

HOW TO AVOID

**SPAM
FILTERS**

Introduction

If you send enough email campaigns, you'll inevitably run into spam filter issues. According to [ReturnPath](#), only about 79% of permission-based emails sent by legitimate email marketers reach the inbox. Spam filters and ISPs are working harder than ever to reduce inbox irrelevance, so it's important that you understand what spam is, how spam filters and firewalls work, and some of the steps you can take to avoid being flagged.

What is Spam?

There are a variety of definitions and interpretations of the word itself, but at its core, spam is unsolicited, irrelevant email, sent in bulk to a list of people. For example, let's say you purchased a list of email addresses from a local business organization. On the surface, that list of addresses seems like it could contain some great prospects for your business, and you want to send them an email with a relevant offer they can't refuse. But, since those people didn't give you explicit permission to contact them, sending an email to that list would be considered spam.

Spam laws

As an ESP, we are required to enforce spam laws, not just because it's a legal obligation, and not just because it's the right thing to do. Spam negatively impacts deliverability rates, and we want to make sure your emails reach their recipients. We have some very strict rules that must be adhered to in all countries, but you may find that your country has additional requirements. We'll cover the laws in the United States and Canada in this guide, but please refer to [this article](#) for details on MailChimp's requirements and requirements of the laws in place internationally. If you have any questions regarding the details of the laws or any potential legal ramifications, we encourage you to consult an attorney who is familiar with this topic.

[The CAN-SPAM Act of 2003](#) became law on January 1, 2004. According to the FTC, if you violate the law, you could be fined \$11,000 for each offense—that's \$11,000 for each email address on your list. ISPs around the country have already successfully sued spammers for millions of dollars under this law. If you send commercial email (generally sales or promotional content), you should familiarize yourself with the requirements of CAN-SPAM. A few key points of the law include:

- Never use deceptive headers, From names, reply-to addresses, or subject lines.

- Always provide an unsubscribe link.
- The unsubscribe link must work for at least 30 days after sending.
- You must include your physical mailing address.

[Canada's Anti-Spam Legislation \(CASL\)](#) went into effect on July 1, 2014 and carries penalties of \$1-10M per violation. CASL is very similar to the CAN-SPAM Act, but has some minor differences and covers all electronic messages, not just email. [This article](#) details the basics of CASL.

Spam Filters

Spam filters consider a long list of criteria when judging the spamminess of an email. They'll weigh each factor and add them up to assign a spam score, which helps determine whether a campaign will pass through the filter. If the score exceeds a certain threshold, your email will get flagged as spam and go straight to the junk folder. Each spam filter functions a bit differently, though, and "passing" scores are typically determined by individual server administrators. This means that an email could pass through Spam Filter A without issue, but get flagged by Spam Filter B.

As for that list of spammy criteria, it's constantly growing and adapting, based on—at least in part—what people identify as spam with the *Mark as spam* or *This is junk* button in their inbox. Spam filters even sync up with each other to share what they've learned. There's no magic formula—and spam filters don't publish details regarding their filtering practices—but there are steps you can take to avoid landing in your subscribers' junk folder.

- **Campaign metadata:** Spam filters want to know that you're acquainted with the person receiving the email. We recommend using merge tags to personalize the To: field of your campaign, sending through verified domains, and asking recipients to add you to their address book.
- **Your IP address:** Some spam filters will flag a campaign if anyone with the same IP has sent spam in the past. When you send through MailChimp, your email is delivered through our servers, so if one person sends spam, it could affect deliverability for our other users. That's why we work vigilantly to keep our sending reputation intact, and it's important that all users abide by our Terms of Use.
- **Coding in your campaign:** Spam filters can be triggered by sloppy code, extra tags, or code pulled in from Microsoft Word. We recommend using one of our templates or working with a designer.

