THE NEW RULES FOR EMAIL DELIVERABILITY

...or, how to keep your email list from getting crushed.

Matt McGlynn, CTO
Randy Paynter, CEO
Care2.com

care2

OVERVIEW

Internet Service Providers (ISPs) are cracking down on high-volume email senders, such that even legitimate organizations are suffering. The best practices of the past few years are no longer sufficient. To prevent plummeting inbox rates—or to begin recovering from a recent penalty—you will need to quickly embrace the new rules of email deliverability.

This paper will list the critical industry changes, illustrate the costs of failing to meet current standards, and explore solutions in detail.

WHY NOW? WHAT CHANGED?

Consolidation of ISPs means a very few companies control access to most of your organization's house file. It is likely that 30%-40% of your subscribers use Google (Gmail), with perhaps another 20%-30% hosted by Microsoft (Hotmail/Outlook.com). These ISPs have implemented aggressive filtering systems to prevent unwanted messages from reaching the recipient's inbox.

To make sure you get the highest possible percentage of messages delivered to your subscribers' inboxes, you need to make the big ISPs happy. And that's not easy. The increasingly restrictive policies of these few companies make it impossible to continue with mailing practices that worked a few years ago.

WHAT HAPPENS IF YOU DON'T KEEP UP?

A variety of potentially terrible outcomes await those senders who ignore the changing landscape: Individual messages or campaigns could be delivered to the "spam" box, even for your best subscribers. Over time, your former active readers become lapsed and inactive, creating a cascading problem of diminished engagement.

Third-party blacklist operators could red flag your outbound mail server IP addresses. This can cause many ISPs to reject your incoming mail, long before your subscribers see it.

Large ISPs could apply a penalty, causing 100% of your messages to be delivered to the "spam" box. Recovering from any of these problems can take months, assuming you can figure out what went

wrong and fix it. Some senders find they have to take radical measures to recover, such as slashing their list size by 80% or more.

Blacklists and penalties could happen at any time. Therefore, the best time to begin preventing such problems is right now.

GUIDING PRINCIPLE: DON'T LOOK LIKE A SPAMMER

Email providers use numerous signals to determine whether to deliver a message to the recipient's inbox or "spam" box. These signals can be grouped as follows:

CONTENT

Do the words, links and images of the message appear to be spammy?

SENDER REPUTATION

What is the complaint rate for the servers used to send this mailing? Are the IP addresses whitelisted or blacklisted?

RECIPIENT BEHAVIOR

Has this recipient been engaging with mail from this sender? Have other recipients of this mailstream been engaging with this mail?

LIST HEALTH

Does the list include dead accounts, hard-bouncing addresses, or traps?

While all the above items deserve attention — and this paper addresses all of them to some degree — we will focus on list health and hygiene. The addresses that you allow to remain on your house file significantly determine your Sender Reputation and the inbox rates for your email campaigns — which in turn determine open and click rates, which in turn determine revenue. This is true whether you send mail from your own infrastructure or employ an ESP (Email Service Provider) to send campaigns. Developing good mailing list hygiene has become one of the most critical requirements for running a successful email marketing program.

TWO DANGEROUS TRUTHS THAT YOUR EXECUTIVE TEAM NEEDS TO UNDERSTAND IMMEDIATELY

Today's "best practices" result largely from two specific, relatively recent changes in the industry.

Neither of these were true 10 years ago, but both are true today:

1. Some email addresses are toxic.
2. Formerly good addresses can become toxic.

It used to be true that a few bad addresses wouldn't affect the inbox rates for the rest of the campaign. Those days are over. Now it is possible that a few bad addresses can destroy the reputation of your brand and your outbound mail IP addresses in the eyes of the ISPs who host all of your subscribers' inboxes. Sender reputation problems due to toxic addresses could cause a 20-100% drop in inbox rates overnight.

Said another way, every email address on your list is not an asset. Some of them are liabilities. Here is an example: a formerly good address on our list, on the domain mail4.dak.pp.ru, was adopted by Project Honeypot <http://www.projecthoneypot.org> and converted to a spamtrap address without warning. Every subsequent message we sent to that address caused the sending IP to lose its SenderScore Certified status, which in turn caused a measurable drop in inbox placements among SenderScore partner ISPs (including Microsoft).

