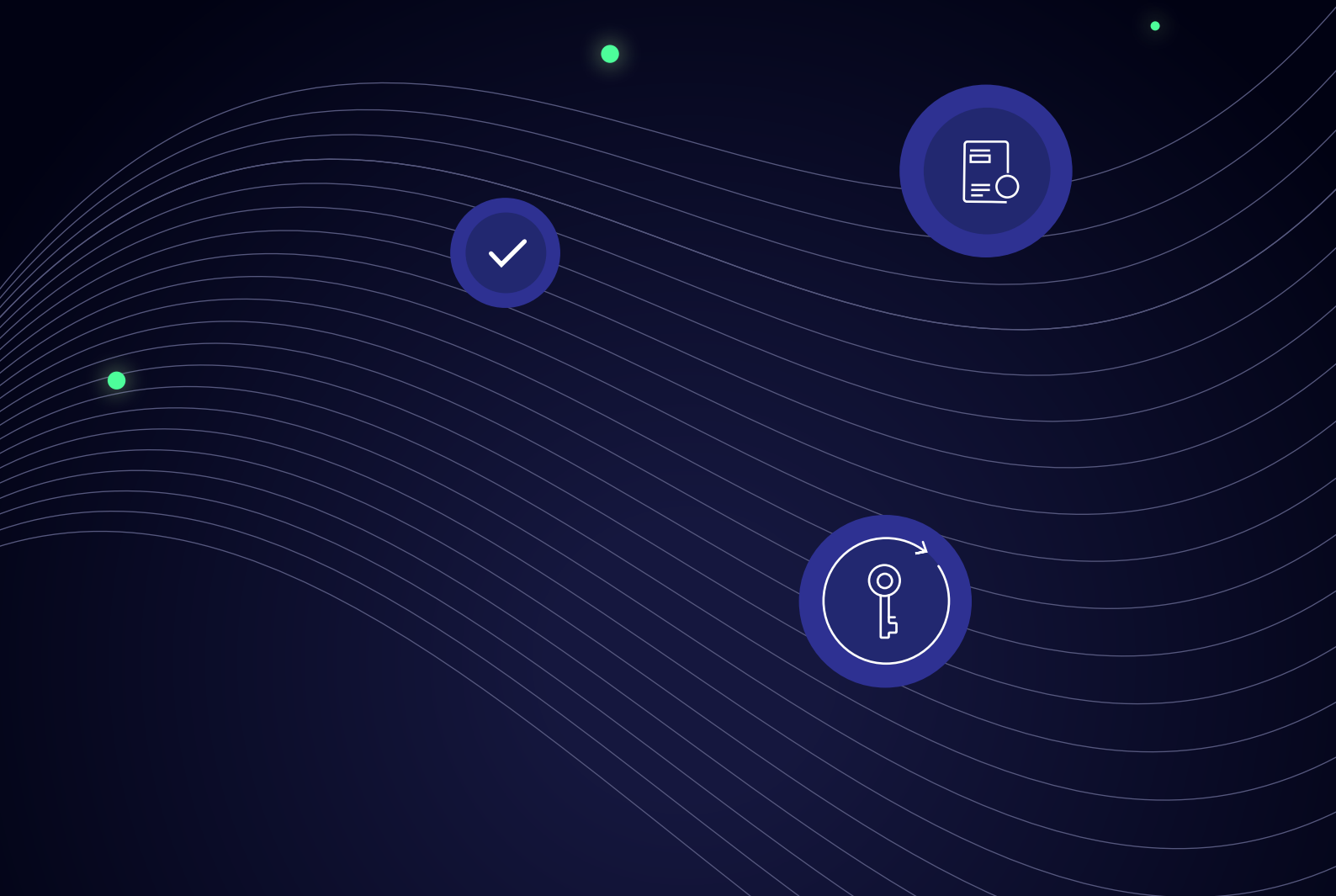
Zoho ZeptoMail

Transactional email deliverability guide



Email communication is a staple for any business with an online presence. Transactional emails tend to be the most important type of this communication, especially because they convey essential, time-sensitive information to your clients. It's beneficial to have great deliverability for any email, but when it comes to your transactional emails, it becomes a must-have.

If you're new to transactional emails, the term "deliverability" either confuses you or scares you, but it shouldn't do either. This detailed guide will help you understand deliverability, the importance of good deliverability, and how to achieve it for your emails.