- **Content and formatting:** Some spam filters will flag emails based on specific content or images they contain, but there's not an all-encompassing set of best practices to follow or things you absolutely need to avoid. But, we do have a few recommendations.
 - Design your campaign to be clear, balanced, and to promote engagement from your subscribers.
 - Make sure your subscribers have opted-in to receiving your emails.
 - Be consistent. Try not to stray too far from the content and design that your audience already associates with your brand, website, or social media channels.
 - Test, test, test! Use A/B or Multivariate Testing to learn how changes with your content affects delivery and engagement.

Email Firewalls

Firewalls are a lot like spam filters in that they are designed to regulate incoming email based on a set of rules that have been established by the email server. Think of them as gatekeepers. They're used by ISPs, large corporations, and small businesses alike, and they all communicate with one another to help identify spam and stop spammers. But how does this server know what spam is? Your own recipients teach it. When you send an email to your list, and someone on your list thinks it's spam—or doesn't remember opting-in to your list, or if you never had permission in the first place—that recipient can report you to [SenderBase](#), the world's largest email monitoring network. Your ESP should be registered at SenderBase, so they can properly investigate every complaint generated in response to their users' campaigns. MailChimp's staff receives copies of any complaints that come in, so we can disable the sender's account and investigate immediately.

Firewalls rely on reputation scores to block emails before they even get to the content-based spam filters, and they all calculate sending reputation differently. Once you've been reported, you'll remain on the radar of these firewalls; this helps prevent someone from switching between different email servers to send more junk after being reported. These gatekeepers will know to block all emails with your name in it from now on, no matter who sends it or where it comes from.

Omnivore

[Omnivore](#) is MailChimp's abuse-prevention algorithm that keeps our system clean by predicting bad behavior in a campaign before it even gets out the door. Spam filters are equipped to catch obvious and evil spam, but they're not as effective at predicting permission issues. ESPs often have a hard time detecting ignorant spammers too. Omnivore can predict lack of permission within a user's list and send a warning to help them develop better practices before it's too late.

How it works

Each time you import new addresses or send a campaign to new recipients, Omnivore will scan for addresses that have never received campaigns from your MailChimp account. Then, it checks to see how many of those addresses are likely to be spamtraps, or to generate abuse complaints and hard bounces. Omnivore is very accurate in predicting list performance, and uses an algorithm to assign a level of risk to a group of addresses. When that level of risk is determined to be too high, we'll prevent you from sending to them. If your list gets flagged by Omnivore, we recommend looking both into the collection methods and, if applicable, prior methods of management. In many cases, you may just need to reconfirm the affected list before sending can be resumed.

If you're not a spammer, how does Omnivore affect you? Well, because it prevents abuse on such a massive scale, you'll achieve better deliverability by default. Even problem-free senders benefit from a self-cleaning system

Abuse Reports

When people receive email that they think is spam, they can just click a button in their email client to label it as such. In most cases, once that button has been clicked, an abuse report is created and sent to the recipient's email program or ISP. If enough of these reports are received, an automated warning message will be sent to the sender.

When you use MailChimp, an abuse complaint will be generated each time someone marks your campaign as spam, thanks to the Feedback Loop in place for most ISPs. We'll immediately remove that recipient's email address from your active list and into the [abuse complaints area](#) of your account. Once abuse complaints reach our threshold, you will receive a warning from our abuse team. If the complaint rates exceed that threshold, your account will be suspended, and our team will need to conduct an investigation into your list collection process. High levels of spam and abuse from a user can result in the IP addresses being blacklisted by ISPs and anti-spam organizations. And, if you use MailChimp for sending—or any email marketing service, for that matter—that means your emails can affect the deliverability of hundreds of thousands of other legitimate marketers. It's very serious—one bad apple can truly spoil the whole bunch. That's why we've developed Omnivore, we're constantly monitoring incoming complaints, and we have a team of human reviewers that review MailChimp accounts.

