THE NEW EMAIL REVOLUTION

SAVE TIME, MAKE MONEY, AND WRITE EMAILS PEOPLE ACTUALLY *WANT* TO READ!

ROBERT W. BLY

Skyhorse Publishing

Contents

CHAPTER 2.

CAN SPAM Laws, SPAM Filters, Junk Folders, ISPs, and Other Barriers to Email Deliverability

Forty percent of all emails in the United States are spam.[12] Globally, estimates are as high as 86 percent.[13] Despite the CAN-SPAM Act passed by Congress in 2003—as well as state-of-the-art spam filters—spam remains an everyday reality for anyone with an email account. You've probably received spam this very day, offering you a "free membership" perhaps—or worse, someone from Nigeria asking you to send money so he can help you claim a fortune waiting for you.

12 "Global Spam Map," Trend Micro (as of December 15, 2016), http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map. In Canada, the numbers are even higher, at 65 percent.

13 cf. "E-Mail Spam Goes Artisanal," Bloomberg, https://www.bloomberg.com/news/articles/2016-01-19/e-mail-spam-goes-artisanal.

But spam is of special concern for business owners, marketers, and anyone who *sends* emails. Email authors may be unaware of when they can and cannot send emails to people whom they do not know—and what they are allowed and not allowed to say in them.

Laws, spam filters, junk folders, ISPs, and other barriers to email communication can undermine your email campaigns if you aren't careful. Email communications can cause big problems for you if they break the law or aren't getting delivered

When you follow the simple guidelines in this chapter, you'll know just what you're allowed to email and what not—and how to get it delivered.

Defining Spam

Spam is defined differently. Some define spam as unsolicited bulk email, in which an identical or almost identical message is sent to multiple recipients.

For instance, Spamhaus identifies spam as follows:

> An electronic message is "spam" if (A) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (B) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent.[14]

Others define spam as unsolicited *commercial* emails.

As email authors, however, we should primarily be concerned not with the definition of spam, which is somewhat subjective, but simply with what is regulated by law. And the law regulates commercial

14 "The Definition of Spam," Spamhaus, https://www.spamhaus.org/consumer/definition/.

messages in general, whether solicited or unsolicited, spam or no. The Federal Trade Commission (FTC) defines a commercial message as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[15]

The CAN-SPAM Act passed by Congress in 2003 covers commercial messages of any kind, whether solicited or unsolicited. So commercial emails, not spam per se, should be the central focus for us.

The Difference Between Commercial Emails and "Relationship or Transactional" Emails

The basic distinction is the message's purpose. If it's an advertisement or promotion for a commercial product or service, it's commercial. If the purpose is to "facilitate, complete, or confirm" a previously agreed-upon commercial transaction, it's transactional or relationship. Included in the latter definition are warranty information, product updates or upgrades that regard the previously agreed-upon commercial transaction, and benefits and other communications information to your own employees.

It is primarily *commercial* messages that are regulated by the CAN-SPAM Act. While there are some less rigorous requirements for transactional/relationship emails, nonetheless, it is commercial emails that are of greatest concern.

The CAN-SPAM Act

In 2003, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act[16] to regulate commercial

15 "CAN-SPAM Act: A Compliance Guide for Business," FTC, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

16 15 U.S.C. sec. 7701–13.

messages. This was a result of the onslaught of unsolicited emails of a commercial nature—and particularly those that were sexually oriented.

The CAN-SPAM Act does not prohibit commercial emails, it merely regulates them. The Act applies to any commercial message sent electronically. Again, a commercial message is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." That means business-to-consumer (B2C) *as well as business-to-business* (B2B). B2B emails are *not* exempt from the CAN-SPAM Act.

Nor are *solicited* commercial emails exempt from this Act. If someone has "opted in" to your email list through a signup box on your website or has otherwise asked to receive your emails, your email messages are still regulated by the CAN-SPAM Act and you must follow its restrictions. These solicited emails are sent to those who have given "affirmative consent" (opted in) to receive your commercial messages. As you'll see, the restrictions in this case are slightly less rigorous, though these solicited emails must still adhere to the majority of restrictions for commercial email.

