ortto

The complete guide to email deliverability

Welcome 👋

Despite countless new and trending platforms, email remains the most powerful, frequently-used marketing channel — and for good reason.

Through email, businesses can communicate directly with their contacts about important updates, products and services, and company news. However, the way people interact with those emails has major consequences on the continuing effectiveness of email as a marketing tool.

A comparison: Think of a billboard ad. It gets erected and stays there for a period of time (providing there's nothing illegal on it), and how one person reacts to it will not change how many others see it. A person can dislike it, love it, or feel ambivalent about it, but it doesn't take away from the ad's permission to be there.

The story is different with email. If a company sends an email and the recipient dislikes that email, there are a number of actions they can take that will affect whether the company's emails will be delivered to inboxes in the future. This practice is called email deliverability.

In this ebook, we will delve into the technicalities of email deliverability and why it is in equal parts important and challenging for businesses. We will list the factors that hurt deliverability and provide actionable email marketing best practice tips that will improve it. The goal is to help you ensure maximum ROI on your email marketing efforts so your business can continue to grow with email.

Ready, set, grow.

ortto

About Ortto

Ortto (formerly Autopilot) helps marketers engage at every stage of the customer lifecycle.

With Ortto, you can get your customer data, marketing automation, and analytics working together in a platform underpinned by AI to execute data-driven marketing campaigns with ease

Ortto has been supporting businesses across a range of industries since 2012, from multi-national to high-tech startup. Our customers include Microsoft, Westfund, TrustRadius, Macquarie University, Unbounce, frame.io, and LiveChat.

ortto

Table of Contents

01.

An introduction to email deliverability

In this section, we lay the groundwork: What is email deliverability? How does it relate to email security? And why it should be at the top of every email marketer's agenda?

Chapter 1:
What is email deliverability?

Email deliverability has a lot of components. At a fundamental level, it's about doing the work to earn your place in the inbox. In this chapter, we will set the scene by defining some key terms.

Email deliverability vs. email delivery

The terms email deliverability and email delivery may seem interchangeable, but there are key differences.

Email deliverability describes the likelihood that an email accepted by a receiving mail server will be placed in the recipient's inbox (high deliverability), filtered to the spam folder, or withheld from the recipient altogether (low deliverability). In short, the goal of email deliverability is for an email to land in a recipient's inbox where it is more likely to be viewed.

Email delivery, on the other hand, refers solely to the server-to-server transfer of emails and isn't concerned with inbox placement.

Email delivery
Whether an email is successfully transferred from the sending server to the receiving server.

Email deliverability
Whether an email is successfully transferred from server to server and where it finally lands for a subscriber (i.e. the recipient's inbox or spam folder).

Email deliverability and security

> "As someone who works in email deliverability, our biggest enemy is the malicious actors, the really, really bad people. It's not just spam, it's malware, it's spoofers, it's phishing."
>
> **- Travis Hazlewood, Head of Email Deliverability at Ortto**

Every marketer hopes that their emails are delivered to and well received by the intended audience – and no marketer wants their emails to go to the spam folder. Achieving this is becoming increasingly difficult — but it's not because mailbox providers want to make marketer's lives difficult.

Boiled down, email deliverability is about security, because email as a means of communication is very insecure. There are so many moving parts to email, which requires mailbox providers and internet service providers (ISPs) to identify and protect end users from manipulative/bad actors.

Ortto's Head of Email Deliverability, Travis Hazlewood explains how he and his industry peers work against a common enemy and the threat to security. "As someone who works in email deliverability, our biggest enemy is the malicious actors, the really, really bad people," says Hazlewood. "It's not just spam, it's malware, it's spoofers, it's phishing."

Key terms relating to email security

Negative Activities

Spam

Spam refers to emails that are malicious, unsolicited, undesired, and/or irrelevant.

Most email spam is commercial in nature and is a form of attention theft. Spam is also dangerous since it may contain links to lead to phishing websites or sites that are hosting malware or include malware as file attachments.

> *160 billion spam emails are sent every day. That's 46% of the 347 billion daily emails sent, considered spam. (Email Tool Tester)*

Spam: A brief history

The first spam email was sent in 1978, but it wasn't until the 1990s and 2000s when it became a huge problem. In 2003 the CAN-SPAM Act of 2003 was signed into law.

In 2002, Yahoo Mail added a spam filter to email. The provider's technology automatically separated the solicited emails from the unsolicited 'junk' emails. This differed from Microsoft's email provider Hotmail's efforts to filter spam, which blocked a set list of domains that allegedly sent unsolicited emails.

While the creation of the spam filter was a definite step forward, its means of identifying such traffic started with some very crude but desperate attempts (cough, cough, spam words). As time has progressed though, the filtering systems have evolved to identify spam through more nuanced approaches.

While spam filters are not perfect, they have experienced significant improvements. The quantity of spam being accurately identified and filtered now would have seemed only a pipe dream to mailbox providers in the past.

Did you know?

The term ‘Spam’ derives from the 1970 Monty Python sketch in which every item on the restaurant’s menu is Spam, the canned pork product. Years later, the word was adopted by the zeitgeist to refer to unsolicited, repetitive, and ubiquitous electronic commercial emails (aka junk mail) of a similar nature.

> “The spam folder is a security feature; a necessary part of the email experience.”
> **- Travis Hazlewood, Head of Email Deliverability at Ortto**

Malware

Malware is an umbrella term for all the different types of malicious software being used by cybercriminals. Most malware is installed without the infected person ever realizing it.

In email, malware utilizes downloadable functions like file or attachment downloads to insert itself into the victim’s system. Between sender best practices and receiver security systems like Apple’s Mail Privacy Protection, much is being done to attempt to protect the end-user (aka the subscriber) from exposure to such attacks.

Spoofing

Spoofing is the act of posing as a person or a program by falsifying information to gain an illegitimate advantage. A spoofing attack can happen via email, phone call, etc., and is used to gain access to personal information, spread malware, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack.

Phishing

Phishing is a type of cybercrime where hackers try to gain access to sensitive information, such as usernames and passwords, by pretending to be a person or organization they trust (see spoofing).

Phishing emails are designed to trick us into taking a potentially dangerous action, like clicking a link or downloading an infected attachment. They do this using emails disguised as contacts or organizations you trust so that you react without thinking first.

Positive Activities

2Domain authentication

Domain authentication is the method of legitimizing a source of traffic using DNS records that only the domain owner can add. The current main domain authentication types are SPF and DKIM, which can be reviewed in the Glossary below.

CAPTCHA

CAPTCHA is a type of security tool/feature that can be added to signup forms to protect against bots adding real and/or fake addresses to lists without actual consent. (Most common forms are Google's reCAPTCHA and Intuiting Machine's hCAPTCHA)

Address book/safe-senders list

The Address book/safe-senders list (depending on what each provider calls it) is a list where contacts' information is added by a recipient in their mailbox settings to identify traffic that is safe and desired. This can oftentimes circumvent spam filters for a sender to the specific recipient that has included them on this list.

Express consent

Express consent is the type of consent earned by A) clearly outlining what content type is being opted into on a signup source, B) not forcing opt-in for any other purpose than the outlined content, and C) honoring that opt-in by only sending content that is desired and requested.

Sender reputation

Sender reputation is a score that an Internet Service Provider (ISP) assigns to an email sender (i.e. an organization). The higher the score, the warmer the reputation and the more likely the ISP will be to deliver emails to the inboxes of recipients. A cold or low reputation may cause the ISP to send emails to spam folders or not deliver them altogether.

Chapter 2:

Why is email deliverability important?

