Hello.

If you send enough email campaigns, you’ll inevitably run into spam filter issues. According to ReturnPath, you can expect 10-20% of your emails to get lost in cyberspace, mostly due to overzealous filters. Legitimate email marketers who send permission-based emails to people who requested them get spam filtered all the time. Unfortunately, there’s no quick fix. The only way to avoid spam filters is to understand what spam is and how the filters work. In this guide, you’ll learn:

- What spam is
- How spam filters work
- Common mistakes to avoid
- How to prevent false abuse reports
- How to understand email firewalls

Even if you’re sending perfectly legal and engaging email newsletters, you need to have an understanding of the spam world. It will help keep you out of trouble and make you a better email marketer. Now, let’s get started.
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.
How Spam Filters Work

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 determine a spam score, which then determines whether a campaign will pass through the filter. They might look for spammy phrases like “CLICK HERE!” or “FREE! BUY NOW!” Then they'll assign points every time they see one of those phrases. Certain criteria get more points than others. Here's a sample of criteria from SpamAssassin:

- Talks about lots of money (.193 points)
- Describes some sort of breakthrough (.232 points)
- Looks like mortgage pitch (.297 points)
- Contains urgent matter (.288 points)
- Money back guarantee (2.051 points)

If your campaign’s total “spam score” exceeds a certain threshold, then your email goes to the junk folder. Passing scores are determined by individual server administrators, so unfortunately, what passes some filters doesn't pass all of them. 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.

Spam filters don't publish their filtering practices, as doing so would give spammers the knowledge needed to bypass filters and harm their users. But even though there's no magic formula, we can still help you avoid common mistakes that result in emails landing in junk folders.

Avoid these common mistakes
MailChimp has been helping email marketers create and send email campaigns since 2001. During that time, we’ve found that there are a few common mistakes frequently made by email marketers that can result in accidental spam filtering:

- Using phrases like “Click here!” or “Once in a lifetime opportunity!”
- Excessive use of exclamation points!!!!!!!!!!
- USING ALL CAPS, WHICH IS LIKE SCREAMING AT THE TOP OF YOUR LUNGS VIA EMAIL (especially in the subject line).
- Using bright red or green colored fonts.
- Using bad content. This one’s broad, but important. Email delivery expert Laura Atkins details content-based filtering in this article.
- Coding sloppy HTML, usually from converting a Microsoft Word file to HTML.
- Creating an HTML email that’s nothing but one big image, with little or no text. Spam filters can’t read images, so they assume you’re a spammer trying to trick them.
- Using the word “test” in the subject line. Agencies can run into this issue when sending drafts to clients for approval.
- Sending a test to multiple recipients within the same company. That company’s email firewall often assumes it’s a spam attack.
- Sending to inactive lists. These are lists which have not engaged in the campaigns through opens and clicks. Because subscriber engagement is a huge part of getting emails into the inbox, when an ISP sees low engagement rates they will often begin to bulk the campaigns to the spam folder. Then they will block the domain and IP addresses used to deliver the campaigns.
- Sending to stale lists. Permission generally goes stale within about 6 months, so if your subscribers haven’t heard from you within that timeframe, you’ll need to reconfirm your list.

Frequently asked questions

How can I tell if my emails were spam filtered?

For starters, look at your open rate. If it suddenly dropped from your average, then you probably have a spam-filter problem. An abnormally high bounce rate is another indicator. Look through your bounces and read the SMTP replies.
Most established ESPs, like MailChimp, have been accepted into feedback loops with providers like Hotmail, Yahoo!, and AOL. When a recipient on their network reports an email as spam, an alert is sent to the sending server. MailChimp receives those alerts and stores them under your account, so you’ll know how many people reported your campaign as spam. MailChimp will also automatically unsubscribe and remove those people from your list.

**Can I check my campaign before I send it?**

You sure can. MailChimp offers a tool called [Inbox Inspector](#) that you can use to thoroughly scan your email campaign and test for appearance and content-related spam triggers. All monthly paid accounts include 25 inspections per week. Pay as you go and free plans can purchase single Inbox Inspections for $3. Learn more about the Inbox Inspector’s spam filter checker [here](#).

Inbox Inspector tells you whether your email will be stopped by spam filter, but if you want to find out why your email was blocked, you’ll need to systematically isolate the different variables in your campaign. Make a copy with a different subject line. Still getting blocked? Change the content. Still blocked? Remove the links. And so on.
Preventing False Abuse Reports

You don’t have to be a spammer to get reported for spamming. Sometimes an email gets reported as spam, even if it’s not. Sometimes it’s a simple mistake, like when an inexperienced user clicks the spam button to unsubscribe from an email.

But mistake or not, getting reported for abuse is serious. If a major ISP like AOL receives even a small handful of complaints about your emails, then they’ll start blocking all email from your server. And if you use MailChimp—or any email-marketing service, for that matter—that means your emails can affect the deliverability of thousands of other legitimate marketers. One bad apple can truly spoil the whole bunch. (By the way, this is why we created Omnivore, which we’ll get to in a minute.)

Since it’s inevitable that you’ll receive spam complaints every now and then, ESPs like MailChimp are constantly monitoring abuse reports from ISPs, blackhole lists, 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, you’re unfortunately guilty until proven innocent. There is no negotiating—they don’t have time to listen to excuses or long-winded explanations. And who can blame them? They’re too busy trying to handle countless other spam complaints.

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. Incidentally, that’s why our list management system uses double opt-in, and why our terms of use prohibit purchased, rented, and third party lists. Those types of lists generate too many complaints, even they were originally collected in a legitimate manner.
How abuse reports work

When people receive what they think is spam, they can just click a button in their email program to label it as such. Once clicked, an abuse report is often 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 to deliver your emails, we are that sender and the warning messages are sent to our abuse team. If the warning message includes the identity of the person who filed the complaint, MailChimp will automatically remove them from your list.

