WARNING SIGNS THAT YOUR CLIENT IS SPAMMING

MailChimp

warning signs that your client is spamming

HELLO.

We originally created MailChimp to help creative agencies (web developers, freelancers, advertising agencies and more) send beautiful HTML email campaigns on behalf of their clients.

Now, we manage more than 300,000 MailChimp users with millions of subscribers. So we've helped a lot of agencies help their clients with email.

Unfortunately, this also means we've had to shut down a lot of agencies for their clients' bad email-marketing practices: sloppy list management, poorly designed emails, purchased and old lists. These bad practices get the client—and the agency—reported for spamming, and often blacklisted. In some cases, we've seen people's mistakes tarnish their reputation and follow them, even when they move from server to server or switch email-marketing services.

Luckily, most email-marketing nightmares like this are preventable. You just need to recognize the warning signs and learn how to deal with them.

WHAT EXACTLY IS SPAM?

Seems like a silly question—we all receive spam, and we all know what it is. But do you know the technical definition? Learn it, so that when challenged by a stubborn client, you can easily explain to them why they're spamming.

Email is spam if it's:

1. Unsolicited (the recipient didn't opt in for it) and
2. Sent in bulk (it's part of a larger collection of messages that all have substantively identical content).

Spamhaus Definition of Spam:
http://www.spamhaus.org/definition.html

Some clients will argue, “I send unsolicited emails to prospects all the time from my computer.” You can tell them that’s not spam, because it wasn’t sent it bulk to 500 other prospects.

Some clients will say, “But I get spam all the time—how come I can’t send it too?” Sounds extremely stupid, but most newbie email marketers actually think spammers are doing something that technically makes it legal and okay to send spam. Like there’s some kind of “spam license” you can apply for. Just explain to your clients that most spam is actually sent illegally, via virus infected, hijacked computers called **botnets**, and they’ll get the picture.

SPAM COMPLAINTS AND FEEDBACK LOOPS

Whenever a client sends a bad email campaign, the recipients will click the “Report spam” button in their email programs. Most people think nothing of it—they figure it just teaches their spam filter to throw away the email. But here’s what really happens behind the scenes:

1. A complaint is sent to their ISP (like AOL, Yahoo, Comcast, etc.). The report has a copy of the email in it.
2. The ISP scans the email’s header and tracks down the originating server
3. The ISP sends us a feedback loop (FBL) warning.
4. If an email campaign causes too many spam complaints (about one per thousand recipients), the ISP blocks future emails from the sending server.

Feedback loops (FBL) like the one described above are being used more and more by large ISPs. The reason is simple: ISPs are dealing with billions of pieces of spam a day. They can’t sort through what’s legit and what isn’t—technology can only sort through so much. So they put the ultimate decision in the hands of the recipients. If a recipient says it’s spam (even if they opted in for it), then it’s spam. End of story. Of course people make mistakes, which is why they set thresholds for complaint levels before blocking senders. But the point is that the technical and legal definitions of spam don’t matter so much anymore. All that matters is what recipients think is “unwanted” or not. So your clients better be sending stuff that people specifically requested.

This is why email-marketing services like MailChimp are set up to receive FBL alerts from ISPs. Then we automatically clean complainers from your list. Too many complaints from one campaign, and we can get blocked. And since you’re sharing our system with tens of

thousands of other users from around the globe, we have to be rigorous about monitoring FBL complaints.

You know how they say you're more likely to die in a car accident than a plane crash? Same concept with abuse complaints. You may think your client is safe and sound as long as they're not sending nasty pharmaceutical or online gambling spam. But it's far more likely you'll get blocked by ISPs because of complaints from your own subscribers about seemingly innocent newsletters. So it's important to know why people complain and how to prevent it.

CAUSES OF ABUSE COMPLAINTS

Here are the most common reasons we end up having to shut down and agency's client for too many spam complaints:

Old lists (surprise factor)

If your client has been collecting email addresses on their website for years and this is their first email campaign to the list, some people won't remember the client ("Who the heck are you, and how'd you get my email address?!?") These people *will* report you for spamming. You want to avoid the surprise factor as much as humanly possible with email marketing.