Email deliverability wields immense power. It is the gateway to effective communication with customers, enhanced brand reputation, and ultimately, increased revenue. In this chapter, we'll look at the reasons why good deliverability matters.

1. Mailbox providers have a duty to protect their users

Mailbox providers are doing their job in protecting email users from malicious acts. While it's frustrating to jump through hoops, security practices exist for a reason. There have been countless cases of unfortunate and dangerous incidents via email.

When making a filtering decision, mailbox providers are stuck between a rock and a hard place. They have to do their best to find and filter out all dangerous and undesired traffic as accurately as possible while also making sure not to accidentally block desired traffic.

The failure of not blocking enough could cause more damage than the frustration around not receiving an expected email, so when providers come down to a questionable situation it is often likely they will err on the side of safety to protect their users.

Therefore, trying to get around mailbox safety with black-hat tactics and behaviors is not ethical. It also won't work, as mailbox providers' algorithms are becoming more advanced. Honest and ethical practices are more profitable in the long term.

2. Senders have to earn the inbox

The sender has a duty to ensure that there is no risk to their email recipients. Email deliverability best practices are about proving yourself to be a good, reliable, and safe sender so that the mailbox provider doesn't have to be unsure when the inboxing decision comes.

Senders should expect to have to earn the inbox rather than it being the default placement – just like a company has to earn the respect of customers by providing continuous positive experiences.

3. Email is the most important form of marketing communication

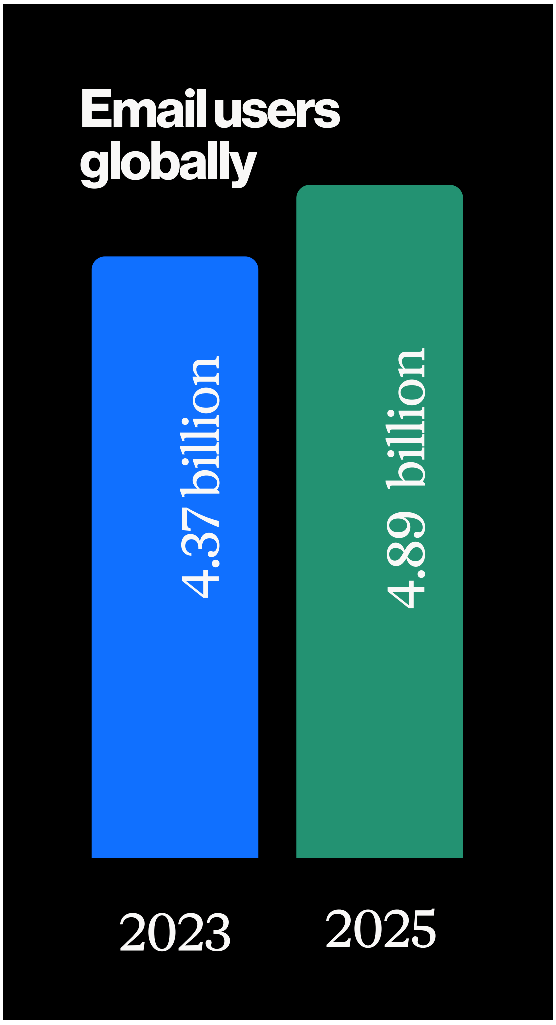
Email is the most popular method for receiving marketing communications. It is also cost-efficient and yields impressive ROI.

Email marketing statistics

- In 2023, the number of global e-mail users amounted to 4.37 billion and is set to grow to 4.89 billion users in 2027. (Statista)

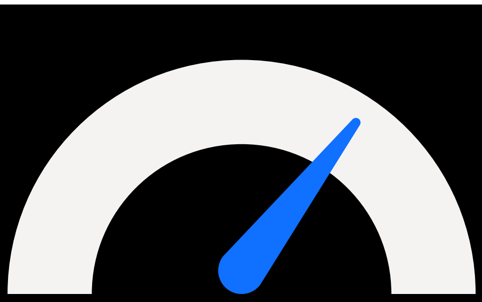
- Email is cost-efficient and effective, and therefore offers an unbeatable ROI when compared to other digital channels. In fact, for every $1 you spend on email marketing, you can expect an average return of $36. (Litmus' 2021 State of Email Survey)

- It is expected that 392.5 billion emails will be sent and received daily around the world by 2026. (Statista)



- Product awareness and promotions were the key objectives of their e-mail marketing campaigns for 2024. Retention and newsletters came second, each named by 14.6% of respondents. (Statista)

- In 2023, the global e-mail marketing market was valued at 8.3 billion U.S. dollars and the source projected that the figure would increase to 18.9 billion by 2028. The compound annual growth rate (CAGR) for that period is expected to amount to 18.8%. (Statista)



3,500%

average ROI for email marketing

Aside from using email to send communications, email marketers can leverage what they know about their contacts (e.g. product preferences and purchase history) to provide them with a very targeted, one-to-one experience. This fosters the kind of brand loyalty that leads to more sales and an enhanced online reputation.

4. Good deliverability practices improve your email content

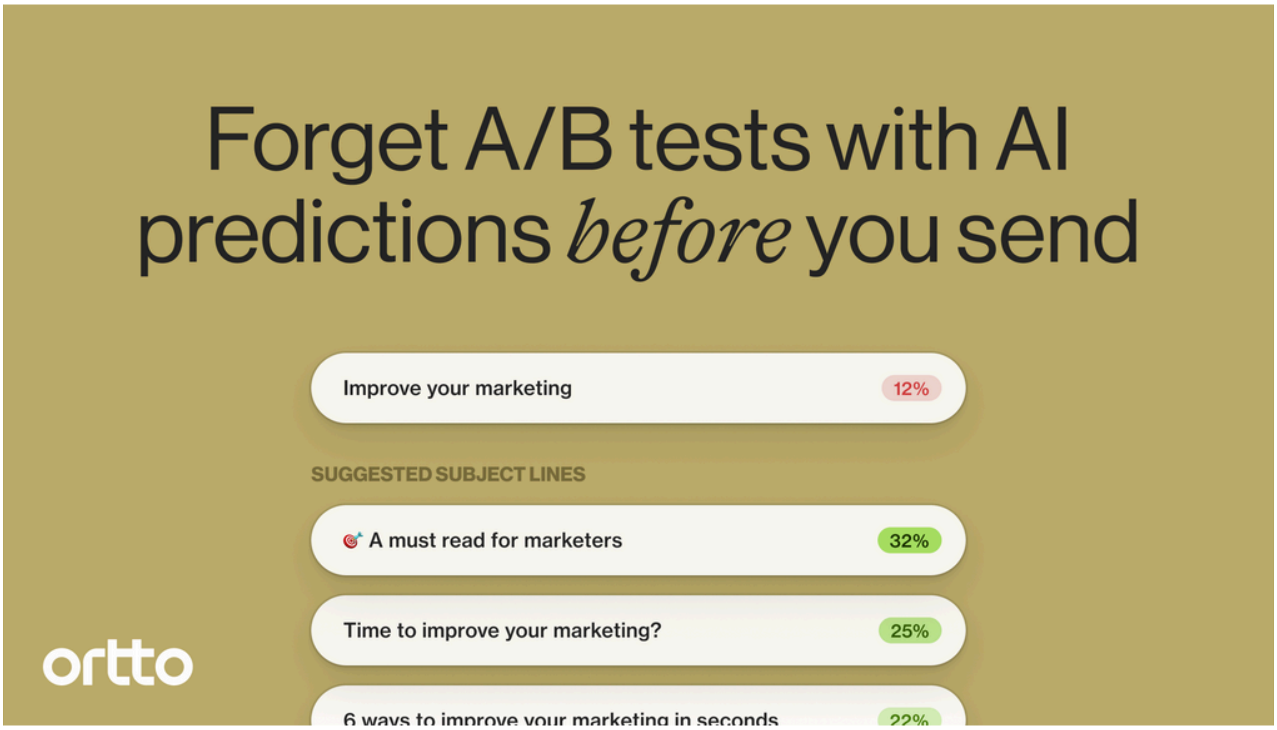
While there are many technical and maintenance elements in the list of deliverability best practices, the evolution of the filtering algorithms now leans so heavily on subscriber engagement.