Compliance Basics: A 10-Point Checklist

Many of these points are basic and already second nature to opt-in email marketers: no fraudulent transmission data, no harvesting email addresses. Others are more complex, such as rules regarding inclusion of a physical postal address. These are good starting points in ensuring your email program is in compliance with the law:

- Don't use fraudulent transmission data, such as open relays, which are Simple Mail Transfer Protocol (SMTP) email servers that enable users to send emails that hide the source of their emails. Also avoid using false headers, which deceive recipients as to the source of the email.

- Don't use misleading sender or subject lines.
- Add your postal address to all email. The signature or "sig file" is ideal for this. Your email provider almost certainly allows you to create and then automatically add to all your outgoing emails a sig file with your name, address, and any other information you wish.
- If your email list isn't opt-in or double opt-in ("prior affirmative consent"), include a clear notice that states the email is an advertisement or solicitation in commercial messages. Please note that if your list is opt-in or double opt-in, you're exempt from this provision. Double opt-in is a process of gaining permission to send an email to someone during which the recipient confirms that the email address is theirs—typically by clicking on an email link they receive from the sender. Double opt-in isn't required, but it's ideal because it prevents people from placing someone other than themselves on a list.
- Include a "clear and conspicuous" unsubscribe mechanism in every email. And the unsubscribe mechanism must be simple: a link click or simple reply email.
- Have a process for handling unsubscribes within the ten-day limit mandated by the CAN-SPAM Act. Ensure unsubscribe handling is in place electronically, as well as for unsubscribes received via postal mail (and any other contact information you include in the email, such as phone and fax).
- Offer recipients a way to receive some types of email from you while blocking others, along with a "global unsubscribe" option to stop all future email from your organization. All quality email marketing services offer these options as a feature of the service.
- Don't share the address of anyone who has subscribed to the list or who has unsubscribed.
- Don't harvest email addresses or use automated means to randomly generate addresses.

- Remove any sexually oriented material from your messages. The law requires such material be readily identified in the subject line as "SEXUALLY-EXPLICIT" in all caps. When "initially viewed," the message body should include only instructions on how to access the sexually oriented material, as well as your postal address, a notice the message is an advertisement or a solicitation, and a working unsubscribe mechanism. You can ignore this if the message is sent to someone who opted in.

Another note, not so much on compliance as protection. Under this law, if you want to protect email addresses on your website from being harvested, add a privacy policy notice saying you don't "give, sell, or otherwise transfer" these addresses to "any other party for the purpose of initiating, or enabling others to initiate," email messages.

To download the complete text of the CAN-SPAM Act of 2003, visit: https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf.

Special Restrictions for Emails Sent to Wireless Devices

Some email addresses cannot legally be sent unsolicited commercial emails at all according to the CAN-SPAM Act. These include email addresses given by wireless carriers to customers specifically for the purpose of mobile messaging. Because these messages in many cases would cost the recipient money, you must first have the recipients' affirmative consent to send them commercial messages. That means they must opt in to your list or otherwise give permission to be emailed.

Also, you must gain this affirmative consent in a way that doesn't cost them anything, as well as inform them that they:

- Are consenting to receive commercial emails on their mobile device.
- May receive charges for these messages (depending on their carrier and plan).
- Can opt out at any time.

A list of the domains to which unsolicited emails are prohibited can be found at https://www.fcc.gov/consumer-governmental-affairs/domain-name-downloads (this list is continually updated).

These are a small minority of email addresses, however. You are *not* prohibited from sending unsolicited emails to most email addresses as long as they do not have a domain extension (e.g., joeblow@abc.com is from the domain abc) on the domain name list found when you click on the link in the paragraph above.

