2018

THE 250ok DELIVERABILITY GUIDE

250ok

TABLE OF CONTENTS

CHAPTER 01

INTRODUCTION

At 250ok, we take email seriously. We know some people want to etch email's headstone, but we aren't down with that. We are, however, fully invested in the death of bad email. And believe us, it's a jungle out there. Thus, we created... The 250ok Deliverability Guide.

This can serve as your handbook to creating effective emails designed to keep your recipients safe and engaged, while your business reaps the benefits of a good sender reputation. You'll find details on the finer, lesser-known mechanics of email, and how you can (and should) use that information to craft better, more effective emails that actually get seen. This is your new go-to. So let's get started.

CHAPTER 02

DELIVERABILITY 101

YES, there is a fundamental difference between delivery and deliverability. Delivery describes the number of messages sent to a mailbox provider that didn't bounce during the transmission process. Deliverability, however, concerns the exact location of these messages, whether that be the inbox, spam folder, or other. Deliverability is the conversation about what makes a message safe and cleared for landing at mailbox providers (MBP) like Gmail, AOL, Yahoo, Microsoft, etc.

At its most basic level, email can be delivered or bounced, meaning it does not end up in the intended recipient's mailbox (their inbox, spam, or otherwise). Bounces can be either transient (a.k.a. soft bounce), where the server will continue to try to deliver the message because the error received was temporary and could theoretically be resolved, or permanent (a.k.a. hard bounce), in which the server is not trying again because the error won't be resolved—for instance, the email address does not exist or the message is blocked from delivery.

Beyond that, deliverability can get complex. The mail is delivered, but where did it go? What caused a soft or hard bounce, and what can you as the sender do to resolve it? Is your email battling specialized filters (a process used to determine whether or not emails are legit) that put your hard work in a spam folder?

All of this information funnels into your email delivered rate and inbox placement rate (IPR). While your delivered rate describes how much of your email reaches its destination, the IPR gives you an idea of not just how many emails are delivered, but how many land in the actual inbox.

Are you confused yet? We'll help you figure this all out.

CHAPTER 03

INFRASTRUCTURE & AUTHENTICATION

Subdomains

A subdomain is an extension of a brand's web domain and can be used for a variety of purposes. For example, email.brandname.com is a common subdomain used to denote commercial email. Email subdomains are the preferred set-up for most email service providers (ESPs) when working with marketers. They maintain the best opportunities for brand recognition between a consumer and a brand. They are also easy to configure and allow for separate opportunities to use email authentication that will not impact your corporate domains.

Domain Name System (DNS)

The Domain Name System (DNS[1]) translates plain text requests for information into IP addresses for computers to use, locate and access information. For example, when a user asks to access www.250ok.com, the web browser will ask (via DNS), "Where do I find this website?" DNS will respond, "At the following IP address: 209.43.65.226."

DNS contains several different types of information based on the request: An A record translates a hostname to an IP address to identify the destination for the requested domain, such as a mail server or website address; a TXT record is commonly used as a human-readable note or contact as well as the domain's authentication policies; an MX record identifies where emails should be sent to for this domain; and several other useful records enable the communication of information between two devices.

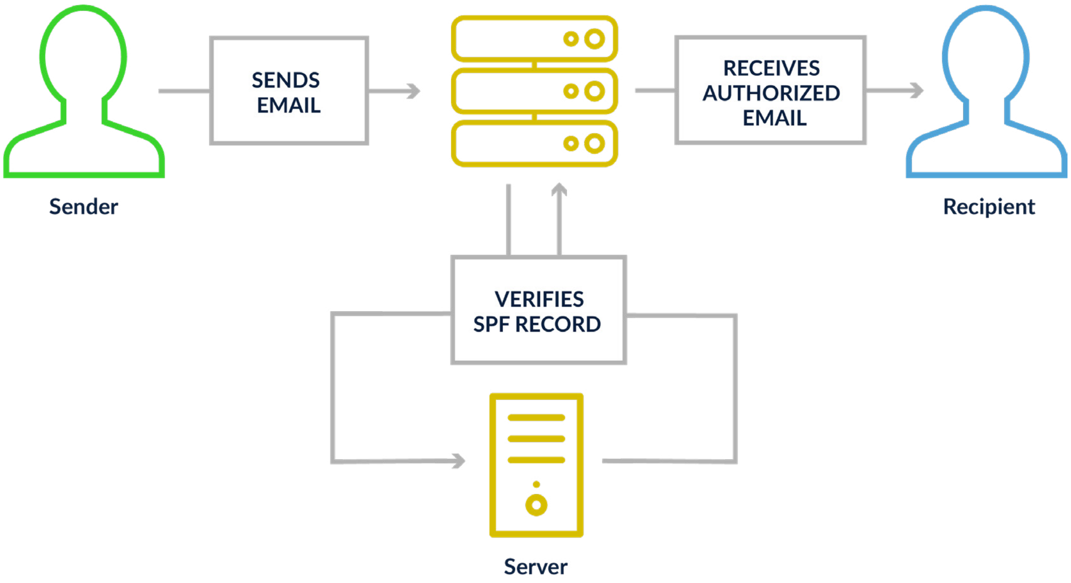
Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is a path authorization mechanism (figure 1.1). Email spam and phishing often use a forged "from" address, so publishing and checking SPF records are recommended anti-spam techniques. Why? Because SPF confirms whether or not a message claiming to be from a given domain was allowed to be sent over a given IP appropriately. It refers to a list of authorized sending IPs for a domain published in the DNS records for that particular domain. This is why it's absolutely critical to keep those IP addresses up-to-date within your DNS records.