This gives you further motivation to improve your email content. The decisions around opens, clicks, and other forms of engagement that affect deliverability can be just as much due to unfocused marketing content as being filtered into the spam folder.

5. You need to compete in the inbox

With billions of emails sent and received every day, and nine out of 10 marketers using email to distribute content, inboxes are unsurprisingly full. Senders have a hard job of competing against other senders to win the attention of recipients as it is, let alone dealing with issues relating to deliverability.

Pairing smart sending features (like Ortto's send-time optimization) with smart marketing approaches (like [Ortto's AI-powered subject line suggestions]) can help elevate visibility, engagement, and overall deliverability.


Forget A/B tests with AI predictions *before* you send
Improve your marketing
12%
SUGGESTED SUBJECT LINES
🎯 A must read for marketers
32%
Time to improve your marketing?
25%
6 ways to improve your marketing in seconds
22%
ortto

6. It's part of delivering a positive experience to your audience

Good email deliverability is earned by providing a positive, safe, and engaging experience for recipients.

A personal mailbox is becoming more and more like a physical mailbox at their home. Your actions in your email marketing approach should honor their welcoming you into their home (subscribing to your content) and reward them for trusting you by not abusing the send allowance/cadence with untargeted and oversaturated efforts.

Your strategies should prioritize giving value, and you should intentionally limit how often you contact them and with what content. These types of things affect ongoing engagement with subscribers which, in turn, affects deliverability.

7. Plugging a knowledge gap will give you the best shot of earning the inbox

If you want your email efforts to reach their full potential, technical familiarity is required. Without it, you could miss the inbox or cause domain reputation damage that is difficult to restore.

In no way are we implying that every email marketer should have an understanding of email deliverability to match a specialist who is working in the field day in and day out. What we are referring to here is developing a working knowledge of relevant terms and best practices to eliminate the likelihood that an email marketing team will encounter a serious problem — that is exactly why this handbook exists.

To close this chapter, a great email marketer today is one who familiarizes themselves with deliverability best practices and marries them with creative content and campaign strategies. When these things come together, emails reach the inbox, get noticed for the right reasons, and drive revenue.

Now, let’s get into those details that can help you and your email marketing team reach its greatest potential in email deliverability.

02.

Email deliverability best practices

By now, you should have a good understanding of what email deliverability is and why it matters. In this section, we will explore the ways to improve email deliverability organically and sustainably.

Chapter 3:
The 10 factors that hurt email deliverability

Email deliverability is complex by nature, and there are many factors that influence it. Below are 10 to take into consideration.

1. Missing domain configurations

As deliverability has evolved, mailbox providers require more technical configurations to authenticate traffic sources with the sending domain.

Two main pieces have become required:

- SPF and DKIM domain authentication
- DMARC presence on domain

Without these, deliverability penalties are being given even to senders with strong engagement rates to push more of the industry into following this authentication practice.

2. Poor reputation

Poor sender reputation has a large impact on email deliverability, specifically, domain reputation and IP reputation.

Domain Reputation

Domain reputation is how 'trustworthy' a domain is, and is affected by the quality of the sender's emails, including the quality of their recipient list.

Mail providers like Google determine whether recipients like the content they are emailed by that domain, and give the sender a rating based on things like open rate and replies, which impacts email deliverability.

A bad domain reputation, whether due to non-engagement or user complaints, can cause emails from a domain to be filtered to the spam folder by default or even be, in effect, 'blacklisted' to the point of non-delivery with a provider.

IP Reputation

Domain reputation is how ‘trustworthy’ a domain is, and is affected by the quality of the sender’s emails, including the quality of their recipient list.

Mail providers like Google determine whether recipients like the content they are emailed by that domain, and give the sender a rating based on things like open rate and replies, which impacts email deliverability.

A bad domain reputation, whether due to non-engagement or user complaints, can cause emails from a domain to be filtered to the spam folder by default or even be, in effect, ‘blacklisted’ to the point of non-delivery with a provider.

Actions that harm sender reputation include – but are not limited to – the following:

□ How many emails are marked as spam?

□ How many emails are left unopened?

□ How many recipients unsubscribe or opt out of email communications?

□ How many emails bounce?

The above actions relate to recipient engagement, which we will explore more below. Since sender reputation is built upon the positive or negative responses of recipients, poor engagement is the cornerstone of poor reputation.

3. Poor engagement

Poor engagement refers to negative activities on the recipient’s side that can lead to poor sender reputation.

Poor engagement may involve any and/or all of the following:

- High bounces (≥5%)
- Low opens (≤15%)
- High complaints (≥.05%)
- High unsubscribes (≥1%)

Note: The above metrics are a general threshold for ongoing poor-engagement trends across multiple bulk sends.

Engagement terms glossary

Opens

Open rate is an email marketing metric that measures the percentage of emails that are opened by recipients (as opposed to emails that are left unread, deleted, marked as spam, or undelivered).

Clicks

Click-through rate is the proportion of visitors who follow a hyperlink to a particular website or landing page.

Bounces

A bounce is when an email is returned to the sender because it cannot be delivered. This can occur for multiple reasons and can be categorized as a ‘soft’ bounce or a ‘hard’ bounce.

Hard bounce

A hard bounce equates to a 'hard stop' received by the sender from the recipient-side server. It can be due to a misspelled or disabled address or to an outright block of the sender. Essentially, it means that either the address does not exist or the address wishes you to think that it doesn’t exist and discontinues any further sending.

Soft bounce

A soft bounce equates to a temporary issue of some sort. It can be due to a temporary block, a connection issue, or a myriad of technical issues surrounding the email receiving process. Essentially, it means there is a problem at this time that may be resolved at a later date.

Delivered

Delivered or 'delivery rate' is the amount of subscribers whose email delivery attempts were accepted by the receiving server, as opposed to bounces or invalid attempts to suppress addresses.

Unsubscribe

Unsubscribe rate is the amount of email subscribers (newsletter, product updates, etc.) who choose to no longer receive communications from an organization via email and therefore unsubscribe.

These are usually tallied with the email campaign through which they clicked the unsubscribe link.

Complaints

Complaint rate is the amount of subscribers who have reported an email as spam or phishing.

While some elements can have a more immediate impact on reputation than others, like complaint rates, all of the elements advised above help to paint a picture of the subscribers' experience with a sender's content and marketing practices.

A trend of negative metrics growing towards the advised thresholds can be a forewarning of growing negative experiences with sending practices.

To help protect your sending reputation, monitor for poor engagement metrics before they grow to a problematic level and implement corrections quickly.

4. Bad subscriber acquisition practices

Subscriber acquisition refers to the process by which subscribers are added to your sending audiences. How a marketer collects subscriber addresses can make or break their eventual sender reputation.

