THE FUNDAMENTALS OF EMAIL MARKETING

EVEREST

TABLE OF CONTENTS

SECTION		PAGE
1	Introduction	3
2	What Happens After You Hit Send	4
3	How To Measure Email Success	10
4	Debunking Common Email Myths	14
5	Basic Email Terms	18
6	Getting to the Inbox Checklist	22
7	Continue Your Email Education	28

INTRODUCTION

It seems like email marketing has been around forever—we should know we have been around for over 20 years. While not as new and exciting as other marketing channels like social media and digital advertising, email still holds strong as one of the most effective marketing channels, with an average return of $42 for every one dollar spent (DMA, 2019).

You might think its effectiveness lies in its simplicity. After all, you just need to hit send and you are done, right? Wrong. Email is actually quite a complex marketing channel, and reaching its true potential takes some work. Unless you have access to the right data—and know where to look—unexpected problems may arise.

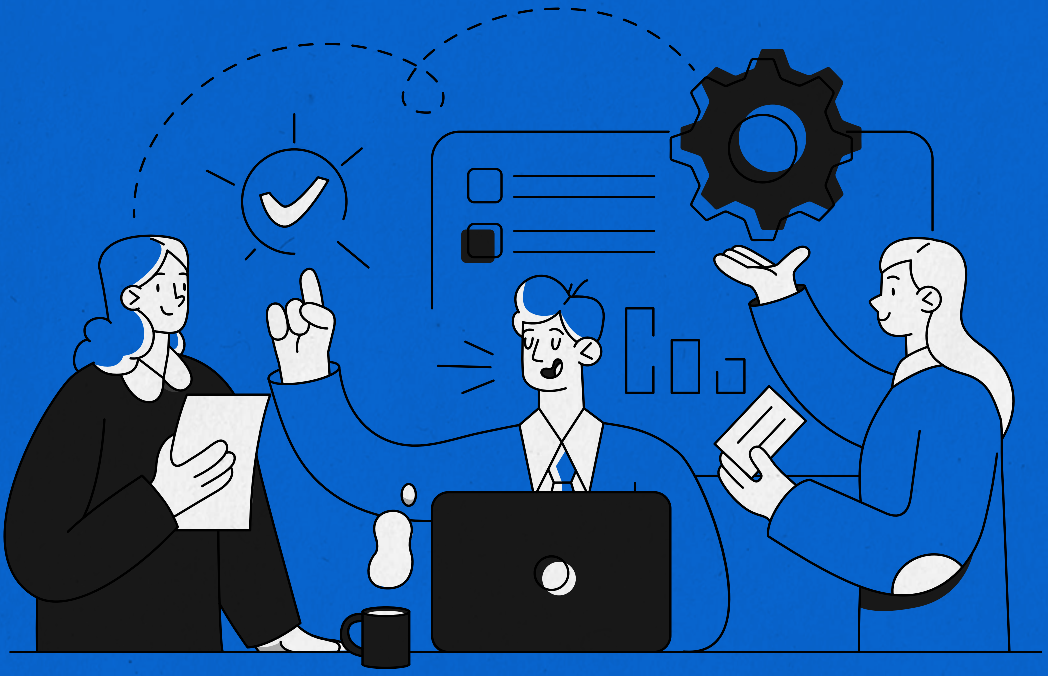
To help marketers understand and take advantage of this channel we created a guide to walk you through the basics of email marketing. In this guide we cover how email really works, as well as terminology, tips, and pitfalls to avoid.