Accidental abuse reports

You don't have to be a spammer to get reported for spamming. Even legitimate marketers who only use opt-in lists can have their email reported as spam, even if it's not. Sometimes it's a simple mistake, like when a user clicks the spam button to unsubscribe from an email. Since it's almost inevitable that you'll receive complaints every now and then, ESPs like MailChimp are constantly monitoring abuse reports from ISPs, blacklists, and anti-spam networks, so we can immediately pinpoint problems as they arise and investigate the account in

question.

Every major ISP cares about reducing unwanted email for their customers, so when you receive an abuse report, there's no negotiating; you're guilty until proven innocent. As long as your email list has been collected legitimately and you are able to prove without a doubt that any complaint you received is a simple mistake, you're in the clear. But if we have reason to question your list collection practices, your account will be disabled—or shut down altogether.

Tips and Best Practices

In email marketing, it's important to remember that permission is key. Without permission, you could be reported for abuse whether or not you're a legitimate marketer. The following tips can help you prevent spam complaints as you start sending email to subscribers:

- **Choose your opt-in method wisely.** MailChimp's standard signup forms, by default, use the [double opt-in method](#). Double opt-in is valuable because you'll know (and have proof) that each and every recipient gave you permission to send them emails. But, there are a number of other popular signup methods (API, integrations, etc) that allow for single opt-in, and we certainly are not discounting the validity of those, either. Ultimately, the most important thing is that your recipients give you permission to email them. You'll need to consider your audience and the applicable legal requirements in your area to determine which opt-in method is right for you.
- **Don't use purchased, rented, or scraped lists.** Not only are they against our Terms of Use and notorious for providing bad addresses that lead to high bounce rates and blacklisting, they don't actually help you grow your business. Sending to a list that hasn't given you express permission can impact your ability to market your business, potentially damage your brand, and even result in legal ramifications. Instead, allow your list to [grow organically](#).
- **Don't assume that you have permission.** Even if your intended recipients are already your customers (or your colleagues, or people you met at a trade show, etc), do not send promotional email without getting permission first. Add a signup form to your website. Give customers the option to sign up for your list when they make a purchase from your store. Offer incentives—like discounts, coupons, or free downloads, for example—to encourage your customers or colleagues to become list subscribers.

- **Set expectations when people join your list.** If your subscribers think they're signing up for monthly newsletters and you start sending them weekly promotions, they might not be subscribers for much longer. Tell people what you'll be sending and how often you'll be sending it. If you want to send out different content (monthly newsletters, weekly special offers, etc), consider setting up groups in your list so subscribers can choose what content they want to receive from you.
- **Don't wait too long before contacting your subscribers.** Every mailing list can go stale if it's not used regularly, even if subscribers were originally collected via double opt-in. Lists with a lot of stale addresses can lead to high rates of bounces, spam complaints, and unsubscribes. In addition to keeping an up to date [permission reminder](#) in each campaign, consider setting up a process where new subscribers receive emails from you right away, perhaps through a welcome email sent with MailChimp's Automation features. If you're worried that your list has gone stale, we recommend [removing the list and reconfirming outside of MailChimp](#).
- **Treat your email campaigns as an extension of your website, store, or brand.** Your customers probably already have an idea of what type of content, imagery, and design elements to expect from you, so don't stray too far and risk harming that recognition factor. If you have any questions about what content, designs, or [subject lines](#) your customers will respond to and engage with, don't just leave it to chance—use MailChimp's testing features to find out.
- **Don't hide the unsubscribe/opt-out link in your campaigns.** MailChimp (and the CAN-SPAM Act) requires that an [unsubscribe link](#) be present in every campaign that you send. When the link is prominent, people who no longer wish to receive your emails will be able to quickly and easily remove themselves from your mailing list. When the link is hard to find, the recipient might be more inclined to mark your message as spam, resulting in an abuse complaint within your MailChimp account.

Education and Support

Thanks for taking the time to learn how you can avoid spam filters when sending with MailChimp. If you have any questions that were not addressed in this guide, review our collection of [Knowledge Base articles](#) or feel free to [get in touch](#) with our team.