Good list acquisition practices look like this:

- Signup forms that outline explicitly what content a subscriber is signing up for
- A checkbox for marketing content in a purchase process is set unchecked by default
- Some form of CAPTCHA security to protect signup sources

Poor list acquisition practices look like this:

- Content gates that require an email address to see a blog, etc.
- Giveaway gates that require an email address to enter to win

Bad list acquisition practices look like this:

- Purchasing lists of addresses
- Scraping addresses off of the internet
- Referral benefit programs requesting subscribers to provide a friend/colleague's address for discounts, etc.
- Acquiring through opt-out instead of opt-in practices (see Ch. 4)

Following best subscriber acquisition practices is about using methods that give the subscriber full visibility and autonomy in the subscribing experience before a single email is sent.

5. Poor list management

List management refers to the process of organizing, auditing, and cleaning out subscribers whose inactivity will lead to poor sender reputation.

If you don't continually clean your email lists, you will repeatedly send emails to old or unengaged subscribers. These will contribute to ongoing negative engagements, which will harm your sender reputation and cause you to miss the inbox.

To mailbox providers, a passive recipient's permission to send is eventually revoked by inactivity. As a sender, aligning with that perspective will mean you are aligning with the mailbox provider's idea of what makes a good sender.

Permission to send should have an expiration date. At Ortto, permission to send ends at 12 months of no engagement for an address. Good list management practices should include a re-engagement attempt and sunsetting of such addresses before they reach the 12-month mark. Poor list management would be little to no maintenance of this kind so that lists of unengaged addresses grows until the majority of the audience is unengaged.

6. Spammy send practices

The close-your-eyes-and-send-to-everyone approach to email marketing has not only been retired but is now considered a form of "spammy send practices."

These practices look like this:

- Unfocused content
  - Filling an email with every ounce of content possible without awareness of subscriber preference or interest.
- All-or-nothing list setup
  - Sending all content types to the entire subscriber database instead of separating each content type with its own list.
- Generalized approach
  - Not utilizing personalization tags or dynamic content that elevates items or information that the subscriber has shown previous interest in.
- Unregulated send frequency
  - Sending too frequently or too sporadically.
- Unresponsive send strategies
  - Creating email marketing strategies that do not take into account response metrics from previous campaigns.

A word on spam trigger words

Salesy, manipulative words in emails don’t provide a positive experience for the recipient. Language with the intention of evoking an urgency that is not warranted or earned has been utilized regularly in malicious activities and unsolicited reach-outs.

If your content uses such language, now would be a good time to re-evaluate your approach. Not because the spam words are causing spam filtering, but because it is more likely your practices are responsible.

7. Poor ramp-up experience

Because of the amount of malicious activity that occurs around email, systems rely on tools that identify good senders from bad by attributing reputation to certain technical elements, like the IP address or the domain attributed to the sent email.

Making a sudden change without slowly ramping up your sending volume, using either new IPs or domains that lack reputation, or new-to-you IPs/domains not usually associated with your emails, can cause spam filters to become suspicious and trigger more easily.

Also, not alerting your subscribers of the change before it occurs can either cause a lack of trust (if you start sending from a new email address they don't recognize) or a lack of proactive searching (should the change cause extra filtering). People need a heads-up and systems need time to evaluate and recognize the new change.

8. Bad links/URL link shorteners

Links have become one of the greatest vulnerabilities around email, especially due to the success rate of phishing, spoofing, and the social engineering tactics that often accompany such activities.

Malicious actors have so staunchly abused link shorteners like bit.ly and file-download links like PDFs, that security systems are more likely to outright reject an email the link is deemed too unsafe to let through.

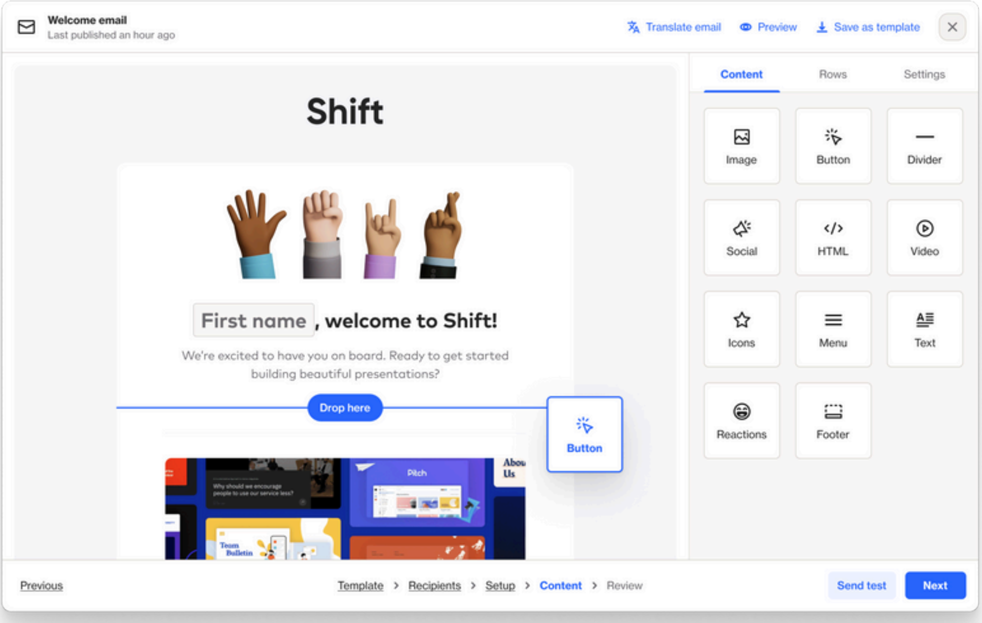
These types of links hide the quality of the content behind them so well that even good senders who include them in content can experience sudden deliverability issues.

9. Bad image-to-text ratio

Sending emails that are made up of only an image or multiple images can look suspicious to security systems who are not able to parse the information being provided in said images (at least not yet). Malicious actors use this tactic to hide spoofing as well as other abusive activities.

Security systems also understand there are many human elements possibly missing to cause a warning, such as a lack of alternate text for visually-limited users or those with image-blockers turned on.

This is why the concept of an image-to-text ratio in deliverability is important, and how a balance of the two can help protect from a misapplied filtering experience.



Shift

First name , welcome to Shift!

We're excited to have you on board. Ready to get started building beautiful presentations?

10. Technical issues with ISPs

If you're sending to high-risk providers like banks and government bodies, in most cases, you can't just hit send and deliver easily.

Because of the vulnerability and important information at stake on their end, such mailbox owners have to create some of the most stringent security limitations around external mail being received by them.

Sometimes it's as easy as requesting they add your sending address/IP to their internal allowlist or it could require an end-to-end encrypted delivery connection like transport layer security (TLS), which is not defaulted on by most providers.

The message is clear: Not taking the time to understand your audience's technical needs can lead to an inability to deliver a single message to them

Chapter 4:
How to improve email deliverability

Think of email deliverability as a formula: more positive signals (opens, clicks) than negative signals (unsubscribes, 'mark as spam') will improve inbox placement and increase brand visibility and engagement.

Ortto's Head of Email Deliverability, Travis Hazlewood asks that marketers, above all, provide an email experience that's "secure, transparent, engaging, and respectful." Doing so will give them the best chance of earning inbox.

There are three main pillars of deliverability: Get consent, engage meaningfully, and be human. Let's explore each of these.

1. Get consent

Active subscriber consent is the foundation of strong email deliverability.

How you gather your subscribers and empower them to control their subscription preferences can make or break your deliverability experience.

If you are emailing people who do not want to be contacted by you, your open rate will be low and your bounce rates and unsubscribes will soar. This will affect your domain reputation and, in turn, your deliverability. Needless to say, it'll also affect your brand reputation.