Table of Contents

1. What are transactional emails?

Before we dive into deliverability, let's cover some basics about transactional emails. Transactional emails are user-triggered, unique, and automated messages sent from a business to its users. When a user performs an action on your website or application that can be considered transactional, an email is sent to acknowledge the transaction or provide information about the action. These emails are called transactional emails.

2. Marketing emails vs. transactional emails

A category of emails that is often confused with transactional emails is marketing emails. They're a completely different type of email, so they should be handled differently. Both of these email groups have their own purpose in a business, and understanding how each one works will help you use them to your benefit. Here are some of the ways they differ:

When: Transactional emails are triggered by user's action, while marketing emails are scheduled by the business.

Intent: Transactional emails are sent with the intent of communicating information, while marketing emails are sent with the intent of promotion.

Content: Transactional emails are personalized emails unique to each user, while marketing emails have templated content common for all recipients.

3. The importance of transactional emails

So we now know what transactional emails are, but why should we be focussing on transactional emails at all? Businesses consider transactional emails as an operational task owing to the fact that they do not directly convert into sales. While this is true, transactional emails come with a long list of benefits that make them important. Here are some of those benefits:

- **Communication:**

Transactional emails carry essential and crucial information. Keeping this line of communication open and smooth with the customer is key.

- **Brand image:**

Any communication from your business affects your brand image. As one of the most frequent forms of communication, bad delivery of these emails can tarnish your brand reputation.

- **Customer trust:**

More often than not, the transactions that trigger these emails are important ones, such as receipts for goods or services. Leaving your customers hanging with no communication of the transaction can make them question your trustworthiness.

- **Customer experience:**

These emails are requested or triggered by the user, which means they are waiting for them. Delivering these emails well can ensure a good customer experience.

- **Customer retention:**

Happy customers are loyal customers. Getting your communication, brand image, trust, and customer experience right can help keep users happy and retain their business.

4. What is email deliverability? The difference between delivery and deliverability

Most emails are delivered promptly to the recipient's email server, but not all of them find a home in the user's inbox. Some may land in the user's spam folder.

Email delivery is a measure of whether your emails have been accepted by the recipient server, while email deliverability is a measurement of whether your emails will land in the recipient's inbox. While the concept itself might seem simple, how we measure and ensure good email deliverability is more complex.

ISPs have a host of mechanisms in place to safeguard their user inboxes against unwanted emails. Can you blame them? No one wants spam in their inbox. Still, how can you ensure that your emails aren't mistakenly intercepted by these mechanisms? You could say, "Well, my emails are actually legitimate emails that the user needs. For real." But that does not always guarantee you good email deliverability.

Did you know? Up to 85% of authentic emails can end up in the spam folder.

Even when your transactional emails contain essential information for your customers, you could be making small mistakes that take a toll on your email deliverability.

5. Why is email deliverability important?

The importance of good email deliverability stems from the benefits of transactional emails that we previously talked about. With so much to gain from and your brand reputation at stake, the importance of good deliverability is evident more in transactional email sending than any other form of business email communication. Here are the top reasons why you should focus on the deliverability of transactional emails.

Convey crucial information

Transactional emails usually carry crucial information to your customers. For example, a welcome email often contains user credentials and invoice emails contain subscription or purchase information. Good email deliverability ensures that your customer receives this confidential information.

Provide access to account data

Transactional emails like verification and password reset emails are necessary for customers to access their accounts. Ensuring that your users can always access their accounts is essential. If your emails have poor deliverability, these important emails will not reach your customer's inbox.

Support good user experiences

In today's digital world, most users won't tolerate any delay. Transactional emails act as an immediate acknowledgement of a user transaction. To provide a good user experience, these emails have to land in your user's inbox. Good email deliverability and user experience will help with user satisfaction and, in turn, boost retention.

6. How can you improve email deliverability?

Email service providers look at your email reputation to decide how to treat your emails. A good email reputation ensures better deliverability. This email reputation is primarily decided by four factors:

- Sender reputation (the quality of your emails)
- Server/IP reputation (the reputation of your email provider)
- Domain reputation (how service providers perceive the domain in your email address)
- Email engagement metrics (how users interact with your emails)

While a complex formula is at play to decide your email reputation, there are a few measures you can take to ensure that your emails don't end up in the spam folder.