Best Email Practices

While not a requirement by law, getting permission (affirmative consent) to email your recipients commercial emails is an industry best practice. That means getting the opt-in to your list before sending commercial messages at all.

However, that is not always feasible. Email prospecting can be a cost-effective way to get your message out. Just make sure you follow the law. In some cases, getting affirmative consent is impossible, such as when inquiring about a job or when you have no inbound lead strategy in place.

Another industry best practice is to make sure you're monitoring the effectiveness of your opt-out mechanism on a regular basis. Test it regularly to make sure it's working. Sending emails to those who have already opted out (particularly after the ten-day window) is a recipe for disaster in your email campaigns.

Penalties for Noncompliance

The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) have laws and rules that regulate the CAN-SPAM Act and interpret and enforce it. These entities also have the right to bring suit against offenders. Other agencies, ISPs, and states have the right to bring suit as well. Civil penalties can consist of up to $16,000 for each noncompliant email. So, if you are mass distributing a spam email, *the fines can be in the hundreds of thousands of dollars.*

Aggravated violations are especially subject to damages. These include:[17]

- Address harvesting—automatically capturing email addresses posted to websites.
- Spoofing—sending emails through another computer accessed without permission.
- Dictionary attacks—trying many different combinations of possible email addresses to "hit" a valid one.
- Automating the creation of many email accounts to send commercial email.

Violations regarding sexually oriented material are particularly serious and can lead to a prison sentence of up to five years.

Always follow the law in your commercial emails. If you have any specific questions about the law in your own situation, refer to the full text of the CAN-SPAM Act or consult a good attorney.

17 "E-mail Marketing: CAN-SPAM Act Compliance," David J. Ervin and Christopher M. Loeffler, Kelley Drye and Warren LLP, http://us.practicallaw.com/0-503-5278.

Deliverability Basics

In my business as a copywriter, I know that the greatest copy in the world means nothing if that copy doesn't reach my intended audience. Often it's not the message that's the issue—it's getting the message delivered to your target audience. There may be an amazing offer, stellar copy, and a targeted list. But if it doesn't get *delivered,* it's worth nothing.

I'll use an analogy to direct mail. Earlier in the chapter we discussed the CAN-SPAM Act. When sending direct mail, we have strict limits on the envelope size, weight, what is contained in the envelope or package, and so on. We also have limits on the types of items we can send through the mail. Just as the law prohibits us from sending particular items through the mail—poisons, certain types of goods, etc.—so too does the law prohibit us from sending certain types of emails. Similarly, while gatekeepers (such as secretaries) may keep certain mail messages away from the decision maker's desk, in the email world, spam filters, junk folders, and ISPs can also prevent our messages from reaching the intended inbox.

The rest of this chapter will show you how to better your odds of getting your email message delivered.

Issues in Email Deliverability

If we examine the process of sending an email, whether a personal message to a friend or a relative, or an email marketing campaign to hundreds or thousands of recipients, it would look like this:

You, of course, are the author, while the sender is your email program: Outlook, Gmail, Hotmail, or other email service linked to your

ISP (Internet Service Provider). The Internet is that network of connections through which your message travels to get to the receiver ISP, which then delivers the message (hopefully intact and as you anticipate it to look and read) to your recipient.

Globally, average deliverability is only 79 percent. One out of every five emails are not being delivered to the inbox. In the United States, deliverability is only 73 percent. More than a quarter of sent emails aren't even being delivered. Canadian marketers fare better, with 89 percent average inbox placement.[18]

For their 2016 report, GetResponse and Smart Insights surveyed a group of 1,831 customers, mostly senior managers responsible for digital marketing, asking, "How do you monitor and improve deliverability?" On average, across all types of industries, 28 percent of marketers are not managing or testing deliverability. By far the highest incidence of lacking testing of deliverability is the vacations, hotels, and leisure marketers, with 42 percent not testing deliverability before sending the email marketing messages. On the other hand, only 16 percent of travel and transportation marketers fail to test deliverability before sending.[19]

As you can see, deliverability is a big problem for many marketers. With 21 percent of all emails not even getting delivered to the inbox—and 28 percent of marketers not managing or testing deliverability—your care in these matters will put you ahead of much of your competition if you own a business or operate marketing campaigns. Even for personal messages, you can increase your chances of having your email delivered.