Ensure that you are clearly communicating how subscribers can opt into your marketing emails and retain control over their preferences, and empower them to make decisions about what they want to receive. As an email sender, you must honor their preferences to maintain trust and build a list of engaged subscribers.

We've listed some good acquisition practices on the following page.

Implement explicit opt-in practices

Before you put somebody's email address into a subscriber bucket, ask yourself: did they explicitly opt-in to receive this type of email communication from me?

Signup sources should clearly outline the type of content being opted into and those expectations should be honored.

Opt-in vs. opt-out: the basics

Opt-out signup forms are different from opt-in signup forms – and the latter is better for deliverability.

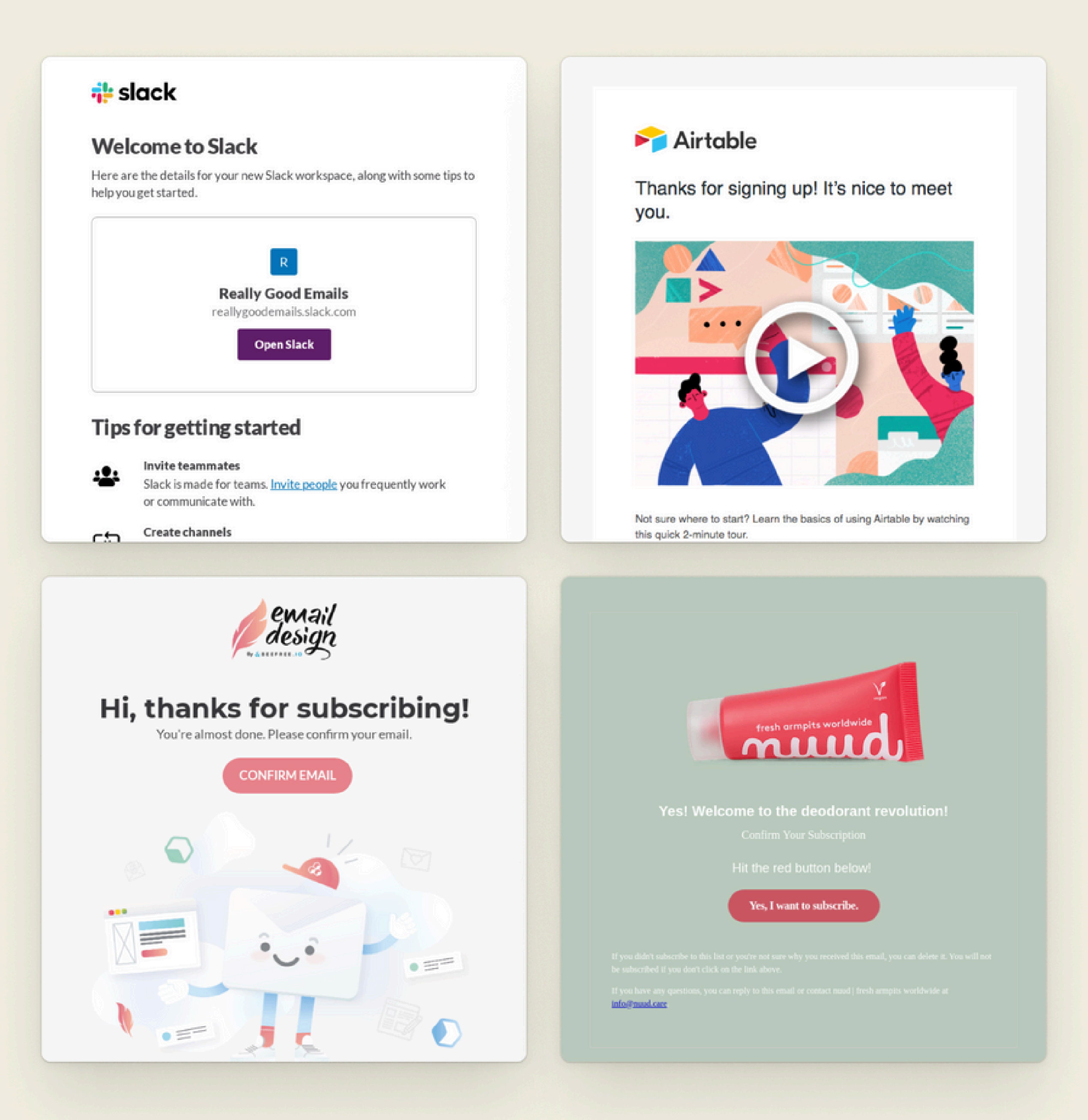
In an opt-out form, checkboxes for content lists are pre-ticked, meaning a submitter has to actively untick boxes if they do not wish to receive communications.

An opt-in form, on the other hand, does not predetermine such a subscription, meaning that subscribers are less likely to end up on content lists they don't wish to be on. Granting more autonomy to subscribers shows that you aren't trying to trick them. This is why Ortto suggests that users utilize opt-in forms – see our usage guidelines.

The gold standard is to promptly send new subscribers a welcome email to request their confirmation of the signup preferences — this is referred to as double-opt-in.

Welcome emails

Source: Really Good Emails



slack

Welcome to Slack

Here are the details for your new Slack workspace, along with some tips to help you get started.

R

Really Good Emails
reallygoodemails.slack.com

Open Slack

Tips for getting started

Invite teammates
Slack is made for teams. Invite people you frequently work or communicate with.

Create channels

Airtable

Thanks for signing up! It's nice to meet you.

Not sure where to start? Learn the basics of using Airtable by watching this quick 2-minute tour.

email design

Hi, thanks for subscribing!

You're almost done. Please confirm your email.

CONFIRM EMAIL

fresh armpits worldwide muud

Yes! Welcome to the deodorant revolution!

Confirm Your Subscription

Hit the red button below!

Yes, I want to subscribe.

If you didn't subscribe to this list or you're not sure why you received this email, you can delete it. You will not be subscribed if you don't click on the link above.

If you have any questions, you can reply to this email or contact muud | fresh armpits worldwide at info@muud.care

Another scenario to consider: A customer may have purchased a product or service and entered their email address because certain contact details were required to make the purchase. This doesn't necessarily mean they want to receive marketing emails from you. Ask them to tick a box that specifies they want to hear from you and then ask them to confirm that they opt in.

When someone does unsubscribe from an email list, acknowledge their preference with an email.

While the above takes care of organic, human activity, there are malicious actors out there who abuse people's mailboxes by finding vulnerable signup forms and adding their addresses unknowingly. Because of this, you should also secure your forms with some version of CAPTCHA to prevent this type of abuse. This will help to ensure your email lists are high-quality and secure.

Use content or offer gates wisely and sparingly

While acquiring addresses with one-time offers or giveaways can result in a large number of subscribers, especially if a partner promotes them, these subscribers may only be interested in that one opportunity and their future email engagement may be little to nothing.

Gated forms can also encourage users to input secondary or temporary addresses, resulting in unopened or bounces, negatively impacting deliverability.

Be wise about what you do and do not gate — and consider partial gates on content. Ensure the gated elements are highly relevant for your ideal customers, and that you have a plan for nurturing those new contacts. Use permissions, filters, and audiences to ensure opt-in gate subscribers are only receiving relevant, useful, and valuable content. You want to avoid subscribing them to all email audiences and types, as this can lead to reputation issues.

Examples of bad gates:

- Content gateways for basic blog posts or whitepapers
- Giveaways
- One-off offers

Examples of acceptable gates:

- High-value content
- Educational programs

Focus on the quality and fit of the subscriber rather than the quantity of subscribers, and you will build higher-quality subscriber lists that engage with your emails and send positive signals to mailbox providers.

