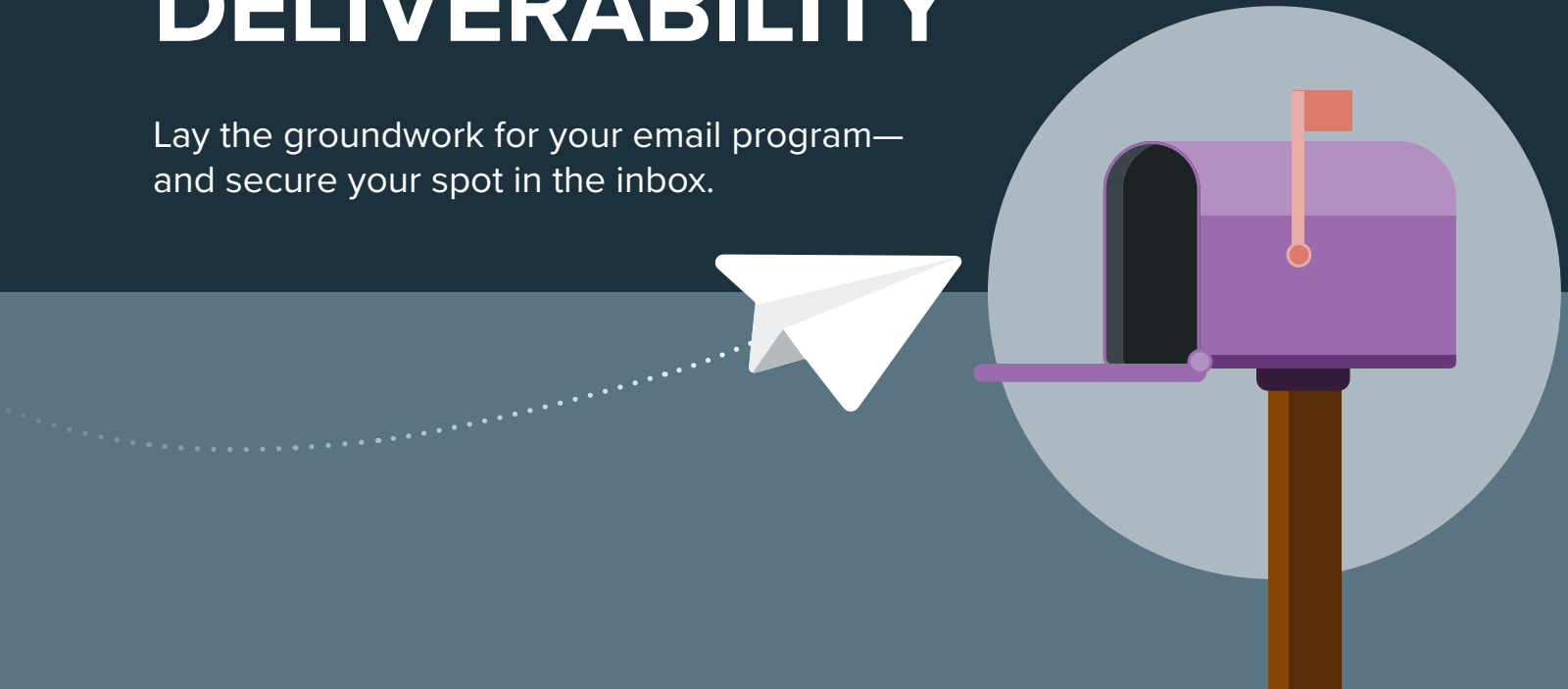
litmus

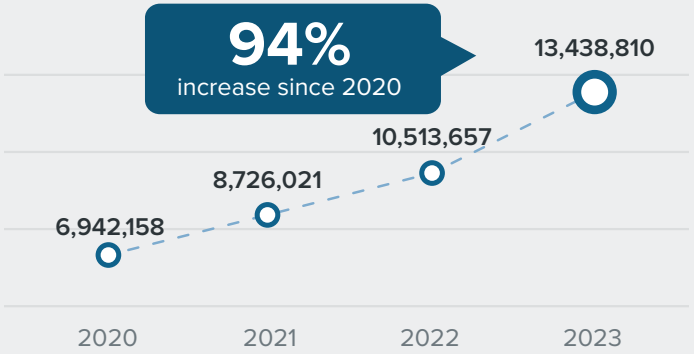
FOUNDATIONS OF EMAIL DELIVERABILITY

Lay the groundwork for your email program—
and secure your spot in the inbox.



Today's email landscape presents its own unique set of challenges. In this evolving digital ecosystem, the uptick in spam and phishing is making it increasingly difficult to ensure your emails reach their intended recipients' inboxes. Email clients know it, too—bad actors, armed with AI, are becoming more adept at cluttering inboxes with unwanted noise.

The concept of spam isn't new. The first spam email was sent in 1978. Since then, email clients have long-established guidelines to help marketers ensure their messages reach subscribers. Most of these guidelines still hold true, but we're seeing email clients evolve their rules to bolster their defense against spam cyberattacks—like Gmail and Yahoo in early 2024.



Source: Bolster AI

Lesson 1 **Email Deliverability 101**
Lesson 2 **Setting Up For Success**
Lesson 3 **Troubleshooting from zero bounce**
Lesson 4 **Maintaining Great Deliverability**

Amidst this dynamic backdrop, we're here to help you learn the basics of email deliverability. From setup to troubleshooting, we'll equip you with the tools and insights needed to navigate the intricacies of getting your email delivered.

LESSON

1

EMAIL DELIVERABILITY 101

In this lesson, we'll explore the essentials of ensuring your emails reach the intended inbox. Learn the what, why, and how of email deliverability as we dissect the factors influencing it and the key metrics to keep a keen eye on. Plus, we'll uncover the inner workings of spam filters, shedding light on how they affect your email campaigns.

1.1 The what, why, and how

1.2 Factors that impact email deliverability

1.3 Key metrics to monitor

1.4 How spam filters work

1.1 The what, why, and how

Missing an important email because it's marked as spam is frustrating. And face it—no email marketer wants to put all that effort into crafting the perfect email, only to find out it landed in the spam folder. So, how can we ensure that our emails consistently reach their intended destination in the inbox? Enter: email deliverability.

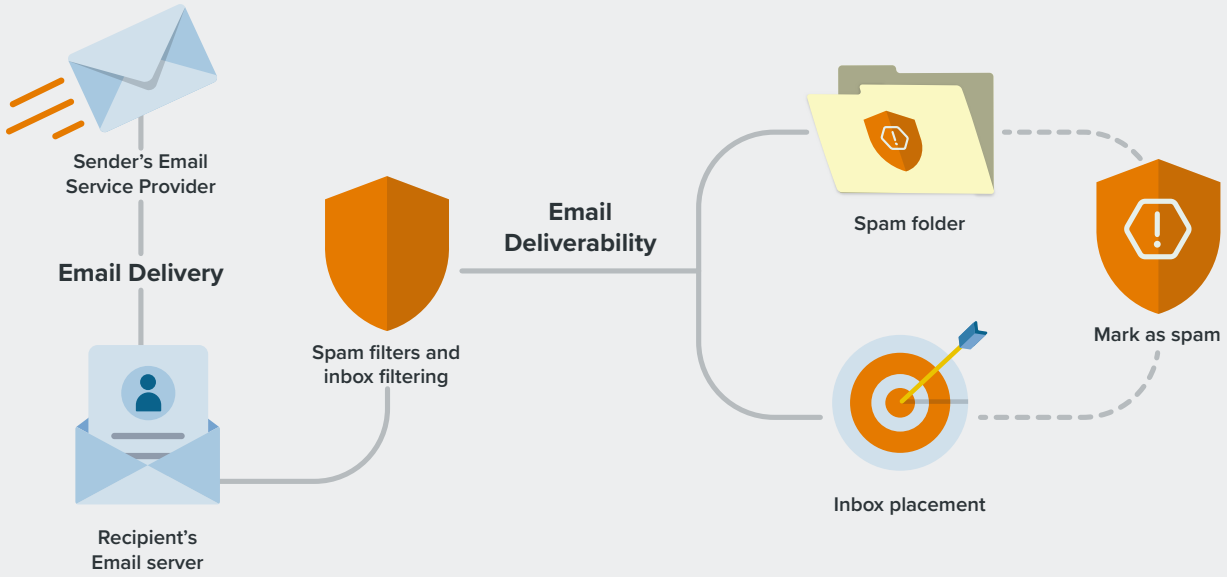
Email deliverability:
/ˈiː.meɪl/ /dɪˈlɪv.ə. əˈbɪl.ə.ɾi/