6.1 Infrastructure

Separate your transactional email sending infrastructure from your marketing email service. There's a very famous Spanish proverb that says, "Tell me who your friends are, and I will tell you who you are." This means that your reputation is a result of the company you keep.

Now, let's apply this to transactional emails and marketing emails. Users don't request marketing emails, so even if it contains useful information, there's a high chance that they'll mark these emails as spam. Additionally, spam filters today are equipped to identify emails that are sent with promotional content, so even before the marketing emails reach the user, they could be classified as spam.

When you send transactional emails from the same platform as your marketing emails, server/IP reputation comes into play. Simply by association, recipient servers jump to the conclusion that even the legitimate emails coming from you could be

malicious. This leads to your transactional emails being classified as spam. By separating transactional emails from marketing emails, you can build a strong email reputation for your transactional emails. With a dedicated transactional email service, you can solve an important piece of the deliverability puzzle.

6.2 Domain reputation

Enable email authentication

With the right email authentication protocols, you can increase your trustworthiness in the eyes of the recipient's email server. Spammers can easily impersonate your brand's email. To avoid these spoof emails from affecting your deliverability, you can put protocols in place that tell the recipient's server which emails from you are legitimate and which aren't. Some of the basic email authentications include:

- **Sender Policy Framework (SPF):**

  SPF records indicate the servers that are authorized to send emails from your domain. An SPF record will look something like this:

  "v=spf1 include:zeptomail.net ~all"

- **DomainKeys Identified Mail (DKIM):**

  DKIM records use encryption and email signatures to verify that the emails sent from your domain haven’t been tampered in transit. A typical DKIM record will look like this:

  k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCiCzf3O5+hAf-BjilORQN-RiWvsiFSXBPyC6YEG5gwoia2DZ4tiK4MXQNVwXlyMgZF7v+qx/FxYbyabeg10jYQ00UvOWqCdKeXvAdRsDjgV2iLE3KQjYZE5gmx00KEaXMtV3bp8CjtrUEnrubTqlN4b3hHh5B75kexci59BLKZE8cQIDAQAB

- **Domain-based Message Authentication Reporting and Conformance (DMARC):**

  DMARC authenticates emails by checking SPF and DKIM records. By adding a

DMARC policy, you can tell your recipient how to handle unauthenticated emails from (or appear to be from) your domain.

6.3 IP reputation

Choose between shared and dedicated IP

The reputation of the IP used to send emails is critical to ensure good deliverability. The concept of reputation here is the same as it is in domains, but with a key difference. Domain reputation is portable. IP reputation is not. If a bad IP reputation is the reason your emails aren't being delivered, the only choice is to change IPs.

IP reputation is closely tied with the type of IP you've chosen for your emails—either a shared IP or dedicated IP. While neither is better than the other, one type will be better suited than the other depending on your usage.

Shared IPs are used by multiple senders and have a shared reputation. Most email platforms, like ZeptoMail, monitor shared IPs and perform quality control to ensure good deliverability for those using the shared IP. While there could be some high-volume senders who benefit from a dedicated IP, using one when your email sending volumes fluctuate can be counterproductive. Based on your needs, you'll want to choose between a shared IP and a dedicated IP wisely.

Pick a service with good IPs

In most cases, businesses use shared IPs to send their emails. If your business uses shared IPs, the best way to ensure deliverability is to pick a provider who enforces good sending practices and has stringent measures in place to maintain the reputation of their shared IPs.

Choose a provider who has measures in place to evaluate each user allowed on their platform to ensure that they're not spammers. Even after the onboarding, the service should have ways to constantly monitor email sending to look for signs that the IP is being misused.

IP reputation factors

IP reputation is a consequence of multiple factors associated with the IP. These factors may also vary from one recipient server to another. Here are some of the factors to keep in mind while looking into your IP's reputation:

- **IP category**
- **IP address age**
- **IP history**
- **PTR records**
- **Reputation of different domains using the IP**
- **Associated URL reputation**
- **Downloadable files or code**
- **Association with malicious activities**
- **Popularity**
- **Hosting location**
- **Real-time performance**
- **Inclusion in allow/block lists**
- **Email sending frequency**
- **Spam complaint rates**
- **Recipient engagement**
- **Bounce rates**

Check your IP reputation

Even if you're doing everything in your power to maintain a good IP reputation, it’s always best to keep checking your IP reputation. You can start by finding your IP address from the header of your email. In most cases, businesses send emails from shared IPs, so you can click the Show Original option in the emails sent in the past week. Look for one of the following in the header info:

- **Received-SPF:**

  pass (zylker.com: domain of example.com designates 136.142.188.253 as permitted sender)

- **Authentication-results:**

  spf=pass (zylker.com: domain of example.com designates 136.142.188.253 as permitted sender)

You can then use the IP addresses obtained to check the reputation or potential threats using one of the well-known IP reputation checker tools.