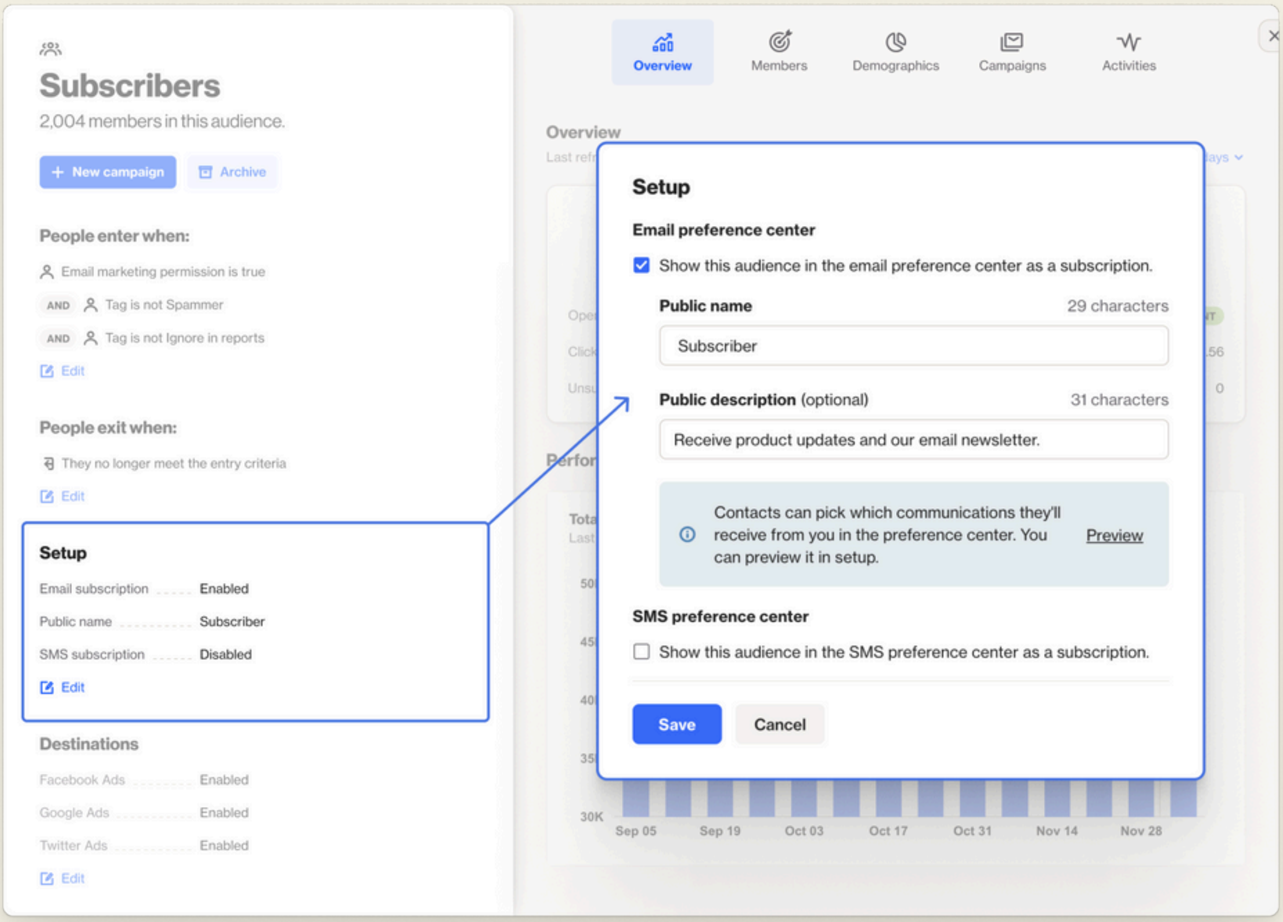
Incorporate an email preference center for various content and communication channels

Unsubscribe accessibility is paramount to good email marketing – and in turn deliverability. Having an email preference center where subscribers can manage the communication and content they receive across various channels is crucial. It lowers the chance that subscribers become frustrated or disgruntled and mark your emails as spam – the proverbial kiss of death for deliverability.

A preference center allows subscribers to self-serve. You must then honor their wishes and remove them from any lists they don't want to be in.

Remember: an unsubscribe is better than a complaint.

Ortto preference center set up



Subscribers

2,004 members in this audience.

+ New campaign | Archive

People enter when:

Email marketing permission is true
AND Tag is not Spammer
AND Tag is not Ignore in reports
Edit

People exit when:

They no longer meet the entry criteria
Edit

Setup

Email subscription	Enabled
Public name	Subscriber
SMS subscription	Disabled

Edit

Destinations

Facebook Ads	Enabled
Google Ads	Enabled
Twitter Ads	Enabled

Edit

Setup

Email preference center

☑ Show this audience in the email preference center as a subscription.

Public name 29 characters

Subscriber

Public description (optional) 31 characters

Receive product updates and our email newsletter.

Contacts can pick which communications they'll receive from you in the preference center. You can preview it in setup. Preview

SMS preference center

□ Show this audience in the SMS preference center as a subscription.

Save | Cancel

Employ list maintenance practices

Subscriber lifecycles are not identical, but we can break down some general, rule-of-thumb guidelines to help give a good idea of how to protect and honor a subscriber's experience.

Studies vary, but it is generally understood that a subscriber's most convertible timeframe is within the first 30-90 days of subscription. After 90 days of no engagement (e.g. an open or a click), they are in danger of being difficult to re-convert, making them a liability to your email deliverability. But let's be honest, people are forgetful and rarely proactive when it comes to their subscription preferences.

The optimum time to re-engage dormant subscribers is between the 90-180 day mark using win-back email campaigns. After that, their lack of engagement will continue to wear on your reputation, and give them an opportunity to become annoyed and respond negatively to your emails (especially if they have not been inboxing for a while but suddenly are, so they think they are being spammed).

Tactics to win back inactive subscribers include:

- Use humor to get their attention: Appealing to them on a more personal level can help them to see your company in a new light.
- Update them about product/company changes: Maybe they were dissatisfied with certain product features or your ways of doing things, so be sure to let them know what you're offering before cutting contact.
- Offer incentives: If all else fails, try to incentivize them to keep interacting with your brand. For example, you can offer them a free coffee if they reply to your email newsletter with feedback or content requests.

You could also ramp down the email frequency for subscribers who display waning interest. This way, you're being careful not to bombard them with content that may push them away – or push them to 'mark as spam'.

Having a regular re-engagement and sunset process of older, unengaged subscribers (6-12 months unengaged) is a great way to both honor your audience's passive preference and retain a strong sender reputation with mailbox providers.

Losing the interest of subscribers is frustrating, but inevitable. There are many reasons why this may be the case: a subscriber's interests may change; they are dissatisfied with the emails they are receiving; they subscribed to fulfill a need that has since been met, or they want to de-clutter their inbox.

It's important to accept that it's okay to let go of inactive subscribers. Relationships run their course, and if you can't re-spark their interest in your company and offering, it's better to let them go.

2. Engage meaningfully

Meaningful engagement is another cornerstone of good deliverability.

Work with your subscribers to identify their desires and expectations, as this will fuel engagement and subsequently improve deliverability. A big component of engaging meaningfully is to personalize content.