1. the rate at which your emails successfully land in your subscribers' inboxes rather than being marked as spam and going to the spam folder.

Each time you hit send, your emails embark on a journey. To get from point A to point B, there are a few checkpoints your email has to pass before reaching its destination, that of which correlates to two essential factors: email delivery and email deliverability.

EMAIL DELIVERY	EMAIL DELIVERABILITY
Measures whether your emails make it to subscribers and don't bounce. *This metric can help give insights on your email list health, but it isn't the whole story since a 'delivered' email could be in the spam folder.*	Gauges whether or not your email makes it into your subscribers' primary, social, or promotional inboxes, and not the spam folder.

Delivery indicates whether or not your emails are received by the servers of your subscribers' inbox providers, whereas **deliverability** specifically looks at *where* your message lands if your subscriber does receive your email. In other words, an email can be counted as delivered even if it's in junk.



A high deliverability rate indicates a healthy email program, while low deliverability results in fewer subscribers seeing your emails. If left unattended, poor deliverability can cause a negative ripple effect.

Ultimately, inbox service providers determine whether your email reaches its destination. They evaluate your email against their established standards using filters and protocols.

These factors include:

- Email engagement
- IP and domain reputation
- Blocklists
- Email authentication

	EMAIL DELIVERY	EMAIL DELIVERABILITY
KPI	Delivery rate	Deliverability rate
How to calculate	(number of delivered emails / number of emails sent) x 100	(number of non-junked emails delivered / number of emails delivered) x 100

36:1

On average, for every $1 marketers spend on email marketing, they receive $36 in return.

While below-average open or engagement rates on a single campaign may not harm your program in the long run, a systematic deliverability issue will. When you're investing the same amount of effort into emails but fewer recipients see and act on them, your ROI diminishes. That's why, to maximize the impact of your email investment, high deliverability is essential.

1.2 Factors that impact email deliverability

Email deliverability isn't exactly black and white. Typically, inbox service providers don't share precisely how they determine their opinion of your organization as a sender. However, as of early 2024, Gmail and Yahoo have shed some valuable insights on what impacts deliverability:

If you send more than 5,000 daily emails to Google and Yahoo email addresses, you must:

- **Verify your sender identity** by authenticating using DKIM, DMARC, and SPF records
- **Implement list-unsubscribe headers** and honor opt-out requests within two days
- **Maintain a spam complaint rate below 0.3%** (no more than three spam reports for every 1,000 messages)

How to Navigate New Sender Requirements from Gmail and Yahoo

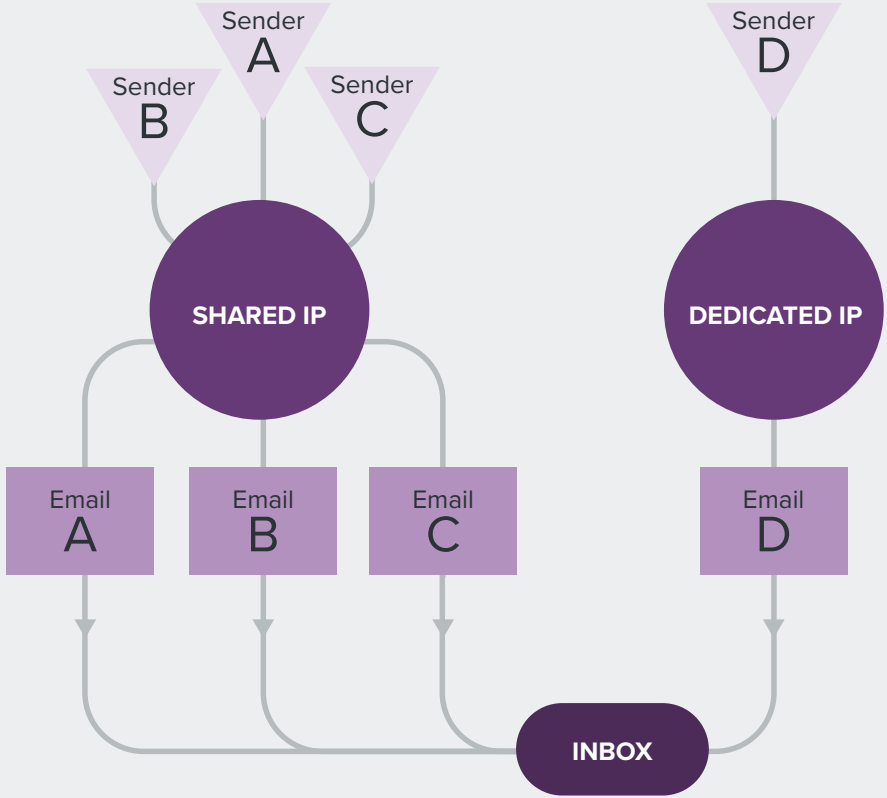
Even if you aren't sending considered a bulk sender (which Google defines as anyone sending 5,000 or more emails in a day), it's in your best interest to abide by these rules, as they overlap with the factors that influence email deliverability.

Factors that can impact email deliverability:

Email volume	A sudden spike in volume could lead to your emails landing in spam. Mailbox filters operate on algorithms designed to track sending volumes and trends.
Send frequency	Be cautious of frequency. Inundating subscribers may lead to unsubscribes and trigger spam filter alerts. Unless you're a recognized sender (like eCommerce), optimal send frequency is once or twice weekly.
Email content and formatting	Ensure your subject line, preheader text, body content, and images are relevant. Refrain from sending any misleading content—like misleading subject lines—and respect subscriber preferences.
List quality and email engagement	Inbox service providers factor in your list quality and email engagement to determine whether your current audience enjoys your content. Keep quality over quantity in mind and remember to suppress inactive subscribers.
Blocklists	A blocklist is a real-time collection of senders suspected as spam or email abusers. There are two types of blocklists: IP-based and domain-based. A blocklist's impact on your email delivery can vary depending on the list.
Email acquisition	Where and how you acquire new email addresses matters. Sources that tend to be problematic include email list rental and a purchased email list—both tactics we don't condone.
File size	Sending an HTML email with a weight greater than 102KB can lead to a poor subscriber experience (like a long load time) and engagement, which can impact deliverability. Generally, you should aim to keep emails under 80KB when possible.
Sender reputation and authentication	All internet service providers (ISPs) are different, but a sender's reputation will ultimately determine if an email makes it into the inbox or the spam folder. While inbox service providers don't disclose their exact evaluation criteria, factors like email authentication, including SPF, DKIM, DMARC, and BIMI protocols, are important (more on that later).
IP address and infrastructure	Your IP address functions as a digital identifier, pinpointing a website's location and allowing inbox service providers to monitor your actions and verify your identity. Some organizations use a shared or dedicated IP address, and both have pros and cons.

