The Complete Email Deliverability Handbook

2024

Brought to you by ongage

Table of content

Introduction

Achieving excellent deliverability is the first thing we, email marketers, set our sights on. We tend to take landing in the inbox seriously. Keeping it that way is a close second. The reason, of course, is the power of emails to reach customers quickly and cost-effectively. In email marketing, reach is a prerequisite.

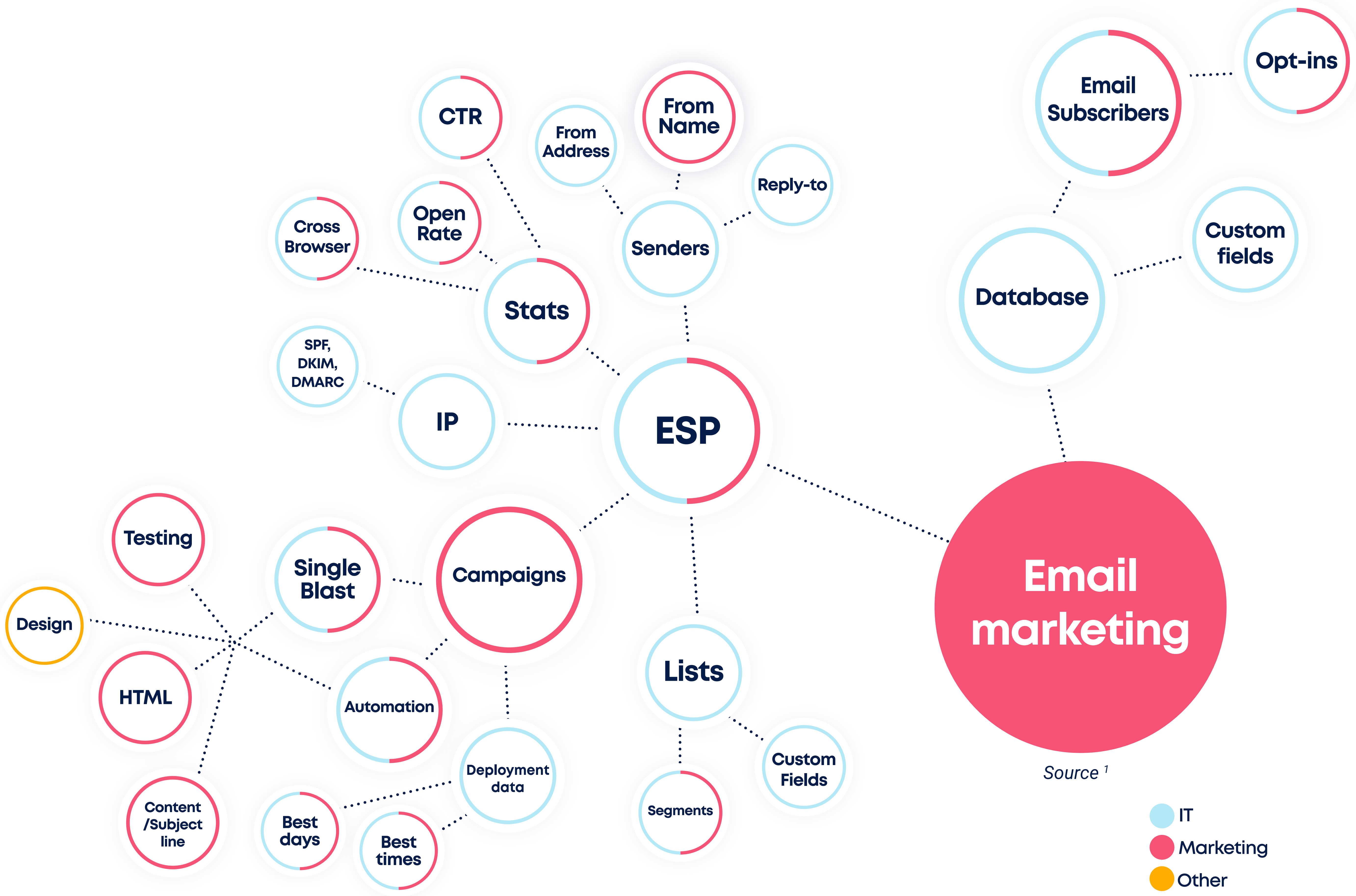
This keeps deliverability our focus at various touchpoints, and it pays off with genuine relationships that cut through the noise. These relationships are an important part of what matters to the internet service providers (ISPs) when they decide if your emails will or not pass muster, but there is so much more.

What you'll find inside

In this handbook, you will find frameworks, workflows, and techniques for both beginners and professionals that ensure your reputation is protected and your email deliverability is as high as can possibly be.

This includes:

- How to measure and identify deliverability and underlying issues.
- What builds reputation?
- Which landmines can hurt your deliverability?



Source [1]

PART 01

Email deliverability: What is it, and why it matters

To answer this, we must first understand the basic difference between delivery and deliverability. Both delivery and deliverability refer to what happens to your email after you send it.

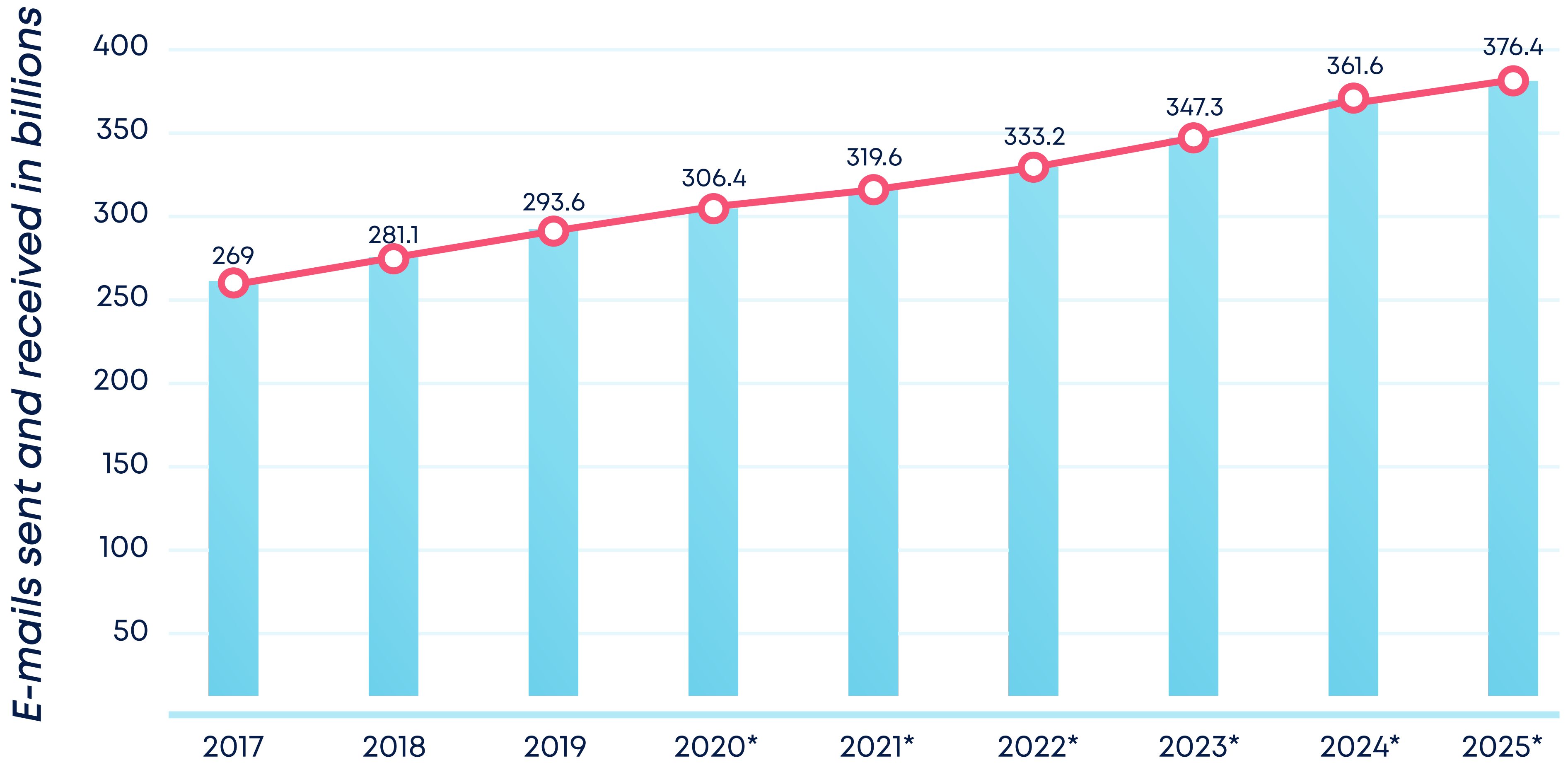
They answer questions like:

- Did it reach the mailbox?
- Where does it land once it arrives in the mailbox? Is it routed to a spam folder, or the inbox?

If the answer to the first question is "yes," it means your email was delivered successfully. Your delivery rate measures the percentage of your emails that made it to the mailbox in simple terms. This implies that you had a viable address, and no technical problems prevented your emails from reaching your subscriber's mailbox.

Where in the mailbox did your email land? That's what deliverability is here to answer. Your deliverability rate measures the percentage of your emails that pass ISPs' spam filters, hop over the spam folder, and eventually land in your subscribers' inboxes.

> "I love this section especially for new email marketers. We all yearn to understand what happens to our email when we hit the SEND button and Ongage lays it out very simply for every level to understand."
>
> **Ryan Phelan**
> Co-Founder of Origin Email Agency

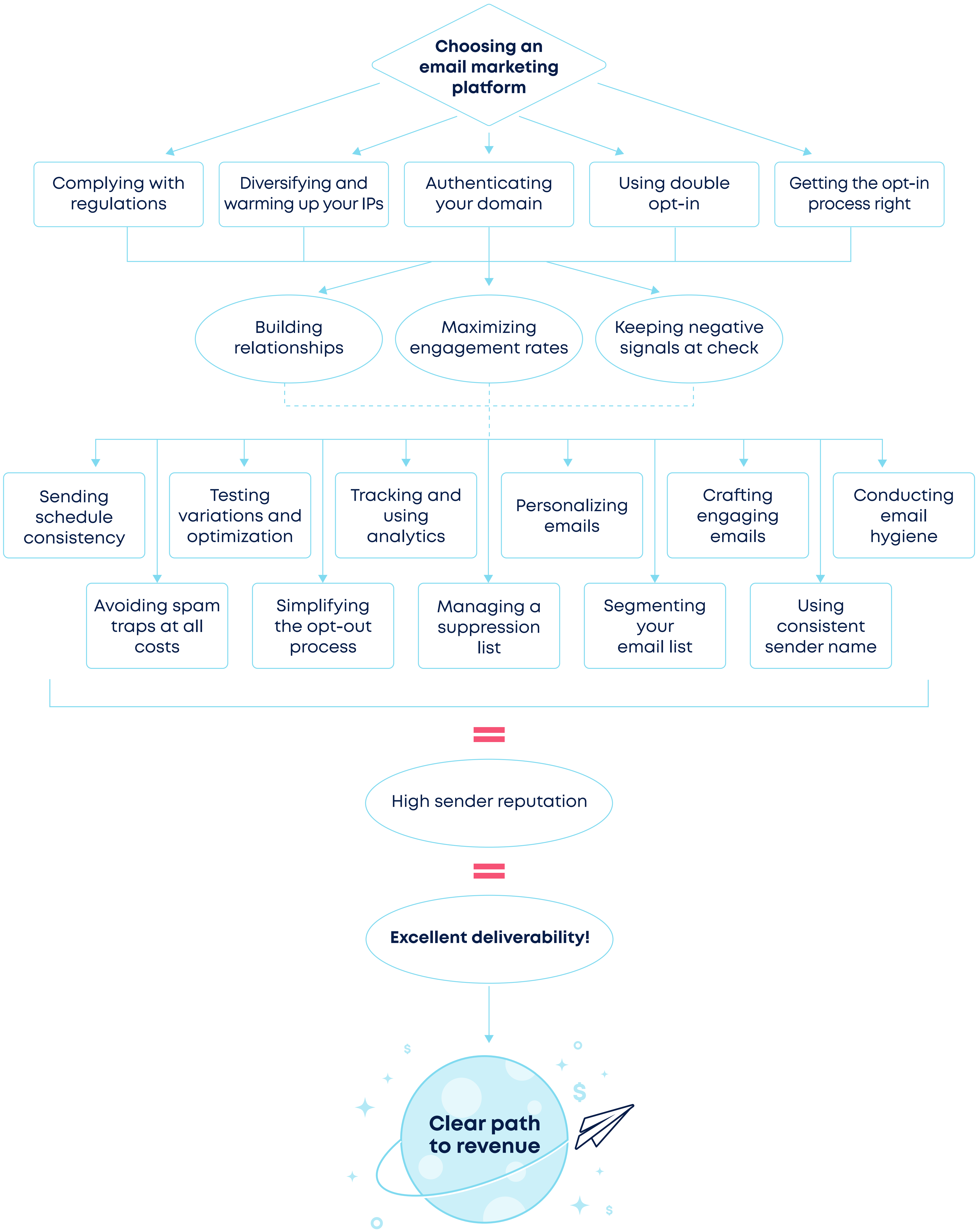


The battle for the inbox is real

The number of emails sent in 2020 per day totaled 306.4 Billion. This number is expected to increase each year moving forward, reaching 376.4 Billion emails per day in 2025.[2]

Workflow:
The complexity of email

Maintaining a good sender reputation is one key to excellent deliverability. There are specific actions you have to do, routines to keep, and regulations with which to comply. In the workflow below, we organize a deliverability `ecosystem' in a hierarchical structure that, if followed to a tee, will keep you on the good side of our friendly neighborhood ISPs.


Choosing an email marketing platform
Complying with regulations
Diversifying and warming up your IPs
Authenticating your domain
Using double opt-in
Getting the opt-in process right
Building relationships
Maximizing engagement rates
Keeping negative signals at check
Sending schedule consistency
Testing variations and optimization
Tracking and using analytics
Personalizing emails
Crafting engaging emails
Conducting email hygiene
Avoiding spam traps at all costs
Simplifying the opt-out process
Managing a suppression list
Segmenting your email list
Using consistent sender name
High sender reputation
Excellent deliverability!
Clear path to revenue

Is there a way to measure your deliverability?

Controlling your deliverability performance can be a challenge because the specifics aren't widely available. The variety of influencing factors and the case-by-case nature of each email campaign (and subscriber) make it even harder to deduce. For instance, an email that reaches one recipient with ease may be blocked from reaching another's inbox.

To discover how your emails perform in terms of deliverability, you'll need to develop a methodology for tracking where your emails end up in the mailboxes (assuming they haven't bounced). Your first step is to look at data from your email platform, examining the total number of emails sent on their journey to the mailbox, and what percentage of them fail to reach it.

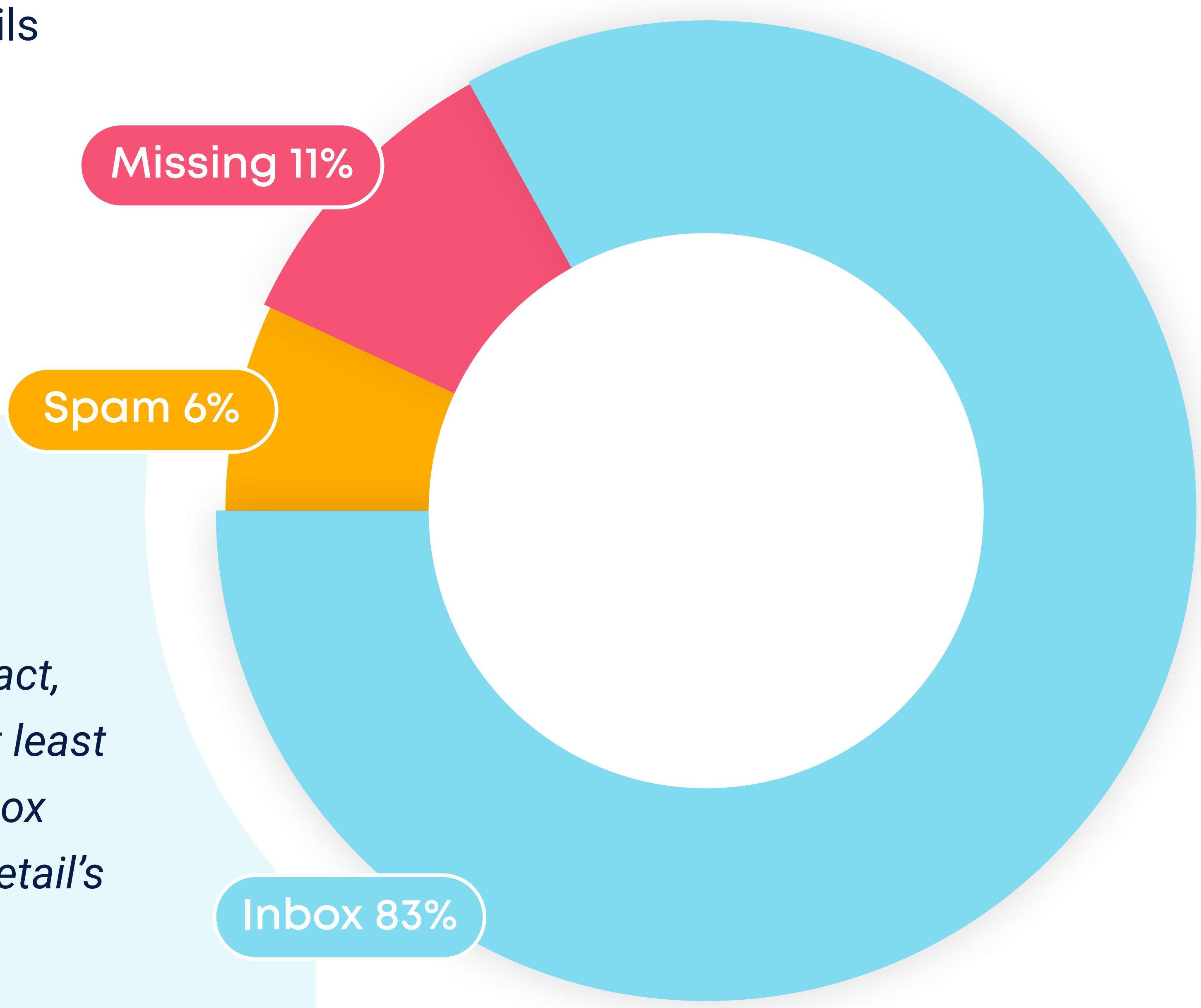
Then, you can use your engagement metrics like clicks and conversions to assess if your emails made it to the inbox.

What do you have to lose?

For email marketing to have a real impact, your inbox placement rate should be at least 95%. However, in 2019, the average inbox placement rate was 83% [3]*, and online retail's email conversion rate was 2.5%.*[4]

This means that 1 in 6 emails don't make it to subscribers' inboxes, and the average sender may be missing out on 42,500 conversions per 1,000,000 emails sent because of deliverability issues.

Think about what 1% of email delivered to the inbox is worth. What about 5% or 10%? For the top internet retailers, this increase could bring millions in additional revenue!



How to calculate your likelihood to land in the inbox

Like spam placement numbers, ISPs don't disclose which of your emails land in recipients' inboxes. As a result, gauging your **Inbox Placement Rate (IPR)** is often a matter of estimating your performance based on positive engagement signals. If your subscribers are opening your emails or clicking through the links you sent them, then you probably reached their inbox.

Another way to gain visibility into your IPR is to use `seed testing' or `seedlist testing.'
At the most basic level, seed testing is similar to sending an email to yourself to see what happens to it. Except, in order to get better data, the emails are sent to a large list of artificial or sender-owned email addresses (the seeds), and the outcome is monitored. Using the inbox placement results from a seedlist test can help you improve your real-world email deliverability performance by understanding if your emails are passing email authentication and spam checks, reaching subscribers' inboxes. That being said, seedlist testing mostly relies on the open pixel, which can be inaccurate and might soon be obsolete due to Apple's MPP (more on that later).

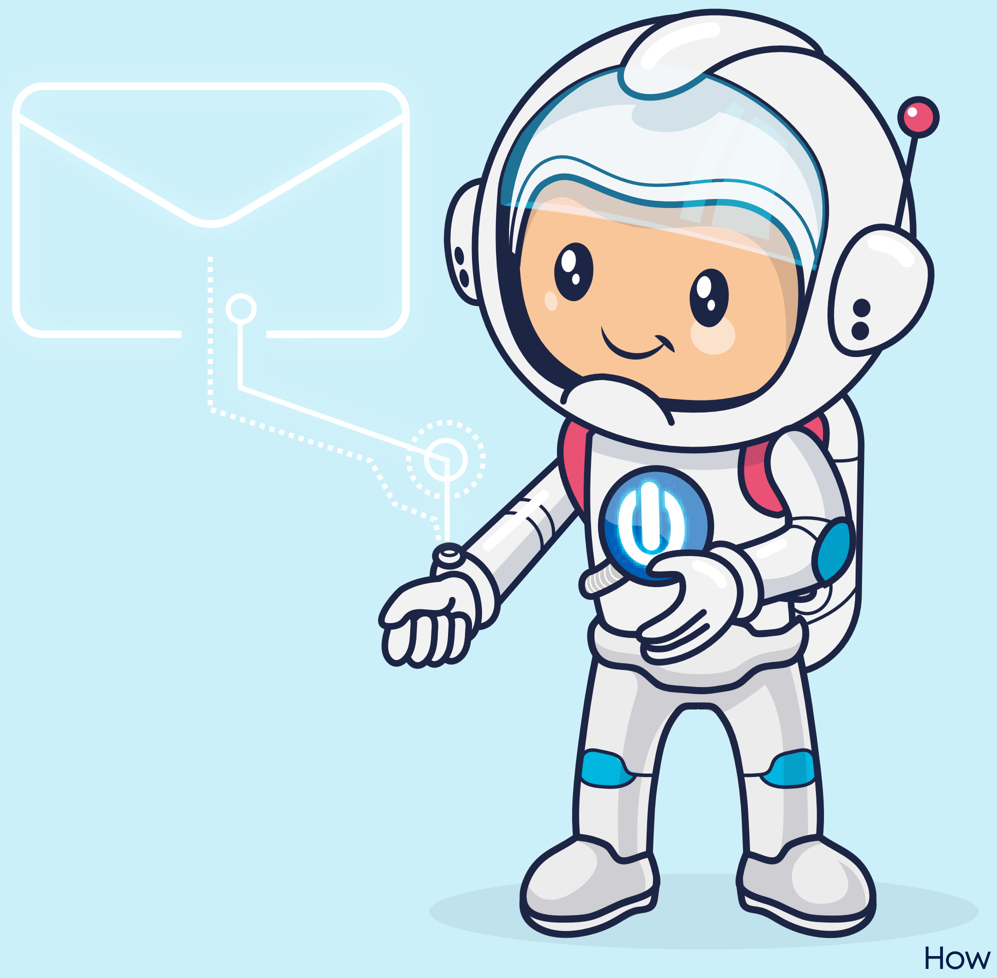
Tip

Even though you can't get final inbox figures from ISPs, you can get some insights into how they rate your domain by using postmaster tools such as:

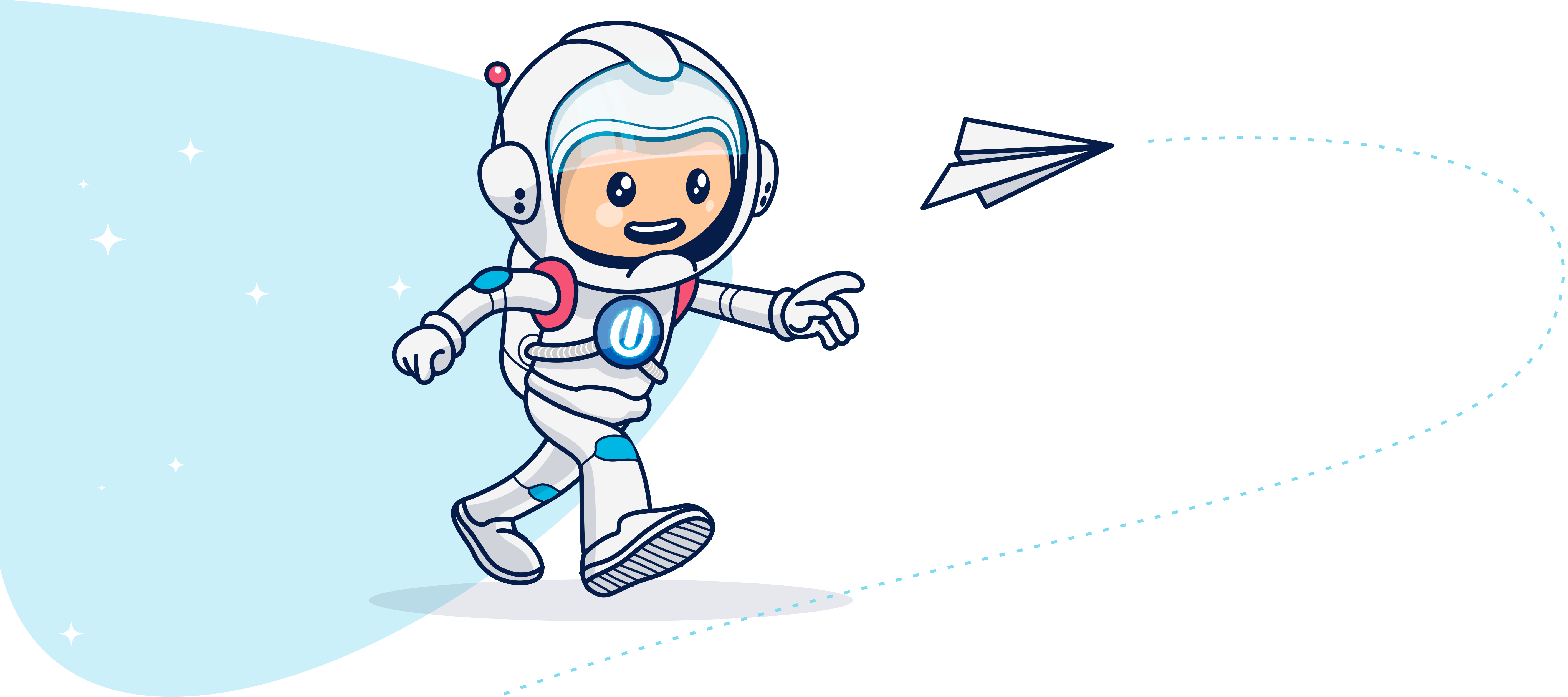
- Google Postmaster.
- Verizon Media Postmaster Tools.
- Microsoft Smart Network Data Services (SNDS).