2

WHAT HAPPENS AFTER YOU HIT SEND

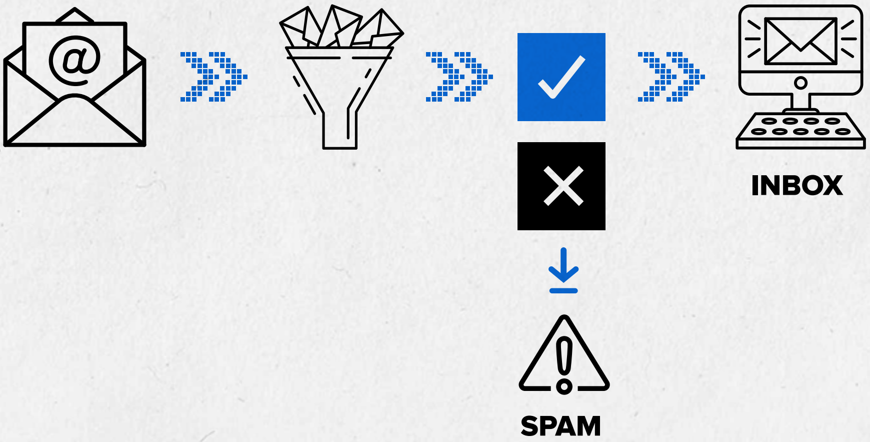
When a marketer hits send, an email's journey has just begun. Before an email reaches its final destination, it must pass through many filters designed to determine the validity of the message and decide where it should be placed. Only when an email successfully navigates these filters can it arrive in the inbox.

There is no avoiding spam filters. They are a necessary part of the email process. Instead, you need to understand how filters work, what they check for, and how to make sure your messages get a passing grade.



What is a Filter?

Email filters are a program mailbox providers use to analyze incoming email according to specified criteria and determine where to place them. Originally, filters were designed primarily to distinguish spam from legitimate email, and either block spammy messages or place them in the spam folder. Today, some mailbox providers also use email filters to categorize messages for inbox organization purposes (e.g., social media and newsletters).



Why Do Mailbox Providers Filter Email?

Mailbox providers have strong motivations to use spam filters. While spam is annoying, it can also be dangerous. Malware and phishing are hugely profitable for scammers and can be costly for consumers—the mailbox providers' customers—as well as the mailbox providers themselves, who face intense market competition. In addition to protecting their mailbox users, spam filters also drastically reduce the load on server resources. Considering that almost half of all mail sent globally is spam, that's a lot of mail to analyze.

How Do Filters Evaluate Email?

Mailbox providers look at three main aspects of mail when making filtering decisions:

1. **Source of the email**
2. **Reputation of the sender**
3. **Content of the email**

What is the Source of an Email?

The source of an email is the identity of the sender. In evaluating an email's source, spam filters look at factors such as past sending behavior, the age of the address the mail is being sent from (i.e., your IP address and domain) and whether the sender is authenticated (allowing the mailbox provider and the subscriber to confirm the identity of the subscriber). Email sent from new IP addresses and domains is treated with caution by mailbox providers. Senders with long-term IP addresses and domains and those that use authentication techniques are seen as more trustworthy.

TIPS ON YOUR SENDING SOURCE

Don't change your IP address if you don't have to

If you are experiencing deliverability issues, changing to another IP address won't solve the issue. In fact, you may be even worse off than before, as mailbox providers throttle messages from new IP addresses.

Use a dedicated IP address

On a shared IP address, you are not the only one contributing to your reputation. Despite your best efforts, if another sender on your shared IP address fails to follow good sending practices, your program will also be affected.

If using a new IP addresses, make sure you properly warm it up

Gradually begin sending a small volume of mail—ideally to your more engaged users—to build up a positive reputation on your new IP address.

Authenticate your email program

Mailbox providers view authenticated email as more trustworthy and are more likely to deliver it to the intended recipient. The most important email authentication protocols are SPF, DKIM, and DMARC

What is Sender Reputation?

