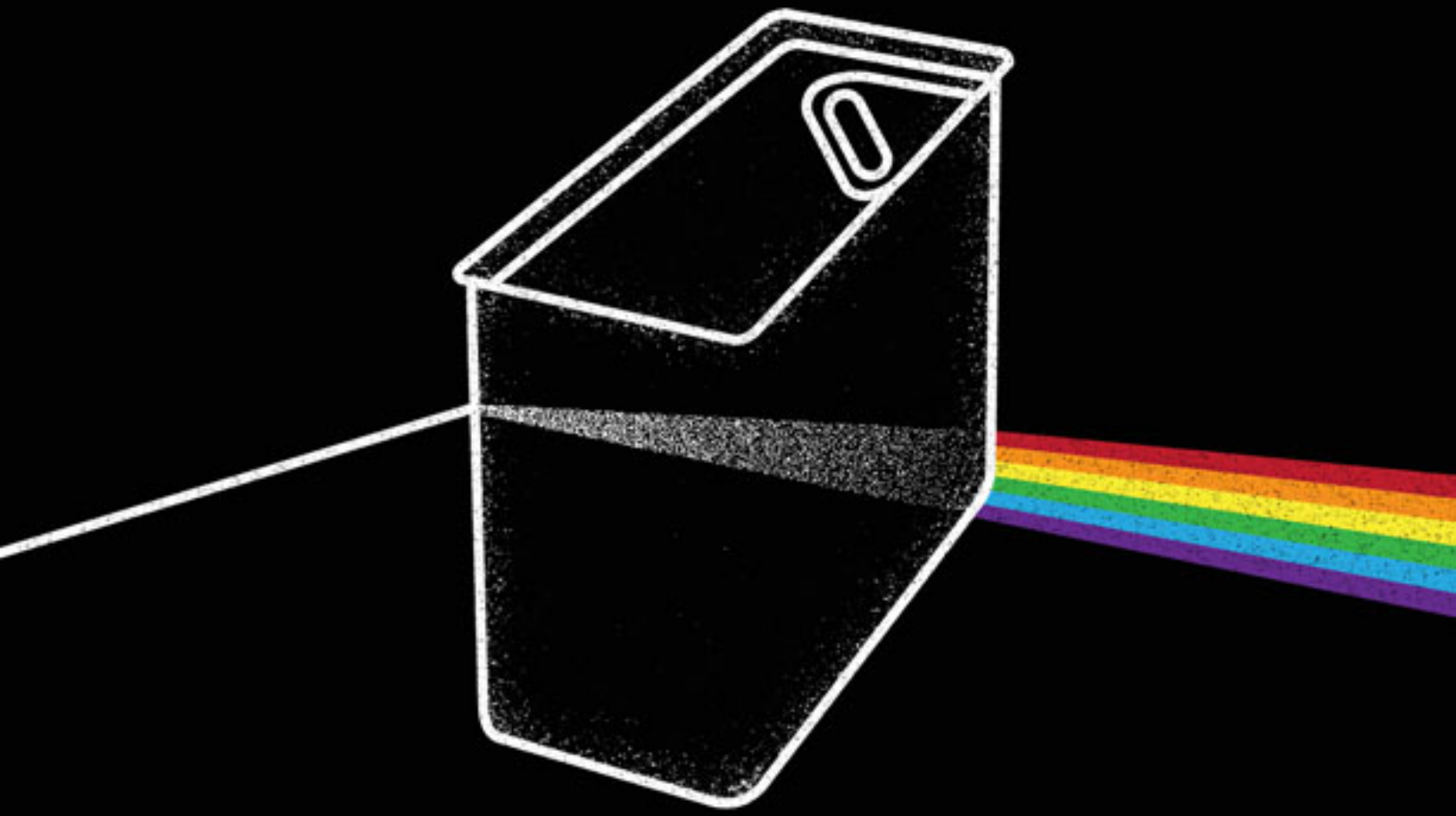


HOW TO AVOID

SPAM FILTERS

PRESENTED BY MAILCHIMP®

MailChimp

avoiding spam filters

HELLO.

If you send email campaigns for long enough, 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 spam filters. Innocent email marketers who send permission-based emails to people who requested them get spam filtered all the time. Unfortunately, there's not a quick fix. The only way to avoid spam filters is to understand what spam is and how the filters work. Here's the rundown.

WHAT IS SPAM?

Spam is unsolicited email sent to a whole list of people. Let's say you just bought a list of email addresses from some local business organization. These are great prospects for your business, right? You want to send them an email with a relevant offer they can't refuse. It's spam if you upload that list into MailChimp (or any other email service provider) and send that list an unsolicited email. It's *not* spam if you take that list and write personal, one-to-one emails to each recipient, and the content is unique for each recipient. If your immediate reaction is, "but what if..." stop now, because you'll probably get yourself reported for spamming.