These tools provide senders with domain and IP-level information about mail performance. The data you'll receive from these tools is anonymized and includes information about mail volume, delivery success, and complaint rates. You can also view your IPs' reputations level (red, yellow, or green) with each ISP. A red or yellow rating doesn't mean that all of your emails are landing in recipients' spam folders. But it is a sign that you should be making changes. Additional information that you may uncover using postmaster tools includes:

- The number of emails reported as spam.
- Your authentication failures. And,
- The reasons your emails bounced back.



Where can your email go after you hit send?



Once you send an email through your email platform, where does it go?
Here are a few of the possibilities:

First option:
Back to where they came from

Emails that aren't delivered are considered as bounced. If the email address or domain you are attempting to reach doesn't exist, or you are blocked from sending mail through the recipient's server, it's a **hard bounce**.

Hard bounces are usually permanent. They can negatively influence your deliverability and get you in trouble with ISPs and your email service providers.
Due to their dangerous nature, most email platforms automatically mark hard bounce contacts as inactive, making sure you won't send to them again.

Soft bounces, on the other hand, allow some room for recovery. A soft bounce may occur when:

- There's a transmission problem.
- The recipient's mailbox was full.
- The email was too large.
- The receiving server was down.
- Your email message appeared suspicious or didn't meet the receiving servers' standards.
- Your domain isn't authenticated.
- And perhaps most importantly, soft bounces can happen when you have a deliverability issue.

This problem may be temporary or can be repaired, so successfully sending to that address in the future is a possibility. But be careful not to overdo it. You don't want to inadvertently spam the address with multiple re-sends or get on the wrong side of your SMTP relay. Follow best practices of excluding contacts that soft bounced more than 3 times in a short period.

Emails that don’t arrive at their destination contribute to your email missing rate. This metric, in turn, can be used to determine your delivery (a.k.a. acceptance) rate. Most email platforms will have this information readily available for you, as they divide the number of emails that arrived to the mailbox by the total send amount before converting it to a percentage.

How to calculate your delivery rate

$$\frac{\text{Emails arrived at mailbox}}{\text{Emails Sent}} \times 100 = \%$$

Second option:
Somewhere, eventually

Sometimes, the ISP won't reject the transmission altogether but might throttle it. This is a warning from the recipient's provider to lower your sending volume and may be accompanied by a soft bounce message.

If your emails are being throttled, you are emailing too much, or sending content that is triggering the receiving server spam filter. Strategies such as the IP warming method that appears later in this handbook can help you overcome throttling issues.

Start tackling throttling issues by checking your mail server data for:

- Sending time.
- Completion dates. And,
- Soft bounce messages to uncover your throttle metrics.

These figures may vary between ISPs, so keep that in mind.

Third option:
The folder of (usually) no return. Spam

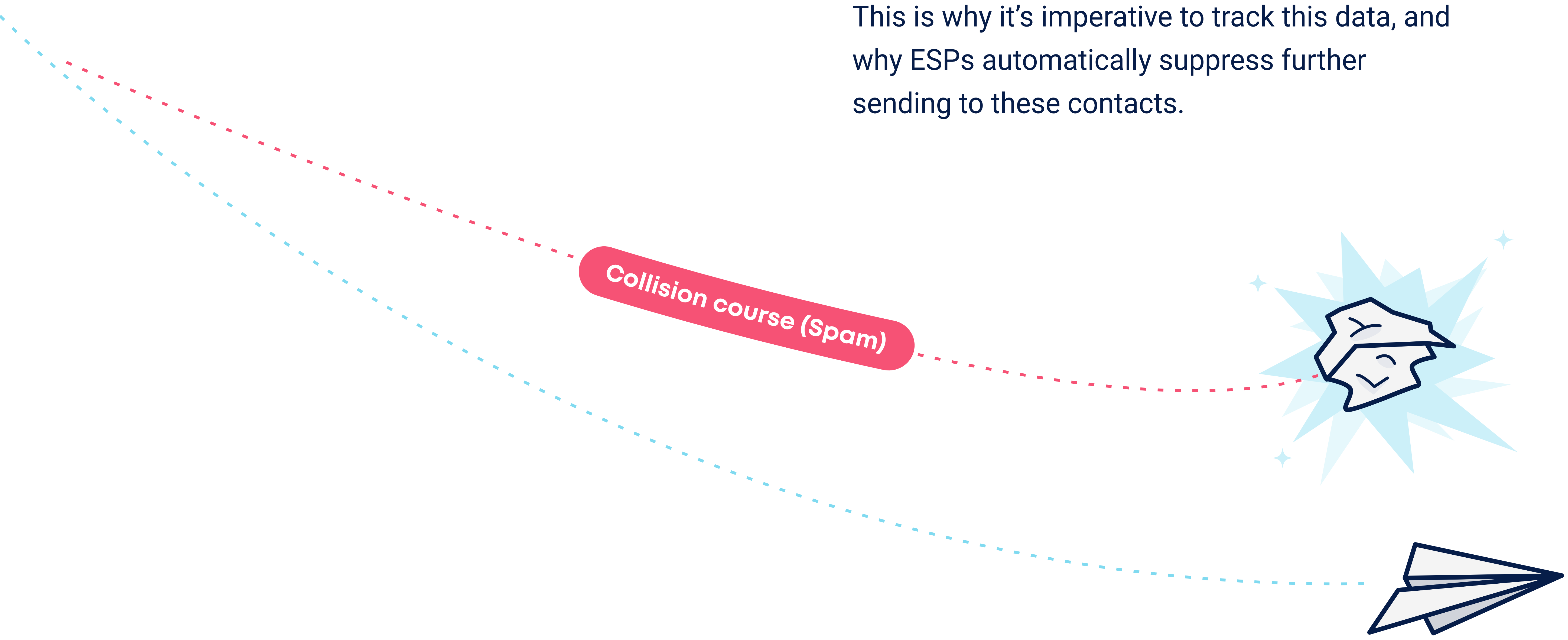
No return is a strong word, we know, but chances are slim.
Your email can end up in the spam or junk mail folder because either:

- Your recipient's mailbox provider thinks it belongs there. Or,
- Your recipient does.

If the provider puts your email in spam, your recipient might find and retrieve it. If it was the recipient's choice to mark you as spam, that email and all your subsequent ones would be sent straight to the spam folder.

ISPs won't tell you how many of your emails they mark as spam. And they definitely don't provide a spam placement rate. That's why we look at the complaint rate, a.k.a spam rate, which reveals the percentage of subscribers reporting your email as spam. You can get this data directly from the ISP by setting up a feedback loop, or by examining your analytics in your email platform.

When an email recipient marks an email as spam, it is a mark against your deliverability. This is why it's imperative to track this data, and why ESPs automatically suppress further sending to these contacts.



Fourth option:
Where you want to be

If all goes well, your email will land in your recipient's inbox. The exact location will depend on your email's content and how your subscriber has configured their inbox tabs.

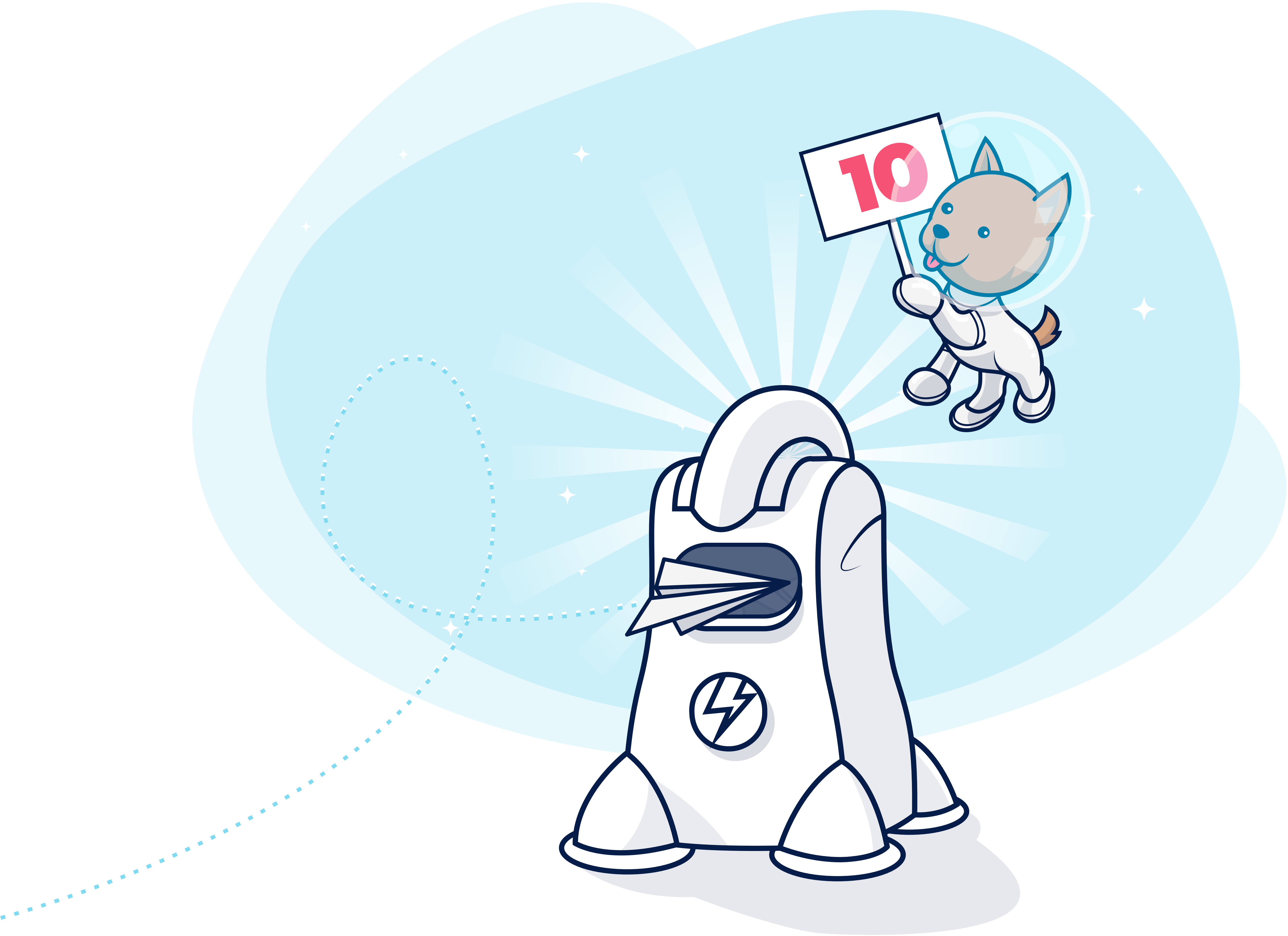
Your emails might land in:

- Their Primary (Gmail) or Focus folder (Outlook). Or,
- Promotions (Gmail) or Update folder (Outlook).

While many email marketers hope to hit the primary folder jackpot every time, making it to any of these folders is considered a deliverability effort win.

The percentage of emails that make it to the inbox out of the total that you send is your inbox placement rate (IPR). This number excludes emails that were blocked or rejected and those that landed in the recipient's spam folder. As mentioned, calculating your IPR is not as easy as discovering other metrics.

> "Don't worry about where your email lands, focus on the value you bring and the message you're sending."
>
> **Ryan Phelan**
> Co-Founder of Origin Email Agency



Why are ISPs acting as gatekeepers for the emails you send?

A lot is invested into sending an email campaign from your side.
You collect email addresses from subscribers and customers, prepare content for them, and you want to reach them with that content. Yet sometimes, ISPs will stand in your way.
Why? Because email users want them to.

You may use best practices for communication and engagement, but not everyone does. A lot of bad actors send emails people don't want. They send emails meant to look like they come from legitimate sources but are aimed at defrauding the recipient (phishing scams). And, some just send so many emails that people get tired of seeing them in their inboxes.

The result of all this bad behavior is that every email sender is now a suspect. Governments have passed anti-spam laws such as CAN-SPAM, GDPR, CCPA, CASL, and more to address these issues to protect email recipients. ISPs decide your emails' deliverability (i.e., whether to allow your emails to reach their customers) by evaluating the likelihood that the message you are sending is spam.

If ISPs decide that your recipient doesn't want to get emails from you, you might develop deliverability problems fast.

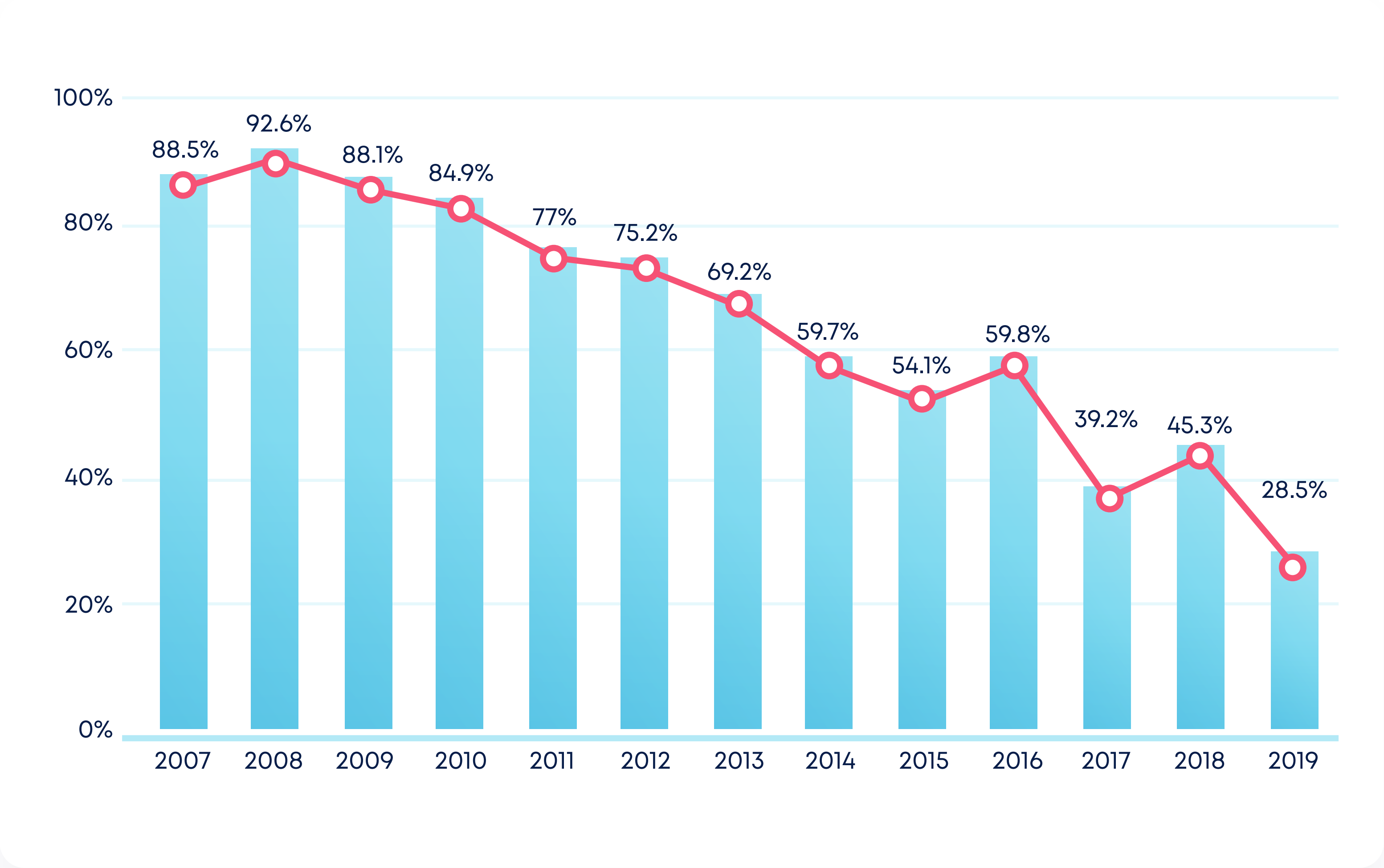
How do you know what not to do?

One of the largest processors of consumer emails, Gmail, publishes bulk sender guidelines to help email marketers stay out of trouble. Other ISPs provide some guidance as well. However, ISPs are not eager to share information about the criteria they use to decide an email's deliverability because this information would make it easier for spammers to get past providers' defenses.

Each ISP uses its proprietary processes and algorithms for filtering the emails they process. These algorithms consider behaviors associated with spammers, feedback from email recipients, and reports generated by third parties to judge the acceptability of your emails.

What email marketers see as a barrier to access, ISPs see as mission-critical customer service.

Global spam volume from 2007 to 2019
(as precentage of total email traffic)



In 2008, the vast majority of email traffic was spam. It's easy to understand why ISPs scrutinize emails, trying to provide immense value to their users. And it works. The proportional volume of spam is ever decreasing.[5]

PART 02

Which factors influence where your email will land?

In reality, your emails' deliverability is out of your control. The recipient and their mailbox service provider decide which emails reach a subscriber's inbox. But there are steps you CAN take to improve the odds of getting to the inbox.

Your deliverability may vary depending on:

- Where you are sending your emails from.
- Who you are sending them to. And,
- Which ISP is in between.

Once you understand the factors that affect your deliverability, you can use this knowledge to improve your deliverability performance and profits. How you and your emails are rated across various factors influences whether a single email reaches its recipient and whether any of your emails will get through a particular provider's gate.

ISPs continually assess your legitimacy and overall reputation as a sender, and clear deliverability metrics can be difficult to acquire.

As an email sender, assessing and managing your deliverability is an ongoing process that includes paying close attention to the factors mentioned above.

As you consider each of the following best practices, keep in mind that the fate of your emails is based on a combination of factors. If the positives outweigh the negatives, your emails stand a much better chance of landing in your subscribers' inbox.

Authentication protocols: How to protect your domain's identity and reputation

How you behave and how consumers respond to you, influences deliverability the most. Combined, these two categories determine your sender reputation. However, before you can earn a good reputation, you first have to establish a legitimate, verifiable sender identity using a set of standardized authentication methods.

> “A poor email reputation is like a hangover. It's hard to get rid of and it makes everything else hurt!”
>
> **Chris Marriott**
> President & Founder of Email Connect

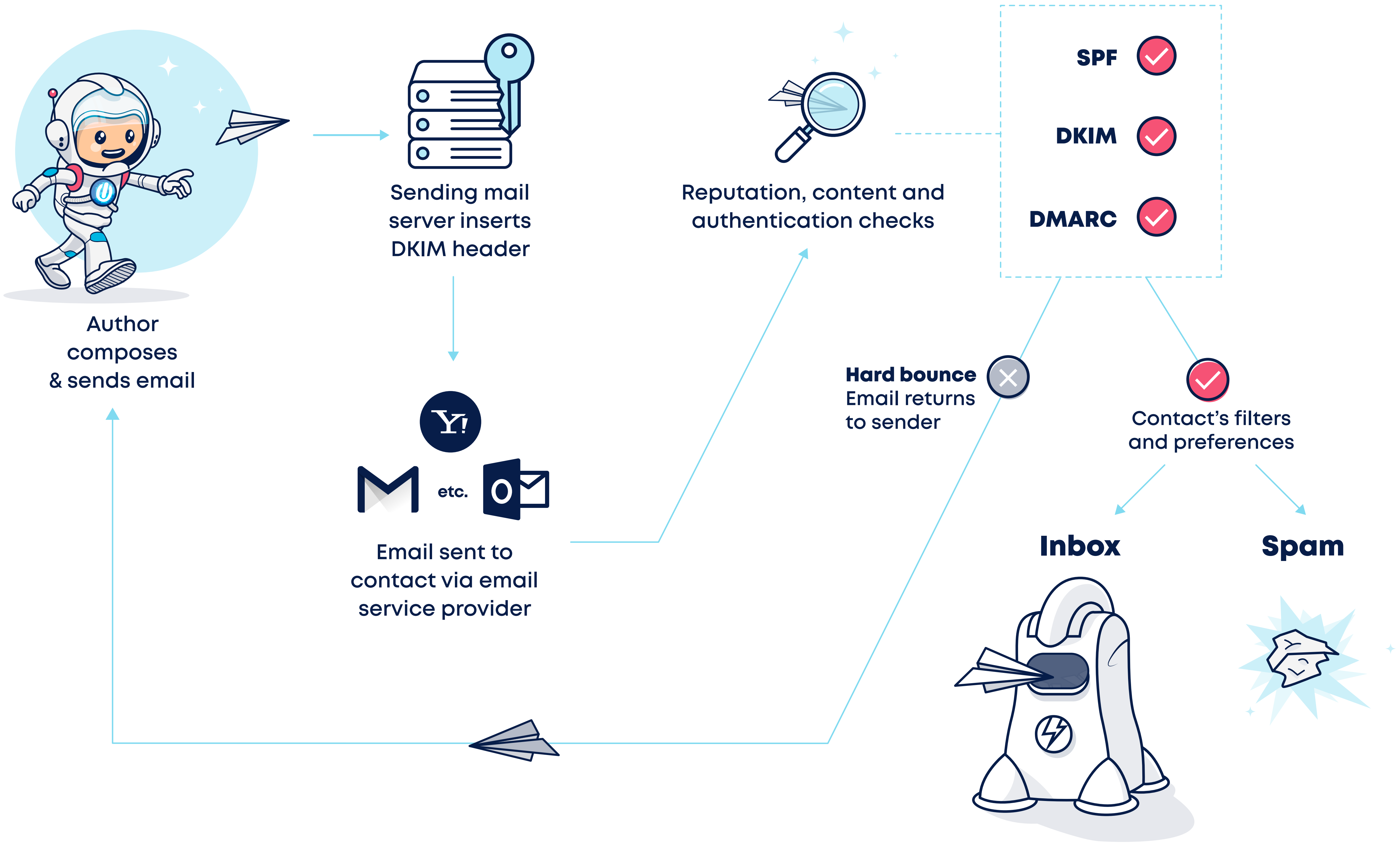
Anyone can send an email and claim it is from your company. Authentication allows other participants in the ecosystem-ISPs, message transfer agents (MTA, more on them in the Glossary), mail delivery agents (MDA), and mail user agents (MUA)-to verify that an email attributed to you as a sender has been sent by you before they transfer or deliver it.

The two main authentication methods that allow you to establish your identity with ISPs are the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) protocols. Many ISPs will block or mark as spam emails from domains that don't employ these protocols.

Two additional protocols also help you establish your sender legitimacy. The Domain Message Authentication Reporting and Conformance (DMARC) protocol enables you to share authentication instructions with other mail agents and receive reports identifying unauthenticated emails being sent in your domain's name. The Brand Indicators for Message Information (BIMI) protocol enables ISPs to display your brand's logo next to your email subject line, telling email recipients that the message is coming from a verified source.

Here's how each of these protocols works to verify your identity and protect your sender reputation:

From send to the inbox: The journey of your email



Author composes & sends email
Sending mail server inserts DKIM header
Y!
etc.
Email sent to contact via email service provider
Reputation, content and authentication checks
SPF
DKIM
DMARC
Hard bounce
Email returns to sender
Contact's filters and preferences
Inbox
Spam

#1 Sender Policy Framework (SPF)

The next couple of sections are filled with technical information. If you have a developer on your team, forward it to them. If you're the person in charge of development in your operation, we highly recommend you keep on reading.

SPF authentication uses DNS Zone associations to identify whether the server sending an email on behalf of your organization is authorized to do so. To use this authentication method, you must publish the IP addresses authorized for use by your domain. When you send an email or a batch of emails, the recipient server checks your list. If the sending server's IP address isn't on that list, the email will be considered unauthorized and sent to spam or blocked.

To implement the SPF protocol, you need to create an SPF record that lists all of your authorized servers-these are -the hostnames or IP addresses that are permitted to send emails for your domain. Do this by gathering a list of your authorized sending domains.

Don't worry about adding your ESPs' domains, as they will have included these on their own SPF lists. (A 0% SPF metric in Google Postmaster usually means your SPF is being handled at the ESP level.)

Then, add this list as a TXT record to your domain settings with your domain host. Identify the record as SPF data by assigning it an SPF version number using the "v" tag. Your version assignment must appear at the beginning of your record.