Spam traps

Some ISPs take old email addresses that they assume aren't being used anymore, and they post them to public websites. Then they wait for spam-bots to scrape them, and spam them. As soon as they get spam to one of these spam trap addresses, they block the spammer. This is why you never send to a list more than a year or two old. It's also why you should never buy an email list, and why you should never scrape emails off of websites. The spam-trap effect is devastating and fast.

Tradeshow lists

When people attend a tradeshow, they usually buy their tickets online and submit their email address. The host them gives their email address to the companies that are exhibiting at the show. Companies can theoretically use this list to find prospects who plan to attend the show, and reach out to them. That's fine, as long as the communication is one-to-one. But if they send an email campaign to the entire list, it's spam, and they'll get reported for it.

Outlook address book dumps

This one's extremely common with small businesses that don't have big fancy customer databases. They just manage everything in their Microsoft Outlook address book. The problem is that their address book won't let them export a list of "only my customers" or "only people who opted in for email marketing." It exports everybody, including "grandma, that dude I met at a tradeshow five years ago, my ISP tech support that I emailed two years ago, and my ex-wife." These people *will* report you for spam. It's not limited to small businesses, either. You may tell your client that you're prepping the big campaign and need their customer email list. Your client will then ask the company sales team to hand over their customer lists ASAP. Guess what the sales team is going to do—dump their entire address book and send it along. They probably won't take the time to sort opt ins vs. non-opt ins.

Salesforce dumps

This is similar to the address book dump but at least you have some sort of classification (theoretically) of emails lists. Be on the lookout for clients who dump all their different lists into one big one. Ask them if they combined their prospects, leads, qualified leads, customer and subscriber lists—and then tell them how dangerous that is.

Purchased lists

It's a no-brainer that purchasing 30 million emails from some seedy offshore company is a bad idea. The thing is, most clients buy lists from local networking organizations, or tradeshows, or publications they advertise in. They sound innocent and totally legit. And sometimes, the intent of the list seller is to let you send one-to-one communications (not spam). But in reality, most people buy those lists to send unsolicited, bulk email. So ask your client if the list was purchased. If they say yes, then whoever sold them the list needs to send the bulk emails. Or, the client needs to send totally different emails, one at a time. Unacceptable responses to this question include "But this list is all legit" and "But this list is all opt-in" and "But this list was expensive" and "But this list came from a reputable industry source that everyone knows."

Organization lists

Your client may be a member of a realtor organization or a local business group. Organizations will often give you their membership directory when you join. This is for one-to-one networking, not mass subscribing them to email marketing. The most vicious spam complaints often come from these lists, because your client's competitors just might be members of the same organizations.

Chambers of Commerce lists

When you see a small or new company that has an inexplicably large email list, it's probably from their local chamber. Again, these lists are for one-to-one networking with other business owners—not mass email marketing.

Lists from previous ESPs

If you're helping a client switch from another ESP to MailChimp, make sure they're exporting the latest *clean* version of their subscriber list. Some clients will mistakenly export their entire list (even those who previously unsubscribed, or bounced). In those cases, you'll need to download the full list, plus the unsub list and the bounce list, then manually clean them before importing into MailChimp.

PROBLEM INDUSTRIES

Now that we all know what spam is, what happens when it gets reported, and how people report it, let's look for the warning signs that your client is spamming.

Over the years, we've identified a few industries that tend to generate more spam complaints and deliverability issues than others. We've got nothing against the people in these industries, but if you're working with one of these types of clients, be on the lookout for warning signs:

Real estate

We see lots of real-estate agents and development companies try to use lists that they get from their local Chamber of Commerce, or from local real-estate organizations. These lists are indeed often meant for networking (one-to-one) but not for contacting in mass. Another common reason realtors get into trouble is through their website contact forms. For example, sometimes they'll have a "Contact me" form, where a prospective homebuyer wants to ask a question about a home listing on the agent's website. After submitting one question to the form, the person gets subscribed to an email-marketing list. The agent assumes they have permission to send regular emails from one little question. Since people are only in the market to buy a home for a limited time, you can understand why they get mad when they keep receiving emails from an agent months after they bought their home.