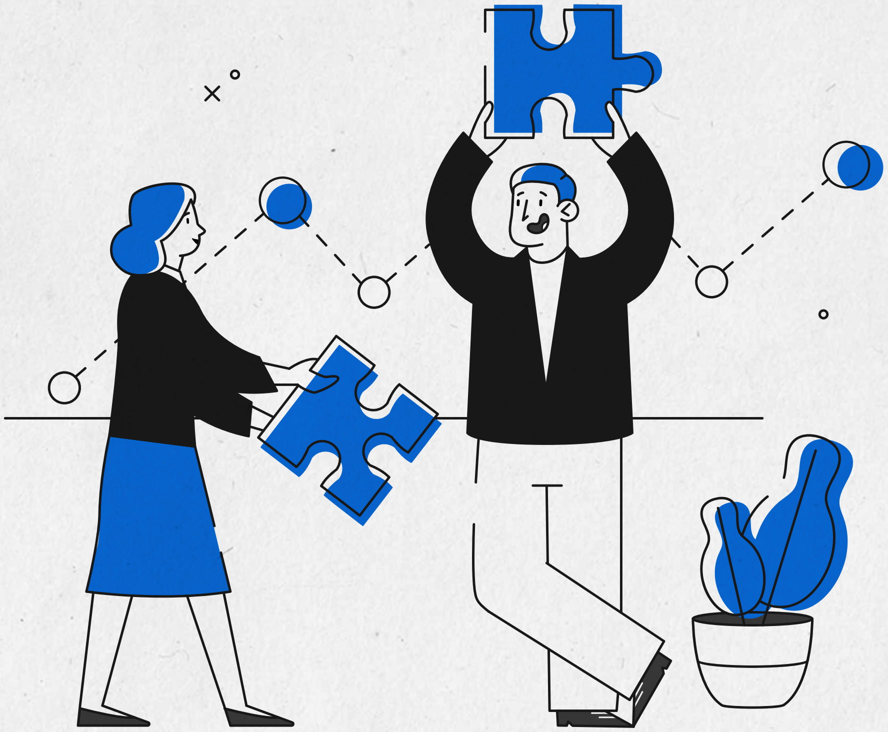
The reputation of an email sender is a score that indicates whether they're viewed as a legitimate sender or a spammer. It is calculated using algorithms that leverage millions of data points to evaluate past sending behavior and judge the validity of the sender. Based on the strength of the reputation score, mailbox providers will make filtering decisions about the email coming from a sender.

Some of the parameters leveraged to determine a reputation score are:

1. **Complaints**
2. **Spam traps**
3. **List hygiene**
4. **Volume**
5. **Blacklists**

Click the links to learn more!

Until senders take steps to improve their reputation, their messages will continue to be delivered to the spam folder.



TIPS ON IMPROVING YOUR SENDER REPUTATION

Monitor your sender reputation

Always check your reputation score before you send and messages to ensure poor reputation won't impact your campaigns.

Keep your list clean

Spam traps, unknown users, and unengaged subscribers can have a detrimental impact on your reputation. To validate whether the addresses on your list belong to a real person, run your list through a list hygiene service.

Sign up your feedback loops

Avoid possible damage from subscriber complaints by signing up for feedback loops. Each mailbox provider offers its own feedback loop service to alert senders when a subscriber complains about a message. Depending on the composition of your list, you may not need to sign up for every feedback loop available—so identify which ones are most valuable to your program before signing up.

What content are filters looking at?

Content analysis technology has the capability to scan every part of an email, including the header, footer, code, HTML markup, images, text color, timestamp, URLs, subject line, text-to-image ratio, language, attachments, and more. For some content filters, every single part of the incoming message is scrutinized. Other content filters may look at only the structure of an email, or they might simply parse URLs out of the message and reference them against blacklists.

TIPS TO CHECK YOUR CONTENT

Check your HTML

Most emails today are created in HTML, so having a nicely formatted HTML message is a good start. Broken HTML can lead to a poorly rendered message and generate complaints if recipients believe it's a phishing attempt. Make sure your HTML is free of syntax errors and formatting errors.

Test your message before you send

Testing message content in a pre-deployment tool such as Everest's Inbox Preview can help to identify potential spam filter issues before you send. Once you identify content that is being flagged by spam filters, continue testing to isolate what is causing the issues (for example, subject line, URLs/links, text, and/or images).