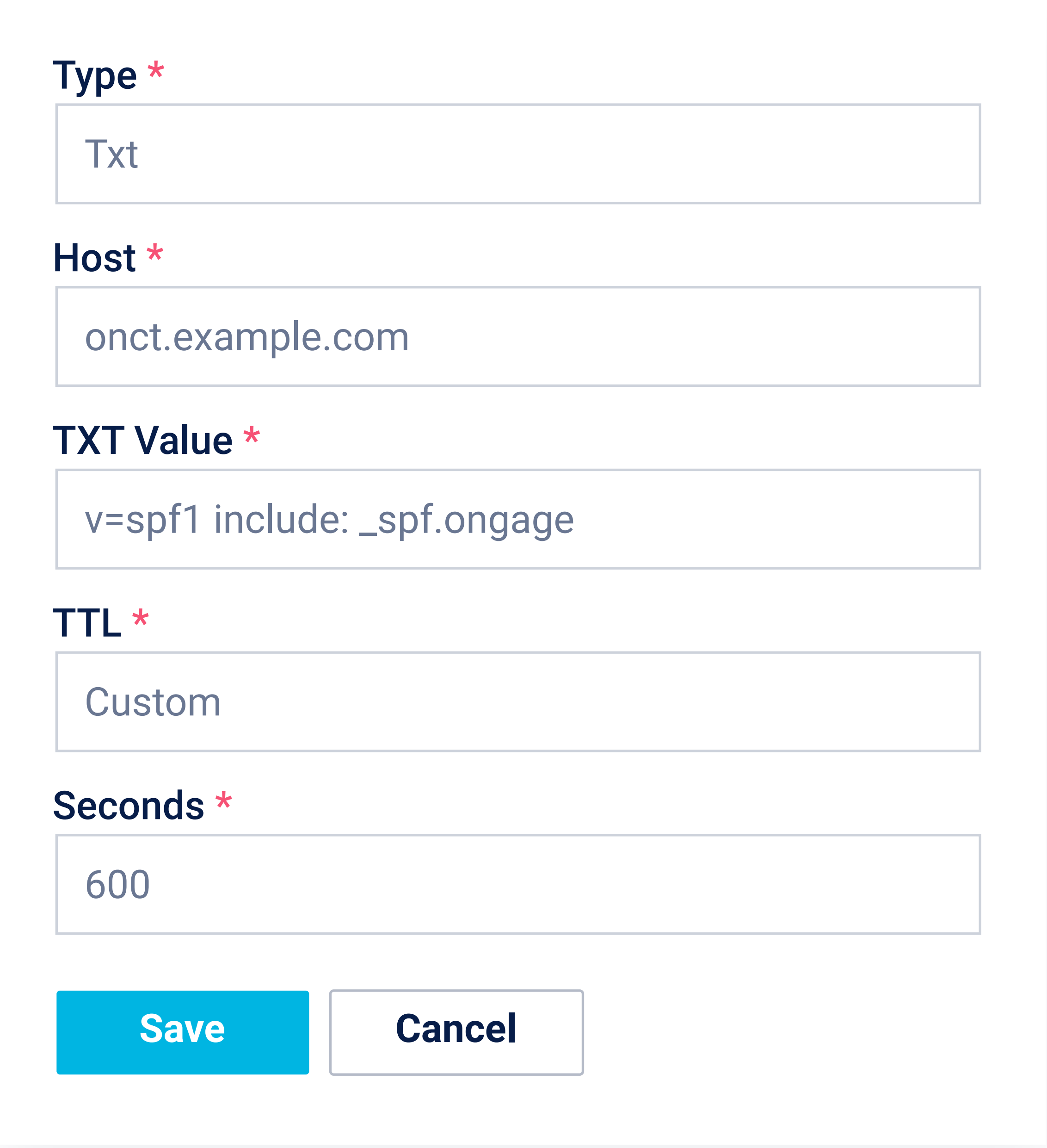
End your SPF record with a tag Indicating the action that you want to be taken if an email representing your domain is sent from an unauthorized address. This tag consists of the word "all" paired with a symbol that tells receiving servers what you want to happen if they don't recognize the sending IP. End your SPF text with "-all" if you want emails from unlisted domains to be rejected as a hard bounce. "All" accompanied by an "~" means that you want the emails to get a soft bounce. They will make it through but will be marked as spam.

If you work through multiple domains, you can use the “include” tag to add your other domain’s SPF data into the SPF record you’ve created. However, be cautious when doing so--one typo and you could accidentally add a spoofed domain’s SPF record.[6]
A completed SPF record will look something like this if you must include individual IP addresses:

v=spf1 ip4:[list of your authorized IP 4 addresses] ip6: [list of your authorized IP 6 addresses] include:[other domain name] ~all

Publish your SPF record by accessing your domain account with your host provider and updating your DNS records with a new TXT record. If you add a new IP address or retire one, be sure to update your SPF record with your domain host.

The process for creating an SPF record in your DNS will look something like the following:



Type *
Txt

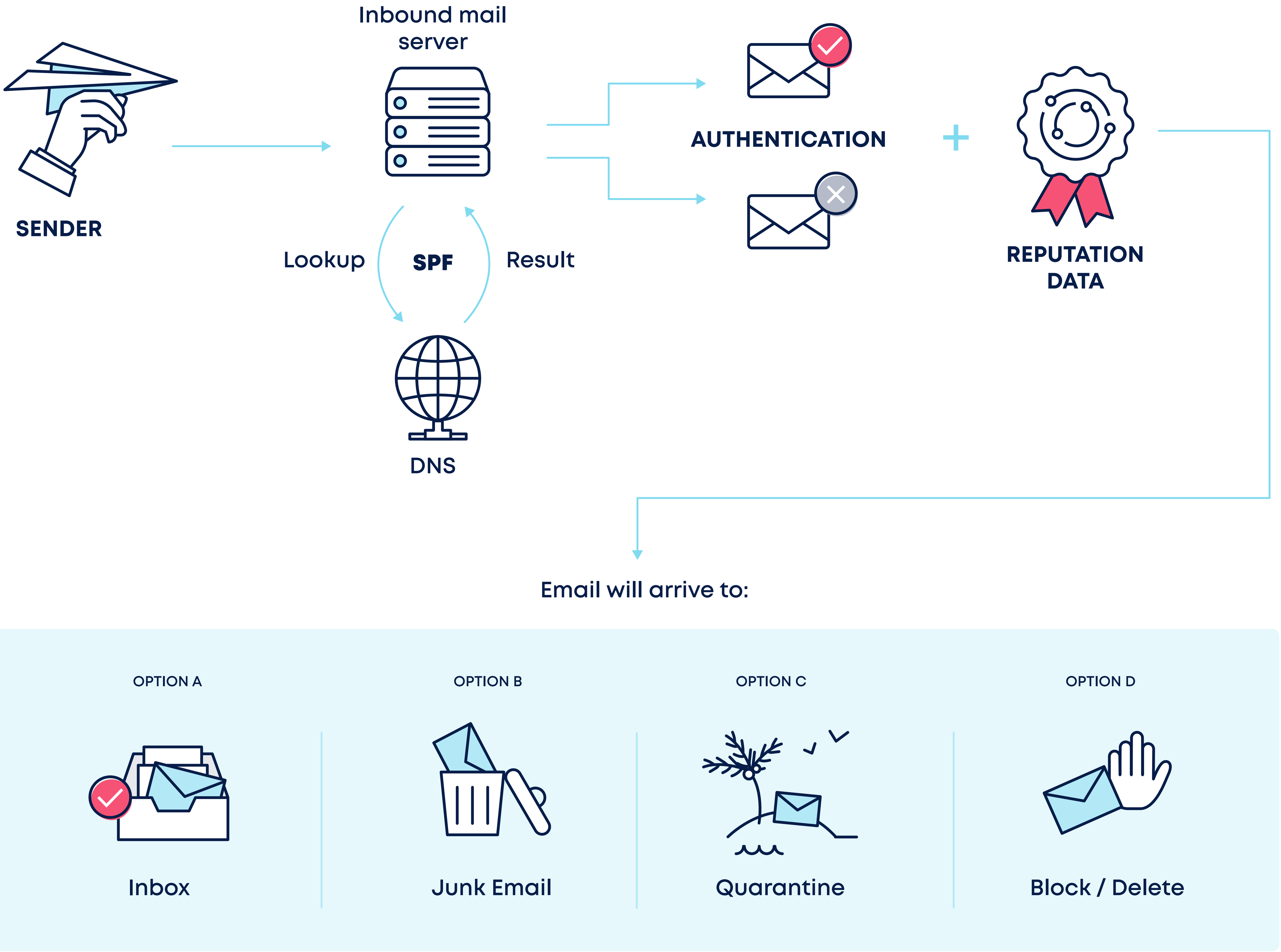
Host *
onct.example.com

TXT Value *
v=spf1 include: _spf.ongage

TTL *
Custom

Seconds *
600

The SPF authentication

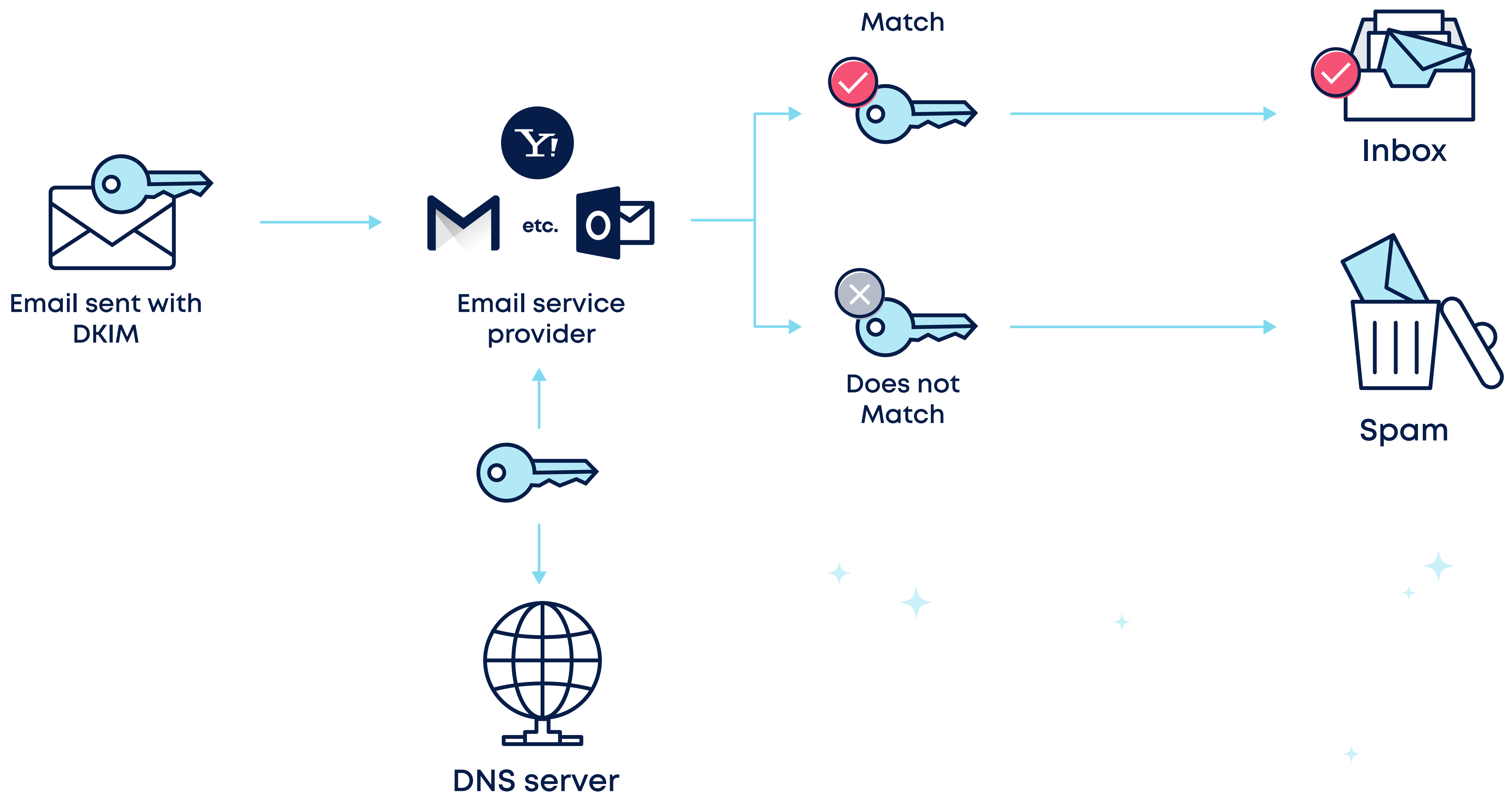


#2 DomainKeys Identified Mail (DKIM)

DKIM authentication goes a step further than SPF by sealing the content of your email using a cryptographic lock referred to as a "DKIM signature." Adding this encrypted lock to emails' headers prevents the email from being opened by anyone who doesn't have the corresponding key.

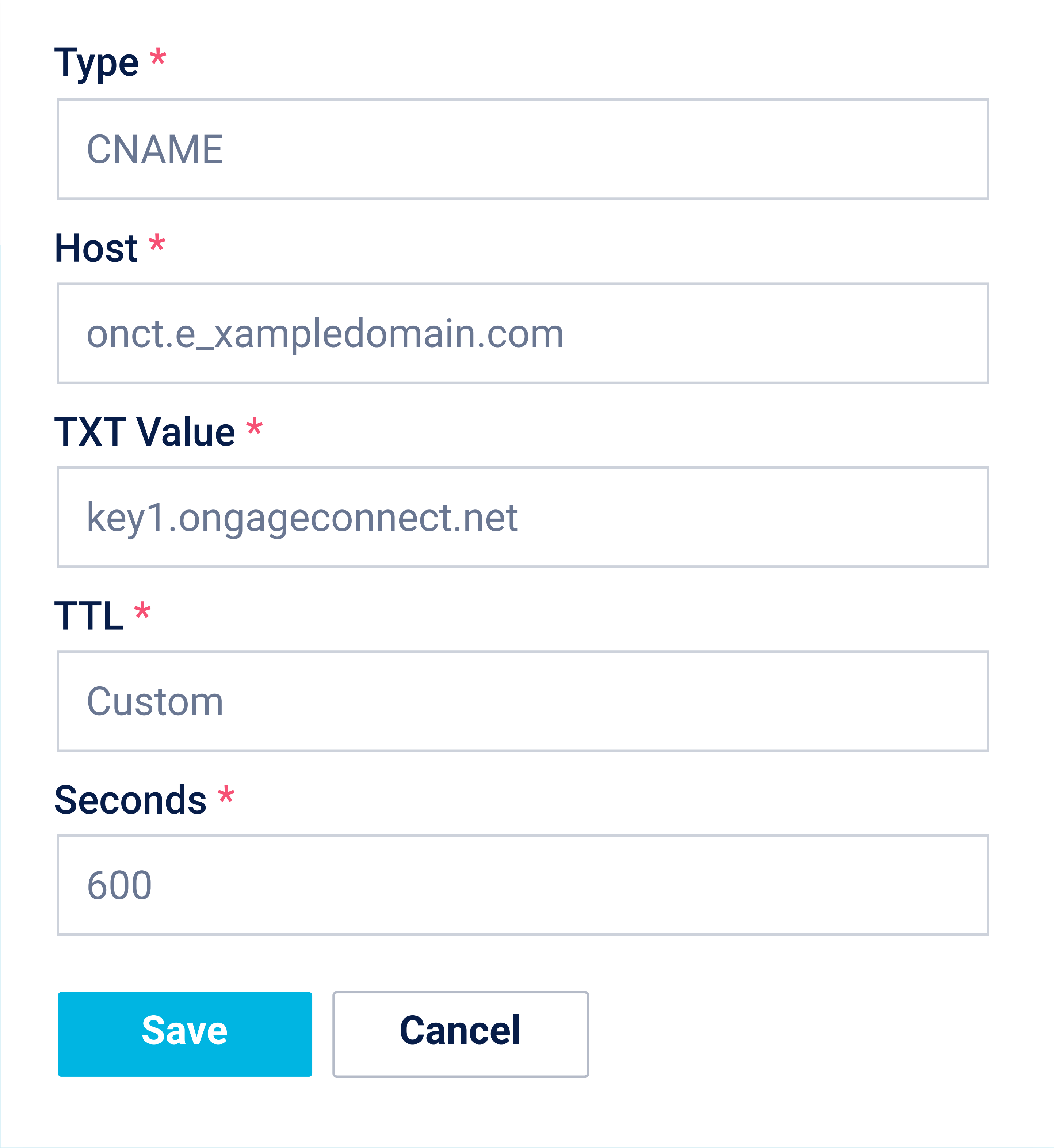
Once a DKIM lock has been opened, it cannot be relocked. So DKIM protocols allow intermediaries such as MTAs on an email's journey to detect whether it was opened or not.[7]
This stops bad actors from turning your legitimate emails into Trojan Horses by tampering with the content as it travels on its way across the internet.
Many ISPs will block or mark emails without DKIM signatures. Some ISPs also use your DKIM signature to send complaint feedback.

The DKIM Authentication Process



To use the DKIM, create a TXT record with the public key's value, or a CNAME record which points to the key. When an email processor receives an email with DKIM "lock," it checks this record to confirm that the key is a match for the email, verifying that the publisher of that key (you) is the authorized sender. Like an SPF record, your DKIM record must include specific syntax or tags to operate properly. DKIM keys must be stored in a subdomain named _domainkey.[domain name] on your DNS.[8] The signature or lock part of the DKIM set must appear in the header field of your email. In most instances, your ESP will create these encoded signatures for each email you send.

The process for creating a DKIM CNAME will look something like the following:



Type *
CNAME

Host *
onct.e_xampledomain.com

TXT Value *
key1.ongageconnect.net

TTL *
Custom

Seconds *
600

#3 Domain Message Authentication Reporting and Conformance (DMARC)

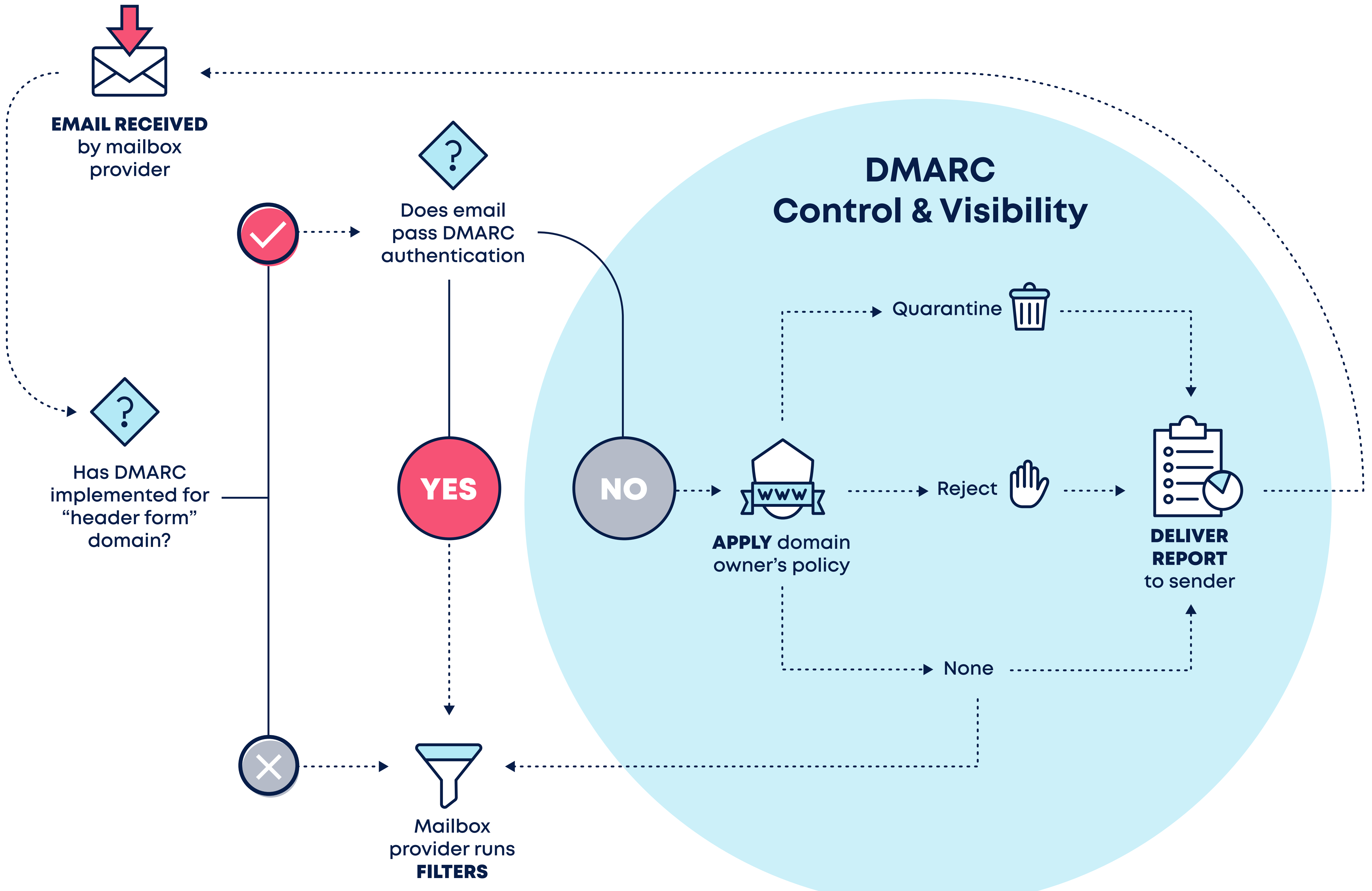
DMARC is a protocol that works with SPF and DKIM. It is a tool used to communicate to email receivers what authentication protocols you have in place and how you want them to handle any emails that fail authentication. Your instructions for what to do with suspect emails are referred to as your DMARC policy. They are represented by the "p" tag for domain-level policies and "sp" for sub-domains in your DMARC record. Emails that fail a DMARC check can be approved, quarantined, or rejected.[9]

DMARC TXT record will look similar to this:

"v=DMARC1;p=reject;sp=quarantine;pct=100;rua=mailto:[Your Email Address];"

To implement DMARC, you must have both SPF and DKIM protocols in place and add a DMARC record in your DNS record. When your sending domain and the receiving server use DMARC protocols, you'll be able to track all the emails that arrive at that server and are identified as coming from your domain by including a report instruction in your DMARC record using designated syntax.[10]

How DMARC Works



EMAIL RECEIVED by mailbox provider
Has DMARC implemented for "header form" domain?
Does email pass DMARC authentication
YES
NO
DMARC Control & Visibility
Quarantine
Reject
None
APPLY domain owner's policy
DELIVER REPORT to sender
Mailbox provider runs FILTERS

#4 Brand Indicators for Message Information (BIMI)

This final means of proving you are who you say you are is aimed not at ISPs and intermediaries but your customers. The recently developed BIMI process allows you to display your brand's logo in the inbox next to the emails it sends. Adding your logo adds transparency and trust to your email communications and increases brand awareness.

Like DMARC, BIMI doesn't work unless you first have other authentication protocols in place. You'll need to set up SPF, DKIM, and DMARC first. Also, make sure your DMARC actions are set to quarantine or reject and applied to 100% of failed emails. If your other protocol settings allow suspect emails to pass through, you won't be able to use BIMI. Add your BIMI data with instructions for displaying your logo to your host settings of your DSN to implement BIMI.

Your BIMI entry will look similar to the following:

```
default._bimi.[Your Domain] IN TXT “v=BIMI1;
I=[Your SVG’s URL]; a=[Your VMC URL]
```

BIMI logos should be square and saved in the SVG format to display well on different resolutions. Before displaying your logo, some receivers will require you to verify your ownership. This can be done by obtaining a Verified Mark Certificate (VMC) from a Mark Verification authority (MVA).[11]
Indicate that verification by including an “a=[Your VMC URL]” segment in your BIMI data.

Supports BIMI	Considering BIMI	Does not support BIMI
verizon media	COMCAST	YAHOO! JAPAN
Google	SEZNAM.CZ	Microsoft
Fastmail		

Building reputation: How to become a trustworthy (and welcomed) sender

Authentication ensures that no one uses your brand name or reputation to access unsuspecting consumers. It also helps to protect you because everything done in your name gets attached to and associated with your sender reputation.

Your sender reputation is that hard-to-pin-down, fluid metric that ISPs use to assess your emails' `worthiness' and if their users would like to see them in their inboxes. As we previously explained, your sender reputation is influenced by your behavior and how email recipients respond to you, and there is much overlap between these factors.

While your exact reputation can vary by ISP, recipient, email campaign, or even a single email, the effects of various reputation factors are cumulative. One message marked as spam may not tank your reputation, but dozens of spam complaints combined with other signals most certainly will.

Further complicating matters, sender reputation attaches at both the IP and domain level.

Being judged at the IP level means that if you use a shared IP or begin using an IP that has a bad reputation, you may be judged based on some other sender's prior bad behavior. Conversely, if you are on a dedicated IP, you are the only one responsible for its reputation.

Judgment at the domain level means that your reputation will follow you across your IPs. You may still be able to segment activities across different IPs to minimize the impact of different email activities, but you won't be able to avoid all the consequences of bad acts.

This is how ISPs identify spammers

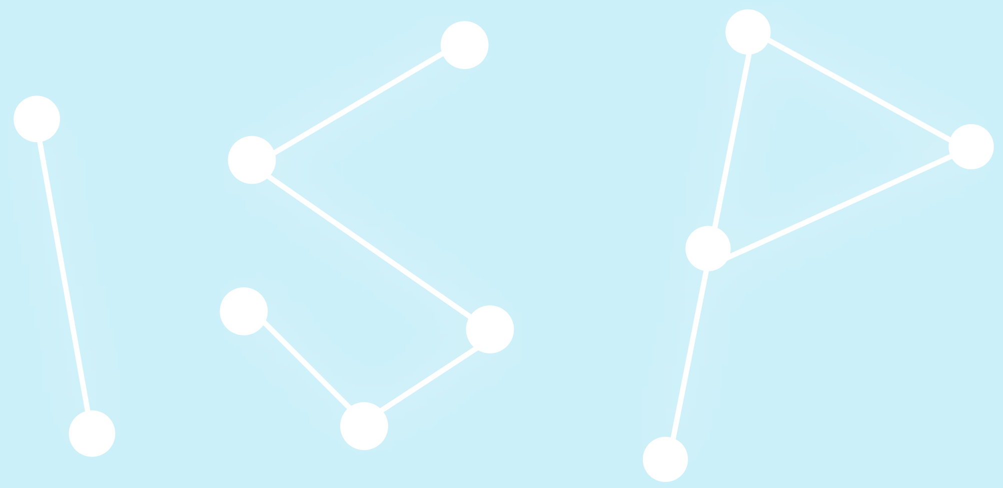
Unfortunately, your brand can be negatively affected if your activities, email content, or customer reactions (a.k.a. engagement) resemble those associated with spammers. ISPs are on the lookout for signs that messages are sent to people who don't want them. They are looking for signals that you may have purchased email addresses or use scraping to build your email list. They are checking if you're moving your sending operations around to hide your activity.

Keep an eye on your domain reputation!

ISPs review your email activity and performance holistically, and so should you. It is important to sustain and monitor both your IP and your domain reputation, as one affects the other.