⬇️ **Dive deeper:** Shared IP vs. Dedicated IPs // Which is right for your emails?

At first glance, a dedicated IP might look like a more enticing option due to its simplicity—but that's only part of the story. Here's what you need to know about using a dedicated email IP address.



1.3 Key metrics to monitor

Ensuring good email deliverability is essential for maximizing your budget and efforts in email marketing—and it starts with monitoring. Here are key metrics to assess and address to ensure strong deliverability:

- **Delivery rate:** the percentage of emails the internet service provider's (ISP) servers did not return or bounce
- **Bounce rate:** the percentage of emails with temporary or permanent unsuccessful delivery
- **Spam complaint rate:** the percentage of your audience who mark an email as spam
- **Open rate:** the percentage of your delivered emails that subscribers opened
- **Click-through rate (CTR):** the percentage of how many people click on a call-to-action in your email
- **Unsubscribe rate:** measures how many people opt out of your emails
- **Inbox placement rate (IPR):** the percentage of your emails that make it to the inbox and not the spam folder
- **Sender reputation:** a mix of factors that inbox service providers use to gauge whether you're a trustworthy sender
- **Hard bounce:** These occur when the receiving server is either unable to deliver or rejects the message. It can also occur when there is no mail server at that address, or the domain doesn't exist at all. A hard bounce indicates a permanent reason that an email can't be delivered.
- **Soft bounce:** This occurs when the recipient exists, but for whatever reason, they couldn't receive your message. Soft bounces typically indicate temporary delivery issues.

Learn how to calculate these

🔥LitTip: Benchmarks for B2B

Generally, we recommend focusing on comparing your current email performance with your past metrics rather than fixating on competitors' actions. However, it can be beneficial to reference typical B2B email benchmarks, especially for showcasing your team's success to management:

- **Aim for a bounce rate of 2% or less** or a delivered rate of 98% or more
- **Maintain an unsubscribe rate within the 1-2%** range to uphold good deliverability
- **Investigate potential issues** if your spam complaint rate exceeds 0.3%
- **Strive for an inbox placement rate** surpassing 80%

1.4 How spam filters work

Internet Service Provider (ISP) filters

Successful email marketing hinges on delivering wanted and relevant messages to recipients. ISPs like Google and Microsoft play a crucial role in blocking unwanted emails. Sender reputation determines inbox placement, with ISP filters scanning email content extensively. While specific rules vary, general guidelines include avoiding excessive punctuation, all caps, image-only emails, suspicious links, and link shorteners.

Desktop filters

Desktop filters are installed by individual users on their computers (like MailWasher). They enable recipients to personalize the way they receive emails by allowing them to set preferences for receiving or blocking emails to their address. These filters usually have user-specific settings and often withhold engagement data (e.g., opens and clicks) from senders.

Corporate filters

Businesses often use gateway or hosted spam filters to regulate incoming emails. In the B2B world, corporate filters are more prevalent, with employee engagement having less impact compared to B2C filters. Corporate filters actively interact with emails using SMTP, impacting delivery and sender tracking. They may thoroughly inspect email content, including following links, especially in cases of suspicion or security concerns, prioritizing security over speed.

Lesson recap

Follow guidelines as enacted by Google and Yahoo:

- [ ] **Verify your sender identity** by authenticating using DKIM, DMARC, and SPF records
- [ ] **Implement list-unsubscribe headers** and honor opt-out requests within two days
- [ ] **Maintain a spam complaint rate below 0.3%**, which is no more than three spam reports for every 1,000 messages

Get familiar with the factors that impact email deliverability:

- [ ] Avoid sudden spike in **email volume**
- [ ] Be cautious of **send frequency**
- [ ] Ensure relevant and correct **email content and formatting**
- [ ] Upkeep your **list quality and email engagement**
- [ ] Be aware of **blocklists**
- [ ] Don't rent or buy lists as part of **email acquisition**
- [ ] The smaller the better when it comes to **file size**
- [ ] Follow protocols to keep up your **sender reputation and authentication**
- [ ] Determine the best approach for setting up your **IP address and infrastructure**

LESSON

2

SETTING UP FOR SUCCESS

From following authentication protocols to mastering IP warmup techniques and carefully monitoring volume and frequency, we'll equip you with the knowledge and strategies needed to ensure your campaigns start off on the right foot.

2.1 Follow email authentication protocols
2.2 Email permission and anti-spam laws
2.3 IP warmup
2.4 Monitor deliverability

2.1 Follow email authentication protocols

One of the first steps an email marketer should take is setting up email authentication protocols for their program.

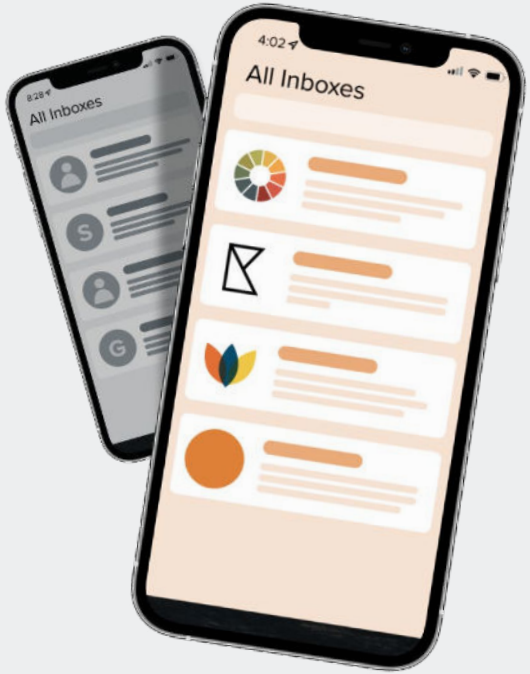
Email authentication refers to mechanisms or protocols that enable you or your mail server to verify the legitimacy of a message using a specific internet domain in the "from" field. Put simply, it questions whether a message from an address like sales@company.com was genuinely authorized by company.com.

Setting up these protocols correctly lets inbox servers know you're legitimate:

- **Sender Policy Framework (SPF):** Allows mail services to double-check that incoming mail from a specific domain has, in fact, been sent from that domain. SPF protects the envelope sender address, or return path, by comparing the sending mail server's IP address to a master list of authorized sending IP addresses as part of the DNS Record.
- **DomainKeys Identified Mail (DKIM):** Allows your organization to claim responsibility for your email. It's an identifier that shows your email is associated with your domain and uses cryptographic techniques to make sure it should be there.
- **Domain-Based Message Authentication, Reporting, & Conformance (DMARC):** Gives you insight into the abusive senders that may be impersonating you–and can help you identify them. It allows a sender to indicate that an email is protected by SPF or DKIM. The sender can then receive a report back on any messages that failed the authentication and identify if anyone using the domain could be a spammer.
- **Brand Indicators for Message Identification (BIMI).** A text record that is used to verify information about your brand that works right alongside SPF, DMARC & DKIM and signals to email clients that you are you.

🔥LitTip: Don’t skip BIMI!