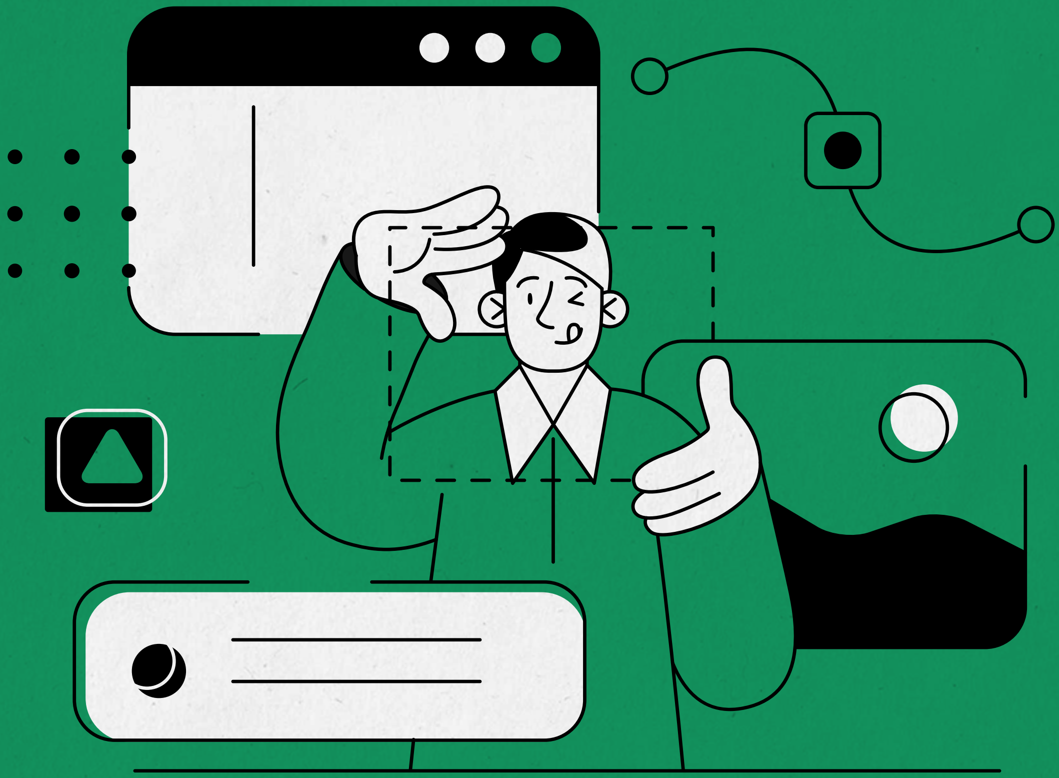
CHAPTER RECAP:

There are many elements that can impact whether your messages reach the inbox or get redirected to the spam folder—or even worse, blocked entirely. Sending from a trustworthy source, having a strong reputation, and clean content will help your messages successfully pass filters and reach your subscribers.

3

HOW DO YOU MEASURE EMAIL SUCCESS?

Now that you have hit send, how can you tell how your emails have performed? There are many metrics that measure how an email program is performing. Having access to all of them is important to not only evaluate how your campaigns are performing, but also identify where any problems may be occurring.



For example, if your latest campaign had a two percent open rate, you might assume your subject line was unsuccessful and focus on creating a more enticing subject line for your next campaign. However, it's possible that only 40 percent of your messages actually reached the inbox—and you'd never know it without checking your inbox placement rate. Unless you look at the problem holistically, you may end up trying to fix the wrong problem, and the real issue will continue to harm your future campaigns.

Having access to the right performance metrics—and understanding how to use them—is crucial to the success of an email program.

Metrics to Measure Overall Program Performance

The first metrics you want to monitor are those that track the performance of your email program as a whole. These are the metrics that measure whether your messages are reaching the inbox.

Bounce rate: Bounce email is the opposite of delivered email. These are the messages that fail to get delivered, regardless of the reason. There are two different types of bounces: hard and soft. Both are further defined below.

Delivery rate: Delivery rate is calculated by dividing the volume of emails delivered by the volume of emails sent. Note: "delivered" doesn't necessarily mean your email hit the inbox—just that it wasn't bounced or rejected.

Hard bounce: Hard bounces are messages that are permanently rejected, typically due to issues with list quality (e.g., invalid email addresses or domains).

Inbox placement rate: Inbox placement rate measures the percentage of sent email that actually lands in the subscribers' inbox—a far more accurate measure than delivery rate.

Rejected rate: Rejected email is a subset of bounced email, and includes only those messages that fail to get delivered due to reputation issues (e.g., complaints, spam traps, blacklisting).

Soft bounce: Soft bounces are messages that are temporarily rejected, typically due to issues with the recipient's mailbox or server (e.g., mailbox too full or server down).