6.4 Email volume and frequency

Warmup

A sudden flurry of email activity from a domain or IP raises red flags to recipient servers. Whether it's a new domain or a new IP, it's advisable to send emails slowly instead of all at once. To combat this, it's always best to gradually increase the volume of emails you send from a new domain. This is known as domain warmup. This will help recipient servers get used to receiving emails from the domain or IP and won't mark them as suspicious.

Consistent sending

When it comes to transactional emails, they're triggered by user's action on your website or application. While it can't be scheduled to be consistent, it's important to ensure that you don't make any drastic changes to your system that cause a huge spike or drop in email volume. Fluctuations in the email sending volume can lead to a drop in sender reputation.

6.5 Email content

Transactional emails usually carry authentic content to your users. There are still a few minor errors that can cause your emails to fall through the cracks. Avoiding these issues can help you ensure that your emails avoid the spam folder.

Use personalized "From" addresses

An email's "From" address often impacts the recipient's first impression of your message. A generic email address that starts with "noreply@", "info@" or "hello@" could cause users to ignore the email or doubt its authenticity. To achieve better user engagement, it's effective to include both the company name and the sender's name in the "From" section of your emails. For example: "Paula from Zylker."

Avoid click-bait subject lines

The subject line can also impact a user's initial impression. With legitimate transactional emails, being straightforward is the best strategy. Along with users, spam filters have an eye for spam-sounding titles. Avoid using all caps or catchphrases like, "Guess what we have in store for you!" You can always have fun with the subject lines, but be sure to keep them short and relevant.

Personalize the emails

Transactional emails are one-to-one communications that are directly triggered by user actions. The information they carry is specific to the user, so why not personalize the email? Something as simple as including the recipient's name can help them feel connected to your business. ZeptoMail's "merge info" option allows you to do this easily in your email templates. Simply add merge tags and automatically replace them with each recipient's details while sending.

Include a plain-text version

A plain-text email is an email with no formatting. Because transactional emails often convey crucial and time-sensitive information, your users should be able to access them at any time. Including a plain-text version facilitates both accessibility and delivery. The plain-text version intimates authenticity to ISPs and helps you avoid spam filters. It's best to ensure that the plain-text version doesn't differ too much from the fully formatted email.

Format the HTML effectively

Emails can be sent in plain-text or HTML. While both work just fine, HTML emails give users a better experience while also giving you an idea of your recipients' engagement with the email. But doing the HTML badly can negatively impact the customer,

which could lead to the customer marking the email as spam. Additionally, broken HTML tags can also trigger spam filters to classify your email as spam. To ensure that your emails are well formatted, you can use pre-built email templates that have already been tested and vetted.

Align with your branding

Your email design and content should immediately make your customers think of your brand. You can use methods like BIMI to add to this. Getting the brand right can allow your email to stand out in your customer's inbox while also avoiding being perceived as spam.

Use good practices for links

Adding links to emails is something most businesses do. It helps redirect users to a relevant location or even include more information than what they could fit in an email. The quality of these links matters greatly for the deliverability of these emails. Here are some do's and don’ts when it comes to links in emails:

- **Only add links to reputable and trustworthy websites**
- **Avoid shortened links**
- **Always hyperlink instead of using open links**

6.6 Mitigate spam complaints

A spam complaint is when a user looks at an email in their inbox and chooses to move it to the spam folder. These complaints are conveyed to the sender server and the senders themselves using email feedback loops (FBL). This is a service provided by the email providers to notify senders that their email has been marked as spam by the recipient. Because the user has marked the email as spam themselves, these complaints carry a lot of weight when it comes to deliverability. While in an ideal situation transactional emails wouldn't raise spam complaints, it's not always the case. Here are some practices you can follow to mitigate spam complaints.

Communicate expectation

It’s always best to set expectations of what the user can expect. As soon as they perform an action on your website or application, you can display a message letting them know that they’ll receive an email associated with it. Once they’re informed, the email won't be a surprise and so it won’t be mistaken for spam.