While SPF, DKIM, and DMARC have served as the long-standing authentication protocols, we strongly advise integrating BIMI into your setup. It was introduced in the past decade, and implementing it now will privacy-proof your email program for years to come.



2.2 Email permission and anti-spam laws

We're not fans of buying email lists simply because you can't buy permission. While you can take the action of purchasing a list, it doesn't mean you're welcome in the inboxes of the email address owners.

Sending emails to individuals who haven't granted permission—and may not be familiar with your brand—can result in spam complaints, potentially leading to being blocklisted. That's why spam laws exist.

First, let's begin by clearly outlining the two primary forms of email permission:

Single opt-in (SOI)

Subscribers are added to your mailing list without requiring explicit confirmation of their opt-in decision.

Double opt-in (DOI) *also known as confirmed opt-in (COI)*

Subscribers are added to your mailing list only after clicking a confirmation link in an opt-in confirmation request email, ensuring explicit consent.

	SINGLE OPT-IN	DOUBLE OPT-IN
Subscriber Experience	Less friction	More friction
List Growth	Faster	Slower
Engagement	More overall	Better overall
Deliverability	Higher bounce rates and bad addresses	Lower bounce rates and cleaner lists

🤔**Which is better?**
It depends—and it's ultimately your call. Here's where we stand on SOI vs. DOI.

Anti-spam laws protect citizens from receiving unwanted, unsolicited commercial or spam emails. These include:

Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM)

Law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

Canada's Anti-Spam Legislations (CASL)

Federal law dealing with spam and other electronic threats. It is meant to protect Canadians while ensuring that businesses can continue to compete in the global marketplace. There are two types of consent under CASL: express and implied.

A note on pre-checked boxes

Certain laws require affirmative action in order to consent to receive marketing emails—like GDPR and CASL.

- For General Data Protection Regulation (GDPR), opt-in must be explicit. You cannot use a pre-checked checkbox on a form.
- For CASL, you will mostly need explicit permission. You cannot use a pre-checked checkbox on a form.

Both CAN-SPAM and CASL focus on transparency and choice around unwanted electronic communication. They both require that all promotional emails include a working unsubscribe link and sender identification.

2.3 IP warm-up

Got a new email domain or IP address? Make sure it's warm before sending emails to avoid spam folders. Whether you're switching ESPs, rebranding, or facing delivery issues, a proper warm-up is crucial.

There are a variety of reasons to consider an email warm-up. They may include:

- Starting with or changing email service providers (ESPs)
- Rebranding following an acquisition or merger
- Transitioning from shared to dedicated IP
- Shifting to a subdomain for email hosting
- Initiating an email reset due to past delivery problems
- Preparing for a high spike in email volume think Black Friday sales or special promotions

Email IP or domain warming is slowly sending emails from a new IP address or domain name and gradually increasing send volume over time.

Because email warming requires time and coordination, it's not something most people want to do just for fun. Here's how to determine if an IP or domain warm-up is necessary for you and how to best execute an IP warm-up.

2.4 Monitor deliverability

Keeping a close watch on your email program's health is crucial for long-term success. Here's how to continually optimize your strategy.

- **Track key metrics:** In addition to the core metrics discussed in Lesson 1, you should track things like sender reputation, subject line performance, engagement rate, and brand security.
- **Check for blocklists:** Being on a blocklist can significantly impact deliverability, so it's essential to stay vigilant! You can manually search on platforms like MX Toolbox and Sender Score (or use a tool like Litmus Spam Testing which can check your IP address and domains against blocklists).
- **Use inbox placement and deliverability tools:** There are tools that go beyond what you can track in your ESP—like Litmus Spam Test, which scans your emails against 20+ different tests, identifying any issues that could prevent you from landing in the inbox. Best of all, it provides actionable advice for how you can fix them, before you hit send.

Lesson recap

- [ ] **Ensure you set up authentication protocols:** SPF, DKIM, DMARC, and BIMI.
- [ ] **Determine whether single opt-in or double opt-in** is best for you.
- [ ] **Avoid using pre-ticked boxes** as it's not GDPR or CASL compliant.
- [ ] **Assess whether an IP warm-up** needs to take place.
- [ ] **Monitor deliverability** by tracking key metrics, checking for blocklists, and using inbox placement and deliverability tools.

LESSON

3

zero bounce

TROUBLESHOOTING *from ZeroBounce*

You've built a foundation for understanding email deliverability. And, you've learned some tricks of the trade to set yourself up for deliverability success.

But what if you find yourself facing deliverability issues? Here's what to do next.

3.1 What to do if you've emailed a spam trap

3.2 What to do if you've been blocklisted

3.3 How to conduct an email deliverability audit

3.1 What to do if you've emailed a spam trap

Sending an email to a spam trap can cause deliverability issues. And it may get you blocklisted.

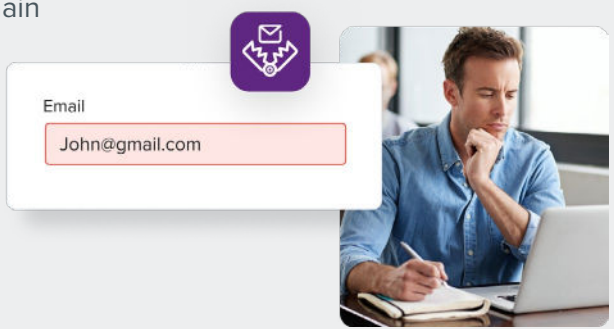
Spam trap: An original or repurposed email address used to bait and identify spammers.

Types of spam traps include:

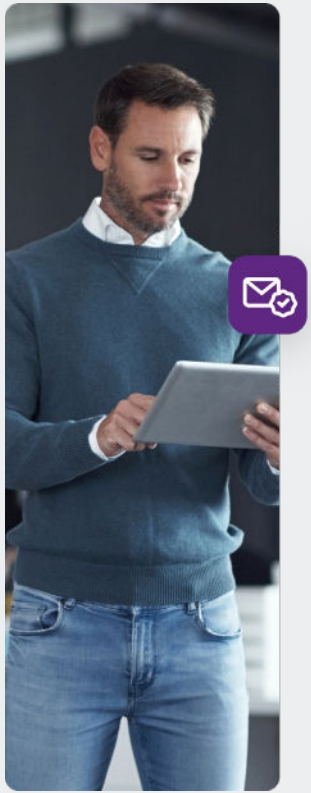
- **Pristine**: An original address that cannot receive emails and exists to catch spammers
- **Recycled**: A previously owned, abandoned address
- **Typos**: An address that contains a deliberate typo within a common email domain

Spam traps can have the following impact:

- Damage to your sender reputation
- Higher bounce rates
- Lower deliverability
- Blocklisting of your domain or IP



If you suspect that you've emailed a spam trap or that your contact list contains one, take the following actions.



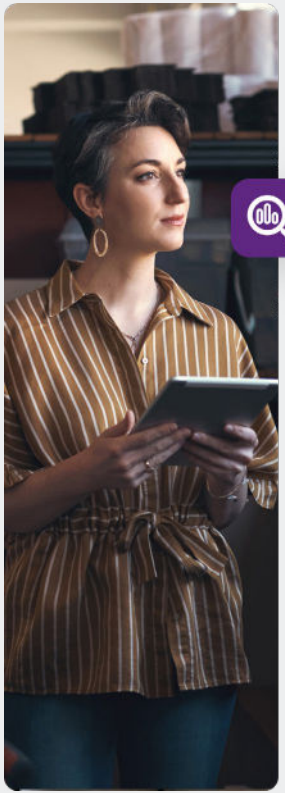
Step 1: Validate your email list

Email validation is the most effective way to identify spam traps. Internet service providers (ISPs) and blocklist services that create spam traps expect legitimate senders to clean their databases. By doing so, you'll avoid the possibility of emailing one.