If the complaints continue within a certain timeframe, that’s it— all email from that particular IP address of the sending server is blocked, at least temporarily. Scary. That’s why we’re constantly monitoring incoming complaints and have a team of human reviewers that review MailChimp accounts.

Reasons for false abuse reports

So, why do legitimate email marketers get falsely accused of sending spam? Sometimes it’s a mistake. But more often than not, it’s the marketer’s own fault. Here are some common reasons marketers get accused of sending spam:

- The marketer collected emails legitimately—perhaps through an opt-in form on their site—but took too long to contact their list. As noted earlier, permission goes stale after about 6 months. If they haven’t been contacted quickly enough, the subscriber might not remember opting-in.

- The marketer runs an online store. They’ve got thousands of email addresses of customers who have purchased products from them in the past. Now they want to start emailing them. Instead of asking people to join the email marketing list, they just start “blasting” offers.
The marketer is exhibiting at a trade show. The trade-show organization provided the marketer with a list of attendee email addresses. The marketer assumes they have permission, and starts emailing full-blown newsletters and promos.

Business folks drop their cards—with email addresses—into a fishbowl at a restaurant counter. For a marketer, it's an easy way to grow their list. But the recipients weren't asking for email, just a free lunch.

The marketer purchases or rents members' email addresses from another organization, then adds them to their list without getting permission.

There's a common theme here. Do you see what it is? Yep: permission.

---

**Ways to prevent false abuse reports**

Getting permission is *extremely* important. 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:

- Use the double opt-in method. This is standard with MailChimp. If you use double opt-in, you have proof that each and every recipient gave you permission to send them emails. Period.

- Even if your recipients are already your customers, don’t send promotions without getting permission first. Set up a separate marketing list for customers to join. Tell them you’re about to start up a great email newsletter or promotions program, and give them reasons to sign up.

- Don't use purchased lists. Even if you acquired them legally, they’re against our terms of use, so you'll get in trouble for it. They're a waste of money, and just plain wrong.
Don’t hide the unsubscribe/opt-out link in your campaigns. It should be prominent. People who no longer wish to receive your emails are either going to unsubscribe or mark you as spam. Which would you prefer? Some folks even place the unsubscribe link at the top of their emails, so it’s easier to find.

Make sure your email looks reputable. If you’re not a designer, hire one. Your email needs to look like it came from your company, not some scammer who’s phishing for information. If your email looks unprofessional, who’s going to trust your unsubscribe link?

Set expectations when people opt in to your list. If people sign up for monthly newsletters but you also send them weekly promotions, they’re probably going to report you for spamming. Tell them what you’ll be sending and how often. Set up different lists (one for newsletters, one for special offers and promotions). Understand that there’s a difference between soft-sell newsletters and hard-sell promotions. Don’t mix them up.

Don’t wait too long before contacting your subscribers. We’ve seen lots of small businesses collect emails at their storefront, but then wait more than 3-6 months before contacting their customers by email. Too often, it’s with a coupon offer during the holidays (when recipients are already getting overwhelmed with offers from other online merchants). Set up a process where new subscribers receive emails from you right away, like a “Top Ten” list that you send weekly, using MailChimp’s Automation features.

Double opt-in

We highly recommend the double opt-in method when managing your email lists. In fact, it’s a requirement of MailChimp’s native signup forms. Here’s how it works:

1. A customer signs up for your email newsletter through a form at your website.
2. They receive an email with a confirmation link.
3. If they click the link, they are added to the list.
4. If they do not click the link, they are not added to the list.

Double opt-in is fast replacing the single opt-in method, in which someone submits a form and is automatically added to a list. Single opt-in increases the likelihood for someone to get added to the list without permission, either erroneously or maliciously.
Email Firewalls

By now, most email marketers know that spammy phrases like “FREE! CLICK NOW!” will trigger spam filters to flag their message. But before an email even gets to that filter, it first has to pass through a gatekeeper or “firewall.” (Yep, spam is now such a problem that spam filters now need filters of their own.) Firewalls are used by ISPs, large corporations, and small businesses alike, and they all communicate with each other to help identify spam and spammers.

If IronPort’s Email Security Appliance thinks your email is spam, it’ll gobble it up and shoot its remains into cyberspace before your recipient’s spam filter even has a chance to look for the word "V1AGRA." It won’t even waste the energy to tell anybody about it (which means it won't appear on a bounce report).

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. If you get enough complaints, SenderBase will propagate your data to all the IronPort servers around the world, letting everyone know you’re a spammer.

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.

IronPort is only one of many email firewalls, gateways and security appliances. There’s also:

- Cloudmark
- Barracuda Networks
- Symantec

All of these gatekeepers rely on reputation scores to block emails before they even get to the content-based spam filters. They all calculate sending reputation differently. You can make sure your reputation is good by sending clean emails to clean lists.
If you think you can send junk, get reported, then just switch to a new email server, you’re sadly mistaken. Once you get reported, your company’s name and domain name are on the lists. 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. This is why affiliate-marketing programs can be so risky. Imagine thousands of sloppy email senders (your affiliates) buying lists and sending emails with your company’s domain name in them. Oof.

---

**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. We started working on Omnivore in 2008, and now we have a tool that’s constantly analyzing email-campaign and user-account data behind the scenes.

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 users’ lack of permission and send them a warning to help them develop better practices before it’s too late. If Omnivore detects an especially suspicious activity, we’ll suspend the account while our team investigates.

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.

---

**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, feel free to contact our support or compliance teams directly.