Photography

We love photographers, but they have a resource called Adbase that they use to contact creative directors around the world and send them their work. This system used to wreak all kinds of havoc on MailChimp.

Those creative directors signed up to Adbase—not those photographers' email lists. Lately we've seen fewer problems, and we think it's because Adbase introduced their own emailer service. Lesson learned: If you're going to buy or rent an email list, whomever you sold you the list should do the emailing.

Video games

Most video-game producers make the same two mistakes: They assume players who opt in for news about one game will be interested in news about a new game (but they don't even mention that old game they originally signed up for). The second mistake is that they often rebrand their companies, then send a newsletter to their list with the new branding, without ever mentioning the old company that the recipient would actually recognize.

Universities and academic groups

Remember when you took the SAT or ACT test in high school? There's a checkbox that says "Do you want to hear from colleges that might have scholarships for you?" Of course you checked the "Yes" box, and of course you gave them your contact info. Universities and academic organizations often buy those lists of students and use them for years. If you're working with a university, ask if they're sending emails to registered students, teachers, etc., or if they've purchased a list. If you're working with an alumni association, find out how old the list is.

Politics

The thing about politicians is that they like to trade lists with each other. Big politician A will endorse little politician B and give B his entire list. B sends a "vote for me, because A likes me too!" email, and the people on the A list ending up hating both of them.

HOW TO SPOT A DIRTY LIST

Here are some red flags to watch for when your client gives you their email list:

They just handed over their list.

If they weren't protective of their list, or if they didn't at least ask you some questions about privacy, assume they're also nonchalant about email etiquette.

Unreasonably large list

If you're dealing with a brand new, or tiny one-man business, but they give you a list of 50,000 subscribers, something obviously ain't right. It's a sure sign they bought their list.

webmaster@

Eyeball their list. If you see lots of "webmaster@" and "info@" and "sales@" then it's a sign they hired an intern to scrape email addresses off of websites.

ALL CAPS

If the entries on their list are in ALL CAPS, that's a sign that something's off. We've seen ALL CAPS come from data entry and OCR systems, and really old legacy databases. You've got to wonder how old this list is, because seriously—nobody stores data in ALL CAPS anymore.

Overuse of the word "blast"

If the client uses the word "blast" all the time when referring to their email marketing (as in "fax blast" and "blast to smithereens"), it's a sign they're just not very experienced with email marketing. Email marketing is not just a one-way "push" medium like direct mail or TV. Email subscribers talk back. They also complain back. A lot.

Talk about "cleaning" their email list

In the direct-marketing world (snail mail, stamps, etc.) it's perfectly normal to take a giant old list of customer addresses and hire a company to clean it of bad addresses before spending a lot of money on postage. But if your client talks about his first email campaign in terms of cleaning, you have a problem. First of all, it tells you he's thinking of email as a cheap form of direct mail. Kind of like the people who use the word "blast" a lot. Second of all, it tells you he's got an old list. Perhaps he's been sending from their in-house email server, and they haven't been cleaning lists and managing unsubscribes all these years. Or it could mean they've already been using another email service, which has been dutifully cleaning bouncebacks and unsubs from their list, but now they see this switch to a new ESP as an opportunity to hit the reset button. So they give you the entire list of subscribers (including those who had unsubscribed). When we catch people "cleaning" their lists via MailChimp, we shut them down with extreme prejudice. We're not cleaners, and that jeopardizes the deliverability of our servers for hundreds of thousands of customers who depend on us.