After you upload your list, the email validation tool will perform a variety of checks, including syntax and SMTP checks. A high-quality tool will also check for disposable domains, spam traps, and other problematic email addresses.

If your list contains any spam traps, remove them from your mailing list. But hang on to the address, as the associated antispam service may also blocklist your domain. This information may help identify where you've been blocklisted.

Be advised: not all email validation tools can detect spam traps. Investigate whether your provider has this capability and a proven track record of consistent accuracy.



Step 2: Investigate your data acquisition process

If you've emailed a spam trap, you shouldn't just clean your list. You must audit where and how you're collecting lead data.

Ask yourself the following questions:

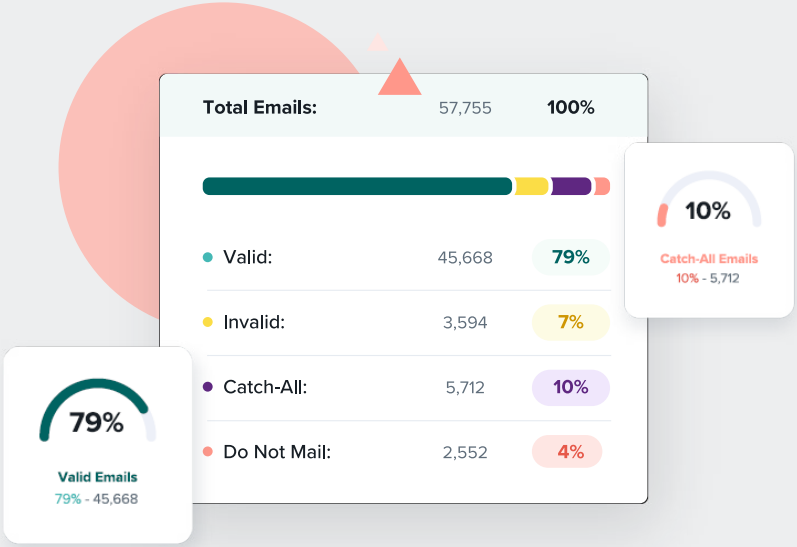
- Have I purchased an email list?
- Am I using a double opt-in process to verify addresses at signup?
- Are my signup forms adequately protected from bot attacks?

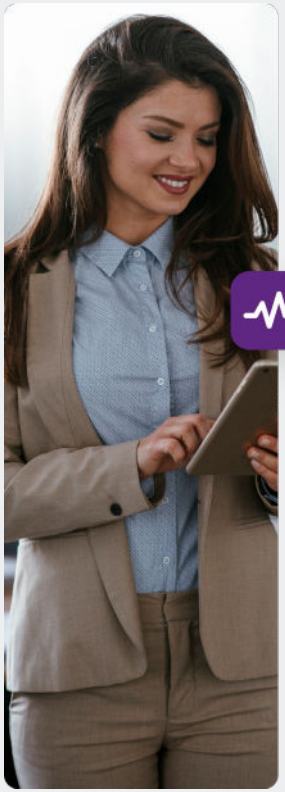
As a rule, you should **never purchase email addresses**. There's no telling how frequently that data has been sold and resold. The data within those lists likely contains outdated and risky data. Even if any contacts are valid, they're not going to be thrilled to hear from a company without opting into receiving communications.

Additionally, consider your signup forms. Are you validating new signups in real time? If not, anyone can submit any data they want into your database.

Finally, ensure that you've implemented a double opt-in process for new signups. This ensures that the address provided is valid and configured to receive emails. It also confirms that there is a legitimate user on the receiving end who is interested in receiving your content.

If your data acquisition process shows weakness in any of these areas, your database will be vulnerable to spam traps. You'll be able to identify where you likely obtained the spam trap from and take immediate action to safeguard your database from risky email data moving forward.





Monitor your campaigns for delivery issues

If your sender reputation is impacted or if your domain has been blacklisted, your deliverability will decline.

ZeroBounce SMTP Deliverability Specialist, Radu Pasarica, shares a few telltale indicators of deliverability problems:

- **High bounce rate:** If your emails bounce back with an error message, check your email blacklist status to see if your IP and domain are safe to use.
- **Blocked emails:** If your emails are being blocked and you cannot connect to the email servers, it may be because of a blocklist restricting your access.
- **Sudden decrease in delivery rates:** If you notice that a significant number of your emails are not being delivered or your new campaign has a lower score than a previous one, it's a strong sign of email blacklisting.

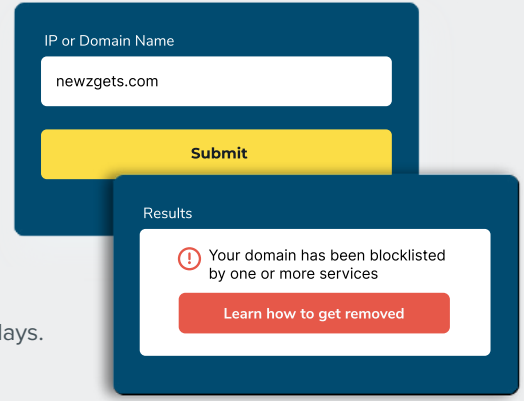
You may also be notified by the blocklist service or by Google if a blocklisting occurs.

zero bounce

3.2 What to do if you've been blocklisted

If you're experiencing deliverability issues, your first stop is an email blocklist checker. Here are some tools you can use to look up your domain and determine if it's blocklisted (sometimes referred to as blacklisted):

- Blacklist, Whitelist, and FCrDNS checker
- ZeroBounce's free blacklist checker



If your domain is listed, follow the attached link to the blocklist service provider's website. Each service operates differently, and you must follow its unique protocol to submit a removal request. Search for your email domain or IP address (whichever's requested) and get your results.

If you're not listed, you're in good shape. If you're blocklisted, follow the provider's removal request steps carefully. Gather all of the data required to avoid unnecessary delays.

You'll likely need proof of domain ownership as well as proof that you've taken action to remedy the issues that earned your domain the blocklisting. Examples might include evidence that you've validated your email list or lowered your bounce rates to an acceptable 2% or lower.

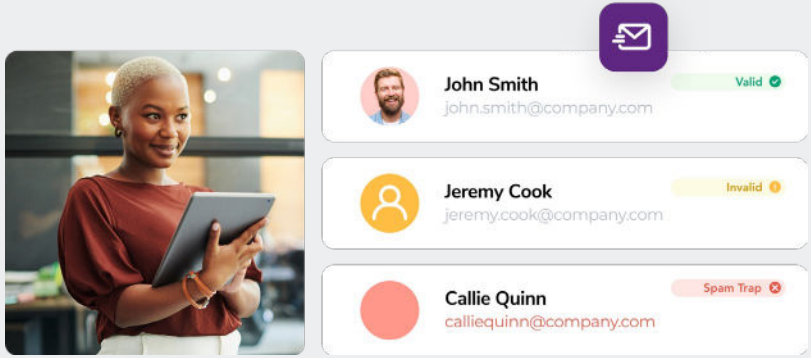
Additional tip: it's recommended that you actively monitor your email domain for blocklist alerts. A blocklist monitor will alert you if you've been blocklisted so that you can take action swiftly.