---

18 "2016 Deliverability Benchmark Report: Analysis of Worldwide Inbox Placement Rates," Return Path, https://returnpath.com/wp-content/uploads/2016/07/2016-Deliverability-Benchmark.pdf.

19 "The State of Email Marketing By Industry," GetResponse, http://www.Getresponse.com/resources/reports/state-of-email-marketing-by-industry-2016.html.

Factors That Affect Whether Your Email Gets Delivered

So where are these undelivered emails going? In many cases, they are intercepted by spam filters and landing in the junk folder. Junk, or spam, folders are ways email servers segment incoming emails. Emails deemed to be "junk" based on complex algorithms will be diverted into the junk folder, and you may never actually see them. You may very well have hundreds of emails sitting in your junk folder right now. Some of them may be emails that weren't junk at all but got diverted to that folder anyway because of server policies.

Sender Reputation

The single biggest issue that affects whether your email gets delivered or is sent to the junk folder is your sender reputation. Sender reputation is a computation made by ISPs and email providers about the trustworthiness of your IP address. With all the spam and phishing emails being sent every day, your sender reputation is a measure of how trusted you can be not to engage in such practices.

The fact is that 83 percent of the time that emails aren't delivered, it is because of poor sender reputation.[20] Sender reputation is typically affected by spam filtering intercepting your emails, as well as spam complaints made by recipients. In every email program, there is the opportunity to label a message as spam. Get enough spam complaints or forwards of your messages to the FCC, and your sender reputation will suffer drastically—another reason why it's important to avoid spamming recipients. You may even be blacklisted.

A blacklist is an access control mechanism that means, "Allow everybody, except email addresses on the blacklist." An email spam filter may keep a blacklist of addresses, any mail from which would be prevented

20 "Reputation Monitor," Return Path, https://returnpath.com/solutions/email-deliverability-optimization/reputation-monitor/.

from reaching its intended destination. There are also a number of online blacklist websites intended to weed out spammers.

You can check out your own sender reputation for free at a number of different websites, such as senderscore.org.

Subscriber Engagement

In addition to sender reputation, subscriber engagement is a major factor in getting your email delivered. Your subscriber engagement is a measure of how involved, or "engaged," your audience is with your emails. Are they being opened? Are the links being clicked?

In other words, your subscriber engagement will be poor to the extent that your emails are being ignored and left unopened, or links aren't being clicked. Your subscriber engagement will be strong to the extent that your emails are being opened and links clicked. When your subscriber engagement is poor, your emails are more likely to be intercepted by a junk filter or land in the spam folder.

Since subscriber engagement is such a big factor in whether your email gets delivered (and it has been more so recently than it used to be), then it makes good sense to regularly clear your list of those who are not engaging. You may want to send an email informing them that they are about to be taken off your list unless they say otherwise. This process can dramatically help the subscriber engagement of your list. Even though you're losing subscribers, your list as a whole is a better one, and you're rendering your emails more likely to be delivered to the inbox. The quality of the list is just as important as, if not more important than, its quantity.

Bounce Rate

In email vernacular, a failed delivery is commonly called a *bounce*, because the undeliverable message literally rebounds back to the sender, often within seconds of being sent. There are, however, two types of bouncing going on.

Remember those large, underfilled pinkish rubber balls used in the lower grades of elementary school? Those things were rather annoying—they didn't really *rebound* back to the thrower, but more or less came back without much velocity or energy. This could be seen as a *soft* bounce—and in the email marketing world, is typically due to a *transitory* problem. This could be where the recipient's mailbox is full, or the recipient mail server is too busy.