The CAN-SPAM Act of 2003

The United States federal CAN-SPAM Act became law on January 1, 2004. According to their website, the FTC says that if you violate the law, you could be fined $11,000 for *each* offense (multiply $11,000 times the number of people on your recipient list). ISPs around the country have already successfully sued spammers for millions and millions of dollars under this law.

We're not lawyers, so we can't give you too much legal advice, but if you send commercial email, you should read through the

CAN- SPAM Act of 2003 and understand the rules. If you have a lawyer, consult with her. There are a couple of points we'd like to highlight.

If you're sending **commercial** email (where you're selling or promoting stuff), here are just a few rules you should know about:

- Never use deceptive headers, from-names, reply-tos, or subject lines.
- You must always provide an unsubscribe link.
- Remove recipients from your list within 10 business days.
- The unsubscribe link must work for at least 30 days after sending.
- You must include your physical mailing address.

To learn more, go to ftc.gov.

TIP: WHAT'S THE WORST THAT CAN HAPPEN?

We did eventually get some legal advice. What we learned is in a guide you can read on our blog. Check it out here:

mailchimp.com/blog/spam-lawsuits-whats-the-worst-that-can-happen

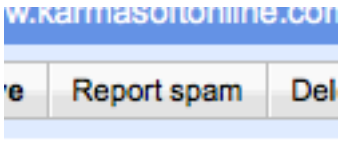
HOW SPAM FILTERS WORK

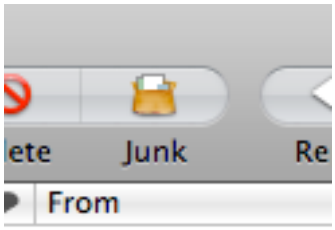
Spam filters look at a long list of criteria to decide whether your email is junk. They might look for spammy phrases like "CLICK HERE!" or "FREE! BUY NOW!" They'll assign points every time they see one of those phrases. Certain criteria get more points than others. Here's a sample of criteria from Spam Assassin:

- 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. You're probably thinking, "What's the threshold I need to stay under?" Sorry, but the number is different for every server. (Related: Compelling Case for ReturnPath Certification.)

As for that list of "spammy" criteria, it's constantly growing and adapting, because spam filters learn more about junk every time someone clicks the **This is spam** button in their email program.





Spam filters even sync-up with each other to share what they've learned. Though there's no magic formula, we can help you avoid common mistakes that send newsletters to junk folders.

Avoid these common mistakes

These are the most common mistakes we see new email marketers make, which result in accidental spam filtering:

- Using spammy phrases, like "Click here!" or "Once in a lifetime opportunity!"
- Going crazy with exclamation points!!!!!!
- USING ALL CAPS, WHICH IS LIKE SCREAMING AT THE TOP OF YOUR LUNGS VIA EMAIL (especially in the subject line)
- Coloring fonts bright red or green
- 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 (since spam filters can't read images, they assume you're a spammer that's trying to trick 'em)
- Using the word "Test" in the subject line (agencies run into this when sending drafts to clients for approval)
- Sending a test to multiple recipients within the same company (that company's email firewall can only assume it's a spam attack)
- Designing HTML email in Word and exporting the code to HTML (That code is sloppy, and spam filters hate it.)

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 hard bounces and read the SMTP replies. Spam filters leave little clues about why they blocked your campaign.

TIP: MAILCHIMP'S DOMAN PERFORMANCE REPORTS

If you want to know if your email campaign had any trouble with particular ISPs, check your Email Doman Performance Report in MailChimp. Read more here:

mailchimp.com/blog/using-email-domain-performance-to-spot-isp-issues

Most established ESPs like MailChimp have been accepted into feedback loops with ISPs like AOL, Netzero, MSN and Hotmail. 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. And MailChimp will automatically remove those people from your list.