3.3 How to conduct an email deliverability audit

If you're concerned about your deliverability (or if you're searching for ways to improve campaign performance), consider performing a deliverability audit.

It's recommended to run an audit on an isolated campaign as a variety of factors can impact performance. These factors include:

- Campaign performance
- Email server configuration
- Email content
- Validity of your email list
- Spam filters
- Your email sender reputation



Here's a rundown of what you can do to audit each of these areas.

Step 1: Analyze the campaign's performance

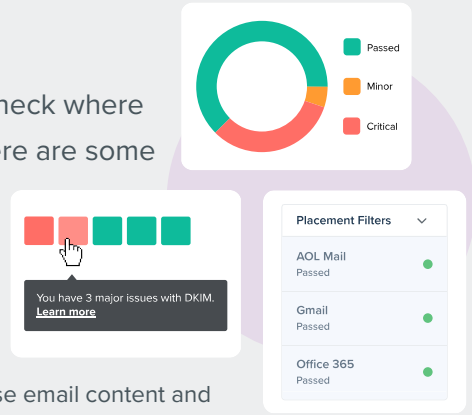
Use your ESP to get a rundown of your campaign's performance. Specifically, look for a high bounce rate, blocked emails, or related error messages.

The number of delivered vs. undelivered emails is often the first sign of deliverability issues.

Step 2: Run an inbox placement test

An inbox placement test is designed to check where (or if) your emails are being delivered. Here are some practical ways to test your content:

- Spam filter tests
- Inbox placement tests



An inbox placement test is an ideal way to diagnose email content and configuration issues. The test runs your email campaign against dozens of popular email providers and their corresponding spam engines. You'll also receive a diagnosis containing relevant error information (return path, from address, authentication alignment, etc.) as well as step-by-step guidance on how to fix your deliverability issues.

Spam filter tests scan your emails, compare them against 20+ spam filters, and determine which (if any) flag your email. Similar to placement tests, it will identify deliverability errors and provide step-by-step guidance on how to handle them. It will also tell you if your domain has been blocklisted.

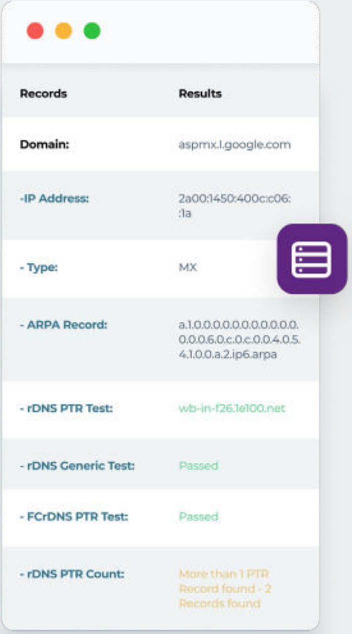
Step 3: Diagnose email server issues

Your email's content may not be the culprit. Improper email server configuration can cause your emails to go undelivered.

Email server factors that can impact your deliverability include:

- **SMTP records:** instructions on how to route your emails (DNS, MX, A, etc.)
- **Email ports:** endpoints that specify the method of message transmission
- **Authentication analysis:** DMARC alignment, SPF, DomainKeys
- **Request for Comments (RFC) standards:** rules for addressing, sending, and delivering electronic messages

An email server test will run diagnostics on each of these areas to pinpoint deliverability threats. Any critical issues should be addressed immediately.



Step 4: Check your email sender reputation

If you've been blocklisted or your deliverability has suffered, this is likely to be reflected in your sender reputation.

You can look up your domain reputation with a variety of free online tools, including Google Postmaster. You'll need to add a DNS record to verify ownership of the domain. Afterward, you'll begin to see data regarding your email campaigns and overall reputation.

Step 5: Validate your email list

Finally, your email list may be the source of your deliverability problems. The best way to identify this is by uploading your contacts to an email validator.

As discussed earlier in this lesson, when identifying spam traps, email validation determines if an email address is valid, invalid, or some other type of high-risk address.

If the list contains invalid emails, your campaigns will have an equal amount of bounces as those addresses do not exist. In addition to invalids, here are some other types of emails that can hurt your deliverability:

- **Disposable domains:** temporary email addresses that self-destruct after a brief period.
- **Abuse emails:** contacts that frequently use (or misuse) the report spam function.
- **Toxic domains:** domains associated with spam or other malicious activity.
- **Catch-all:** an address set up to catch emails sent to invalid addresses on a domain. Catch-alls can be valid but often go ignored by their owners due to spam.

We recommend removing any email contacts without the "valid" status to ensure that your next campaign reaches its destination.

Lesson recap

- [ ] **Validate your email list** to detect spam traps.
- [ ] **Monitor your campaigns** for delivery issues.
- [ ] **If your deliverability is low**, use a blocklist checker.
- [ ] **If you've been blocklisted**, contact the blocklist provider and submit a removal request.
- [ ] **Conduct regular email deliverability audits** to identify and remedy problems before they hurt your sender reputation.

LESSON

4

MAINTAINING GREAT DELIVERABILITY

Now that you know the basics, best practices, and actionable steps to take if you run into an issue, let's dive into how to keep things at bay—or better yet how to achieve and maintain great deliverability.