Unfortunately, just because a bounce is *soft* doesn't mean that repeated attempts to send to the address will be successful. Even if the address is legitimate, the recipient may have abandoned the email account so that the mailbox is perpetually full.

So, a "soft" bounce may be the result of the receiving mail server refusing the connection, either because it's in general too busy or because the connecting mail server is considered to be spamming.

These refusals look something like this:

Server XISP.com is not accepting connections
Connection refused by: XISP.com

Sometimes, if your server is being "temporarily" blocked, the message will be categorized as a "soft" bounce, too:

Anti-spam YISP.com has refused your connection as your mail server has been temporarily blacklisted.

Then you've got those little, hard polymer "super balls," available in those vending machines in pizza parlors and arcades—our local discount store has a rack of them at the exit—in the attempt to capture just a few more cents from the parents of small children. You know what I'm talking about—these super balls rebound so hard, and so fast they could put your eye out if you're not careful! This image is a *hard* bounce. In email marketing, it's generally the result of a *permanent problem*, such as when the

recipient address just doesn't exist. In that case, you'll see an error like this one:

> *Requested action not taken: mailbox unavailable*
> *JOHNB@EXAMPLE.COM is not a valid user*

Basically, hard bounces tell your mail server to *stop trying to send to this address*.

Many ISPs use "hard" bounces to reject messages they consider to be spam. Spam is a scourge not only because it wastes *your* time to delete it from your inbox, but because it wastes your ISP's network resources. A mail server that is busy processing spam has less capacity to handle email people want to receive.

The usual strategy ISPs and organizations have taken to combat spam is to block suspect messages or senders as soon as possible so as to keep their resources free for legitimate mail. In accordance with the rules of the Internet, they are supposed to inform the sender the reason why the mail was refused.

Here's an example of that kind of message:

> *Message blocked for abuse. Please contact the administrator of your ISP or sending mail service.*

Spam Trigger Words

While the bounce rate, sender reputation, and subscriber engagement are important factors in the deliverability of emails, avoiding spam trigger words still plays a role—especially considering the fact that sender reputation is affected by spam filtering.

Years ago, putting the word "Free" in your subject line would likely have automatically triggered a spam filter. Now, that's not necessarily the case, as long as your sender reputation and subscriber engagement are strong.

Nonetheless, you're still taking a chance at nondelivery if you use spam trigger words in your subject lines (or even in some cases in the body of the email). You've certainly seen these kinds of words and phrases in emails you've received. Here's a small sampling of these kinds of terms:[21]

$$$	Affordable
Price	Profits
Cash	Save $
Discount	Credit
Eliminate debt	Lower interest rate
Increase sales	Click below
Visit our website	No fees
Fast cash	100% satisfied

You can find a larger list online at https://blog.hubspot.com/blog/tabid/6307/bid/30684/The-Ultimate-List-of-Email-SPAM-Trigger-Words.aspx.

Be sure to test delivery with good email tracking software or by using a service that tracks delivery for you such as Constant Contact. In some cases, you may find that even though a larger percentage of your emails are going to the spam folder, it's still worth it in terms of response rates and sales to use the spam trigger word. After all, spammers use these terms for a reason: they work.

Recipient's Whitelist or Address Book

Getting the "From" address used in your emails added to your recipients' address book or personal whitelist is a *crucial* step in getting your emails into the inbox, instead of going into the spam folder. You need to remind people to take the step of adding your "From" address to their address

21 "The Ultimate List of Email SPAM Trigger Words," Hubspot, https://blog.hubspot.com/blog/tabid/6307/bid/30684/The-Ultimate-List-of-Email-SPAM-Trigger-Words.aspx.

book/whitelist. Consider adding a single sentence at the top of *each* of your emails.

Here are three examples of effective reminder statements:

To ensure our email is delivered to your inbox, please add the email address messages@ourcompany.com to your Address Book or junk filter settings.

To ensure regular delivery of our emails, please add us (youwanthis@mycompany.net) to your Address Book. Thank you!