There are many reasons that can trigger a hard bounce, check out the Email Marketer's Guide to Bounce Processing to learn more.

Metrics to Measure Individual Campaign Performance

These metrics look at how specific campaigns are performing. Tracking these metrics and comparing them to previous campaigns can provide insight into subscriber preferences and help you create more effective campaigns in the future.

Click-through rate: Click-through rate is calculated by dividing clicks by the volume of email delivered.

Click-to-open rate: This rate is measured by calculating the ratio of total clicks to total opens. Click to-open provides valuable insight into the effectiveness of your email content and design.

Complaint rate: Complaint rate is calculated by dividing the number of spam complaints by the number of emails delivered. Complaints are a strong indicator of negative engagement and this metric is useful for identifying patterns and sources of complaints

Conversion rate: Conversion rate is calculated by dividing the number of conversions by the number of visits. Although a strong indicator of subscriber engagement, this metric typically speaks more to the quality of landing page or website content than email content.

Open rate: Open rate is calculated by dividing the number of emails opened by the number of emails delivered.

Unsubscribe rate: unsubscribe rate is calculated by dividing the number of unsubscribes by the number of emails delivered. Be cautious of using this metric in isolation, as a declining unsubscribe rate can result from various things such as improving engagement, where subscribers don't want to unsubscribe, or decreasing inbox placement, where subscribers don't see your email to unsubscribe from it—two very different situations.

There are many reasons subscribers complain about a messages, check out the Marketer's Guide to Subscriber Complaints to learn more.

CHAPTER RECAP:

Having access to and analyzing all these metrics are important for monitoring the health and impact of your program. Checking just one or two can give you a false understanding of how your program is performing. To accurately measure the performance of an email program, you need to access these metrics and consistently track all of them for any changes that could indicate a problem.

4

DEBUNKING COMMON EMAIL MYTHS

When it comes to the success of your email program, understanding what's not true is just as important as understanding what is true. There are countless misconceptions among marketers, which can cause serious problems if you're among the misguided believers. Here are just a few of the most common "email myths."

It's my email service provider's (ESP's) job to fix my deliverability.

GENERALLY NOT TRUE: You, the sender, are absolutely in charge of your own email deliverability and reputation.

Your reputation is determined by the quality of your lists, number of spam complaints, message quality, and sending history, all of which are controlled by the sender—you—and not your ESP. Sure, your ESP might be responsible for some delivery issues if their infrastructure isn't set up properly, or maybe they assigned you a shared IP address that has poor delivery. But those scenarios are the exception, not the rule. Unless you address the root cause of your poor reputation, no ESP can get you delivered to the inbox.

If I ever have poor deliverability due to a bad reputation, the simplest way to get back into the inbox is to switch to a new IP address and domain.

FICTION: Don't do it! More than likely, you will find yourself worse off.

Hopping from one IP address to another is a common tactic of spammers. To combat this, mailbox providers will typically block or limit volume from new IP addresses until they can learn what type of sender the mail is coming from—hence our consistent advice to warm up a new IP address. If left unaddressed, your reputation issues will follow you to your new IP address and domain. It's better to address and fix the underlying reasons for your poor reputation than switch to a new IP address or sending domain.

If the content of your message has spammy keywords, you'll have inbox placement problems

FICTION: Content plays a very small role in filtering decisions today compared to sender reputation and subscriber engagement.

This is because content-based spam filters return too many false negatives, aren't reliable, and are easy for spammers to work around. More often than not, a good sender reputation will override any content filter. But that doesn't mean content is never a factor. If you're sending third party content or templates used by others, your content might have a bad reputation by association. Keep in mind, too, that spammy content could very well trigger spam complaints from your subscribers—which will also cause inbox placement problems over time.

I have a low complaint rate, so my mail should be delivered to the inbox.

FICTION: A low complaint rate can be misleading if you aren't paying attention to your inbox placement rate.

Complaint rates are calculated based on total number of complaints and total messages delivered to the inbox. So if your mail is getting delivered to the spam folder, you'll have a low complaint rate because it's not possible to mark a message as spam when it's already in the spam folder.