This involves:

- Personalizing email subject lines
- Segmenting audience lists and sending only relevant content
- Ensuring content is highly focused and timely
- Utilizing A/B testing to identify effective approaches
- Providing a robust preference center experience for subscribers to set up-to-date preferences

Senders should also respect recipients by providing unsubscribe accessibility:

- Elevate accessibility of the unsubscribe button so that people choose it over the Spam button
- Utilize two-click unsubscribe
- Remember: An unsubscribe is much better than a complaint

Between passive methods like adjusting strategies based on subscriber engagement, to active methods like subscribers updating their preferences and contact fields, there are so many ways that a targeted, meaningful approach to your marketing content can be achieved.

3. Be human

The final building block is simple but often overlooked: be human.

Be human in the way you speak to your subscribers; in the way you honor their preferences, and in the way you earn their trust. The goal is to be as authentic and as personal as possible in a way that provides value and, in turn, earns the subscriber's attention.

Earn is the keyword. We know that the average person gets over 100 emails per day, and likely doesn't have the time or desire to sift through them all. So, to grab their attention and amp up your email open rates and click-through rates, you should appeal to your subscribers' interests and make them feel seen. The best way to do this is through engaging, natural language.

> "It's not ideal to use [spam words like] 'Free' or all capital letters and a thousand exclamation points, because it's not human. It's not respectful."
>
> **- Travis Hazlewood, Head of Email Deliverability at Ortto**

When your subscribers feel respected, they will not only regularly engage with your content, but will actively seek it out. And, ultimately, this is what email marketing is about – building brand awareness and a loyal customer base to gain preference over competitors.

03.

Advanced section

In this section we will cover technical FAQs and I'll share final thoughts.

Beyond the advised do’s and don’ts communicated above, there are some more technical elements relating to email setup that can be helpful to know in regards to email deliverability.

The following guidance is general in nature, and it is advised that you work with a deliverability consultant to ensure your customer experience is set up in a way that will serve your marketing content and approach.

Below are four common best practice questions and answers:

Should I set up authentication for my domain?

Yes, authentication can help providers be sure that you are who you say you are as a sender. DKIM is currently the most reliable authentication for senders to implement when using an ESP. It is also best practice to include SPF.

Should I separate my organization’s various mailstreams or send all from the same domain?

It is becoming best practice to separate at least some mailstreams by subdomain. This is because:

Bulk sending can impact a reputation fast, both positively and negatively. For example, if a marketing team accidentally does a bulk send to an old list and receives negative reactions which hurts the domain reputation, every other team sending on the same domain level will share the negative effects from that campaign.

However, if the bulk marketing mail was on its own subdomain (“updates.example.com” instead of just on “example.com”) then the company’s other traffic (think internal communications, sales, support, etc.) are less affected by the accidental mistake

You don’t have to separate all mailstreams, as there are other caveats or issues that can occur by over-isolating traffic

Should I use a shared IP pool or a dedicated IP?

This is difficult to answer without knowing the specific sender setup, but most email marketers work best on a shared pool of IPs.

Dedicated IPs take a certain volume of traffic to maintain reputation, which can prove difficult. The ESP who owns the shared IP will monitor and maintain the IP reputation, whereas a dedicated IP would require self-management

The situations where a dedicated IP is most important are:

- If you need a very particular send setup for your subscriber audience (for example, enforced TLS when communicating with banks or other security-heightened organizations)
- If you have a large audience that you send regularly (for example, 1 million+ volume over 30 days)

Note: Dedicated IPs require more attention and maintenance, so speaking to a deliverability expert directly is crucial.

Do I need to ramp up my volume after I change ESPs?

- It is best practice that when you change sending provider (ESP) or IP/domain you ramp up your volume to help you have a smoother transition.
- Follow ramp-up guidelines outlined by your provider for your specific situation. Here is an example of Ortto’s ramp-up guide for general senders moving from another platform to our shared environment.

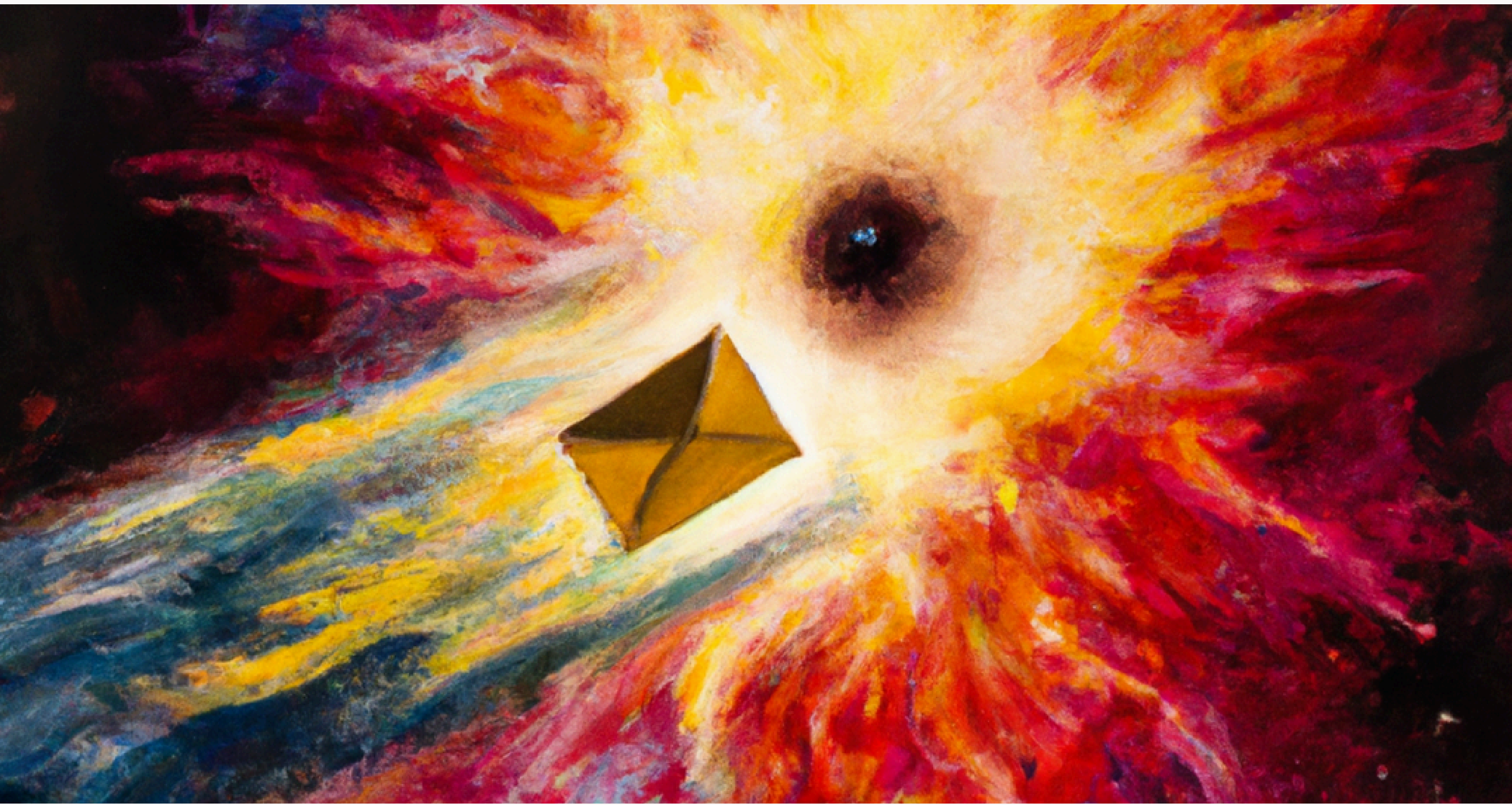
Disclaimer: Talk to a deliverability consultant to determine what is the right fit for your organization

Final thoughts

> "Email deliverability is an arms race against the bad actors who are finding new ways to abuse things. And it's likely there will never be a [end-all] winning point. The direction it is evolving is very smart, but the focus is still: Is this email expected? Is it desired? Is it relevant?"
>
> **- Travis Hazlewood, Head of Email Deliverability at Ortto**

Email deliverability is a constantly evolving beast. What earned the inbox today might not work tomorrow, "and there will never be an end-all winning point," says Travis. No one can know for sure what the next stage will look like, but what we can be sure of is that as technology and the litigation around it grows email marketing will change.