To guarantee delivery of this newsletter, please add ournewsletters@finecompany.com to your email Address Book.

You may wish to go so far as to explain to the reader *how* to set the junk filter settings in a special section of an email message, or devote an entire emailing to this issue. Review the process for the major email applications and Internet Service Providers, and write up a step-by-step instructional email message.

Some companies offer phone support to any reader who may need a "walk-through." Do what it takes to ensure your messages don't get diverted into the bulk or trash folder—never to be opened or read.

10 Ways to Increase Deliverability

Here are 10 ways to help increase the likelihood your email messages will be delivered by the receiving ISP and avoid future deliverability problems:

1. **Understand content filtering basics:** Ignorance of filtering mechanisms is no excuse for not getting messages delivered. Read any bounce messages received, track which messages had high bounce rates and low open rates, and see if you can reverse-engineer offending content.

2. **Monitor delivery and bounce rates by ISP/domain:** Periodically, or better yet after *every* delivery, run reports by major domain and ISP on your messages. Look for unusual bounce, unsubscribe, spam complaint, and open rates at specific domains.
3. **Monitor spam complaints:** Even the best permission marketers receive spam complaints. Monitor the number of spam complaints for each mailing, and establish a benchmark average. Look for mailings with spam complaint percentages that vary from the norm.
4. **Make only one connection per email message:** When connecting to an email server, send only one message per connection. Some systems still try to shovel as many messages through one connection as possible, which can be likened to throwing five hundred email addresses into the BCC field. Generally speaking, however, using a good email marketing program will circumvent this issue.
5. **Limit the sending rate:** Though the ideal send volume depends on the list's nature, make sure to follow the special provisions of your email-sending application. Send bulk emails not all at once but in several different distributions. Keep in mind you will also need to accept feedback in the form of bounced messages—your outgoing speed shouldn't affect your ability to receive bounces.
6. **Always accept bounces:** Some email systems (especially older ones) have a habit of rejecting bounce messages. These "bounced bounces" arrive at the receiving ISP and can raise red flags. Nothing irks an ISP more than sending a response that a recipient doesn't exist, only to have the notification rejected and the mailings continue.
7. **Validate your HTML content:** One of the dirtiest tricks in a spammer's arsenal is invalid, broken, and malicious HTML

code. If you use HTML in your messages, make sure your code is error-free and follows W3C HTML guidelines.

8. **Avoid scripting:** Security risks due to script vulnerabilities in email browsers have increased over the years (scripting is the use of commands within email messages: keywords, buttons, or menu choices, for example). For greatest delivery success, avoid using any scripts in messages. Instead, drive your readers to your website, where use of dynamic scripting can be fully implemented.
9. **Create a reverse Domain Name System (DNS):** A DNS is what translates alphabetic domain names into numeric IP addresses. Make sure your outgoing mailing IPs have valid RDNS (reverse DNS) entries set up. This ensures when a receiving email server checks who owns the IP trying to connect to it, you'll come up as the result, passing one of the many basic checks ISPs do to deter spammers. What is a reverse DNS? Reverse DNS is the process of using DNS to translate IP addresses to hostnames, and is nothing more than the opposite of forward DNS, which is used to translate hostnames to IP addresses.

   Remember these two things: Internet hostnames are the names which we use to refer to domains on the Internet, such as *www.gothere.com* or *www.freewill.org*. IP addresses are the numbers which Internet routers use to move traffic across the Internet, such as 216.17.138.115 and 216.136.204.117.

   I know this sounds complicated, and your eyes are glazing over, so **contact your web hosting provider for assistance.** This is exactly the right situation to contact technical support; they'll make it seem easy.
10. **Set up an SPF:** A *Sender Policy Framework* (SPF) is an additional step to verify an email sender's identity. The protocol is fairly easy to set up; your network administrator should be able to do it in less than five minutes.