Here is another example: A Yahoo mail user accidentally typed his address into our website as joe@ynail.com. Typing ynail.com for ymail.com is an expensive typographic mistake, because any IP that sends mail to ynail.com will soon get listed on the MAPS Realtime Blackhole List (RBL). Ynail.com is one of many "typo domains" that have been purchased by blacklist operators to punish email marketers. If your IPs become listed on the RBL, Trend Micro's "Spam Investigators" will require you to re-confirm your entire mailing list — which will likely result in a loss of 50-80% of your subscribers. These examples illustrate the high cost of allowing bad addresses onto your list, and of allowing existing subscriber addresses to become bad.

LARGE ISPS KNOW YOUR LIST BETTER THAN YOU DO

Large ISPs create internal reputation scores for high-volume senders. If your domain or infrastructure develops a bad reputation score, your future campaigns will be delivered to the spam box.

All of these factors reduce a sender's reputation score:

- Repeated sends to abandoned accounts
- Delivery attempts to non-existing or hard-bouncing accounts
- Spamtrap hits
- Spam complaints from subscribers

Therefore, it is critical to remove such addresses from the list — and to prevent them from being added in the first place.

THE MANY TYPES OF EMAIL ADDRESSES THAT WILL HURT YOU

Any email address that does not represent a single human subscriber is potentially harmful. We can break down some specific subtypes below. It is worth understanding the various types, because each one requires its own unique mechanisms for prevention and removal.

NON-DELIVERABLE DOMAINS

Many domains have no mail service (MX records) defined. For example: example.com. Your outbound mail servers cannot send mail to such addresses. This is a relatively harmless problem; the only cost is that such addresses waste resources on your mail systems, and artificially lower your open and click rates.

OBFUSCATED ADDRESSES

Some subscribers enter their email address in an obfuscated form, such as joe@REMOVEexample.com or tedNOSPAM@example.com. The best case result of sending email to one of these addresses is that it is undeliverable. The worst case is that the address is a spamtrap. Example: the domain nospamsprintnet.com is registered to Trend Micro, operators of the Mail Abuse Prevention System.

ABANDONED ADDRESSES

Because free email accounts are easy to obtain, they're easy to forget. Any address whose owner has stopped logging in, or stopped reading mail, is a potential liability. The best case is that your Sender Reputation suffers due to low readership or engagement rates. The worst case is that the subscriber's ISP converts the abandoned account to a spamtrap.

TEMPORARY, "BURNER" ADDRESSES

We have found thousands of websites that offer free, temporary, time-limited, throwaway email addresses. Example: <http://www.throwawaymail.com/>. There is no point allowing these on your list.

BOUNCING ADDRESSES

Delivery attempts to non-existent users result in a hard bounce. ISPs monitor senders for this behavior; repeated sends to bouncing addresses will damage a sender's reputation.
Complainers: When your subscriber flags your email as "spam," it sends a very strong negative signal about your mailstream to the subscriber's ISP. Repeated or sustained spam votes will significantly reduce future inbox rates.

SPAMTRAPS

A spamtrap is a seemingly legitimate, deliverable address that will generate immediate penalties against you. A single email sent to a spamtrap address can cause your outbound mail IP to be blacklisted.

TYPO DOMAINS

Typographic mistakes in email addresses can result in a non-deliverable address (relatively harmless) or a spamtrap hit (very harmful).

SOLUTIONS

Now that we have thoroughly explored the costs and risks of retaining harmful addresses on a mailing list, we can discuss solutions.

We will cover list hygiene in detail, because every email marketer has the sole responsibility of managing the addresses on his or her list, even if the campaigns are sent by an ESP. If your organization sends email campaigns using internal tools, your IT staff will have additional responsibilities to ensure that the infrastructure is set up properly — and we have advice for this too, which you'll find below.

First, and most critically, we need to clean up the list:

- Add only good addresses to the list
- Remove the bad addresses from the list

Add only good email addresses to your list.

The best way to prevent future deliverability problems is to refine your address acquisition strategies. Make sure new subscribers are a good fit for your list.

If you're working with a 3rd party to help build your list, be cautious with co-registration campaigns and incentivized offers. The latter can work well if the incentive and the audience are aligned with your mission, but too often, incentives are used to attract individuals who care nothing about your mission and simply want the incentive.

In addition, particularly in this polarized political climate, make sure the organizations you work with are aligned with your mission. Even a handful of new signups who don't share your organization's values can wreak havoc on your Sender Reputation.

1. Get permission.

If you are renting, sharing, appending or scraping email addresses, stop. Not only could some of these practices get you in legal hot water, they're also a quick way to damage your Sender Reputation.