Among other reasons, an ISP may take a closer look if you:

1. Display unusual or suspicious sending patterns or IP behaviors, like:
   - Sending thousands of emails in your first use of a new IP address.
   - Having a notable spike in the volume of emails you send.
   - When you're sending emails on an erratic schedule.
   - Switching between different IPs and/or ESPs frequently.
2. Send emails containing dubious content such as:
   - Deceptive or "click-bait" subject lines.
   - Unconventionally formatted images or text.
   - Broken, hidden or otherwise suspect links.
3. Have high spam rates and/or low engagement rates or constantly falling in spam traps.



Looking at the list above, you might be wondering what happens if you:

- Made mistakes in the past?
- Want to change your delivery agent? Or,
- Need to add more IPs to handle increased volume? Or,
- What if you just acquired a massive list of sign-ups for a new newsletter or promotion?
- What if you just made a bad design call when designing your latest email campaign?

Are you doomed to have a bad reputation?
Sometimes there are legitimate reasons for you to take actions that look suspicious.
So it's critically important to be aware of how your actions can affect your reputation and be proactive about minimizing the impact.

For instance, don't send every email campaign to everyone on your list. Instead, segment your email list so that the campaigns you send are relevant to your audience. Watch your metrics. If your subscribers are dropping out or reporting messages as spam, it's time to re-evaluate your email strategies.

Maintain a steady cadence of emails and vary your frequency based on the recipient's rate of engagement. If you need to add IPs or switch ESPs, do so with intentionality and a plan.

Carefully evaluate all of your choices and what you hope to accomplish before you make a switch. Pay attention to your domain-level activities, too. Coordinate your activities across departments. If your compliance team needs to send an annual disclosure to everyone on your list, that might not be the best day to send an all-subscribers promotional email. That's why using a sending calendar to monitor future campaigns, and important dates, is a must for any email marketer.

In the following sections, we focus on what to do, and more importantly, what not to do to keep your reputation unblemished and your deliverability rates high. From preparing your IP for prime time to keeping your subscription lists clean, we dig deep into the factors that ISPs use to decide who's in and who's out.

What is an IP warm-up process and how it reduces deliverability issues?

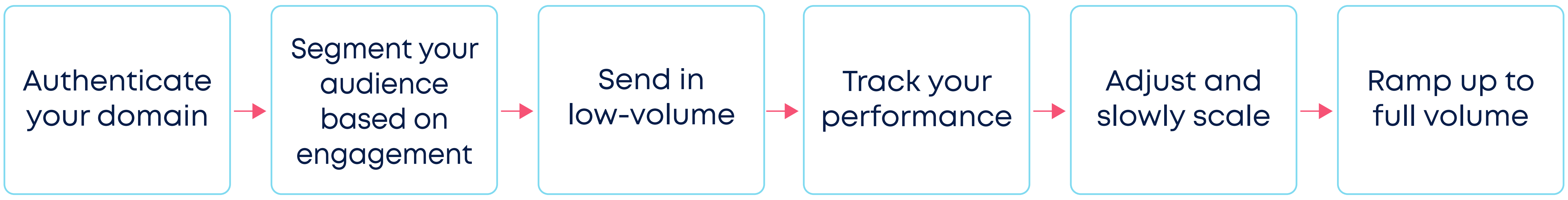
When you add a new, dedicated IP to your sending roster, it doesn't have a reputation--good or bad. That's good because you aren't paying for someone else's past mistakes.

But, it's also not so good because ISPs may not trust it yet. The process of building up a new IP's reputation is known as an IP warm-up or warming. The gist? Instead of going straight to boil, slowly turn up the heat on your new IP to give it a solid sender history.

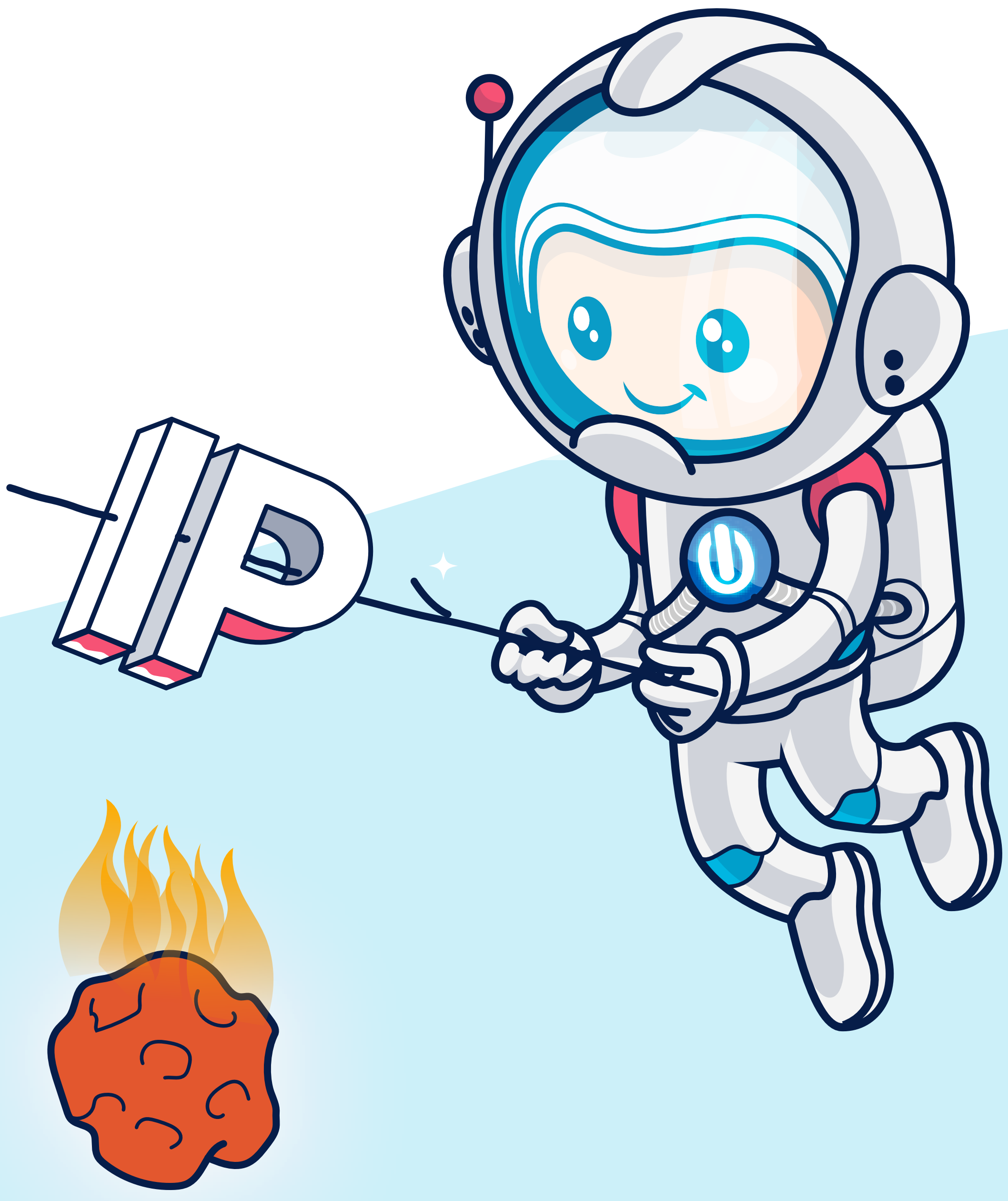
You can also use these warm-up strategies to rehabilitate a burned IP--one with a bad reputation in need of repair. Just remember that healing takes time.

> "A certain way to get your domain blocked is to start sending emails on a new IP without the warm up process. Read this chapter to learn more."
>
> **Tali Hasanov**
> results-driven digital marketer

Warm up your IP in 6 easy steps



Authenticate your domain → Segment your audience based on engagement → Send in low-volume → Track your performance → Adjust and slowly scale → Ramp up to full volume



1. Claim and authenticate the IP

Make sure your new IP address is added to all your necessary DNS records.

2. Set your new IP up for success

The first series of emails you send from your new IP address should go to your most active subscribers. This reduces the likelihood of the IP getting tagged with negative reputation signals such as low engagement or spam complaints. Use historical campaign data or other metrics to choose a set of recipients that demonstrates solid open and click-through rates or recent interaction with your brand. Create a warm-up segment from this group.

3. Don't email everyone at once

Ramp up your send rates on the new IP by folding email addresses into your mailing mix slowly. For example, you might send an email to the first 200 recipients on your list on day 1 and the next 400 on day two, continuing until everyone on the list has received an email. Alternatively, you can use a build-on strategy. On the first day of your warm-up campaign, using this strategy, send emails to 200 of the list. Then, on the following day, send a new message to that 200 plus an additional 200.

Email sending limits and the rate at which you can pump up the volume will vary between ISPs. Don't be surprised if you see greater signs of deliverability sensitivity with some ISPs than others.

4. Monitor your progress

Early engagement metrics are vital for establishing your IP's sender reputation. Keep watching for warning signs like falling open rates, and scale back your warm-up at the first hint of trouble. That being said, open rates may soon become obsolete due to Apple's Mail Protection Privacy (more on that later), and you may need to monitor other metrics like your click rates to assess your IP's reputation.

Further, you can use tools like Gmail Postmaster, Microsoft SNDS, and Verizon's new Email Deliverability and Performance Feed to help you assess the IP's performance and identify deliverability issues.

5. Proceed toward full speed

Now you are ready to test bigger campaigns using the IP. Add subscribers that are less engaged and continue to ramp up your daily send volume slowly.

6. Onward and upward

After biding your time and checking your metrics, you should be ready to send your new IP on its way. Ramp things up to full volume and continue to monitor the results. You might have to scale up and down a couple of times before your metrics settle down. Don't worry if this is the case. It's a normal part of the warm-up process.

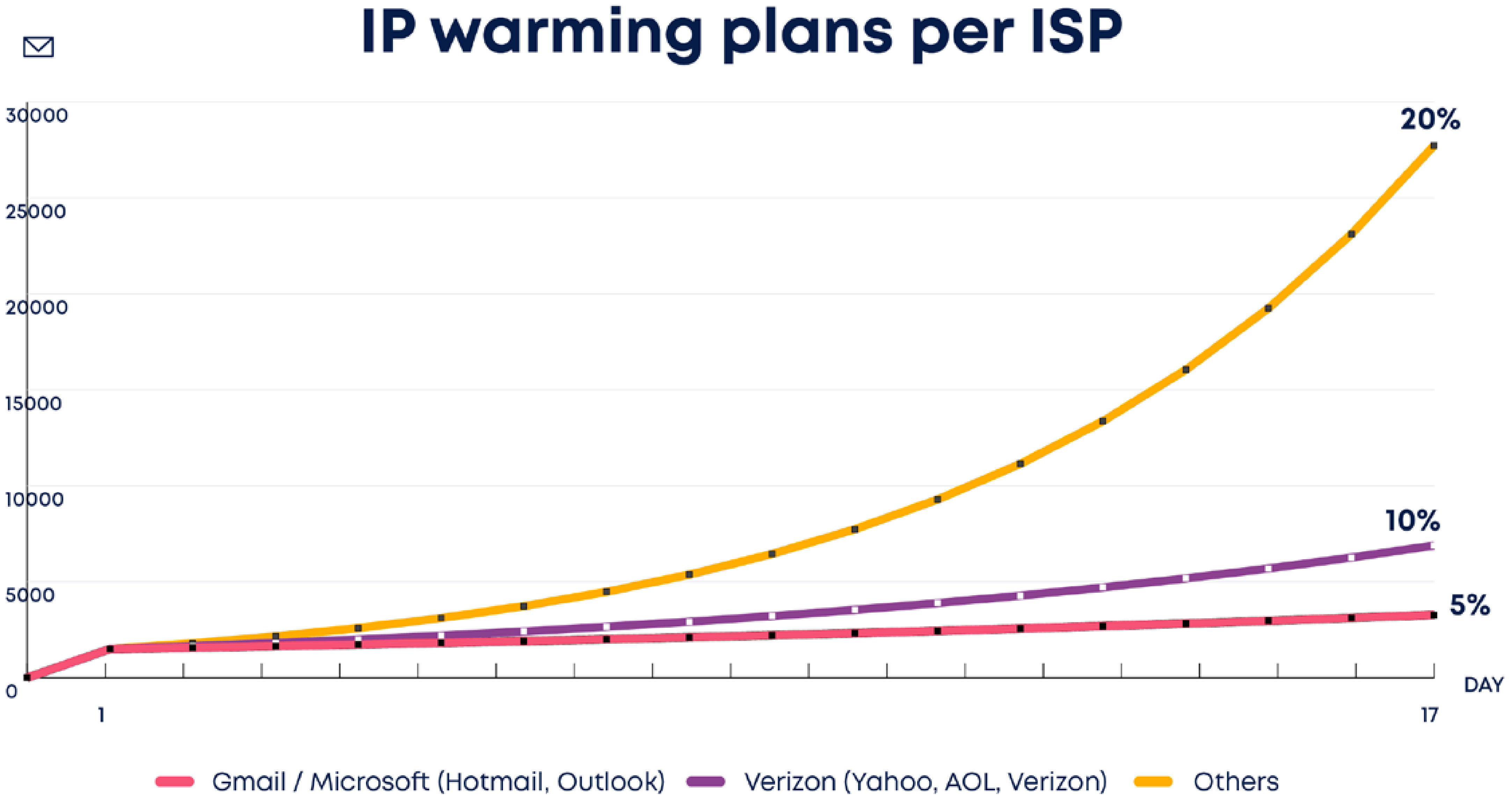
Good to know

If you already have a stellar domain reputation, you might find ISPs are warmly welcoming messages from your new IP. This is the upside of ISPs monitoring not just your IPs, but your domain as well.

When it comes to IP warm-up patience pays off

According to Gmail's bulk sender recommendations, increasing your sending volume too quickly will harm your deliverability. The guidelines indicate that the greater the total number of emails you send, the slower you should increase your send volume. However, you can increase your volume more quickly if you send new emails daily rather than weekly.[12]

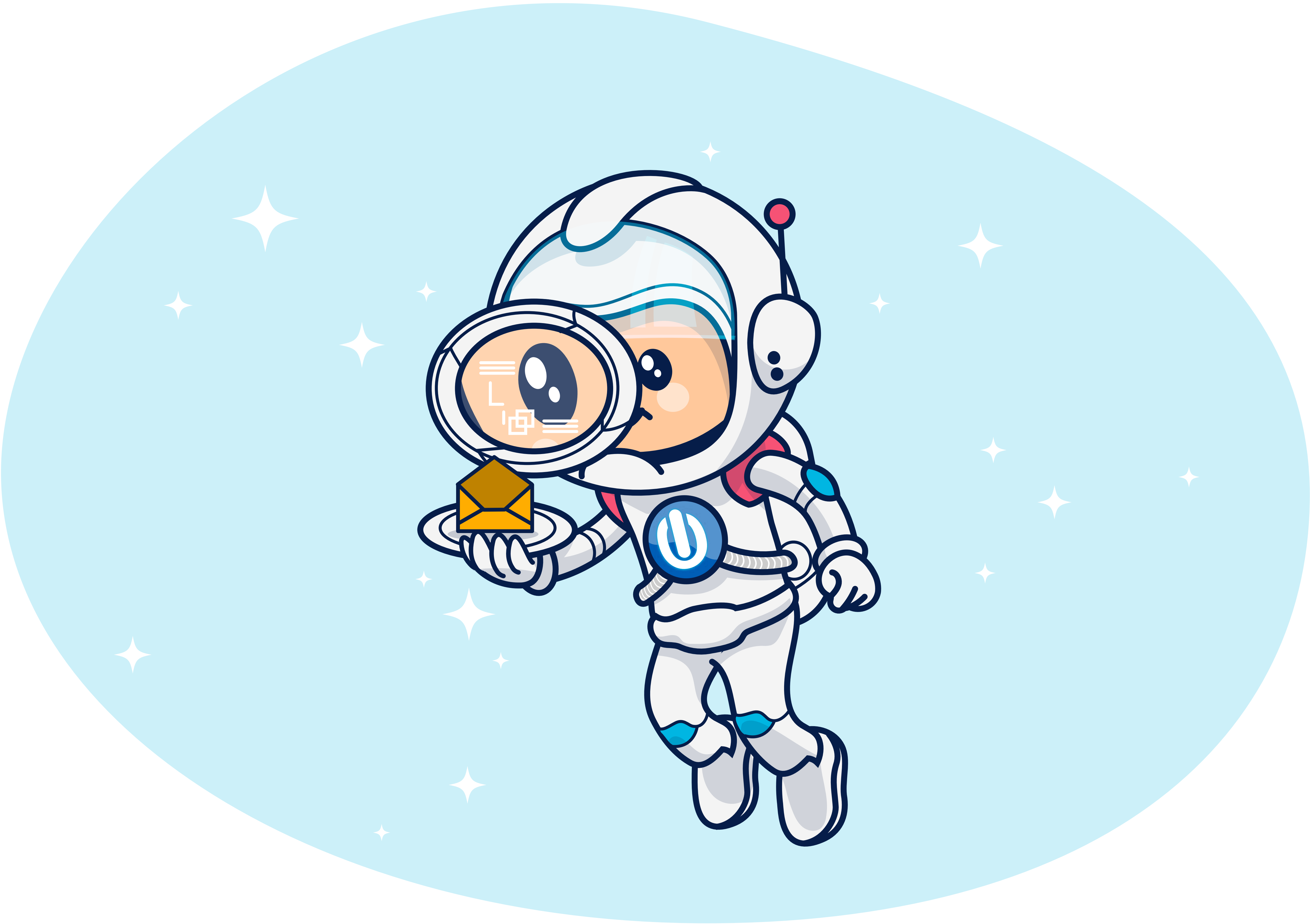
IP warming plans per ISP



How to create credible content that makes it past the gatekeepers

Our engagement rises and falls according to the relevancy and creativity of the content that we send. That's a given. But did you know that your content matters to the service providers handling your emails as well?

ISPs evaluate your emails' subject lines and body content for signs of spam. Using the wrong words, formats, or codes can really hurt your deliverability.



What's on the inside (of your email) matters

To increase your chances of making it through the ISPs' spam-filtration processes, your emails need to be correctly formatted and not include suspicious content such as trigger words, unrelated links or hidden text. This goes for both your subject line and email body, as ISPs look at your email message as a whole.

As a baseline for deliverability, Gmail recommends that senders follow the Internet Message Format (IMF) standards published by the Internet Engineering Task Force (IETF) for text-only emails and the HTML standards published by the Web Hypertext Application Technology Working Group (WHATWG) for HTML messages.[13] [14]
To make it to your recipients' inboxes, follow these best practices as well.

Don't hide text in your email messages

Spammers sometimes use tiny fonts, color-on-color text, or other methods to disguise content, usually hoping that an unsuspecting consumer will click on a camouflaged link.

Don't include shortened, broken, deceptive, or excessive links

Many links in one email, links that lead to compromised reputation or blocklisted websites (use MXToolBox to figure this one out), or URLs that don't match their anchor text may indicate to ISPs' filters that the email is phishing or otherwise up to no good. Granted, if you are sending a newsletter with a curated list of resources or similar content, limiting the number of links in your email may be challenging. But, if you suspect deliverability problems, your links may be the problem.

Keep your HTML clean and clear

If you send emails in HTML, test your code to make sure it is valid and renders correctly. Also, include a text-only version of your email for improved deliverability and accessibility.

Avoid the spammy copy

The rules that apply to email subject lines apply to the body of your emails, too. Avoid all caps, excessive punctuation, dollar signs, and words and phrases that feed fear or greed, make exaggerated claims, or otherwise make a hard sell.

Watch your ratios

Text-to-links, text-to-HTML, text-to-images. Any of these ratios can trigger suspicion if they appear off. Although more and more senders are using graphics and animation to communicate with their customers, spam filters still go on alert when senders use only images to convey their message.

This doesn't mean that you need to cut out the pictures. But, if you are not getting the engagement you expected, then take a second look at your ratios. Also, when you use images in your emails, add captions or introductory text to improve your ratios. Create alt-text for each image as well. This step helps convince filters that your images aren't spam and increases the accessibility of your message.

So far, we've looked at deliverability measures that help you stay on the good side of ISPs by proving that you are a legitimate business with a reason to contact their mailbox users. The next step in building your deliverability is to make sure that those users want to hear from you. This is where fixing your deliverability issues has the power to make a big impact on your bottom line.

Making contact only with those prospects who are genuinely interested in hearing from you will improve not only your deliverability but also your conversions. We'll explore how to build and maintain your dream list of engaged subscribers in the following sections.

Do	Don't
Write in proper HTML	Hide text
Use alt-text	Direct to bad links
Include a text-only version	Write spammy copy
Test and preview your emails	Insert too many images

How engagement rates boost your sender reputation

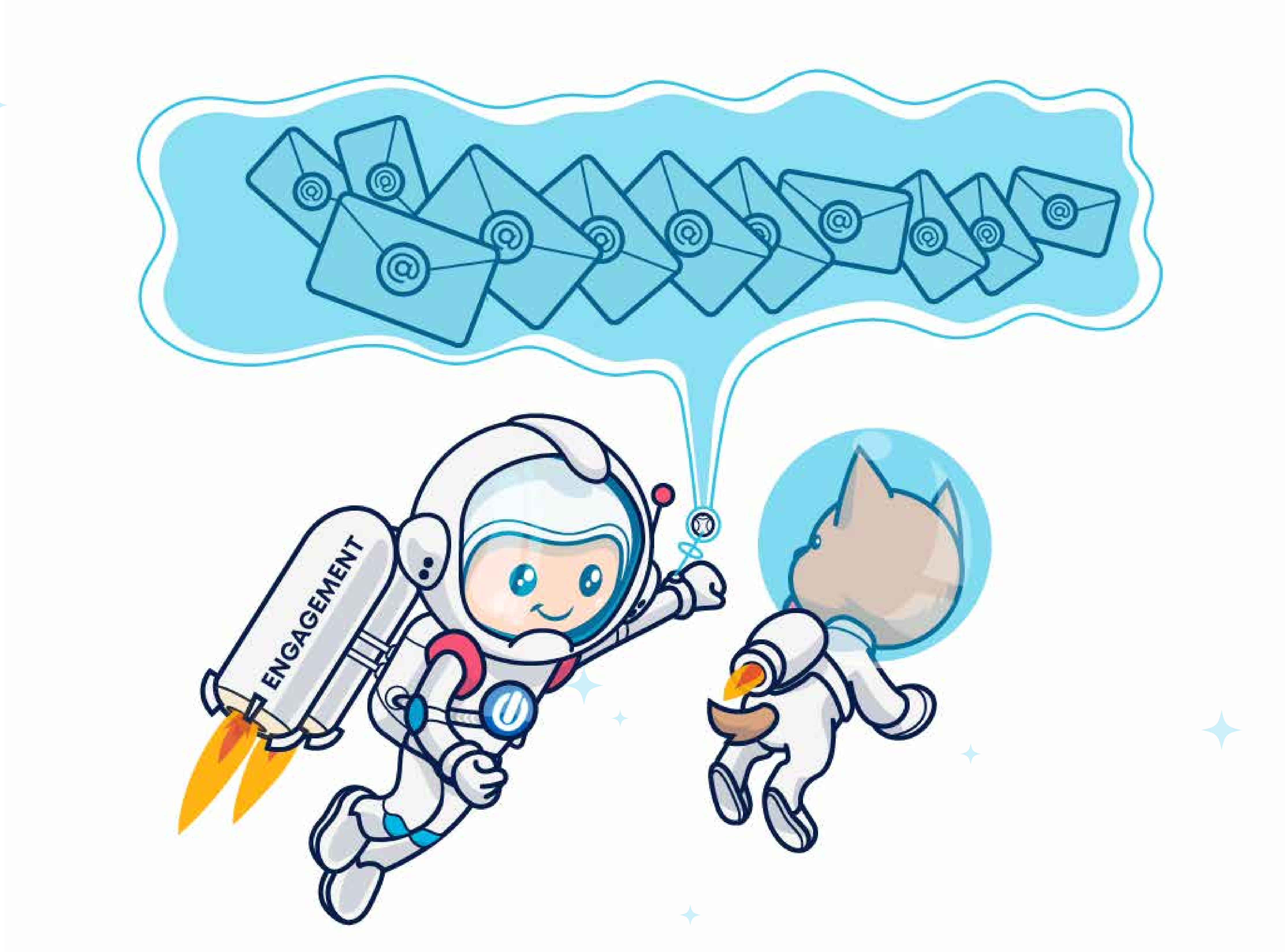
Deliverability is rooted in customer experience. ISPs filter emails to provide their customers with a better email experience. In the same way, the success of your email campaigns is rooted in customer experience. If your email recipients aren’t interested in or are not engaged with your emails, those emails have little hope of generating conversions. Unwanted emails will only drag your deliverability rates down fast.

ISPs use your email engagement rates and other customer-focused metrics when deciding whether your emails belong in their customers’ inboxes. Ensuring that you can continue to reach potential customers means making sure your email list is focused on people who want to engage with your brand.