Your complaint rate can help you measure how subscriber preferences and act as an early warning for potential problems. However, it should be analyzed in conjunction with other metrics to understand how your content is preforming.

Because of engagement-based filtering, deliverability doesn't really matter anymore.

FICTION: You need access and understanding of both deliverability and engagement metrics to get the full picture on how your program is preforming.

Engagement metrics do exactly what their name implies: they look at how your customers are engaging with your mail—not whether they received it. Deliverability metrics look at where your mail gets delivered (inbox, spam, or missing) and serve as the foundation of evaluating the effectiveness of your email program. Looking at both deliverability metrics and engagement metrics is the only way to gain a holistic view of your email program, understand how it's performing, and identify any potential problems.

CHAPTER RECAP:

Having misconceptions about how email works can be very damaging to your program. Following these myths can seriously hurt your program and your email ROI. It's important to make sure you are aware of these and other email myths that can lead you astray.

5

BASIC EMAIL TERMS

If you're new to email marketing, there is a lot of email-specific jargon that you might be unfamiliar with. To help you translate the language of email into plain English, we've compiled this quick glossary of 20 important email terms.

Authentication:

The process of verifying the digital identity of the sender of a communication. In email marketing, the most widely used and accepted forms of email authentication are SPF, DKIM, and DMARC.

Blacklist:

Lists of IP addresses that have been reported and listed as "known" sources of spam. There are public and private blacklists. Public blacklists are published and made available to the public—many times as a free service, sometimes for a fee. There are hundreds of well-known public blacklists.

Block:

A refusal by a mailbox provider or mail server to accept an email message for delivery. Many mailbox providers block email from IP addresses or domains that have been reported to send spam or viruses or have content that violates email policy or spam filters.

Domain:

A particular organization's registered name on the Internet (i.e., validity.com).

Email client:

A program used to read and send email messages. Unlike an email server, which transports mail, an email client is what the user interacts with. Email clients can be software applications like Outlook, Express, and Lotus Notes or webmail services like the ones provided by Yahoo, Hotmail, and Gmail.

Email service provider:

A company that sends emails on behalf of their clients. An email service provider (ESP) may also provide other email-related services like list management, deliverability monitoring, and performance reporting.

Feedback loop:

Feedback loops allow senders to receive alerts when a subscriber complains. The mailbox provider forwards the message complained about back to the sender at a designated email address that has been set up, primarily so that the sender can suppress this user in their database.

Inactives:

Inactives are also referred to as "non-responders." Defined as the email recipients who have not taken any action on your emails (opens, clicks) within in a certain amount of time.

Infrastructure:

Refers to the actual hardware used to deploy your emails or have emails deployed on your behalf by an email service provider (ESP). The hardware is commonly referred to as your mailing transport agent (MTA).

IP address

A unique number assigned to each device connected to the internet. An IP address can be dedicated or shared. A dedicated IP address allows the sender full control of emails sent from their IP address and the resulting reputation. A shared IP address means other senders are mailing campaigns utilizing the same IP address.

List hygiene

List hygiene Is the act of maintaining a list so that hard bounces and unsubscribed names are removed from mailings to protect their reputation and inbox placement.

List-unsubscribe

The list-unsubscribe header is text you can include in the header portion of your messages, allowing recipients to see an unsubscribe button they can click if they would like to automatically stop future messages. List-unsubscribe is currently being used by Gmail, Outlook.com/Hotmail, and Cloudmark.

Postmaster

The person who manages mail servers at an organization. Usually the one to contact at a particular server/site to get help, information, or to log complaints.

Pristine spam traps

Pristine spam traps are email addresses created solely to capture spammers; also called "honeypots." These email addresses were never owned by a real person, do not subscribe to email programs, and of course will not make purchases. Many spam trap operators will post (seed) pristine traps across the internet on various participating websites. They are usually hidden in the background code of webpages and are acquired by a spambot scraping email addresses.

Recycled spam traps

Recycled spam traps are email addresses that were once used by a real person. These email addresses are abandoned email accounts that are recycled by mailbox providers as spam traps. Before turning an abandoned email address into a spam trap, mailbox providers will return unknown user error codes for a year. Once a mailbox provider reactivates (recycles) the abandoned email address, mail is once again allowed to be received by the email address. If you're hitting recycled spam traps this typically indicates a problem with your data hygiene.