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

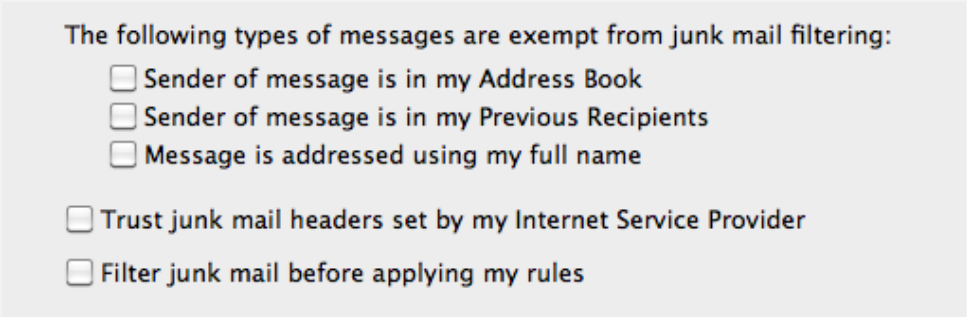
MailChimp comes with a spam-checker tool called the **Inbox Inspector** (mailchimp.com/inboxinspector) that you can use to thoroughly scan your email campaign for spammy keywords, plus all the other stuff that spam filters look for (like image weight and HTML coding errors). Running one test before you send your campaign can save you lots of time and money.

Inbox Inspector tells you whether your email will be stopped by spam filters. 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 got blocked? Change the content. Still blocked? Remove the links. And on and on. MailChimp has a tool called **Delivery Doctor** that automates this testing process. You'll find the Delivery Doctor at the bottom of the Pre-Delivery Checklist screen (the last step before sending out your campaign).

TIP: AVOID JUNK FOLDERS WITH MERGE TAGS

Using your recipients' names will also help you avoid spam filters. Here's a quick case study:

Apple Mail is the free email application that comes with every Apple. We love it for its built-in spotlight search functionality. Check out Apple Mail's Junk Mail filter settings:



The ways Apple Mail tries to tell if you're friend or foe.

1. If you're in the recipient's address book, you're a friend.
2. If the recipient has ever sent you a message before, you're a friend.
3. And here's the interesting part: *If you know the recipient's full name, you must be a friend.*

Collect first and last names in your signup form.

If you set up a list in MailChimp, the corresponding signup form always includes FNAME and LNAME fields by default. Some people claim that asking for too much on your signup forms will make fewer people sign up. Here's what we think: If you've got good content, people will give you their names.

Merge FNAME and LNAME Into Your Campaigns.

Actually *use* that data by merging it into your campaigns. Whenever you create a campaign in MailChimp, the Campaign Setup screen asks if you want to "Personalize the To: field". Check the box, then enter the merge fields that correspond to your FNAME and LNAME columns in your database (just click the orange **MERGETAGS** link for a cheatsheet, and we'll tell you exactly what to type into that field).

PREVENTING FALSE ABUSE REPORTS

You don't have to be a spammer to get reported for spamming. In fact, we've found that totally clean lists that are 100% double opt-in will get one or two abuse reports per 50,000 recipients. Sometimes it's a simple mistake, like when an inexperienced user clicks the **Report Spam** button as an easy way to unsubscribe from an email or file away what they consider junk.

But even if it's a mistake, 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 in our system. One bad apple can truly spoil the whole bunch. By the way, this is why we created Omnivore, which you'll learn about later.

And since it's inevitable that you'll receive spam complaints every now and then, ESPs like us are constantly monitoring abuse reports from ISPs, blackhole lists and anti-spam networks, so we can immediately pinpoint problems as they arise and re-distribute email delivery to different servers and IP addresses while we investigate the account in question.

When you receive an abuse report, you're kind of "guilty until proven innocent." All the major ISPs care about is reducing unwanted email for their customers. There's no negotiating, and 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 the bajillions of other spam complaints coming in.

But as long as you collected your email list legitimately and can prove without a doubt that any complaint you received is a simple mistake, you're in the clear. But if there's *any* question about your list-collection practices, your account will likely be shut down. Incidentally, that's why our list-management system uses double opt-in, and why our terms of use prohibit purchased, rented and opt-out lists. That kind of stuff generates too many complaints, even when they're technically legit.

How Abuse Reports Work

When people receive what they think is spam or junk mail, they can just click a button in their email program to label it as spam. When they do that, an abuse report is often created and sent to their ISP. If their ISP receives enough of these reports, they fire off an automated warning message to the sender. If you're using MailChimp to deliver your emails, we're that "sender." So our Abuse Desk staff receives these warning messages. Usually, the report is very terse. It hides the identity of the person who complained and usually includes a copy of the email you sent, plus something to the effect of:

Hi. Our customers are complaining about your emails. You need to address this issue ASAP, or we'll start blocking all email from your servers.

If the complaints continue within a certain timeframe, that's it—all emails from that particular IP address of the sending server is blocked, at least temporarily. Scary, huh? That's why we're constantly monitoring incoming complaints. It's why we have human reviewers to approve new accounts before they're allowed to send campaigns. It's why we monitor our outgoing mail queue all the time, and why you might hear from one of our reviewers with tips on how you can make your email seem less spammy.