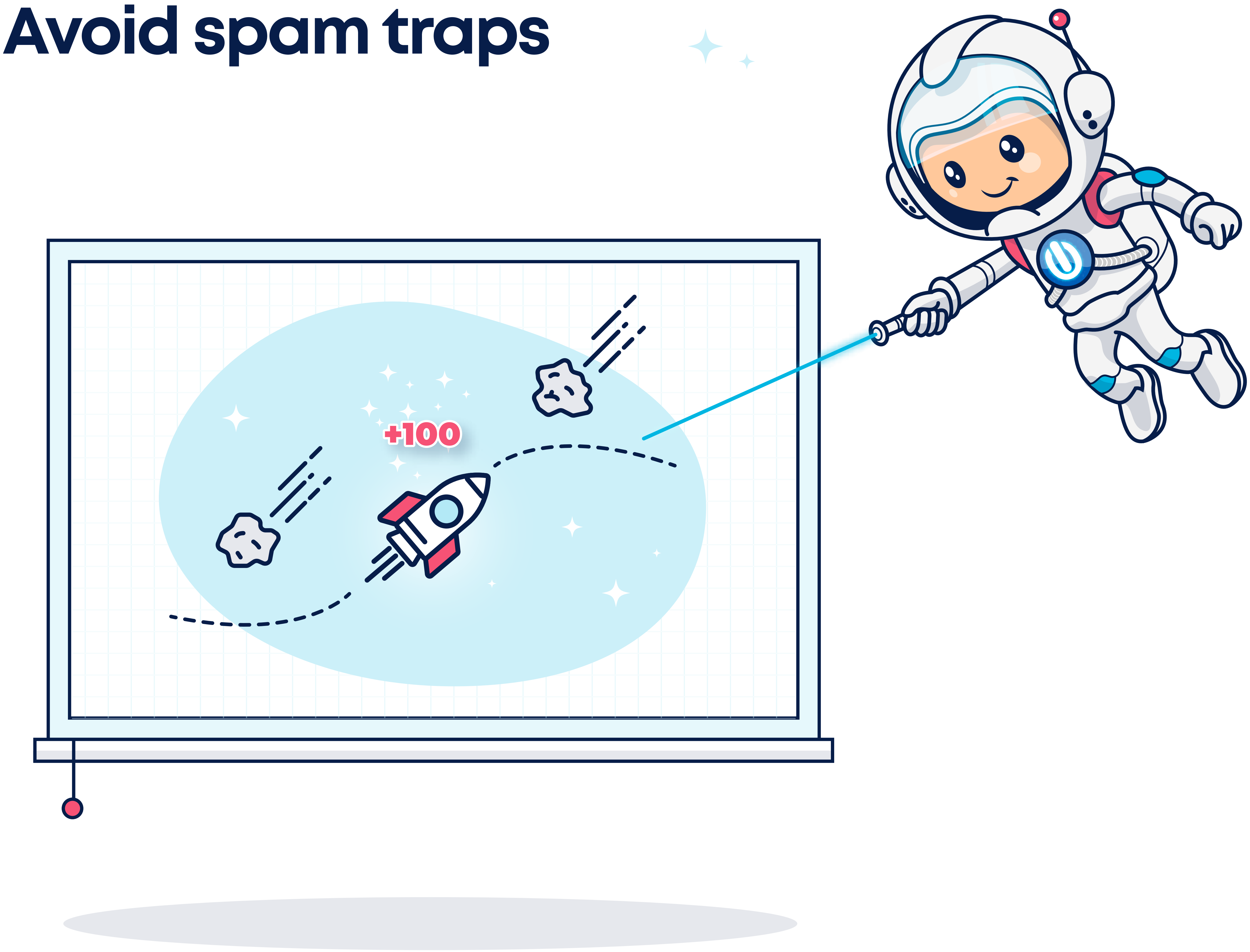
Use the following strategies to develop and maintain subscriber lists that demonstrate your good behavior to ISPs and generate high engagement with your customer base.

"Want to have better email conversions - fix your email deliverability first!"

Tali Hasanov
results-driven digital marketer



First step: Avoid spam traps



How do you gather your list of contacts?

If you purchase or scrape the email addresses you use, you may get more than you bargained for. In addition to low engagement from uninterested recipients, these email addresses may land you in hot water with the law and ISPs' spam filters. This usually happens due to the email recipients themselves, who receive your unsolicited emails and report them as spam. That's not good for your sender reputation, and it's not the worst that can happen. Your emails may not reach an actual person at all. Instead, the email you purchased or obtained by scraping sites may be a spam trap.

Spam traps are created to catch bad senders in the act. Spam traps come in two varieties. **Pristine spam traps** are wholly fake email addresses. They exist to catch emailers who send messages to people without first gaining their consent. (Fake people can't opt into your email list.)

The other type of trap, **a recycled spam trap**, is designed to catch spammers who purchase old email lists or fail to prune their lists. These traps use emails that were valid at one time but are no longer connected with an active user. Sending emails to one of these recycled addresses is a clear signal that you aren't focused on contacting people who have expressed interest in your brand (at least not for a very long time).

Sending emails to either spam trap type can reduce your deliverability metrics with any ISP that detects them. You may also end up on a list of known spammers if you are caught in a spam trap. Sometimes referred to as a DNSBL, Blocklist, or deny list, anti-spam vendors and organizations build and share these lists to serve their clients.[15]
Clearly, buying or scraping your way to a send list is a bad idea. What should you do instead? Use paid ads and organic sign-ups to gain consensual subscribers to your lists.

Then, verify each email you receive to ensure that it has been entered correctly and that your new subscriber genuinely wants to hear more from you. In some countries and industries, the use of double opt-in as a verification method is not widespread. However, if you want to make sure that everyone on your list is interested in your content, it's recommended.

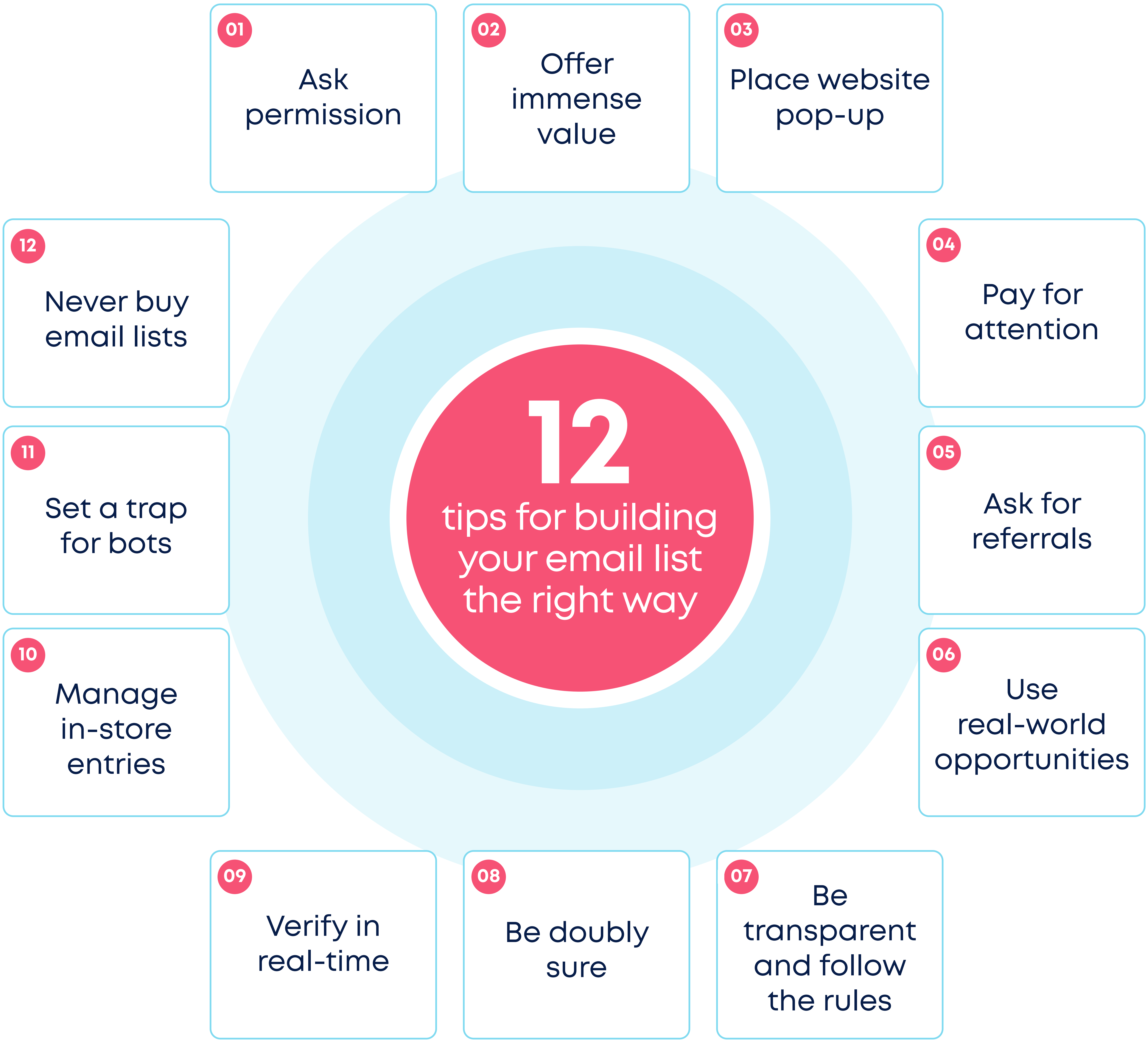
Two main spam traps

There are two main types of spam traps ISPs and blocklist sites use. Falling in one can be devastating for your deliverability, but luckily it's possible to avoid them.

Pristine and Recycled spamtraps

Questions to ask yourself	**Pristine spamtraps**	**Recycled spamtrap**
What's the danger level?	Very high	Low-medium
Where it can be found?	Public websites	Your legit email list
Who created it?	Blocklist operators	ISPs
Is the email address real?	No	Yes
What's the best way to avoid it?	Never buy or scrape lists	Remove inactive subscribers (more about the criteria later)

Second step: 12 tips for building your email list the right way



12 tips for building your email list the right way

01 Ask permission

02 Offer immense value

03 Place website pop-up

04 Pay for attention

05 Ask for referrals

06 Use real-world opportunities

07 Be transparent and follow the rules

08 Be doubly sure

09 Verify in real-time

10 Manage in-store entries

11 Set a trap for bots

12 Never buy email lists

Start by using the following strategies to pre-qualify your email subscribers and collect addresses from individuals who want to hear from your brand:

01

Ask permission

Ask visitors to your website and customers to sign up to receive emails from you. If someone is interested in your brand, they may volunteer to learn more.

02

Offer a reason for people to say “yes”

Incentives or lead magnets are an effective way to get people to become subscribers. Offering something of value may be just the nudge someone needs to take the next step and enter their email address into your contact form. Remember, though, that some subscribers may only be interested in the incentive and not remain engaged with your brand. If most of your incentivized subscribers unsubscribe soon after receiving their first email or fail to engage, you may want to reconsider your incentive or messaging.

03

Place website pop-up where they most expect them

Too many pop-ups can drive viewers away. But a well-placed request, with the right offer, may be just the ticket to get someone to join your email list. Plan your pop-up so that it makes the ask after someone has lingered on your website long enough to show their interest.

04

Pay for attention

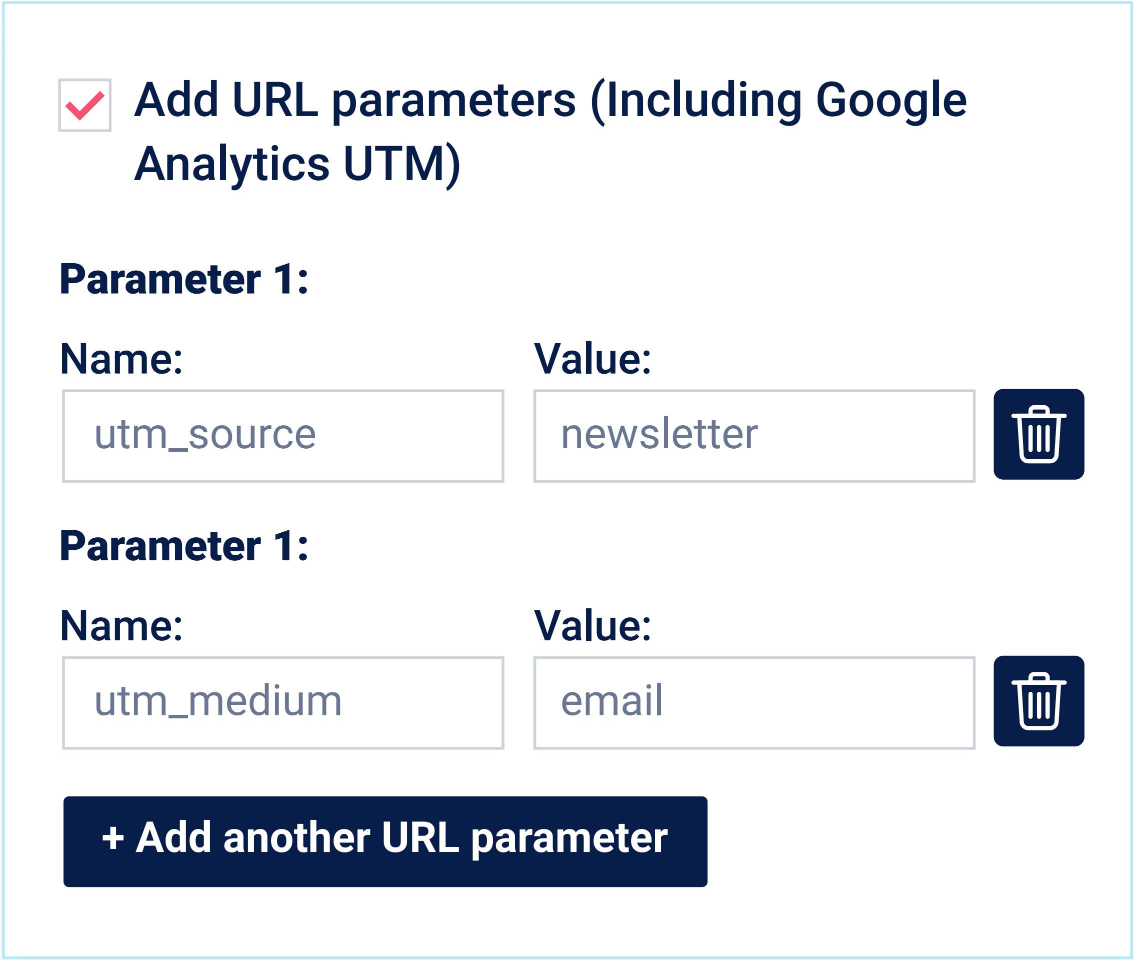
A well-executed PPC campaign that invites people to learn more about your brand is a standard part of the awareness stage of the marketing funnel. Take advantage of a special promotion, or receive a free download can help you identify and sign up individuals who aren’t already familiar with your brand. Consider a retargeting campaign to help you capture the ones that got away.

05

Ask for referrals

You’ve invested a lot of time and effort to connect with your subscribers. Why not leverage that goodwill? Ask your existing subscribers and customers to invite their friends to subscribe to your lists. Encourage them to participate by offering an incentive.

The best referral incentives are double-sided, meaning both the referrer and their friend get a benefit when the friend signs up. Create unique links using dynamic tokens to keep track of which subscribers have made referrals.



☑ Add URL parameters (Including Google Analytics UTM)

Parameter 1:

Name:	Value:
utm_source	newsletter

Parameter 1:

Name:	Value:
utm_medium	email

06

Don’t forget to use real-world opportunities

Develop processes for gathering emails at the point-of-sale, at trade events, through print media, and other contact points in the physical world to expand your reach beyond the digital one. Make collecting emails in person easier by installing kiosks or offering tablet sign-ups at events or in your retail stores. Yes, consumers could use a smartphone to visit your website and sign up, but by offering them a device, you get them to interact with your business physically for the first time and that interaction sets the tone for the rest of the relationship.

07

Be transparent and follow the rules

When asking for email addresses, be sure to follow the laws of each applicable jurisdiction. This includes any **disclosure** and right to be forgotten provisions. The EU’s General Data Protection Regulation (GDPR), in particular, requires that before email marketers can gather or use someone’s contact information, they must fully explain how the information will be used and gain the person’s “specific, informed and unambiguous” consent.[16]

GDPR is considered to be the most stringent of all compliance rules. It’s a good practice to abide by it, as doing so guarantees you follow the Canadian CASL, the US CAN-SPAM Act, the Californian CCPA & CPRA, and more.

Beyond just a legal requirement, though, being transparent about your intentions helps you build better subscriber relationships and prevent deliverability issues. When you ask someone to sign up for your mailing list, tell them what kinds of emails they can expect to receive from you. Will you use their email to send discounts or promotional news? Will you share additional resources or information?

Subscribers who know what they are signing up for when they share their email address with you are less likely to report your follow-up communications as spam.

Maintain good communication practices when you send emails to your subscribers. Add a permission reminder that explains how you obtained their email address. This should help you avoid complaints from consumers who don’t remember signing up for your mailing list.

Then, verify your new subscribers’ email address and their interest before adding them to your active mailing lists using a combination of the following steps:

08

Be doubly sure

One way to ensure that your email list is populated with accurate addresses from individuals who have consented to receive messages from you is with a double opt-in. Using this method, you first obtain the subscriber’s email address through contact or sign-up form. Then, you send an email to the address they provided, asking them to confirm their interest and consent. If you received an incorrect address, the address was entered by a third-party, or the recipient has changed their mind, this method lets you find out sooner rather than later. As previously mentioned, double opt-in isn’t a mandatory practice, but we do recommend it to ensure the quality of your list.

The address is real, but is it active?
40% of millennial and Gen Z consumers say they use a special email address for spam.[17]

09

Verify in real-time

Sometimes people make typos a.k.a. syntax errors. Sometimes they enter a fake email address because they want the incentive you've offered but really don't want to hear from you again. Either way, false registrations aren't going to improve your engagement or deliverability metrics. Avoid intentional and unintentional address errors by using real-time validation software to check the email address at the point of capture. Verification services can check for missing characters, typos and confirm whether an entered domain or recipient name exists.

10

Manage in-store entries

Acquiring leads via in-store requests is still a thing even in this booming digital age. These email addresses provided by your sales staff must go through the same scrutiny other email addresses go through. That means verifying each one of them to make sure they're real and valid addresses.

11

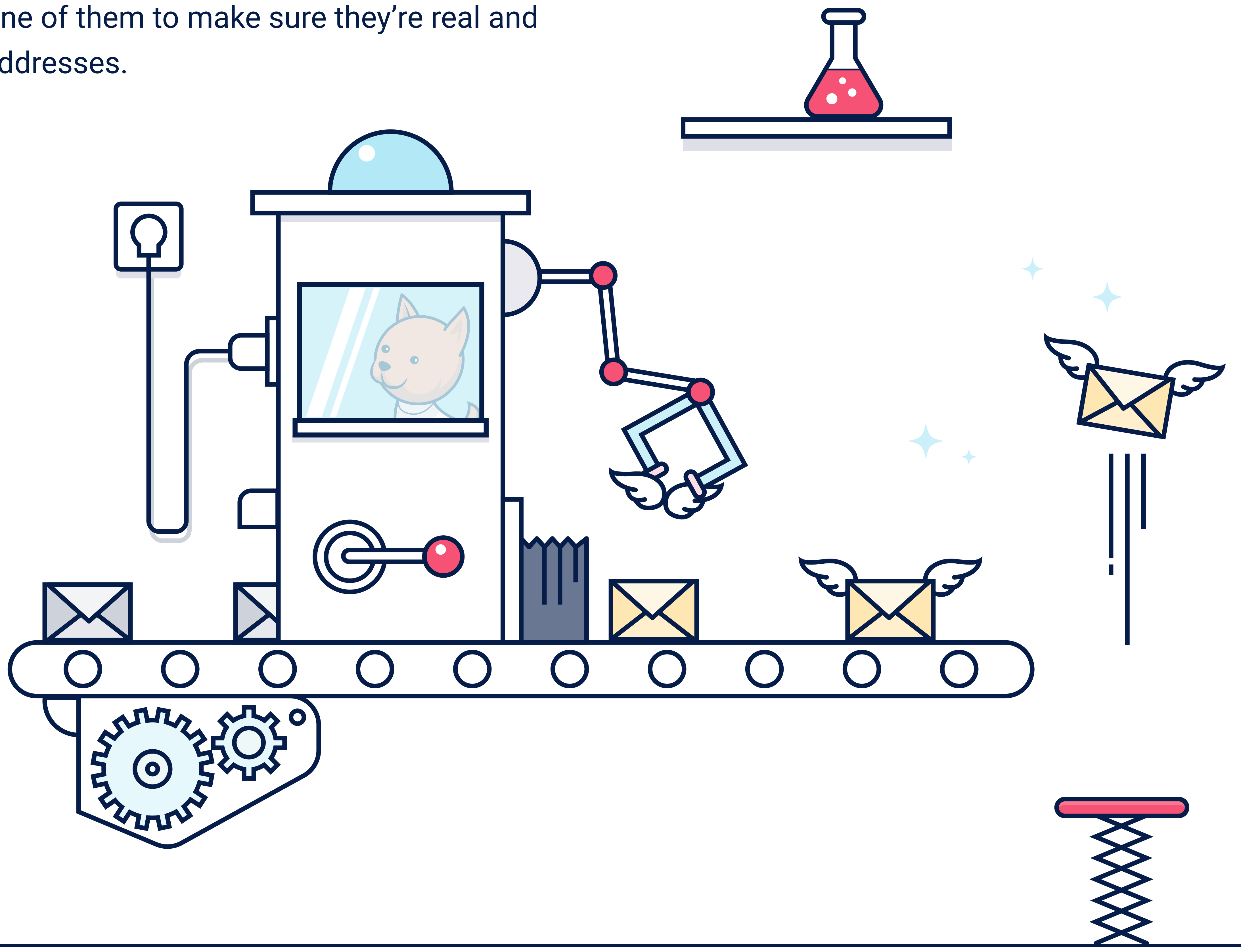
Set a trap for bots

Do bots try to join email lists? They sure do. The easiest way to keep the bots away is to use some type of CAPTCHA to catch them. But this can annoy your human guests. Another option is to create a hidden field that only bots can see. By adding a hidden (non-visible) field to your sign-up form, you can trap the bots and filter out their fakery.

12

Never buy email lists

All of these tips will help you find leads who want to hear from you, growing your list organically. Sometimes, email marketers want a big - ready to send list - and take the easy way out, purchasing email lists, or scraping email addresses from websites. While tempting, doing so might net you hefty fines while tarnishing your sender reputation. Slow and steady wins the race.



Third step: Maintaining an accurate and engaged list of subscribers

Building your list and checking it twice is just part of what it takes to ensure your subscriber list isn't harming your deliverability. In addition to spam reports and bounce rates, subscriber engagement levels have a major impact on how ISPs view you as a sender. Are you sending messages that your customers want to receive? Are the emails on your mailing list still active?

Preserve your reputation by keeping your subscriber list clean and your emails engaging with the following best practices:

First, remove inactive subscribers from your mailing lists

This may seem counterintuitive. Your mailing list is your lead list, so why would you want to take people off of it? But think about it. Chris Marriott refers to them as "silent unsubscribes" and over time they are going to have the same negative impact on your sender reputation as real unsubscribes have. If they aren't good leads, there's no reason to keep them on your list, even if contacting them doesn't take much effort.

Your inactive subscribers harm your engagement metrics and incur additional costs while adding little value to your campaigns. How can you clear your list of people who aren't that into you? Here are your options.

- Remove repetitive soft bounces
- Use bulk email validation
- Implement sunset policies
- Create a preference center
- Make unsubscribing easy

It is natural for subscribers to come and go from your mailing list over time. Your email churn rate is the metric that tracks how many net subscribers you lose in a given period. Churn rates vary significantly across industries. The yearly list churn average is 22.5% to 30%.[18]

Make opting out easy

Every email you send should include a straightforward way for recipients to opt-out from future messages. This is not only a good marketing practice, but it is also the law in many jurisdictions, including the EU and North America. Include a clearly labeled link to your unsubscribe page in your email.

Don't try to hide your link behind vague language or make customers jump through a series of hoops to say farewell, like logging in to their account to unsubscribe. Subscribers who encounter friction when they try to opt-out may decide to skip the hassle and mark your email as spam instead. You'll still lose the subscriber and take a hit to your deliverability score. To make things even easier for the uninterested, add an easy-to-find unsubscribe function to your emails, like a "List-Unsubscribe Header."
This feature will cause an Unsubscribe link to appear next to your email's header, so readers don't have to search for the opt-out option.

With the rise in anti-spam laws, most sender agents now offer automated unsubscribe features.

Recipients who click on either of these unsubscribe options are automatically removed from the sender's active lists. Regardless of how someone unsubscribes, it is important to act quickly to honor their request. Be sure to monitor your incoming email channels for unsubscribe messages as well and respond right away to any you receive.

Offer subscribers options

Whether to continue receiving emails from your brand doesn't have to be a binary decision. If you give your email recipients subscription options, you'll improve their email experience and learn more about their preferences. To do that, create a preference center that will allow your subscribers to change their preferred email address or opt-down to receive fewer communications from your brand.

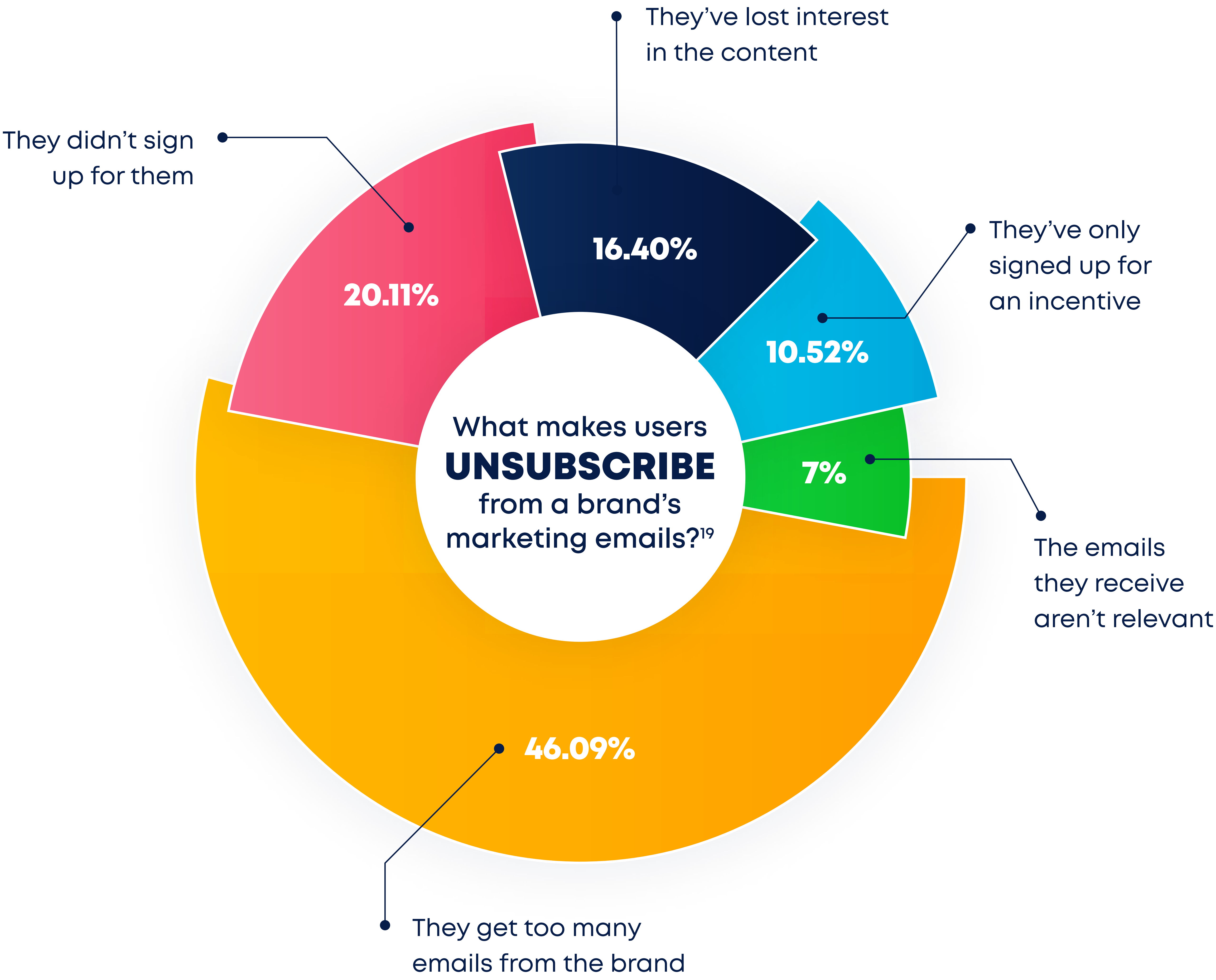
To eliminate friction and ensure regulatory compliance, provide these options in addition to the full unsubscribe selection should always be easy for people to find and activate. But make sure you are prepared to honor opt-down requests, as hard as it might be to email someone less often!