4.1 List hygiene

4.2 Drive engagement

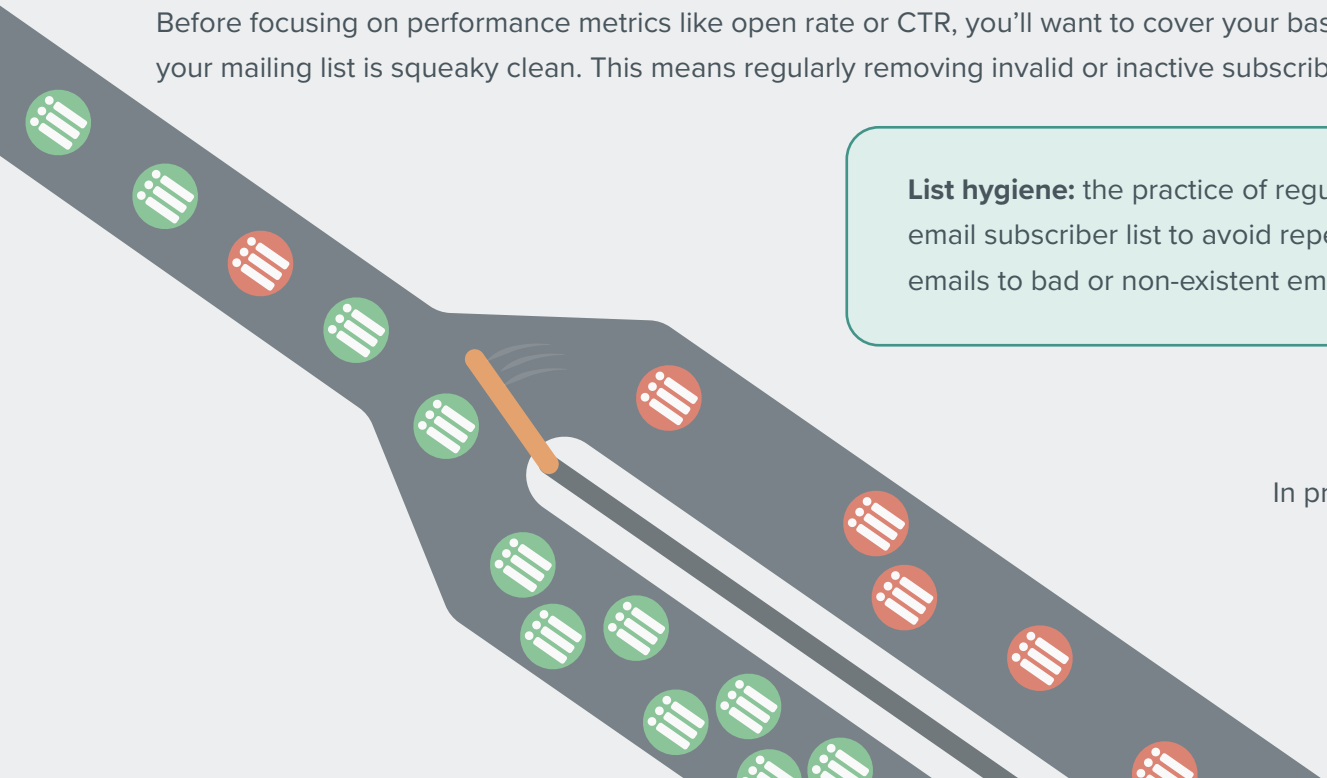
4.3 Review segmentation regularly

4.4 Resources

4.1 List hygiene

Just like a car needs regular cleaning and maintenance to support its longevity, so does email deliverability. The backbone of an email program is its subscribers—specifically its mailing list.

Before focusing on performance metrics like open rate or CTR, you'll want to cover your bases by ensuring your mailing list is squeaky clean. This means regularly removing invalid or inactive subscribers from your list.



List hygiene: the practice of regularly cleaning your email subscriber list to avoid repeatedly sending emails to bad or non-existent email addresses.

In practice, list hygiene looks like this:

Step 1: Identifying invalid email addresses

Invalid email addresses are ones that don't exist or will bounce when delivered. They can end up on your list for a variety of reasons: typos in an email address, subscribers using a disposable email, a full inbox, or even a spam trap.

3 reasons an email address is invalid

1. **Bad format:** Email addresses have a standard format (pictured below). If any of these pieces are missing or duplicated, then the address is not valid.
2. **Bad domain:** If the format is correct, but the domain name doesn't have an email server associated with it, then it is not a valid email because there is no email server to receive messages sent to it.
3. **Bad account:** If the first account name doesn't exist or is incorrect, then it is not a valid email address.

These can be identified through a list verification process, e.g. with an in-form verification tool or asking folks to enter their email twice so it matches.

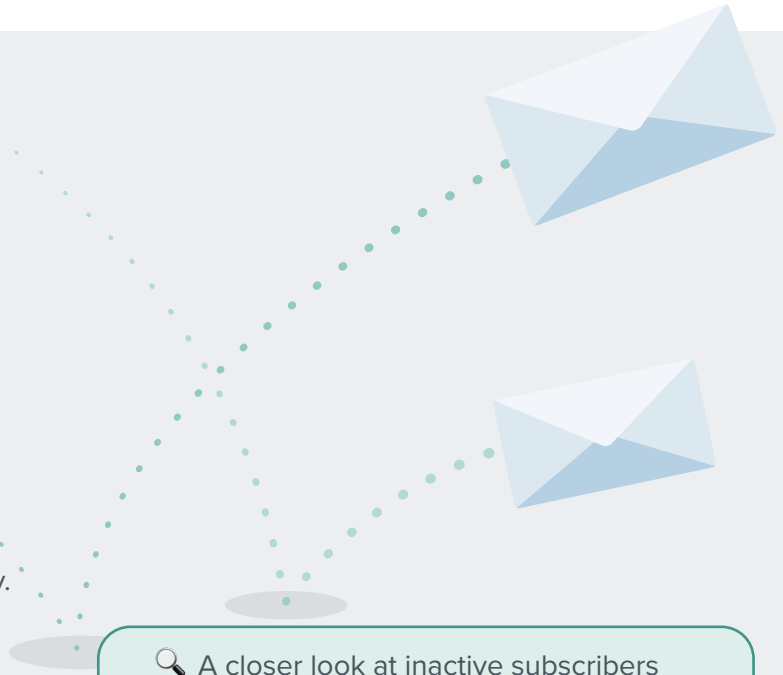
accountname@domainname.suffix

Step 2:
Removing invalid email addresses

While a few bounces shouldn't affect deliverability, too many will eventually make it difficult to reach the inbox. For this reason, hard bounces related to invalid emails should also be removed immediately.

Step 3:
Re-engage inactive subscribers

When it comes to subscribers, quality beats quantity. Inactive or unengaged subscribers can harm your email reputation. Run a re-engagement campaign to identify these subscribers (e.g. ask a segment of people who haven't clicked in an email in the past 90 days if they still want to receive emails) and determine whether you want to attempt to win them back or move on to Step 4...

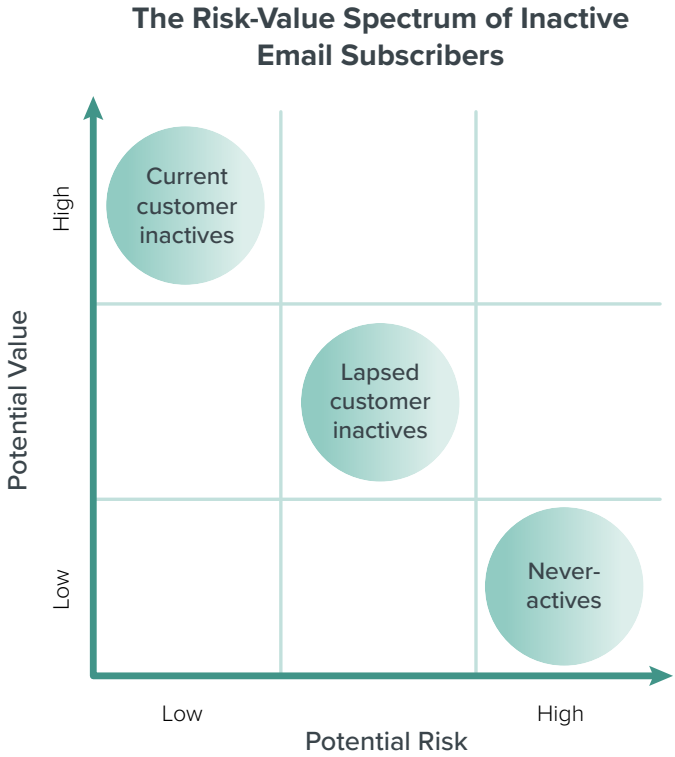


🔍 A closer look at inactive subscribers

Not all inactive subscribers are the same! There are three types: never-actives, lapsed customer inactives, and current customer inactives.

Step 4:
Say goodbye to inactive subscribers

Saying goodbye isn't a bad thing! If subscribers still don't engage after a re-engagement campaign, consider letting them go. Depending on parameters that are important to your brand, it can actually benefit you to remove inactive subscribers to ensure you aren't hitting spam traps and getting blocklisted before your next email campaign. Plus, many ESPs charge based on the size of your list.