Reasons for False Abuse Reports

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

- The marketer collected emails legitimately (through an opt-in form on their site), but took too long to contact his list. People receive full-blown email newsletters "out of the blue" and they don't remember opting in two years ago. By the way, here are some tips on re-engaging old subscribers: mailchimp.com/blog/how-to-reactivate-inactive-subscribers

- The marketer runs an online store. They've got thousands of email addresses of its 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. Instead of emailing those people an invitation to join their list (along with a little explanation about how they got their emails from the tradeshow), the marketer assumes they have permission, and starts emailing full-blown newsletters and promos.

- Fish bowls and business cards. Yep, we've all dropped our business cards into a fish bowl somewhere to win a free lunch or a door prize of some sort. To marketers, it's common sense that the fish bowl is a list-collection technique. To prospects, it's just a shot at a free lunch.

- Purchasing or renting members' email addresses from an organization, then just adding them to their list without getting permission first.

There's a common theme here. In all of the above cases, the missing element is **permission.** The marketers are caught up in legal rules and definitions. But it's not enough to be legal—you've got to be polite, too.

Ways to Prevent False Abuse Reports

Hopefully by now you understand that permission is extremely important, and that without permission, you're going to be reported for abuse (whether the email is legit or not). So here are some ways to prevent false spam complaints:

- Even if they're your customers, don't send promotions without 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 (or free prizes) for signing up. Don't just send them promotions out of the blue.

- Don't use purchased lists. They're a waste of money, and they're just plain wrong. Even if you acquired them legally, they're against our terms of use.

- Don't hide your opt-out link. Make it very prominent. People who no longer wish to receive your emails are either going to click your **Unsubscribe** link, or their **This is spam** button. Which would you prefer? Some marketers are even placing the unsubscribe link at the top of their emails, so it's super easy 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 would 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.

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

- Don't wait too long before contacting them. We've seen lots of small businesses collect emails at their storefront, but then wait more than 3 months (sometimes years) before contacting their customers. Too often, it's with a coupon offer during the holidays (when recipients are already getting overwhelmed with offers from other online merchants). Setup a process where new subscribers receive emails from you right away, like a "Top 10" tips that you send weekly, using MailChimp's Autoresponder tool.

Double Opt-in

We *highly* recommend the double opt-in method when managing your email lists. In fact, it's the only way MailChimp's built-in list management system will work. Here's a quick overview:

1. A customer signs up for your email newsletter through a form at your website.

2. He receives an email with a confirmation link.

3. If he clicks the link, he's added to your list, and you store the IP address, date, and time of registration. Now you've got proof of opt-in, should you ever need it in the future (like if you receive a false or malicious abuse report).

4. If he doesn't click the link, he's not added to the list.

Double opt-in is fast replacing the single opt-in method, where someone submits a form, and bam—they're added to a list. There are too many chances for someone to get signed up to a list without his permission, either erroneously or maliciously. And there's no need to even discuss the old opt-out method anymore. That's getting phased out, due to all the spam complaints marketers get from people who never saw the opt-out check. Don't be so desperate to grow your list that you put your company's reputation on the line.

EMAIL FIREWALLS

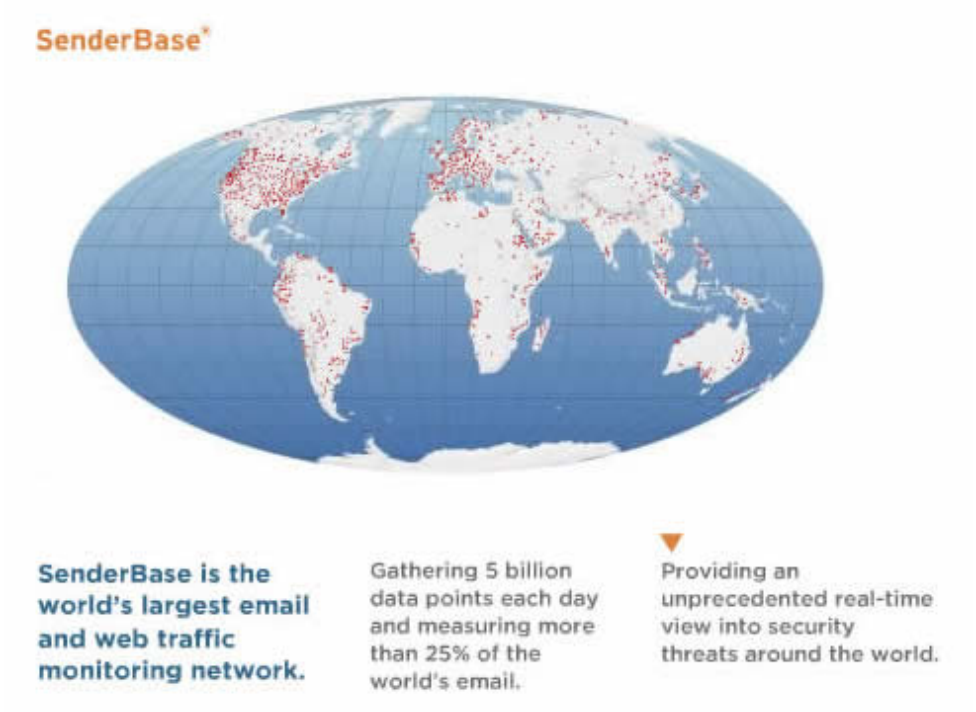
By now, most email marketers know to avoid using spammy phrases like "FREE! CLICK NOW!" or the spam filters will trash your message. But did you know that before your email even *gets* to a spam filter, it has to get through a gatekeeper? Yep, spam is so bad that spam filters now need spam filters to help them. These gatekeepers look kinda like this:

Looks vicious, doesn't it? They're all over the place. ISPs use them. Large corporations use them. Small businesses are starting to use them. What's really scary is they all talk to each other. It's how they learn what spam is, and who should be blocked (Gulp—are they talking about *you* right now?).

That's a picture of IronPort's Email Security Appliance. If it thinks your email is spam, it'll gobble it up and fart its remains into cyberspace before your recipient's puny little spam filter even gets a chance to look for the word V1AGRA. It won't even waste the energy to tell anybody about it (like in a bounce report).

Ever send to your email list and wonder where 5-10% of the emails seem to go off to? Ever wonder why the numbers don't seem to add up in your deliverability reports? It was probably one of these big, mean appliances.

How the heck 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 purchased a list from someone, that person can report you to SenderBase. Get enough complaints, and they'll propagate your data to all the IronPort servers around the world, letting everyone know you're a spammer:



Incidentally, your email service provider should be registered at SenderBase, so they can properly investigate every complaint generated in response to their users' campaigns. At MailChimp, our staff receives copies of any complaints that come in, so we can suspend the sender's account and investigate immediately.

IronPort is only one of many email firewalls, gateways and security appliances you should learn about. Also see:

- Cloudmark
- Barracuda Networks
- Postini
- MessageLabs
- Brightmail

All of those big, mean, ruthless gatekeepers rely on "reputation" scores to block emails before they even get to the content-based spam filters. They all calculate reputation differently. To get a feel for how the do it, check out this article on the MailChimp Blog: http://www.mailchimp.com/blog/cloudmark-fingerprinting-algorithm/

So you better make sure your reputation is good by sending clean emails to clean lists.

If you think you can send junk, get reported, then 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. They'll know to block ALL emails with your name in it from now on—no matter who sends it or where it came 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.

OMNIVORE

Omnivore is MailChimp's fancy 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. Sometimes people just don't know better—if a well meaning business owner sends an unsolicited email "blast" to a list he got from a tradeshow, he's technically spamming. Omnivore can predict his lack of permission and send him a warning—it'll help him learn better practices before it's too late. If Omnivore detects an especially suspicious activity, we'll suspend the account while our team investigates.

So you're not a spammer—how does Omnivore affect you? Since our technology prevents abuse on such a massive scale, you'll achieve better deliverability by default—because even problem-free senders benefit from a self-cleaning system.

MORE INFORMATION

Check out these resources for more info on spam filters, blacklists and firewalls:

- Mailchimp.com/deliverability – Lots of good stuff here.
- Guidelines for proper list management from MAPS, a major anti-spam blacklist service.
- AOL's Feedback Loop – The automated system that lets you know when your emails are generating spam reports.
- Abuse.net – Sort of a "411" for abuse complaints. If you send email that someone thinks is spam, this is where they (of their ISP) look for contact information.
- ESPC (Email Senders and Providers Coalition) – Organization for ESPs, ISPs, and email marketers in general. Best practices and legal issues are discussed here. We're a member. If you send (or receive) lots of email, you should consider joining.
- Returnpath.net – Continually check your reputation with ReturnPath's SenderScore Reputation Monitor.
- URIBL.com – Plug in your domain name into this lookup service to find out if you're on any blacklists. They'll even provide instructions on how to get off the blacklists.

We hope this guide has helped you keep your email newsletters out of spam filters. If you have any questions that weren't addressed here, feel free to contact our support team at mailchimp.com/support. We'll be happy to assist you.