Be proactive about list hygiene

Regularly re-validating your email list should be foundational to your list hygiene program. As we previously wrote, sending messages to stale emails can ruin your sender reputation. You'll want to remove old, inactive addresses before they become bad stats. But, you don't have to prune every inactive email address right away. First, try re-engaging with those subscribers that still show potential.

Create segments based on recipients' activity levels then use customized campaigns to rekindle those relationships that have cooled. Use automation to initiate these "win-back" campaigns before you abandon all hope and use a granular approach based on specific recipient behaviors. Has the subscriber never engaged with your brand or has their interest recently lapsed? Would a personalized message with a discount offer get their attention?

Implement automated sunset policies to deal with emails that are in the zone between "gone for good" and "maybe just taking a break." Use an automated email sequence and cadence to gradually reduce your contact with these subscribers before you decide to shelve them permanently.

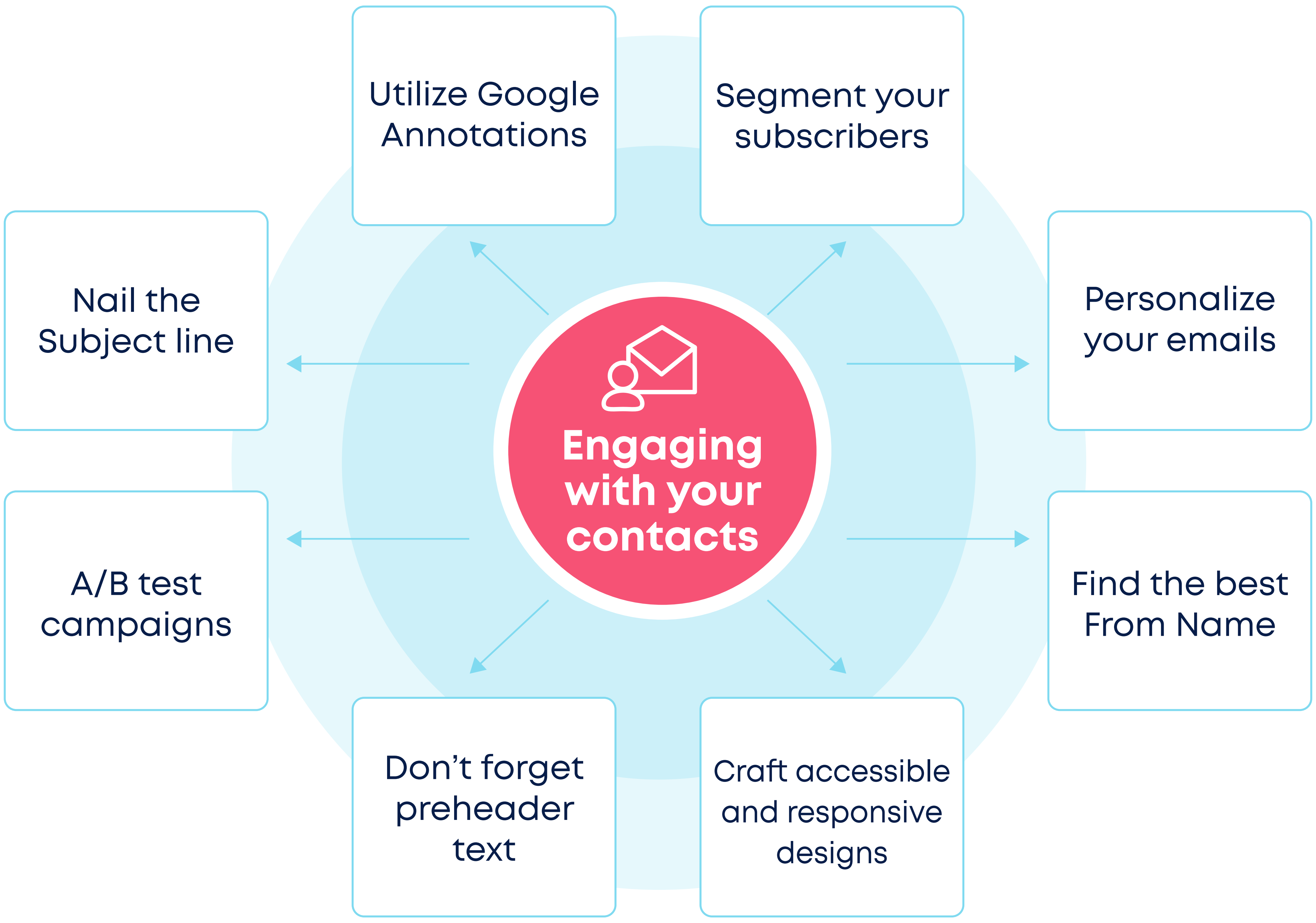


Second, focus on engaging your best contacts

As we have seen, ISPs are watching email open and click-through rates. How often your subscribers reply to or forward your emails influences your sender reputation as well.

You need to deliver content your subscribers want to see and an email experience that surprises and delights to keep your engagement rates in the green zone.

Here are some of our favorite ways to do that.


Engaging with your contacts
Utilize Google Annotations
Segment your subscribers
Personalize your emails
Find the best From Name
Craft accessible and responsive designs
Don't forget preheader text
A/B test campaigns
Nail the Subject line

Make a good first impression

ISPs treat unread messages as a negative reputation signal, and if your emails are deleted without being read, you won't achieve your marketing goals. Getting subscribers to open your emails is critical and requires planning.

According to a recent study, the top factors influencing whether recipients will open an email from you are the content of your subject line, your brand identity, and your preheader text.[20] If you want subscribers to open your emails, these three elements need to be attention grabbers. Use their combined power to amp up your open rates.

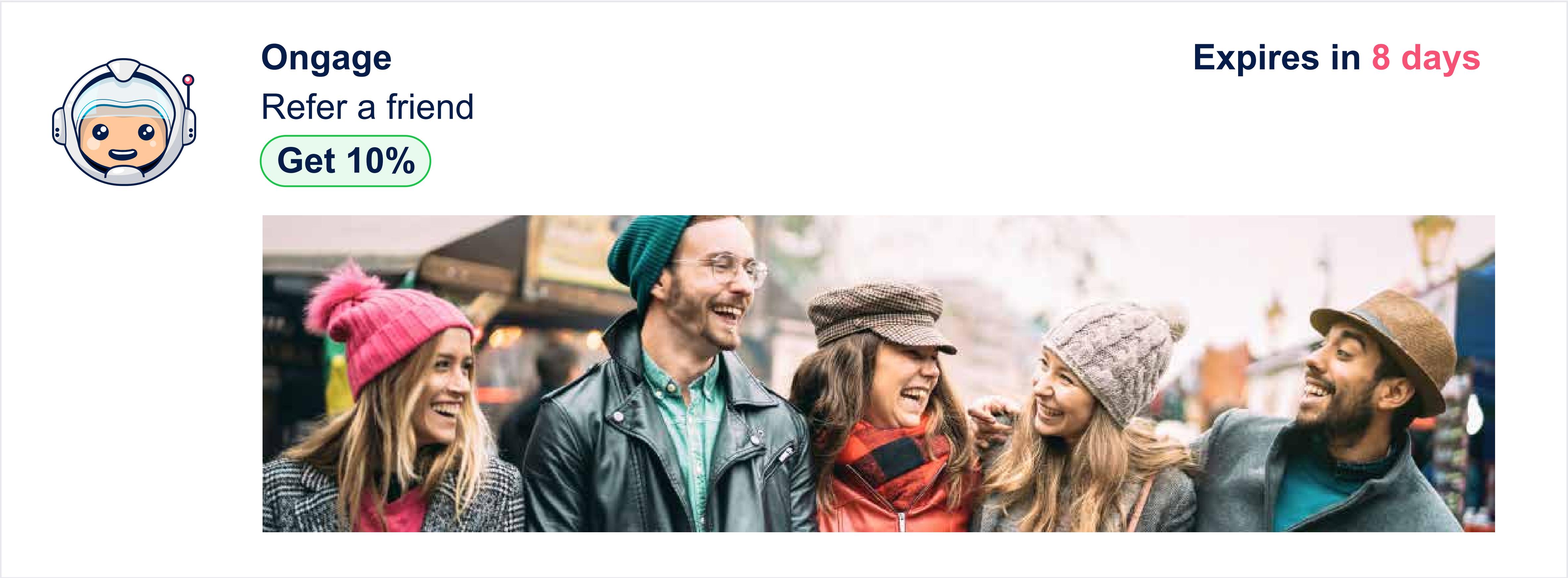
Your **subject line** should build curiosity, trigger emotion, and tell subscribers what's in it for them. But, be careful not to go too far, or your subject line may trigger spam filters. You may need to test a few subject lines to find that fine line between persuasive and pushy. Tell recipients who you are by including your brand's name in the email's **'from' field** and using BIMI verification so your logo appears alongside your message in recipients' inboxes.

Then, bring home the open with your preheader text.

Without adding customized preheader text, the email preview will default to your email's first lines, which sometimes make no sense when taken out of context. You don't want that to happen. Be strategic when you compose your preheader text. This is your chance to gain precious extra characters in your subscriber's inbox queue. Don't waste space repeating your brand name or content that already appeared in the subject line. Instead, think about how your preheader text can expand or supplement those two elements to create a complete and compelling message with which your subscriber would want to engage.

If your emails are destined for the Promotions tab, you can take advantage of Google's annotation feature to grab your recipients' attention. Using JSON-LD, add a script tag in your email's HTML header to add details such as the discount you are offering or a promo code.[21]

Promotional annotations aren't supported by every mail sender yet, but you can expect these and other features to surface as providers continue to fight for inbox share.



Ongage
Refer a friend
Get 10%

Expires in 8 days

This is how your emails can look when they land in the Promotions tab, using Google Annotations

Get up close and personal

Even more important than the subject line and pre-header text is the body. The real payoff. A one-size-fits-all is not a good approach for today's email marketing campaigns. Customers expect you to know who they are when you contact them and provide them with content that matches their interests. If you want to keep your engagement rates high and stay out of your recipients' spam folders, you'll need to tailor your emails and add personal touches carefully. One way to segment your mailing list effectively and personalize the emails you send is to integrate your email marketing platform with your CRM.

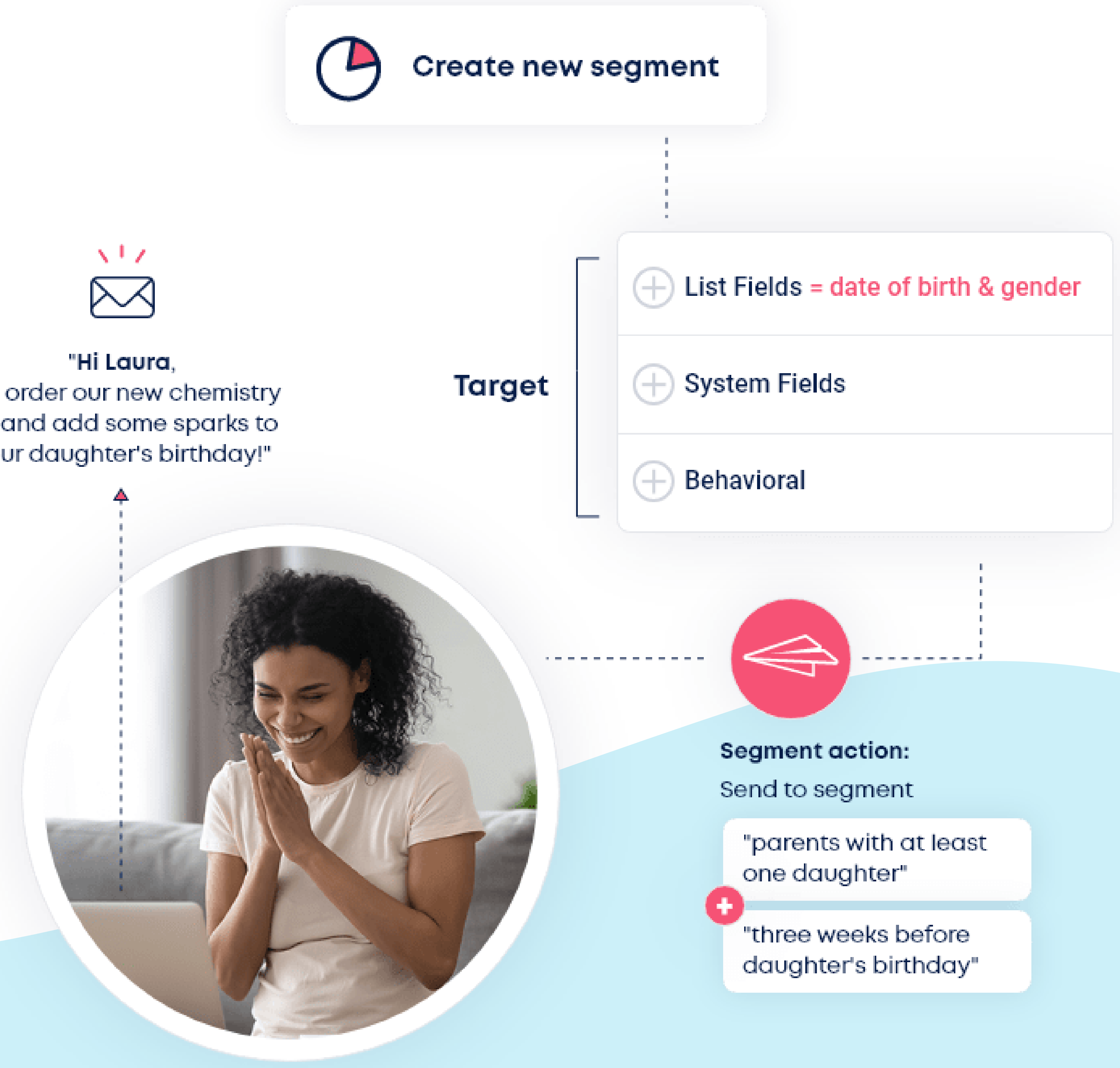
Integration of these two sources of data allows you to cross-leverage both.

- You can use email subscriber behavior data to supplement what you've learned about them through other channels. And,
- You can utilize your CRM data to improve your list segmentation and message personalization. Making the extra effort to send your subscribers information selected just for them will boost your engagement and your revenue.

Segment your lists and create custom campaigns for subscribers in different geographic regions, varying age and interest groups, or customer persona. You can also combine automation with segmentation to send event- or trigger-based emails, including transactional emails and re-engagement campaigns.

Your personalization efforts should go beyond just mentioning recipients by name. Hyper-personalization is already here, live and kicking.

Use dynamic content feeds and micro segments to match your message to members of who meet hyper-specific criteria such as a recent purchase, an upcoming anniversary, or other triggers. Schedule birthday best wishes and send them at your customer's favorite time of day for checking emails. With the right data, you can deliver in-the-moment content that is hyper-customized and hyper-relevant.



Create new segment

Target

List Fields = date of birth & gender

System Fields

Behavioral

"Hi Laura,
Pre order our new chemistry set and add some sparks to your daughter's birthday!"

Segment action:
Send to segment

"parents with at least one daughter"

"three weeks before daughter's birthday"

Remove friction and deliver delight

Maximize your engagement rates by making interacting with your emails easy and stress-free. If your subscribers have to work too hard to understand your email or figure out how to take the next step, they are likely to move on. Craft your emails so that even if something goes wrong, such as an image fails to render, your recipient will still get the message. Further, be sure to use a responsive design that adjusts to your recipients' resolution.

There's no doubt about it nowadays, emails should be first optimized for mobile viewing and interaction as the number of consumers who use mobile devices to check their emails continues to climb.

- 62% of all email opens occur on mobile in 2019.[22]
- 81% of consumers responding to a study in the fall of 2020 said they use smartphones to check their messages.[23]

How can you make sure that you look good on mobile?
First, keep screen sizes in mind when choosing your font sizes and make your CTA large enough for tapping, not just clicking. Then, avoid oversized image files while including alt-text and other accessibility features. Finally, test the appearance of your design across multiple devices.
Another way to reduce friction is to make sure your subscribers can reply to your emails. This helps you identify your most engaged contacts and boost your sender reputation. Today's consumers are channel-agnostic, so you want to provide them with choices to staying in touch with you. Use a functional reply address and include your brand's contact information in each of your emails. Including your contact information is not only a legal requirement in many jurisdictions. It's also good for engagement.

Finally, don't forget to monitor your reply email account and other contact channels--wherever and whenever your customers reach out to you, you should be prepared to respond.

Are your emails compatible with today's consumer?

Responding to a survey conducted in 2020, 20% of consumers said they had received emails that were broken or not viewable on mobile. What happens if your subscribers can't view your email on their mobile device? 62% of the survey's respondents said they ignored or deleted unreadable emails.[24]

PART 03

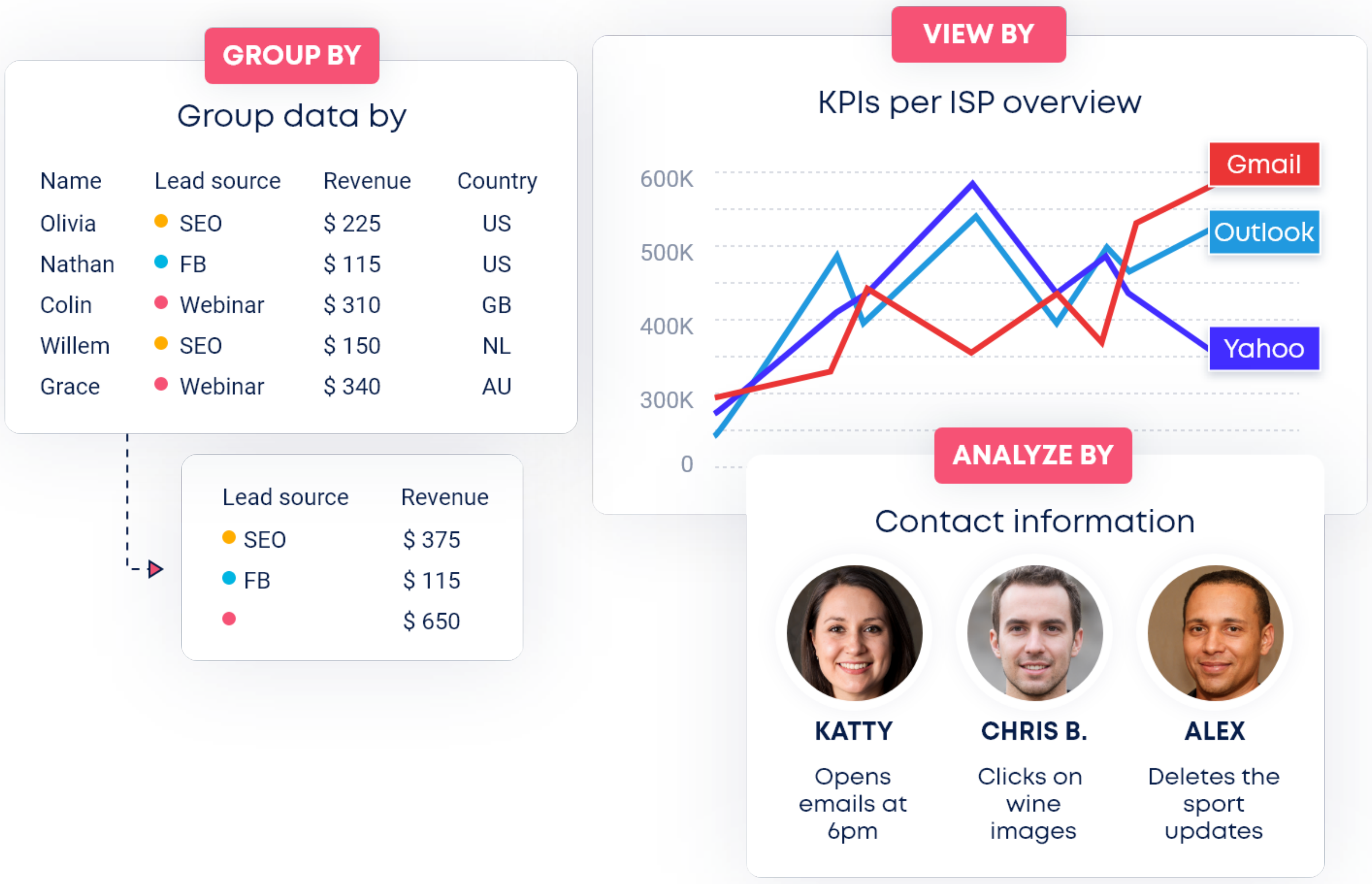
Stay on top with continuous analysis and adaptation

Like “don’t be spammy,” some best practices are fundamental to email deliverability and engagement. Other strategies will change over time as ISPs adjust their anti-spam measures and consumer preferences change. To maintain top deliverability rates and earn your subscribers’ attention, you’ll need to be prepared to adjust quickly to new information.

How will you know when to pivot? That requires vigilance. Develop and nurture an email marketing program that captures data from multiple sources and uses that information to implement continual improvements.

From the beginning, take a holistic view of your email marketing campaigns and deliverability profile. Combine information from third-party mail service vendors, ISPs, industry guides, and your internal analytics tools to develop the strategies that suit your business model and your markets.

Stay on top of your subscribers’ behavior and deliverability results. Sort your results by date, campaign, location, ISP, device operating system, and other data points to evaluate performance and make strategic decisions.



GROUP BY

Group data by

Name	Lead source	Revenue	Country
Olivia	● SEO	$ 225	US
Nathan	● FB	$ 115	US
Colin	● Webinar	$ 310	GB
Willem	● SEO	$ 150	NL
Grace	● Webinar	$ 340	AU

Lead source	Revenue
● SEO	$ 375
● FB	$ 115
●	$ 650

VIEW BY

KPIs per ISP overview

ANALYZE BY

Contact information

What should your analytics strategy measure and track?

01

Deliverability begins with authentication, and so should your monitoring and analysis

Keep your authentication records up to date. Schedule regular reviews of your SPF records to ensure that each valid IP and domain is included in the TXT file and that inactive addresses are removed. Also, regularly monitor your DMARC reports. Keep an eye out for spoofing attempts and close any gaps in your security before bad actors have a chance to damage your reputation.

02

Monitor ISPs' responses to your IPs

Are email batches sent from specific IPs or to specific mail providers being throttled? Develop a plan to monitor and analyze how your IPs are performing. Streamline your monitoring process by running updated reports that notify you when your bounce rates exceed certain thresholds.