Reputation

Sender reputation determines the validity of an incoming sender by analyzing past sending behaviors. Mail box providers evaluate this metric when determining where to deliver incoming mail—the inbox or the spam folder.

Spam:

An email message that you did not ask for and do not want from somebody you do not know, who wants to sell you something. All spam is unsolicited, but not all unsolicited email is spam. Most spam is sent in bulk to a large number of email addresses and advertises some product.

Throttling:

The practice of regulating how many email messages a sender deploys to one mailbox provider or mail server at a time. Some mailbox providers bounce email if they receive too many messages.

Unknown user:

Bounce error code generated by a mailbox provider when an email address is not registered in its system.

Whitelist:

The opposite of a blacklist, A whitelist is a record of senders who meet established standards for reputation, engagement, and sending practices, thus proving themselves to be legitimate and responsible senders.

CHAPTER RECAP:

All this email jargon might seem complicated at first, but knowing these terms will help you understand how email works and allow you to discover new tactics available for you to optimize your program and create for a better experience for your customers. Looking for more email terms? Check out our Deliverability Glossary.

6

GETTING TO THE INBOX CHECKLIST

Reaching the inbox is an ongoing challenge. As we have shown in this guide, there are a lot elements to running a successful email program. With so many factors, its hard to know where exactly to begin in order to optimize your email program. To get you started, we complied a check list of tactics to start with.

□

Send emails from a dedicated IP address

Sharing is caring, except when it comes to your email reputation. On a shared IP address, you really don't have control over your sender reputation—because even one bad sender on your IP address will cause deliverability problems for everyone. When at all possible use a dedicated IP address to protect your deliverability.

□

Know your Sender Score

Your Sender Score is like a credit score that tells email providers and spam filters how trustworthy and wanted your emails are. Your Sender Score can range from 0 to 100 and it changes daily, so checking it before you hit send can prevent any deliverability surprises. Find out your Sender Score now.

□

Identify problematic reputation metrics

Mailbox providers look at a variety of signals—not just content—to determine whether your mail should be sent to the inbox or the spam folder. These include your complaint rate, how many nonexistent addresses you send to, blacklists, spam traps, and hundreds more. To quickly identify which factors you may need to address before you send your next campaign make sure you are evaluating all your performance metrics.

□

Make sure unsubscribe links are working and visible

A working unsubscribe link isn't just a nice to have, it's the law. CAN-SPAM requires that all unsubscribes are valid and functional, that they don't require a login to unsubscribe, and that unsubscribe requests be honored within 10 business days.

□

Authenticate your sending domain

Authentication helps identify ownership of a mailing domain and is the first step in protecting your brand from fraud. After authenticating with SPF and DKIM, creating a DMARC record for your email marketing efforts ensures that your email is properly authenticating, and provides warnings for authentication failures and fraudulent activity.

□

Take care of subscriber complaints

Every time a subscriber marks your emails as spam or junk, you can receive an emailed report that includes a copy of the address that complained. If you send a lot of mail, an automated solution will make this process easier. The Everest Universal Feedback Loop solution eases the sign-up process for many of the publicly available feedback loops.

□

Know your subscribers

If you don't know your audience, you'll struggle to create a great subscriber experience. Email marketers that report above-average open rates, revenue growth, and improvement in email effectiveness also know more about their email subscribers. This includes what email client they're using, when they're opening emails, the type of mobile device or browser they're reading emails on, and the geolocation where they're reading emails.

□

Know the law

As a business, it's important that you adhere to all applicable laws and regulations. Each country and territory has legislation related to email and data practices. It's imperative that you fully comply with these laws and regulations wherever you send email—not just where your business is located.