Only send email to people who have specifically opted in to your brand, whether directly on your site or through a clearly identified permission-based opt-in on a partner website (such as Care2.com/ThePetitionsite.com).

Do not message leads that were collected as part of a multiple or group opt-in. If the recipient of such messages didn't realize he or she would receive mail from multiple organizations, your messages will likely be flagged as spam.

2. Validate individual addresses at the point of collection.

Analyze all new email address submissions, before sending a single message. It is not uncommon for 10% of new subscription requests to use bad addresses. All new subscription requests should be analyzed instantly, so that the user can provide a corrected or updated address if necessary. Specific filtering techniques are detailed below.

3. "Onboard" new subscribers.

Send a welcome message as soon as possible. Make sure to give the recipient a reason to be happy s/he signed up for your newsletter. Describe the newsletter's content and messaging frequency. Include an "unsubscribe" link; if the recipient is not interested in your content, it is far better for him or her to unsub than to click the "spam" button.

Sidebar: The double optin fallacy

The "gold standard" for building a clean list is to require every new subscriber to click an emailed link confirming his/her desire to join your list. Existing subscribers can be "re-confirmed" by the same process.

We do not recommend this practice. Only a small percentage of supporters will successfully complete the confirmation process. Many potential subscribers won't ever see the confirmation message, won't realize what they're supposed to do, will get scared off, or will suffer technical challenges.

To be sure, the cost of not employing round-trip confirmation is strict adherence to the hygiene practices described elsewhere in this document. Nonetheless, we find it far superior to lower the barrier to entry, but aggressively prune low-value subscribers (as detailed below), than to block a majority of new members from joining in the first place.

Remove bad addresses from your list.

You have spent a lot of time and money to build your list, so it is painful to remove any addresses. Recall that some addresses are toxic. If your list hygiene practices have been lax, it is likely that a small percentage of addresses are costing you thousands of dollars per year. A few spam traps, or a handful of complainers, could significantly reduce the performance for even large lists. Successful email marketing requires ongoing, proactive removal of low-value and high-risk addresses.

1. Unsubscribe all the obviously bad addresses.

This can be a relatively quick process. Remove all non-deliverable, obfuscated, and temporary addresses, the role accounts, the dead and typo domains. See details in the HOW TO DETECT, BLOCK, & UNSUBCRIBE BAD EMAIL ADDRESSES section below.

Chances are, none of those subscribers have ever received your emails anyway, so there is literally no loss to the business — but potentially some significant gains — when you delete them.
Purge lapsed and inactive subscribers.

The idea is simple, but the implementation of this is admittedly challenging, both for technical and political reasons. The goal is to remove subscribers who are no longer actively engaged with your email and/or your organization.

It is possible that the population of lapsed/inactive subscribers contains a disproportionately high percentage of complainers. Further, if you have never purged inactives, it is very likely that this segment of your list contains converted spamtrap addresses. Finally, every non-engaged subscriber is dragging down your Sender Reputation metrics. Therefore it is critical that these low-value, high-risk addresses are purged regularly.

See details in the PURGING LAPSED AND INACTIVE SUBSCRIBERS section below.

HOW TO DETECT, BLOCK, & UNSUBSCRIBE BAD EMAIL ADDRESSES

Multiple filters are needed to identify and block bad addresses. We have suggestions for each potentially problematic address type. Some of these filters should be applied at the point of collection, in "realtime" — meaning, the test is performed as soon as the address is typed by the user,

so that the user can correct the address if necessary. Other tests can only be applied later, after an address is on the list.

NON-DELIVERABLE ADDRESSES

If possible, new email address submissions should be checked in realtime to determine whether mail service (MX hosts) exists for the given domain. Better still, use a 3rd-party validation system such as FreshAddress to determine whether the specified mailbox actually exists.

OBFUSCATED ADDRESSES

Any address containing "remove," "removethis," "spam," or "nospam" should be rejected at the point of collection. Ideally, the user would be shown an error message and given an opportunity to correct the address. If you are cleaning up an existing list, any address matching these four words should be unsubscribed.

TEMPORARY ADDRESSES

Temporary/throwaway domains can be identified using a service such as https://www.block-disposable-email.com/. Alternatively, do a web search for [temporary email address] and make a list of domains manually. Reject any such submissions at the point of collection; allow the user to provide an alternate address.

BOUNCING ADDRESSES

Most ESPs will remove bounces from your list automatically. If you don't use an ESP, your IT department must set up bounce processing. See the INFRASTRUCTURE CHECKLIST section below for more information.