03

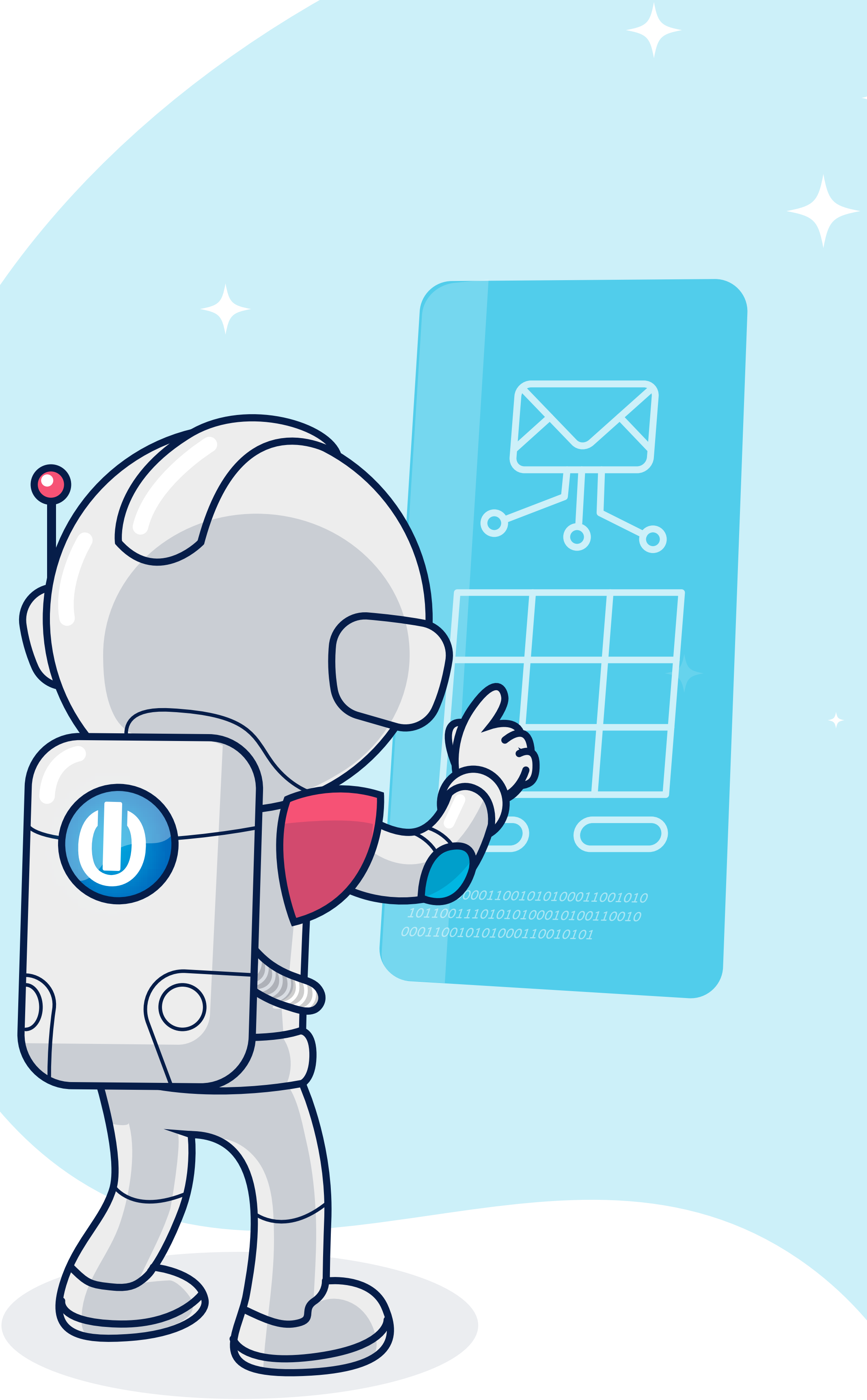
Gather and manage your third-party reports

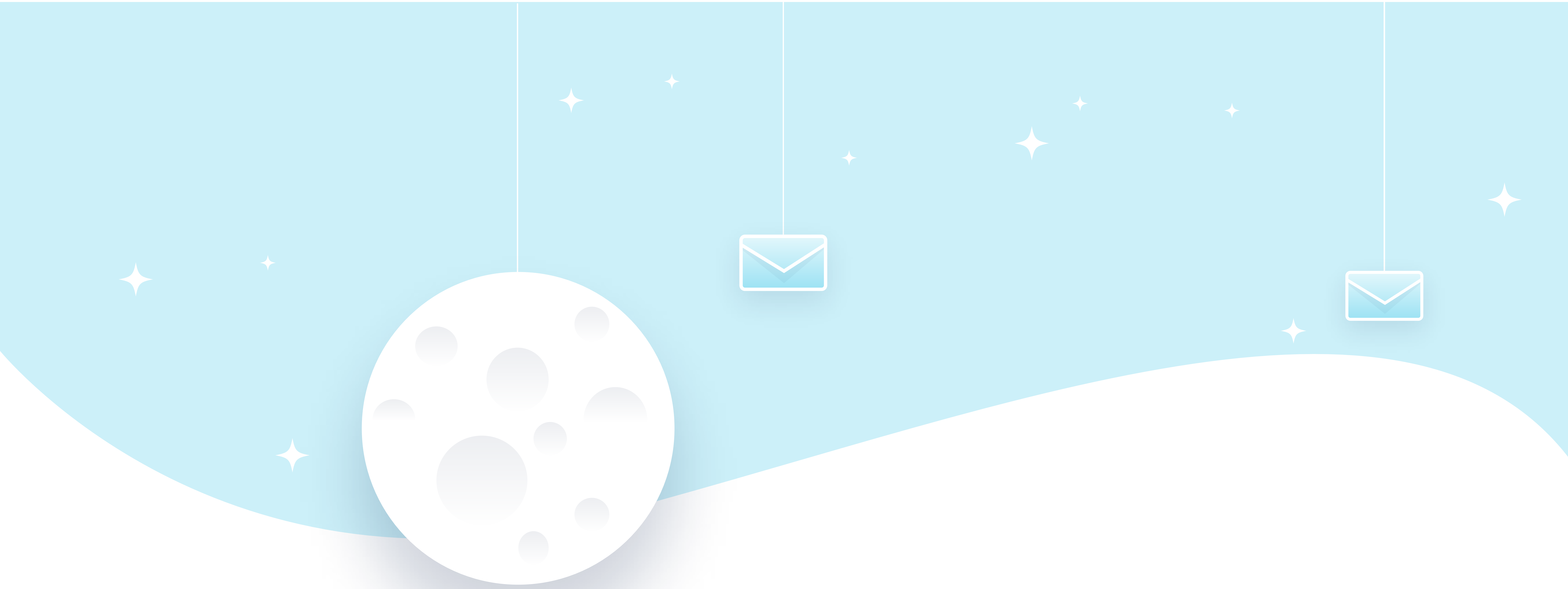
Collect and analyze third-party reports, including spam complaints, blocklists, and other data about your email list. Use this information to improve your email capture practices and eliminate spam traps from your lists.

04

Embrace deliverability testing tools

Take some of the guesswork out of determining the deliverability of your email content by using tools to analyze your subject lines and other deliverability factors. Use seedlist tests to detect and quantify deliverability problems, analyze key KPIs per ISP to help determine deliverability, and also test campaigns pre-launch with Mail-Tester.





05

Continually verify and validate your mailing lists

Mailing list hygiene is not a one-and-done activity. Incorporate regular batch re-validation of all addresses into your email program. Divide your full email list into several smaller batches and re-validate them on a rolling schedule so that every email is reviewed at least twice a year. If you've followed all the other list best practices, these tests should prove that you've done a great job! Save time by automating this review process and your system for placing stale or invalid emails on your suppression list.

06

Use multiple strategies to monitor and test the quality of your content

Your engagement will plummet if your email doesn't show up looking good. Use tools that enable you to screen your emails for accessibility, mobile compatibility, broken links, and bad images. Validate your HTML and preview what your emails will look like on various devices.

07

Track your engagement metrics at every touchpoint

This is a big category and an important one. How subscribers engage with your emails directly impacts both deliverability and profitability. Subscriber engagement is your gateway to conversions and revenue. In addition to tracking your engagement at several touchpoints, you should use your CRM and mail analytics tools together to filter and segment recipients based on different characteristics. Maximize your engagement by optimizing your emails for each segment. The more granular and personalized your approach, the better your results will be.

Let's dive in-depth into this important metric!

ISP	Sent	Success	Hard bounces	Soft bounces	Opens	Clicks	Unsubscribes	Complaints
Gmail	2,500,000	2,480,000 (99.20%)	5,000 (0.20%)	15,000 (0.60%)	1,044,080 (42.10%)	231,786 (22.20%)	4,960 (0.20%)	25 (0.00%)
Yahoo	1,500,000	1,486,500 (99.10%)	4,500 (0.30%)	9,000 (0.60%)	630,276 (42.40%)	153,787 (24.40%)	3,270 (0.22%)	15 (0.00%)
AOL	750,000	741,750 (98.90%)	2,250 (0.30%)	6,000 (0.80%)	295,217 (39.80%)	78,232 (26.50%)	1,409 (0.19%)	7 (0.00%)
Outlook	250,000	247,000 (98.80%)	750 (0.30%)	2,250(0.90%)	95,836 (38.80%)	18,976 (19.80%)	445 (0.18%)	2 (0.00%)
Total	5,000,000	4,955,250 (99.11%)	12,500 (0.25%)	32,250 (0.65%)	2,065,409 (41.68%)	482,781 (23.37%)	10,084 (0.20%)	50 (0.00%)

What are the engagement touchpoints you should track?

First metrics: List growth related

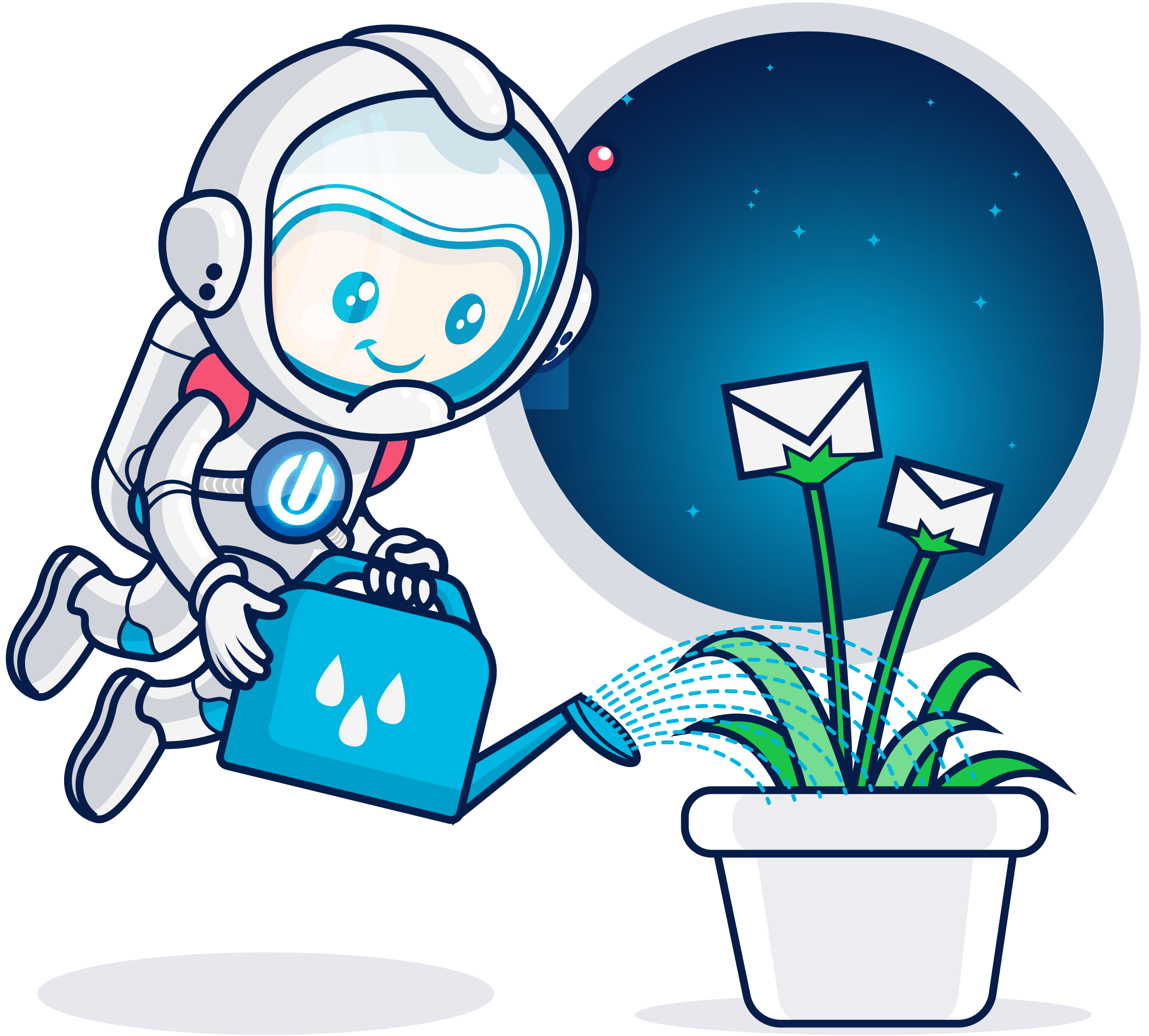
How many subscribers do you have?
And how many do you keep?

Tracking your subscriber engagement begins before the first email is sent and continues through each subscriber's lifecycle.
The first metric you should monitor is your **subscription rate**.
How many new subscribers are you adding to your lists each period? You'll then use this number to calculate your **list growth** and **subscriber churn** rates.

How many people unsubscribe from your list each period? And what is your net subscriber loss or gain?
Other metrics that can give you insights into the attractiveness of your messaging efforts are your **lapse rate**, or the number of subscribers whose engagement drops over time, and **relapse rates**. Relapse rates reflect the success of your re-engagement campaigns. What percentage of subscribers resume interacting with your emails after you've showered them with special attention?

How to Calculate Your Growth Rate

$$\frac{\text{New Subsribers - Opt Outs - Invalids}}{\text{Previous List Size}} = \text{List Growth Rate}$$



Second metrics: Initial user actions

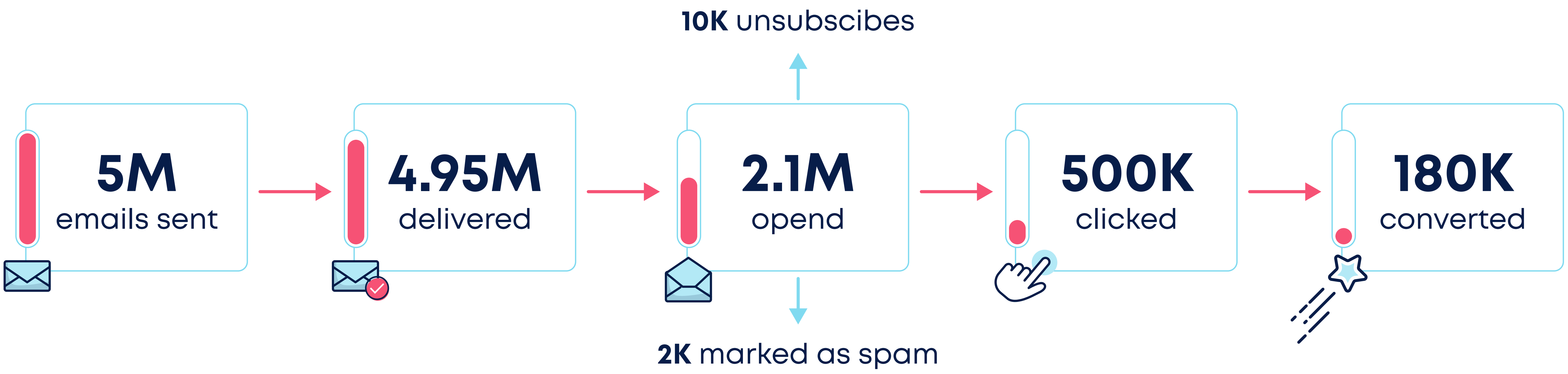
What happens to your emails after they make it to the inbox?

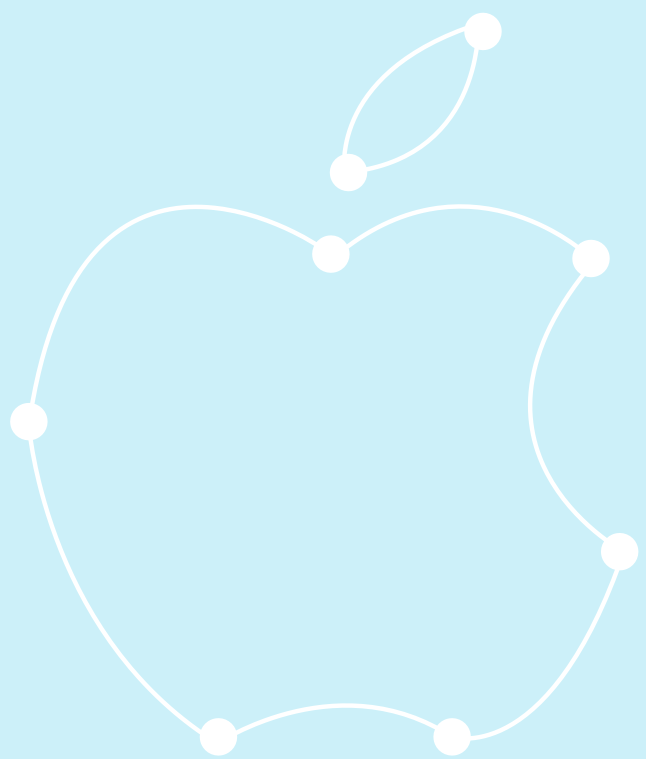
For deliverability purposes, open rates are interpreted as a signal that an email has been **read**. Your sender reputation will decrease if ISPs detect that your emails went unread.

What's happening with open rates?

In early June of 2021, tech-giant Apple announced their "Mail Privacy Protection" initiative, which will launch with iOS 15. In short, it means that email marketers won't be able to accurately deduce the IPs and open rates of emails that are read via Apple's mail app.
Apple may be the first to do so, but don't be surprised if companies like Google follow them shortly after.
What does this mean for email deliverability? While this policy is a cause of concern for email marketers and presents real challenges, email marketing will remain one of the most profitable, cost-effective channels.
Like in the introduction of Gmail tabs and other privacy policies, we learned, evolved, and became better marketers.
And Apple presents us with another chance to do so. Instead of keeping our focus on open rates, we should turn our gaze into other metrics. Metrics that signal a much stronger intent compared to the opening of an email, like clicks, conversions, and revenue. And metrics that are more accurate than the open rate, which can signal many different user intentions.

First, your email may be opened by someone who then **unsubscribes** or **marks it as spam**. That doesn't point to resounding engagement success. On the other hand, if the user opens your email and marks it as a favorite or preferred sender or **"not spam"** it means that you're doing something right. These are both positive deliverability signals. Unfortunately, measurements of these positive activities may be hard to come by.

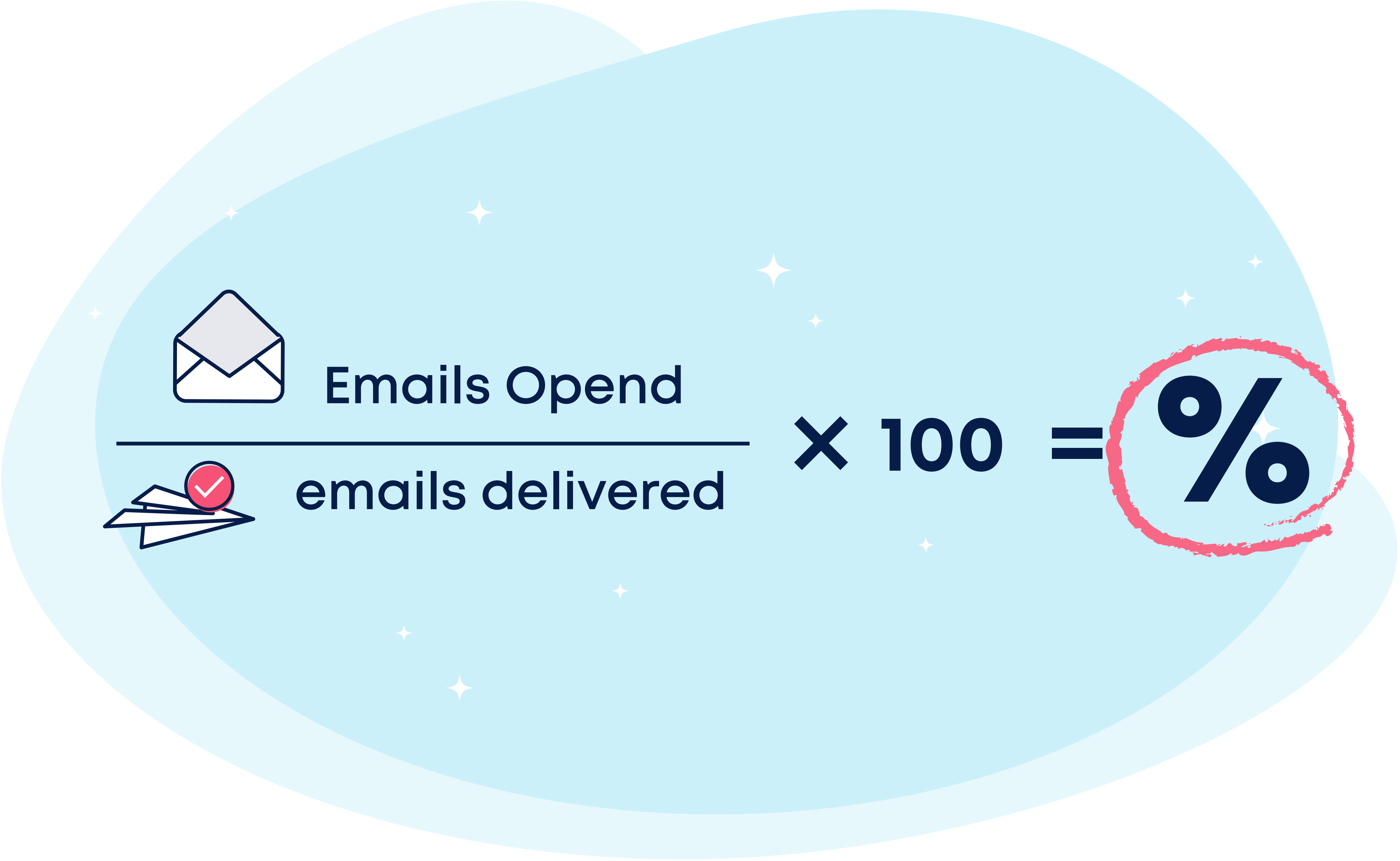




Open rates triggered by a pixel embedded in each email may not represent every open or every open by a human subscriber. Sometimes, a mail service app blocks the pixel, or otherwise, it fails to report back, so those opens never register. Other times, the pixel may be triggered by automated security or pre-loading function and report an open, even though your subscriber hasn't seen your message.

Finally, since each open counts as a unique action, repeat opens can cause open counts to be inflated. Repeat opens may not be a significant cause of overcounts for your brand. However, as more recipients check and interact with their emails from multiple devices, this metric may require more attention.

How to Calculate Your Open Rate



Third metrics: Strong intent user actions

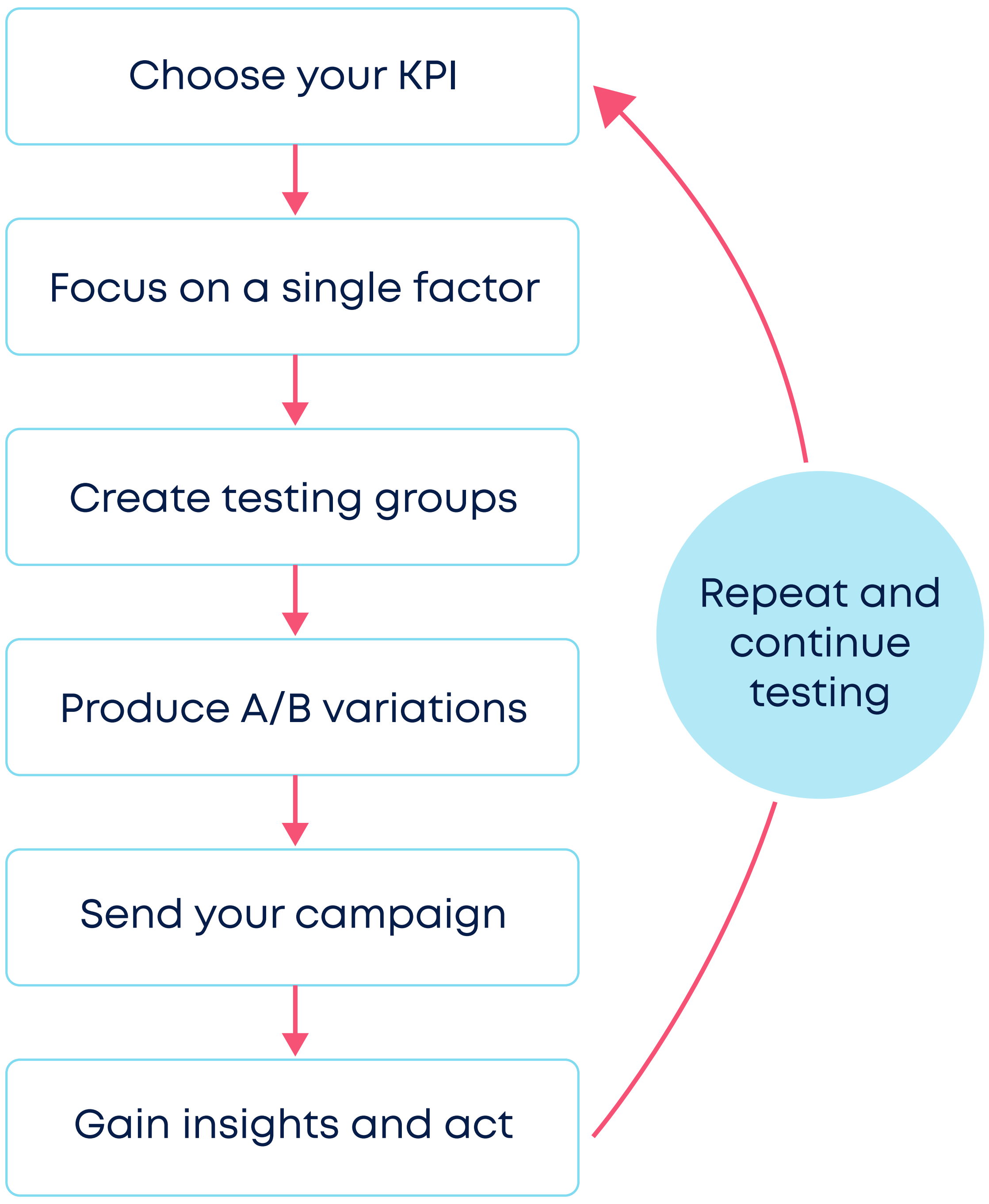
To gain a deeper understanding of your engagement levels, compare your delivery rates with your click-through and conversion rates. Both of these metrics indicate whether or not someone who opened your email took an affirmative action based on what they saw inside.

Unless you have an issue with your metrics, your CTR for a campaign will always be higher than your conversion rate. The greater the difference between the numbers, the more likely it is that the content in your email is a hit, but your landing page is lacking.

While perhaps not as exciting as a click you were trying to earn, **replies** to your emails are another good indicator that your subscribers have opened and are engaged with your emails.

Finally, use campaign ROI and revenue per email metrics to go beyond and capture the revenue streamers that truly matter.