In a nutshell, SPF is just a single line within your DNS entry that identifies which IP addresses are approved to send email for your domain. Taking the single step of checking the existence and/or accuracy of your SPF record can have positive effects on your delivery rates.

The recommended steps are as follows:

a. Determine the IP address or addresses of your email marketing server(s) by contacting the responsible IT representative within your organization or your hosting service.

b. Make sure that those IP addresses of your email marketing server are a published part of your public SPF record. Many senders publish the IP addresses of their own company's internal email server in their SPF record, but neglect to list the IP addresses of their email marketing server in that record. For maximum deliverability, your organization's SPF record should contain both sets of IP addresses.

c. If you haven't already published a full SPF record for your organization, do so as soon as possible. The publishing process is relatively easy, and there are several free tools available to help you do so, listed in the resources section.

SPF adds another layer of authentication to your outgoing email and protects against "phishing" attacks on your brand. You should know that some ISPs, such as AOL, *require* SPF to be implemented to be considered for their whitelists.

Today, nearly all abusive email messages carry fake sender addresses. The victims whose addresses are being abused often suffer from the consequences, because their reputation gets diminished and they have to disclaim liability for the abuse, or waste their time sorting out misdirected bounce messages.

You probably have experienced one kind of abuse or another of your email address yourself in the past, for example when you received an

error message saying that a message allegedly sent by you could not be delivered to the recipient, although you never sent a message to that address.

Sender address forgery is a threat to users and companies alike, and it even undermines the *email* medium as a whole because it erodes people's confidence in its reliability.

See if you can determine what may have caused the problem. It could be the subject line, or perhaps you've sent too many messages in too short a time. Remember, a high number of spam complaints may result in an ISP blocking current *and* future messages. Some resources you can use to monitor complaints are located in the resources section.

Avoiding the "Promotions" Folder

It's not just the spam folder we have to be vigilant about.You may have noticed that your incoming emails are automatically segmented into different folders. If you have a Gmail account, for instance, your emails are segmented into "Primary," "Social," and "Promotions." Other email providers divide folders into "Inbox" and "Clutter" or similar terms in addition to the junk folder; 90 percent of commercial email lands in the Promotions folder.[22]

Why should we try to avoid having our emails land in the Promotions folder? Because it is less likely your recipient will read them. Not everyone reads emails that are in the Social and Promotions folder. It takes extra effort to click on those tabs—and it's reasonable to assume that many people *never* check those folders at all (or even know they exist).

This has been shifting lately, however. More people are indeed checking their Promotions folder and reading the content, according to Return Path.

22 "Happy Holidays, Marketers: Gmail Teaches Consumers to Shop from the Inbox," Return Path, https://blog.returnpath.com/happy-holidays-marketers-gmail-teaches-consumers-to-shop-from-the-inbox/.

Nonetheless, how do we better our chances of getting our emails read and get them in "Primary" or "Inbox" instead? Thankfully, it's relatively simple.

Here are a few methods to help keep your email out of the Promotions folder and in the Primary folder instead:

- *Personalize.* Address the person by name if you can. Yet personalization is not always possible or feasible. For instance, since email opt-in boxes convert better with fewer fields, you may not include "Name" in your email signup, in which case you will not be able to collect names and personalize your emails. Personalizing your emails does, however, tend to lead to higher rates of engagement by your subscribers, which can help your emails get delivered. Test to see what works for you.
- *Limit images and design.*Use plain text or properly formatted HTML. Fancy graphics or too many images can trigger the Promotions folder. Think about a personal email you would send to a friend. In most cases, you would send a plain email with no design whatsoever. This is not to say that design is out of the question, but in many instances it does make delivery more challenging. *If* you use design in your emails, this is all the more reason to make sure your HTML is flawless. The more design, the more opportunity for HTML tags to be unclosed or otherwise defective. Make sure you use an online HTML validator, which analyzes and cleans up email HTML. You can validate your email's HTML by visiting https://www.htmlemailcheck.com and copying and pasting your code into the box.
- *Limit links*. An abundance of links can land your email in the Promotions folder, especially if the links are to different websites. Then again, if you are linking to a website, it makes sense to provide a link "above the fold," near

the top of your email, to increase your conversion rates. Just limit these links as much as is feasible for your own promotion.