Configure a reply-to address

Not setting a reply-to address or using a no-reply address means that your users can’t reply to your email. This can be a detrimental practice for multiple reasons. Primarily, it keeps you from communicating effectively with your customers. By preventing customers from responding, you’re decreasing your email engagement. Email engagement is considered an important measure of legitimate emails, and lowering your engagement affects your email deliverability.

Avoid spam-trigger words

Seeing spammy subject lines or email content is an immediate red flag. As soon as users see something like "sale," "off," or "discount," it raises an alarm in their mind that makes them think it’s spam, so avoid using words and phrases that are often found in spam emails. Keep the content to the point, relevant, and personalized.

Give the user control

Not every transaction requires an associated email. To make it a better experience and not overwhelm the users, give them settings that allow them to pick what they want to receive emails for. By giving them the control to choose, they don’t have to resort to marking your email as spam to stop receiving it.

Protect public forms

Spambots are built to target public forms to submit email addresses repeatedly. Because your system perceives this as an action, you’ll send a transactional email. If these addresses are valid, the email is going to be unsolicited because the customer never submitted the form. This will lead to an overwhelming number of spam complaints. You can avoid this by taking these measures:

- Enable double opt-in through email address verification
- Employ Captcha in the forms to mitigate automated submissions.
- You can include a honeypot field in your forms that only the spambot can view. So any submission with valid values in the honeypot field can be disregarded as spambot submissions.

Test your emails

Your emails are received across devices, clients, and browsers. It's in your business's best interest to thoroughly test your emails to see if they work well in each of these environments. By not appearing broken or badly formatted, you can reduce the risk of users marking your email as spam.

6.7 Measure performance

Even after you've sent the email, it's crucial to keep an eye on the email analytics and watch how your deliverability measures are faring. You should gather insights from the data you have and keep updating the measures you take to boost deliverability. When you track your transactional emails, you can gather these data points to gain insights about your delivery:

- Sent emails
- Delivered emails
- Bounced emails
- Delivery speed
- Open rates
- Click-through rates
- Device tracking
- OS tracking
- Browser tracking
- Email client tracking

Monitor feedback loop and complaints

Most major ISPs provide access to feedback loops. A feedback loop is a channel that allows users to raise complaints about emails while marking them as spam or unsubscribing. Monitoring these feedback loops can help you course correct if your email deliverability is poor. As an alternate to feedback loops, you can also set up an abuse-reporting mailbox to capture complaints from recipients.

Purge your recipient list

If you keep sending emails to email addresses that don't exist or have been incorrectly entered into your system, your bounce or spam rate can skyrocket. As a result, your email deliverability can take a hit. Clearing out these email addresses or creating an email suppression list can help build your email reputation.

While you might have to use a paid service to purge and adjust your mailing list with other email service providers, ZeptoMail provides a Suppression List feature that automatically collects email addresses for reasons like user not found, spam, or feedback loop complaints. You can also manually add email addresses to this list as you see fit.

Enable double opt-in

Double opt-in is a process that requires users to verify their email address and actively confirm an email subscription. This is usually done through an OTP or email verification. While this may not directly affect your deliverability, it will improve the quality of your mailing list. Users can promptly correct any mistake in the email address, which reduces unnecessary bounces.

Monitor and handle bounces

Monitoring and reducing bounces is one of the most important aspects of maintaining a good email reputation and, in turn, good email deliverability. Monitor your bounce stats consistently to keep them under the accepted rate. ZeptoMail provides users with detailed stats on clicks, opens, and bounces. Users can also stay notified by configuring webhooks for specific email events, like bounces. Using this information to purge your email list will help build your email reputation.

Use a custom tracking domain

If your email tracking domain is the same as your email sending domain, it can sometimes cause a decline in your domain reputation. While it may vary from server to server, it’s best to use a custom tracking domain that can isolate your email tracking activities from the sending activities.

Take corrective measures

Measuring performance means nothing if we don't gather any insights from it. After collecting all of the important data, you should be able to decipher what each means and what could be better. Watching these data closely and taking corrective measures as soon as possible is the best way to ensure good deliverability.

Of course, your transactional emails are legitimate, as your users actually triggered them. In spite of the authenticity of these emails, having these measures in place will ensure that your customers receive important transactional emails on time, every time.