



ZeptoMail
by Zoho Mail

Transactional email deliverability guide



Email communication is a staple for any business with an online presence. Transactional emails tend to be the most important element of this communication, especially since 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.

Table of Contents

1. What is email deliverability?	01
2. Why is email deliverability important?	02
3. How to improve email deliverability?	03
3.1. Build your email reputation	03
3.2. Set up email systems and protocols	05
3.3. Create relevant email content	07

1. What is email deliverability?

Most emails are delivered promptly to the recipient's email server, but not all find a home in the user's inbox. Some may land in spam. 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 are not 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 guarantee you good email deliverability.

A quick did you know: 85% of authentic emails usually 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.

2. Why is email deliverability important?

The importance of good email deliverability is felt more in transactional email sending than any other form of business email communication. Let's take a look at why deliverability matters for 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 access their accounts at all times 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 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.

3. How to improve email deliverability?

While sending transactional emails, there are a few measures you can take to ensure that your emails do not end up in the spam folder.

3.1. Build your email reputation

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 simple steps you can take to build a good reputation.

- **Separate transactional emails from marketing emails**

With a dedicated transactional email service, you can solve an important piece of the deliverability puzzle. Users do not request marketing emails, so there is a high chance that they will mark these emails as spam.

When you send transactional emails from the same platform as your marketing emails, server/IP reputation comes into play, and your transactional emails may also be classified as spam. By separating transactional emails from marketing emails, you can build a strong email reputation for your transactional emails.

- **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 mailing list**

If you keep sending emails to email addresses that do not 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.

3.2.Set up email systems and protocols

Adopting the right email infrastructure and protocols is important for good email deliverability. Infrastructure covers all software and hardware involved in the email transmission process. Let's consider some best practices and the systems you should have in place.

- **Use 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. In order to avoid these spoof emails from affecting your deliverability, you can have 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
- **DomainKeys Identified Mail (DKIM)** - DKIM record uses encryption and email signature to verify that the emails sent from your domain have not been tampered in transit.
- **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/appear to be from your domain.

- **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 might 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.

- **Choose shared or dedicated IP**

IP reputation is an important factor in your email deliverability. Shared IPs are used by multiple senders and therefore 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 a dedicated IP when your email sending volumes fluctuate can be counter-productive. Based on your needs, you'll want to choose between a shared IP and dedicated IP wisely.

- **Monitor and handle bouncest**

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 email reputation.

3.3.Create relevant 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 great email deliverability.

- **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 spam-like subject lines**

The subject line can also impact a user's initial impression. With legitimate transactional emails, shooting straight is the best strategy. Along with users, spam filters also 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 email**

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. Since transactional emails often convey crucial and time-sensitive information, your users should be able to access them at anytime. 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.

- **Configure a reply-to address**

Not setting a reply-to address or using a no-reply address means that your users cannot 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 are also decreasing your email engagement. Email engagement is considered an important measure of legitimate emails, and lowering your engagement affects your email deliverability.

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