Will these guidelines ensure that your emails stay out of the Junk and Promotions folders? No. But taking these steps will significantly increase your chances of getting your email to the inbox and place you far ahead of much of your competition—many of whom do not test deliverability at all. Always remember: "First, get it delivered."

The "Inner Circle" Secret for Increasing Email Open Rates

In email, a click-through rate (CTR) is the percentage of email recipients who click on any hyperlink within the email. So, if you send an email to your list of ten thousand prospects offering them a free white paper, and two hundred click on the hyperlink, your CTR is 2 percent.

Today, the explosion of spam and the widespread use of email filtering software have depressed click-through rates to new lows. So how can you get more clicks from your email marketing?

According to an article in *The Marketing Report*, a survey by Nielsen/NetRatings found that most people regularly open and read a maximum of sixteen permission-based emails. The only way to break into the inner circle is to displace someone, the survey said.

And an article in *DM News* reports, "Marketers will have to enter that emerging inner circle of trusted companies from whom people are willing to keep reading e-mails."

Okay, but how do you break into this inner circle of email senders whose messages your prospects will open and read?

It's not easy, but there are at least six options that seem to work with some level of success:

1. **Free e-zine.** Write and publish a truly valuable e-zine and offer it free to folks who give you their email address. If you publish regularly (at least once a month) and provide content of genuine worth, readers will come to value your publication and establish a relationship with you. You will have entered their "inner email circle," because they will view anything with your name in the "From" line as being from a trusted adviser and worth their time to at least read and open. A great example of such an e-zine is Agora's *Daily Reckoning* (www.dailyreckoning.com).
2. **News and updates**. Similar to an e-zine, some publishers send short news bulletins to their subscribers on a regular basis. *ComputerWorld* sends a daily online update with short items from the magazine. You can purchase a short online ad in these updates, thereby buying your way into the reader's inner email circle. CMP, a trade publisher, emails a monthly update, *Business Technology Advisor (BTA),* to the subscribers of all its publications. For $200 per thousand, you can sponsor *BTA*, having the entire issue devoted to your firm and products. Since CMP subscribers know and look forward to *BTA*, your message gets a higher readership and response than it would if you send it under your own banner.
3. **Service and upgrade notices**. Software users will read and open emails from the software publisher that contain news about upgrades, technical information, or service policies. If your customers regularly need to receive service and product news from you, get in the habit of delivering it via email. Then they will be "trained" to read your emails, so when you send a promotion, it too will get opened and read.
4. **Transaction emails**. A survey from www.quris.com shows that customers do value and read two specific types of emails: (a) transaction confirmations and (b) account status updates.

You can get your promotional message read by embedding it into routine emails that contain transactional or account status information. A good example is Amazon, whose customers open and read the emails amazon.com sends because they might contain news about their order.

5. **Alert services.** Consumer newsletters, especially investment advisories, have pioneered this approach. When you pay for your monthly subscription, the publisher offers you a bonus: additional content, sent periodically via email, to keep you updated on the topic between regular issues. The catch: You have to give the publisher your email address to receive this free online bonus. The publisher quickly builds an e-list of subscribers who eagerly anticipate and read the emails, because they are viewed as valuable information they pay for as part of their subscription. The most successful publishers keep the information content of the emails high, but also liberally promote products and services to these email alert recipients.
6. **Club or membership.** Your prospects will read emails from clubs, associations, online communities of interest, subscription websites, and other organizations of which they are members. Therefore, if you can create a club or have your email distributed by one of these membership organizations, you can enter the prospect's email inner circle.

As a rule of thumb, whenever you can send email to your prospect using one of the above methods, your chances of getting opened and read increase exponentially vs. sending a typical promotional email.