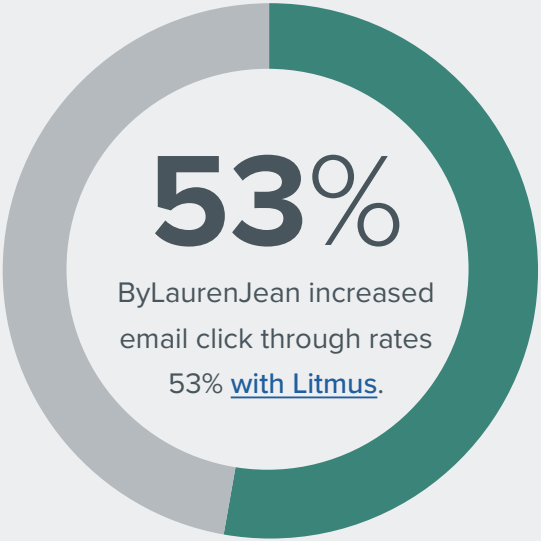
[What You Need to Know to Manage the 3 Kinds of Inactive email subscribers]

4.2 Drive engagement

Engagement is an indicator of how interested subscribers are in your email content. Internet service providers take this into consideration when deciding if your email will reach the inbox or not.

Two important factors for maintaining and improving deliverability are 1) increasing engagement and 2) reducing spam complaints. Said simply, the more relevant the content is, the less likely it will get reported as spam.

How can you increase email engagement? One approach is to focus on email design which creates a more enjoyable reading experience and ultimately drives subscribers toward an action you want them to take. The other is on the content itself.



Design

- **Introduce pattern breaks**, like sharper headlines, compelling imagery, and structure to ensure subscribers are engaged as they scroll.
- **Have clear hierarchy** so it evidently shows subscribers which action to take. For example, a primary call-to-action (CTA) should be styled more prominently than a secondary CTA.
- **Make it scannable**. On average, subscribers spend 8.97 seconds with an email, so they're likely either only reading the top or skimming through your email. Introduce visual anchor points with numbered or bulleted lists, text styling (like bolding, italicizing, or underlining), or even emojis to draw attention to your content.

Level up: How To Create Emails That Sell With Conversion-Centered Design (CCD)

Content

- **Fulfill the expectation set by the subject line**. Provide a consistent journey that starts with the subject line through the landing page. No bait and switch.
- **Humanize your content**. In an era dominated by GenAI, adding a human touch can go a long way to reinforce brand trust. Highlight the no-frills value in what they'll get if they click, or use social proof to show vs. tell.
- **Add personalized, dynamic content to boost clicks**. Make it easy for subscribers to engage with your content by including elements like live polls or Interest Signals. Dynamic content—like live weather reports or product recommendations based on purchase behavior—are also great ways to deliver relevant content that's more likely to get subscribers to click.

Level up: The Email Personalization Handbook: Tips, Tools, and Examples

litmus

Email personalization for all

Whether you're new to email personalization or a pro, you can tap into email marketers' most effective trends with Litmus.

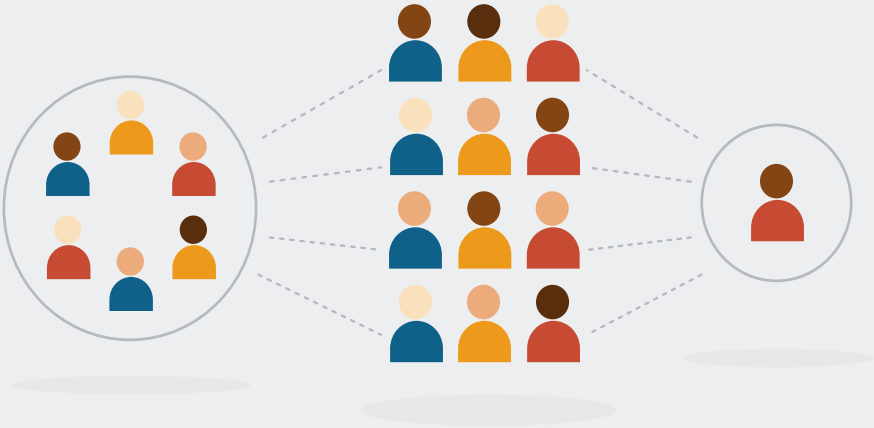
Every Litmus plan includes the tools you need to deliver the right message at the right moment—while making sure it's error-free and ready to drive results—empowering you to make every send count.

Get started today

4.3 Review segmentation regularly

Segmentation goes hand-in-hand with engagement; if you want your subscribers to click your email, you have to send content that's relevant to them.

While segmentation is a marketing basic, it's especially crucial for email engagement and by proxy, email deliverability. This requires you to have a deep understanding of what messages resonate with and truly engage your audience to drive action and which don't.



Nothing in email marketing is truly "set it and forget it," and this rings true when it comes to segmentation. Schedule a time in your workflow, whether that's bi-weekly or monthly, to review your segments and assess whether your segmentation is still the best approach moving forward.

While each email program's audience is unique, here are some top-level segments to consider:

- **Activity:** whether a subscriber has opened an email in the past 90 days or clicked in the past month
- **Geographic:** based on location
- **Content specific:** like subscriber preferences, buying history, or product recommendations
- **Customer vs. prospect:** whether a subscriber has purchased from your brand in the past
- **Role or industry:** specific language or content that's relevant to a subscriber

The key to driving engagement is identifying categories of customers most likely to click-through. By segmenting your audience, you offset the risk of opt-outs brought by spam complaints, emotional unsubscribes (when a subscriber ignores your emails), and over-mailing non-relevant content.

4.4 Resources

Bookmark these resources to keep at hand:

- Email Deliverability Terms You Need to Know [Cheat Sheet]
- The Ultimate Guide to Email Deliverability
- Taking the Mystery Out of Email Deliverability [Infographic]

Level up

Dive into the most important components of email marketing in our series:

- Foundations of Email Design
- Foundations of Email Development
- Foundations of Email Privacy
- Foundations of Email Copywriting
- Foundations of Email Marketing

Lesson recap

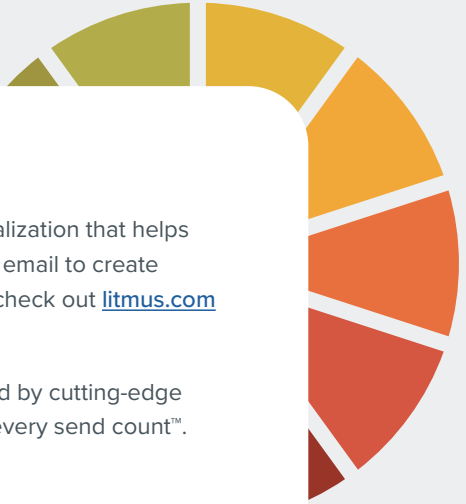
- [ ] Find a recurring time to practice **list hygiene**.
- [ ] Removing **invalid email addresses** promptly to avoid impact on deliverability.
- [ ] Determine whether to re-engage **inactive subscribers** or let them go.
- [ ] Introduce **engagement-boosting tactics** like live polls and sentiment trackers.
- [ ] Actively **review segmentation** to ensure your emails are relevant.

Foundations of Email Deliverability—complete.

Want to stay in touch?

Get how-tos, inspiration, and more from our newsletters—for email pros, by email pros.

Subscribe today



A little about us

Hi! We're Litmus and we offer a complete solution for email optimization and personalization that helps email marketers like you create, personalize, test, protect, review, and analyze every email to create exceptional brand experiences for every subscriber. To learn more about us, please check out litmus.com or connect with us on LinkedIn, Instagram, X, or Facebook.

From solutions for effective email personalization to an airtight QA process monitored by cutting-edge emerging email technology and more, Litmus is here to help your email team make every send count™.

Ready to start sending better emails? Start your free trial with Litmus today!