CHECK YOUR CLIENT'S REPUTATION

If your client has been sending email marketing for a while, then they probably have email-marketing reports for past campaigns that you can look at. Ask them if you can look through some of their old reports (similar to when you redesign their website and need to see their traffic logs). If you can get hold of their email campaign stats, look for:

1. Consistent and unusually high bounce rates (particularly hard bounces and undeliverable emails
2. Unusually high unsubscribe rate
3. Unusually low open and click rates
4. Excessive feedback loop complaints (if your client's ESP tracked them)

A good place to benchmark your client's email marketing stats is: http://www.mailchimp.com/articles/email_marketing_benchmarks_for_small_business/

Domain Reputation (They can run, but they can't hide.)

Spam filters don't just track spammy keywords like "viagra" inside of emails. They track company **domain names**, too. And if spam filters start noticing lots of people reporting lots of unwanted emails that all contain the same domain name, they classify that domain as a "spamvertizer" (a company who seems to advertise with spam). So if your client gets reported for spamming, it doesn't matter if they switch their email servers around, or move to another email-marketing service (like MailChimp). Their domain names will always be blacklisted.

Some tools to check your client's domain reputation:

trustedsource.org
senderbase.org *(SenderBase also controls SpamCop.)*

MAYBE IT'S YOU

We've seen quite a few cases where the client had perfectly fine list-management practices, but the agency goofed and got them blacklisted. Here are some common mistakes agencies make with their client's email marketing:

Rushing the job

An email-marketing campaign is not just about designing an email, slicing it into HTML and hitting send. You've got lists to prep, then import. You've got signup forms, unsubscribe forms, thank you pages, confirmation emails, tracking options and email accounts to set up. Plan well ahead of time, and don't think of an email-marketing campaign as an afterthought ("Your new website is live! Oh, wait—we should probably email your customers something really quick!").

Image-only email campaigns

Usually a result of rushing the job. If you send an HTML email that's nothing but one big giant image, most spam filters will think it's "image spam" and block you. If you're lucky enough to get past spam filters, then your recipients will see a broken image (since images are turned OFF by default in most email programs). When a recipient can't see any message, guess what button they click.

Too fancy-schmancy

Email programs are not like browsers. There are dozens of them out there. They all render HTML email differently. So you've got to keep things extremely simple when you design and code HTML email. Old fashioned tables, inline CSS, and absolutely positively no JavaScript, video, or Flash (they set off anti-virus programs).

CONFRONTING CLIENTS

Now you know how to tell if your client is spamming. So what happens when you find out they want to spam? How do you confront them without losing the project? Every client is different, so we'll leave that up to you. But here are some tactics we've used over the years when talking with MailChimp customers:

Mention the FTC's CAN-SPAM laws. Explain how the FTC fined big companies like Kodak, and they'll usually back down from risky behavior. Some people respond quickly to the threat of a lawsuit. Check it out:
mailchimp.com/blog/kodakofoto-settles-ftc-can-spam-charges/

Don't blame the client. If you know they purchased a list, blame the people who sold them the list: "Those guys should have known better than to sell you an email list that breaks the law…" Then find out if the list seller also has a delivery service (an email coming from them to their list will generate fewer complaints than from your client.

Explain the concept of feedback loops. Remind your client that they can be blacklisted just for getting a few spam complaints from their

own customers. And that that can tarnish their reputation and haunt them even if they change email servers (like having a bad credit history follow you).

Remind them that you don't make these rules. The big ISPs like AOL, Yahoo, Hotmail and Gmail all have terms of service that ban unsolicited mass email.

Most agencies have a hard time challenging a client about their bad email-marketing practices—nobody wants to accuse a paying customer of doing something evil. But getting hit with deliverability problems or blacklisting can be extremely frustrating and embarrassing for you *and* your client. Blacklisting can sometimes take months to get resolved and clear your name. If the thought of begging ISPs and anti-spam organizations for forgiveness doesn't make you cringe, consider this: A few minutes of prevention is worth weeks of non-billable hours.

RESOURCES

Check out the following websites to learn more about spam and email marketing:

spamresource.com/
blog.wordtothewise.com/
boxofmeat.net/
mailchimp.com/omnivore