COMPLAINER ADDRESSES

Most ESPs will remove complainers from your list automatically. If you don't use an ESP, have your IT department set up "feedback loops" to process subscriber complaints. See the INFRASTRUCTURE CHECKLIST section below for more information.

ROLE ACCOUNTS

Most deliverability professionals recommend blocking or unsubbing "role account" addresses such as: sales@ , webmaster@ , support@ , info@ , abuse@ , etc. Many such addresses are delivered to multiple recipients, not all of whom will be engaged with your brand and messaging. Therefore, the risk of complaints from such addresses is high. Find a longer list of role account prefixes in the Adobe whitepaper mentioned in the SPAMTRAP ADDRESSES section below.

SPAMTRAP ADDRESSES

There is no public list of spamtrap addresses; spamtrap operators make new addresses daily. Nonetheless, there are old ISP domains that have been, or are believed to have been, repurposed as spamtrap domains, such as MediaOne.net. Web search will reveal collections of such domains; see, for example, this Adobe whitepaper about spamtraps: <https://is.gd/AdtqPr>

TYPO DOMAINS

Email addresses with typographic mistakes represent both a lost opportunity and a high risk of future problems. The user should be warned in realtime if the address s/he entered appears to contain a typo. At a minimum, your front-end developers could detect common off-by-one errors such as hotnail.com, hotmial.com, gnail.com, yajoo.com, etc. Better yet, integrate a third-party validation library such as <http://getmailcheck.org/>.

PURGING LAPSED AND INACTIVE SUBSCRIBERS

Every dormant address on your list hurts your inbox rates. If any of those dormant addresses is a converted spamtrap address, or if your lapsed subscribers periodically complain about your mail, then this segment of subscribers is doing a lot of harm to your inbox rates.
Define the inactivity period for your organization.

The hardest part of this process is determining how long to allow a subscriber to be inactive before removing the address from your list. As a general rule, organizations that send mail daily or weekly should wait no more than six months before removing an inactive address. We have found that ISPs prefer even shorter periods of inactivity.

Less-frequent mailers could conceivably wait six to 12 months, but only if the organization's inbox rates are good. Suppressed inbox rates (anything below 85%) would indicate a need to shorten the allowed inactivity period.

If you are recovering from a blacklist or penalty, a temporary suppression of everyone except the most active users (15–30 days) can help restore inbox rates.

2. Define qualifying activities.

For some organizations, merely opening an email constitutes a sufficient level of engagement to remain on a list. It is not the best metric, though, for several reasons:

Most open-rate trackers rely on an embedded image in the email. But some email systems do not load images. Therefore most reported open rates understate the actual behavior of subscribers. It represents too light a level of engagement.

Clicks, or on-site activities, tend to be a superior measure of activity or engagement: login, commenting, petition signing, etc. Readers who periodically open your messages but take no further action tend to have a low future value to the organization, and can be safely unsubscribed in pursuit of higher inbox rates.

Before purging inactives, it is best to send a "re-activation" message — a simple message that encourages the user to get engaged, or be unsubscribed soon thereafter.

CONTENT & TEMPLATE TIPS

Here are some tips on improving deliverability for the design and content teams:

- Analyze your message content with a spam score tester. Some ESPs offer this service. There are free alternatives too, such as <http://isnotspam.com>.
- Preview your message templates in all major webmail systems, including mobile devices, to ensure that the messages are rendering properly.
- Make unsubscribe instructions prominent in every message. Do not hide them in hopes that this forces subscribers to stay on the list. If a subscriber has lost interest, you want him/her to unsub rather than complain.
- Consider adding a "report abuse" link to the message template, to generate an email message to you. This may prevent a subscriber from reporting spam to his/her email provider.
- Ask subscribers to add your FROM address to their address book.
- Continually monitor opens, clicks, and any other engagement metrics you can. If these metrics are declining, immediately test better subject lines, new mobile-friendly templates, improved content targeting, new calls-to-action, refined messaging frequency (e.g. fewer but better messages), etc. Ultimately, no amount of list hygiene or infrastructure improvements will rescue a failing list if the subscribers don't want the content.