You can use all of this data to inform future A/B tests and strategy shifts, like this:



Choose your KPI

Focus on a single factor

Create testing groups

Produce A/B variations

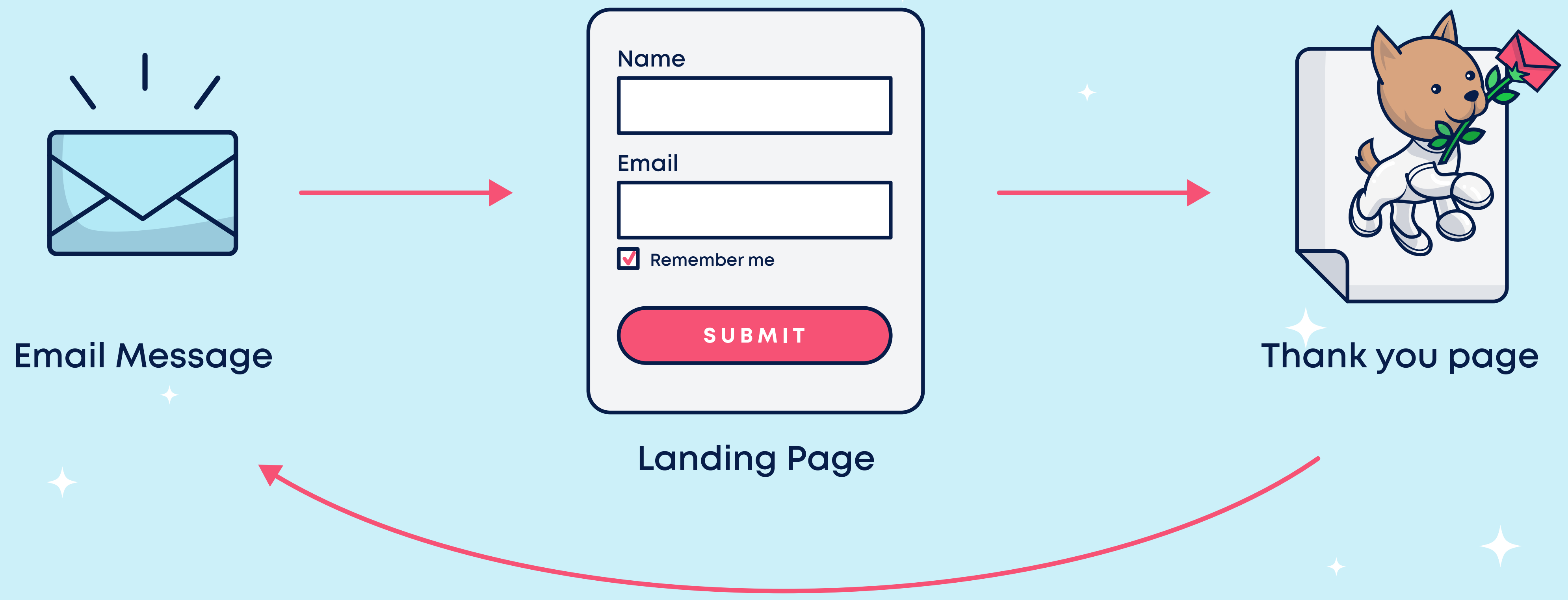
Send your campaign

Gain insights and act

Repeat and continue testing

Click Link in Email Message

Complete Registration



Email Message

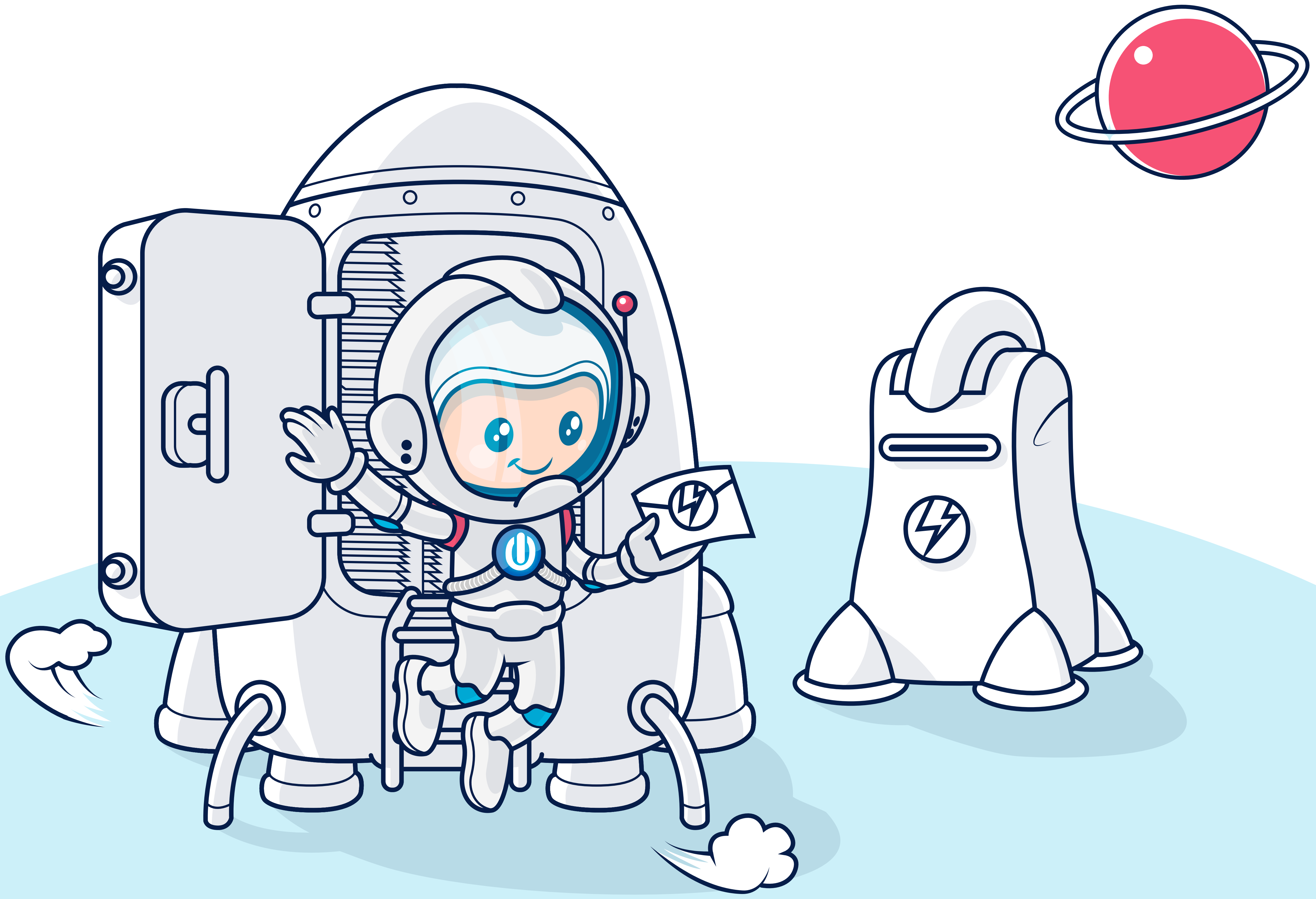
Landing Page

Thank you page

Pixel Fires - Confirms that the user has signed up

Of course, performing this kind of continual analysis requires powerful data tools and proper support to show you how to use them. To ramp up your analytical capabilities, develop a list of priorities. Evaluate metrics you already track and those you want to track moving forward. Identify gaps in your deliverability and engagement, and set timelines for implementation based on complexity and expected ROI.

Then, work with your email sending partners to execute your new measurements and performance strategies.
We'd love to help you with that.



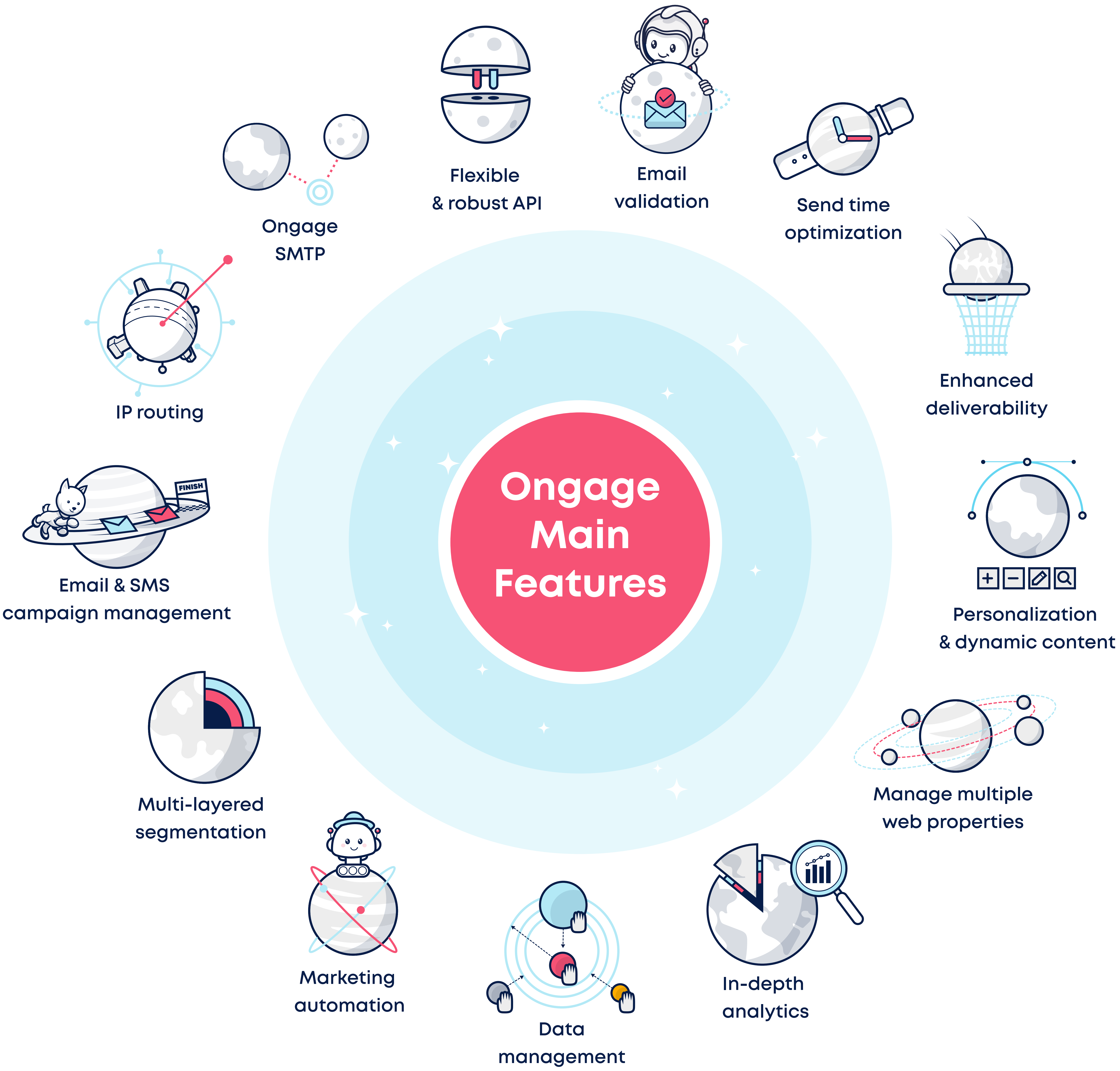
About Ongage

We hope you enjoyed reading this handbook. Ongage will continue to update it periodically to keep it up to date. You'll always be able to find the latest version here.

Who are we?

Ongage was founded in 2010. It's an end-to-end email marketing platform for advanced email operations that need to tackle the challenges of data-driven growth. Our platform focuses on giving you the tools you need to create meaningful relationships with subscribers and does so at scale.

Email marketers and developers use our industry-leading segmentation, personalization, campaign optimization capabilities, and API to fuel the growth of their email operations.
If you're ready to give your email operation all the goodness mentioned above and if you'd like to enjoy a more streamlined email operation management experience, schedule a demo.



Glossary of terms

Authentication
A way of establishing a sender's identity, and ensure the sender is allowed to send from a given domain.

Bounce rate
The rate at which your emails are not delivered.

Blocklist
When your emails are stopped from being sent by spam filters or other factors is called email block.

Can-Spam
Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 is an act from the USA which majorly has laws that control the businesses to send misleading emails to recipients.

CASL
Canadian act that requires Canadian and global organizations that send commercial emails within, from or to Canada to receive consent from recipients before sending messages.

Churn
Churn rate is a percentage of users who have left your mailing list within a given period of time.

Click through rate
Is a metric that measures how many people clicked on an image, hyperlink, or CTA in an email.

DKIM
DomainKeys Identified Mail is a way that an organization takes responsibility for an email that is sent.

DMARC
Domain-based Message Authentication, Reporting & Conformance is an email authentication, policy, and reporting protocol.

Double opt-in
Email address verification by sending a email asking to confirm the subscription.

ESP
Email Service Provider.

GDPR
General Data Protection Regulation is a law from Europe which protects the personal data of the European citizens.

Hard bounce
A hard bounce is the failed delivery of an email due to a permanent reason like a non-existent, invalid, or blocked email address.

Hygiene
Email hygiene entails cleaning out inactive email subscribers from your future email marketing campaigns.

IP warm up
Sending a progressively increasing number of emails out of an IP address in order to build the IP's reputation.

ISP
Internet Service Provider, which is a company or organization that provides services for Internet access.

KPI
Key Performance Indicator, a quantifiable measure of performance over time for a specific objective.

MTA
Mail Transfer Agent, a software that transfers electronic mail messages from one computer to another using simple mail transfer protocol.

Open rate
The percentage of emails opened in an email marketing campaign.

Preheader
The summary text that follows a subject line when the email is viewed in an inbox.

Reply-to
It is the email address that the reply message is sent when subscribers want to reply.

Segment
Selecting a target audience or group of individuals for whom your email message is relevant.

Shared IP
A less costly option than a dedicated IP address, it is an IP address from which many people send emails.

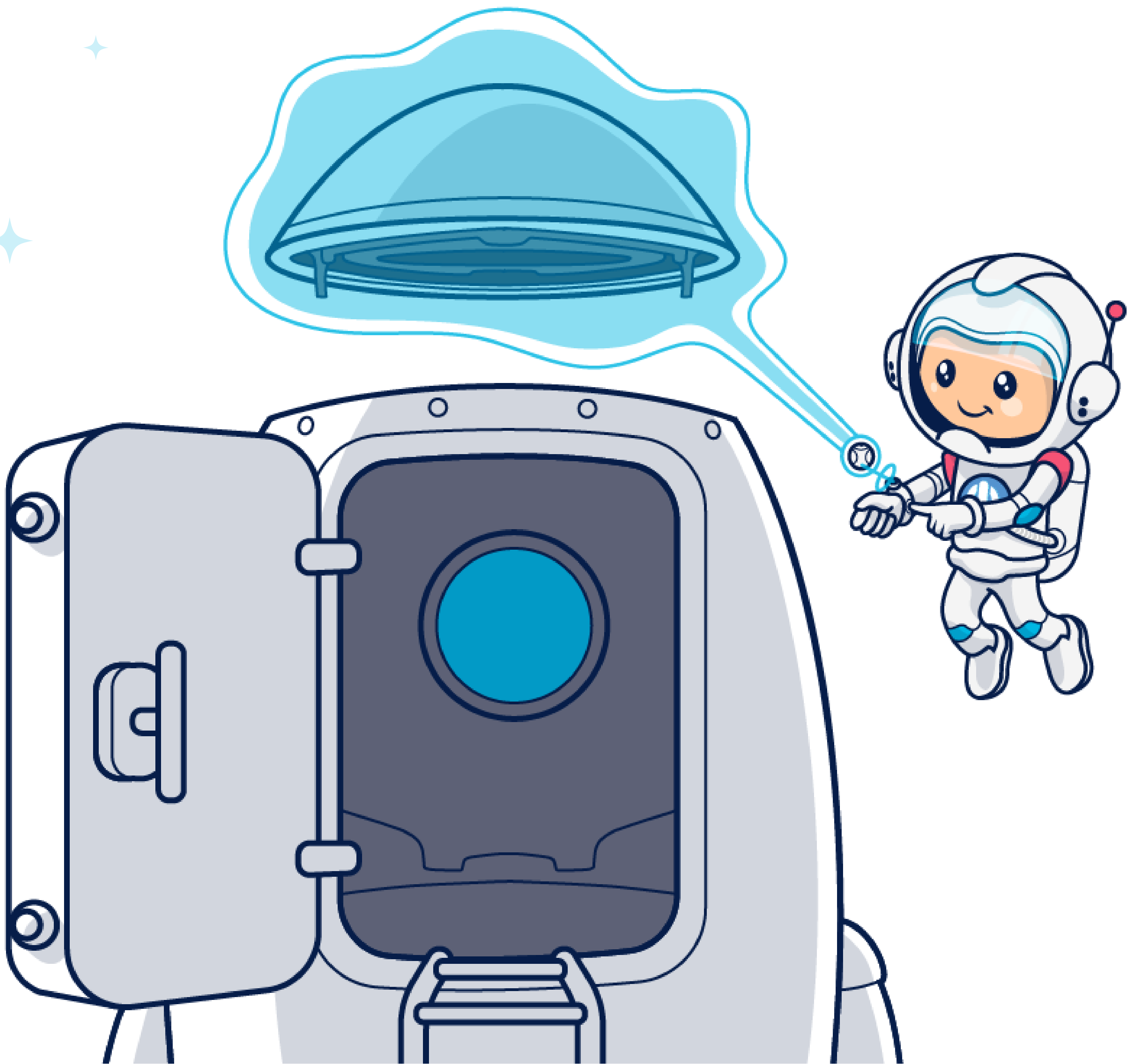
Soft bounce
A soft bounce is the failed delivery of an email due to a temporary issue, like a full mailbox or an unavailable server.

Spam
Email sent to someone who has not opted-in or given permission to email to the sender.

SPF
Short for 'Sender Policy Framework', it's a DNS record that says on whose behalf an IP or domain sends email.

Subject line
The single line of text people see when they receive your email.

Unsubscribe
When people decided the content is not relevant to them and want to unsubscribe. You need to give an opt-out / unsubscribe link in all your email communications.



References

1 Email Marketing: Where Marketing & IT Seamlessly Meet, Digitalmarketing, https://digitalmarketing.temple.edu/shannonatwell/2017/10/18/email-marketing-where-marketing-it-seamlessly-meet/

2 Number of sent and received e-mails per day worldwide, statista, https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

3 2020 Email Deliverability Benchmark, Validity, https://www.validity.com/resource-center/2020-deliverability-benchmark/

4 B2C Retail Benchmark Report, Q1 2020, Eipserver, https://www.episerver.com/guides/b2c-retail-benchmark-q1-2020

5 Global spam volume as percentage of total e-mail traffic from 2007 to 2019, statista, https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

6 Sender Policy Framework: SPF Record Syntax, Sender Policy Framework Project, http://www.open-spf.org/SPF_Record_Syntax/

7 DomainKeys Identified Mail (DKIM) Signatures, DKIM.org, http://dkim.org/specs/rfc4871-dkimbase.html

8 Create a DKIM TXT record, Rackspace Technology, https://docs.rackspace.com/support/how-to/create-a-dkim-txt-record/

9 What is a DMARC record?, DMARCAnalyzer, https://www.dmarcanalyzer.com/dmarc/dmarc-record/

10 Anatomy of a DMARC resource record in the DNS, DMARC, https://dmarc.org/overview/

11 All about BIMI/Implementation Guide, BIMI Group, https://bimigroup.org/all-about-bimi/, https://bimigroup.org/implementation-guide/

12 Prevent mail to Gmail users from being blocked or sent to spam, Google, https://support.google.com/mail/answer/81126?hl=en

13 RCF 5322: Internet Message Format, Internet Engineering Task Force, https://tools.ietf.org/html/rfc5322

14 HTML Living Standard, Web Hypertext Application Technology Working Group, 2020, https://html.spec.whatwg.org/multipage/

15 Understanding DNSBL Filtering, SPAMHAUS, https://www.spamhaus.org/whitepapers/dnsbl_function/

16 How does the GDPR affect email?, GDPR.EU, https://gdpr.eu/email-encryption/

17 New decade, new rules: Customer engagement in the 2020's, Sinch, https://www.sinch.com/blog/new-decade-new-rules-customer-engagement-in-the-2020s/

18 Email Data Hygiene is Make-or-Break for List Success in 2020, FreshAddress, https://www.freshaddress.com/blog/focus-on-email-data-hygiene-for-2020-success/

19 The Future of Email Marketing, Dyspatch, August 7, 2020, https://www.dyspatch.io/blog/the-future-of-email-marketing/

20 The Future of Email Marketing, Dyspatch, August 7, 2020, https://www.dyspatch.io/blog/the-future-of-email-marketing/

21 Get started: How to annotate your email, Google, https://developers.google.com/gmail/promotab/overview

22 Top 10 Email Clients in March 2019, Upland, 2019, https://uplandsoftware.com/adestra/resources/blog/top-10-email-clients

23 Email Marketing Insights, Fluent, September 16, 2020, https://fluentpulse.com/consumer-insights-email-marketing/

24 The Future of Email Marketing, Dyspatch, August 7, 2020, https://www.dyspatch.io/blog/the-future-of-email-marketing/

Writers and contributors

WRITERS

Melissa Pekel

Melissa is VP of Marketing at Ongage. She brings years of company building, startup launching, SaaS to positive ARR, and email marketing experience. In Ongage, she is leading the marketing team while planning and launching the strategic implementation of the entire operation.

Haim Pekel

Haim is VP of Growth at Ongage. His specialties took many companies, from launch to profitability through channel, product, and market fit analysis, followed by implementing strategies creatively. In Ongage, he focuses on developing creative solutions for email marketing challenges.

Ayal Menaged

Ayal is Marketing Manager at Ongage. With an MA in Social Psychology and an Analyst title in his past, Ayal is able to bring valuable insights to the team.

CONTRIBUTORS/EDITORS

Ryan Phelan

Ryan brings nearly two decades of global online marketing experience to Origin Email Agency focusing on driving GTM strategies for high growth SaaS software and Fortune 250 companies.

Chris Marriott

Chris is the President & Founder of Email Connect LLC, the world's leading ESP Search Consultancy.

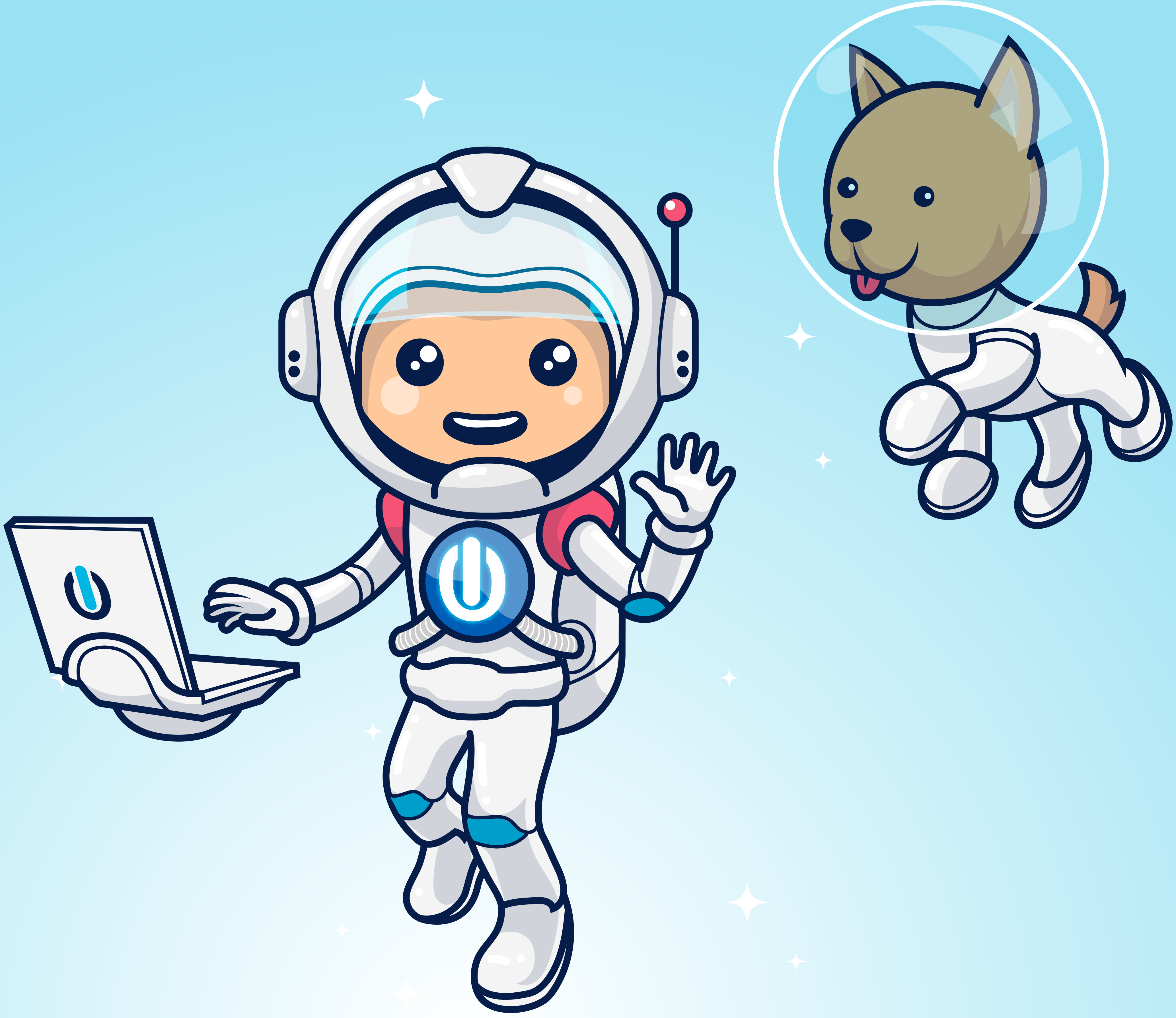
Tali Hasanov

Tali uses her real-world experiences and humour to drive proven, easy-to-implement strategies that deliver powerful and cost-effective digital marketing solutions for B2B and B2C customers.

DESIGNS

Kobi Mori

Kobi is Senior Designer at Ongage. With his degrees in economics and business administration (specializing in marketing) and visual communication design, Kobi strives to improve the brand visibility and growth.



Thank you!

For more in-depth email marketing content, visit our blog:
https://www.ongage.com/blog/

ongage