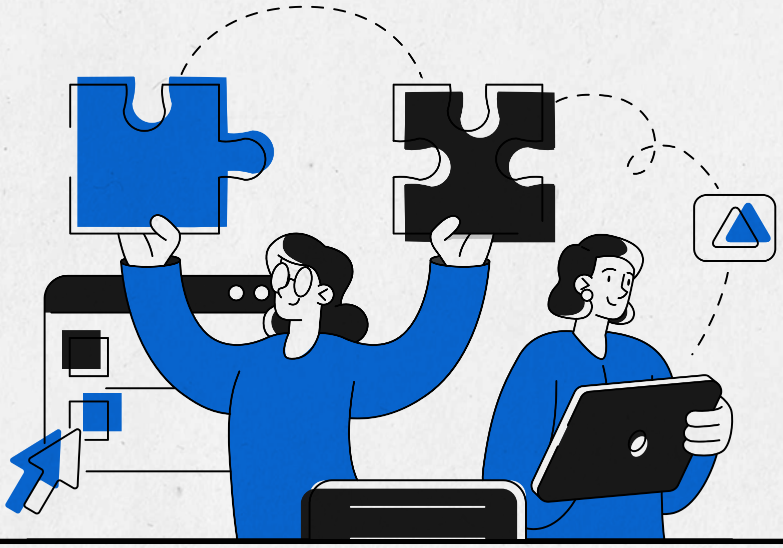
- **United States of America: Controlling the Assault of Non-Solicited Pornography, the Marketing Act of 2003 (CAN-SPAM), and California Consumer Protection Act (CCPA)**
- **Canada: Canada's Anti-Spam Legislation (CASL)**
- **European Union: GDPR (General Data Protection Regulation)**
- **Australia: Spam Act of 2003**
- **Brazil: LDGP**

☐ **Beware the blacklists**

With over 300 publicly available blacklists, good senders ensure they're never on one. Run your content through an automated URL tester and blacklist lookup tool to discover potential issues before you hit send.

☐ **Get whitelisted**

As proven reputable senders, whitelisted senders receive special benefits which may include less stringent filtering, zero throttling, and other perks, resulting in higher inbox placement rates. Some individual mailbox providers—like Yahoo and AOL—operate their own whitelists and only offer these benefits to their own users. Everest by Validity offers universal whitelist—Certification— that provides benefits from multiple mailbox providers.



CHAPTER RECAP:

These ten tips are a great place to start optimizing your program to reach your subscribers inboxes. Before you send your next campaign, make sure you are able to check off all of the items on this list. If not, your emails may be filtered into the spam folder or disappear altogether.

7

CONTINUING YOUR EMAIL EDUCATION

Now that you have the basics down, it's time to become an email expert. To learn more about email, **click the links below** to check out these resources that take a deeper dive into all things email marketing.

- The Ultimate Guide to Deliverability
- The Deliverability Glossary
- Guide to Email Marketing Metrics
- Email Marketing Lookbook
- Marketers Field Guide to Gmail, Outlook.com, and Yahoo

Want some expert advice into your program? Contact us and learn how Everest by Validity can help you improve your email program and ROI.

EVEREST

REACH NEW HEIGHTS OF EMAIL SUCCESS WITH EVEREST

Created by the most respected pioneers of email optimization and deliverability, Everest is the absolute pinnacle of email marketing–the only solution in the world that gives you full control at all critical stages of your email campaigns.

Pre-Send Optimization

Ensuring your campaign is in the best shape possible is crucial to its chances of success with seedlist testing, spam filter checks, collaborative design tools, and more.

In-Flight Monitoring

Get alerted to any blocking, filtering, or placement issues at your most valued mailbox providers in real time. Plus, harness proprietary and exclusive technology to deliver your mail the moment users are active in their inbox.

Post-Send Analysis

Understand your sender reputation, inbox placement rates, your recipient engagement, and other critical signals to help you adjust and improve your email program to increase your ROI.

Learn more at everestemail.com

Businesses run better and grow faster with trustworthy data. Tens of thousands of organizations rely on Validity solutions – including Everest, DemandTools, BriteVerify, Trust Assessments, and GridBuddy Cloud – to target, contact, engage, and retain customers effectively. Marketing, sales, and customer success teams worldwide trust Validity solutions to help them create smarter campaigns, generate leads, drive response, and increase revenue. For more information visit **validity.com** and connect with us on **LinkedIn** and **Twitter**.

validity.com | **US: 1-800-961-8205** | **UK: +44 (0) 118 403 2020**