APPENDIX: INFRASTRUCTURE CHECKLIST

If your organization sends mail campaigns directly — not through an ESP — your IT team must meet these additional requirements to ensure that your campaigns are not blocked:

- Set up multiple clusters of IP addresses, based on permission level. Messages to the most active and most valuable subscribers should be sent from one dedicated cluster. New subscribers, low-value subscribers, and high-risk mailstreams should be sent from a second cluster. Peer-to-peer email, such as "tell a friend" messages, should be sent from a third cluster.
- Set up authentication headers for all outbound mail: SPF, DKIM, and DMARC. Many online resources exist to help with this process. Test the results within any Gmail.com account, via the "show original" option for any message, or via this tool: <http://dkimvalidator.com/>.
- Process unsub requests immediately. If a user unsubscribes, you do not want him or her to have any further opportunity to click the "spam" button on one of your mailings.
- Process hard bounces immediately. Allow at most two consecutive hard bounces before removing an address from your lists. For SMTP 550 errors ("user does not exist"), a single hard bounce is usually sufficient. Note that large ISPs convert some percentage of hard-bouncing addresses to spamtraps; if you don't unsub them when they bounce, those addresses will severely damage your Sender Reputation later.
- Set up "Feedback Loops" (FBLs) for all major ISPs/Mailbox Providers. These FBLs allow you to see individual complaints from your own subscribers, for the purpose of unsubbing them from all your lists. Because a spam complaint has such a strong negative impact on your reputation, complainers must be removed from all lists immediately. Read more here: <https://blog.returnpath.com/what-is-a-feedback-loop/>, <https://sendgrid.com/blog/email-feedback-loops-101/> Note: Gmail, alone among major mailbox providers, does not provide a feedback loop.
- Monitor email blacklists for your outbound email IPs (e.g., <http://mxtoolbox.com/blacklists.aspx>)
- Monitor the reputation of outbound mail IPs (e.g., <https://www.senderscore.org/>)

APPENDIX: THIRD-PARTY VALIDATION SERVICES

There are a variety of companies that offer email address validation services — both real-time checks for new subscription requests and batch processes for cleaning existing lists. Some offer simple SMTP lookups to verify that an address exists; others tap into vast databases of ESP delivery data to predict whether any specific address is likely not only to be deliverable, but to open/click, opt out, or complain.

We have found value in these services at the cost of custom development work to integrate them into the subscription funnel. We have identified gaps that must be worked around:

- Simple SMTP lookups are of dubious value, especially for domains that provide spurious responses (including Yahoo, Prodigy, AT&T).
- Any third-party database of "frequent complainers" might align poorly with your own subscribers' behavior — meaning, use your own engagement data in favor of a third-party opinion about whether an address should be removed from your list.
- Further, these services can be expensive. The cost can be difficult to justify unless you are working to recover from suppressed inbox rates or an ISP/blacklist penalty.

QUESTIONS?

Contact Care2 at http://www.care2.com/aboutus/contactus.html
For Care2 services inquiries, visit http://www.care2services.com/

Care2 is the World's Largest Social Network for Good, with 40 million members. Care2 helps people stand together, start online petitions, and share stories that inspire action.

Care2 is the only service, tailored exclusively for nonprofit organizations and mission-based brands, using proprietary technology to recruit quality donor and customer prospects. Care2 has recruited more than 60 million donor prospects for nonprofit organizations.

care2

ABOUT THE AUTHORS

MATT MCGLYNN

FOUNDER, CTO

Matt is carbon-neutral and solar powered. His work at Care2.com combines a lifelong enthusiasm for environmental conservation with 18 years of experience imagining, designing, and developing software products and services. He joined Randy in 1998 to build Care2 into the world's largest social network for good. His ongoing advocacy of open-source tools, scalability, and high availability created the platform for Care2's ongoing success. As CTO, Matt oversees all aspects of technology at Care2, including leadership of initiatives in site search, SEO, and email deliverability.

RANDY PAYNTER

FOUNDER, PRESIDENT, CHIEF EXECUTIVE OFFICER, CARE2

Randy Paynter is the Founder & CEO of Care2.com and the PetitionSite, the world's largest social network for good, a community 40 million strong, and helped pioneer online advocacy with the launch of the ThePetitionSite.com with over 614 million petition signatures and wins daily. Care2 helps people start petitions and share stories that inspire action while helping over 2,700 nonprofit clients recruit more than 74 million prospective donors worldwide. Care2 is a profitable B-Corporation, or social enterprise, using the power of business as a force for good.

Prior to starting Care2, Randy co-founded one of the web's first viral apps – electronic greeting card service, eCards.com in 1995. Randy holds an AB from Harvard University and an MBA from Stanford's Graduate School of Business.

care2