For now, though, email marketers should ask themselves: Is this email expected? Is it desired? Is it relevant? Tick those boxes, and you'll be on the right track.



Your email deliverability checklist

Now that we've covered everything in detail, let's simplify some of the most important pieces to make sure you're ready to reach the inbox.

Minimum checklist

- Are all sending domains authenticated with SPF and DKIM?
- Do all sending domains have an active DMARC record present?
- Are you compliant with all country-specific promotional email laws and regulations (e.g. CAN-SPAM, CASL, GDPR, etc.)?
- Are all signup forms secured with CAPTCHA?
- Are all signup forms clear and explicit in the content being opted into?
- Do you have a Welcome or Confirmation automation set up for new subscribers?
- Do you have a Preference Center linked in your emails?
- Are your subscribers segmented by content-type?
- Have you set up reports/dashboards for monitoring email engagements?

Advanced checklist

- Have you set up your sending domain with Google's Postmaster Tool?
- Have you set up custom tracking subdomains for click-tracking?
- Have you set up engagement segments/audiences based on time since last engagement?
- Have you set up BIMI for your sending domain?
- Have you set up a re-engagement automation?
- Have you set up a Subscriber Lifecycle automation to regularly re-engage subscribers?
- Have you set up a Sunset automation to remove long-term unengaged subscribers?
- Have you set up custom subscriber fields to utilize dynamic content?

ortto

Your email deliverability glossary

Allowlist
A list of who or what is allowed access to a given device or service.

Blocklist
A list of who or what is blocked access to a given device or service.

Bounce
When an email is returned to the sender because it cannot be delivered.

Brand Indicators for Message Identification (BIMI)
A standard that attaches your brand's logo to your authenticated email messages. (See Sender Authentication.)

CAPTCHA
A computer program or system intended to distinguish human from machine input.

Click-through rate
The proportion of visitors who follow a hyperlink to a particular website or landing page.

Compliant rate
The amount of subscribers who have reported an email as Spam or Phishing.

Dedicated IP
A private internet-protocol address assigned solely to you/your account and not shared by any other senders.

Domain
A string that identifies a realm of administrative autonomy, authority, or control within the Internet. Often, identifies services provided through the Internet, such as websites and email services. (Pulled from Wikipedia)

Domain-based Message Authentication, Reporting and Conformance (DMARC)
A technical standard that helps domain owners protect and block email senders from using their domain in unauthenticated attempts at spam, spoofing, and phishing. (See Sender Authentication.)

DomainKeys Identified Mail (DKIM)
A protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. (See Sender Authentication.)

Domain/Sender reputation
A measure of the trustworthiness of a domain / A score that an ISP or security provider assigns to an email sender.

Email deliverability
Whether an email is successfully transferred from server to server and where it finally lands in a subscriber's mailbox.

Email delivery
Whether an email is successfully transferred from the sending server to the receiving server.

Email Service Provider (ESP)
An email-sending platform a business employs to manage and deliver email marketing communications.

Email list
A collection of email addresses that you have received through your blog or website.

Internet Protocol (IP)
A set of rules governing the format of data sent over the internet.

IP reputation
A measure that assesses the quality of an IP address to determine its legitimacy.

Internet Service Provider (ISP)
An organization that provides consumers and businesses access to the Internet.

Mailbox Provider (MBP)
An organization that provides users with email accounts, and accepts and delivers email.

Malware
An umbrella term for all the different types of malicious software being used by cybercriminals.

Open rate
A metric that measures the percentage of emails that are opened by recipients

Phishing
Phishing is a type of cybercrime where hackers try to gain access to sensitive information by employing spoofing tactics.

Preference center
A page within a site or application that allows users to adjust the communication cadence with a brand.

Ramp-up
The process of increasing email sending volume.

Root domain
The highest hierarchical level of a site.

Sender authentication
The process of verifying that emails are not fraudulent.

Sender Policy Framework (SPF)
An email authentication protocol that domain owners use to specify the email servers they send emails from. (See Sender Authentication.)

Shared pool
An IP or Domain where the usage is shared among users/senders

Simple Mail Transfer Protocol (SMTP)
An internet standard communication protocol for email transmission.

Spam
Emails that are malicious, unsolicited, undesired, and/or irrelevant.

Spoofing
The act of posing as a person or a program by falsifying information to gain an illegitimate advantage.

Subdomain
A subdivision of a domain.

Subscriber
An individual who chooses to receive regular email communications.

Subscriber acquisition
The process where subscribers are added to your sending audiences.

Sunsetting
The process of phasing out unengaged email subscribers.

Transport Layer Security (TLS)
A security protocol that encrypts email delivery for privacy.

References

- 'This surprising simple email trick will stop spam with one click,' Forbes, 2020 - https://www.forbes.com/sites/daveywinder/2020/05/03/this-surprisingly-simple-email-trick-will-stop-spam-with-one-click/?sh=4c6dd7f23791

- 'Yahoo adds spam filter to email, but will it work?' CNET, 2002 - https://www.cnet.com/tech/services-and-software/yahoo-adds-spam-filter-to-email-but-will-it-work/

- 'British man gets 4 years for 'phish' fraud,' NBC News, 2005 - https://www.nbcnews.com/id/wbna9884895

- 'UK spammer sentenced to 6 years,' ZD Net, 2005 - https://web.archive.org/web/20080621230427/http://news.zdnet.com/2100-1009_22-5958081.html

- '$11 billion judgement awarded in spam case,' NBC News, 2006 - https://www.nbcnews.com/id/wbna10726635

- Number of email users worldwide from 2017 to 2025, Statista - https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/

- 'How many emails does the average person receive per day in 2022?' Earthweb, 2022 - https://earthweb.com/how-many-emails-does-the-average-person-receive-per-day/#:~:text=According%20to%20email%20receiving%20statistics,Yes%2C%20that%20is%20a%20lot!

- The ROI of email marketing (Infographic), Litmus, 2021 - https://www.litmus.com/blog/infographic-the-roi-of-email-marketing/

- Number of sent and received emails per day worldwide from 2017 to 2025, Statista - https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

- B2B Content Marketing: Benchmarks, budgets, and trends, Content Marketing Institute, 2021 - https://contentmarketinginstitute.com/wp-content/uploads/2020/09/b2b-2021-research-final.pdf

- 2022 Email Marketing Benchmarks by GetResponse - https://www.getresponse.com/resources/reports/email-marketing-benchmarks

- Digital channels in with personalized communication is used in the United States as of March 2020, Statista - https://www.statista.com/statistics/451788/digital-marketing-channels-with-personalized-communication/

- '68 personalization statistics every digital marketer must keep in mind,' Instapage - https://instapage.com/blog/personalization-statistics

- Frequency with which consumers would like to receive brand emails from selected industries in the United States as of July 2017, Statista - https://www.statista.com/statistics/434649/promotional-email-frequency-preference-usa-consumer/#:~:text=The%20graph%20shows%20the%20preferred,brands%20on%20a%20weekly%20basis.