Another thing to note: SPF is relatively easy to implement, but just as easily screwed up. It's not hard to make a mistake with your records, or let them become stale as your network requirements change or additional services are added to the records. SPF has a limit of 10 DNS record lookups, so formatting your records properly is important. If you think you're having an issue here, talk to an expert (we know a few) to make sure you get this right.

[1] Source: https://www.cloudflare.com/learning/dns/dns-server-types/

figure 1.1 Sender Policy Framework (SPF)



DomainKeys Identified Mail (DKIM)

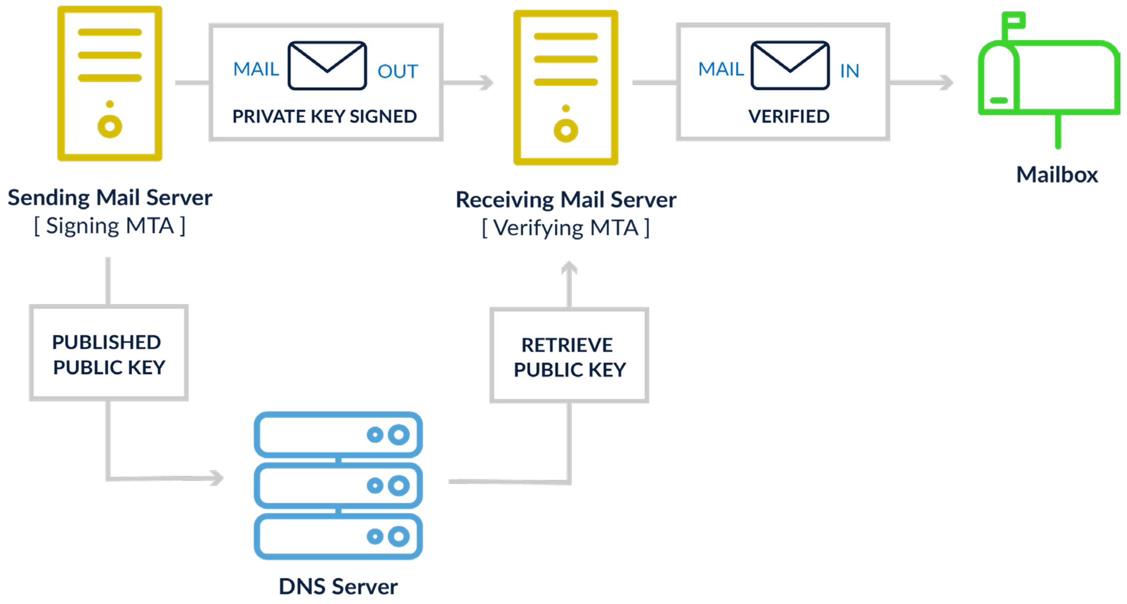
DomainKeys Identified Mail (DKIM) is a content verification mechanism (figure 1.2). It detects if a message was modified since it was sent. DKIM is intended to prevent forged sender addresses in emails (the "from" line), by validating an email claiming to be sent from a specific domain was authorized by the owner of the domain, a technique often used in phishing and email spam. Mailboxes use DKIM to evaluate whether or not a message should be trusted, and it's a critical step in protecting recipients from phishing.

Here's how it works: Upon sending an email, the content and headers are processed using a private key, and the calculated token value is stored in the DKIM-Signature header, along with additional technical information like the signing domain, DKIM version, the signed headers, and the selector used. The recipient does the same only in reverse, using the public key to validate the encoded digest. Values match? Good news, the message was not modified. They don't match? Red flag, it fails authentication. Your ESP will keep the private key on their Mail Transport Agent (MTA) while you will update your DNS records with the public key (some ESPs may manage your domain and will manage this for you).

DKIM is super-important because you'll need it to enroll in some ISPs feedback loops like Yahoo and Gmail, which we maintain is mandatory for monitoring your email health. We wrote this guide[2] to help you set up DKIM, but it doesn't hurt to talk to one of our deliverability experts[3].

[2] Source: https://250ok.com/email-deliverability/5-tips-to-improve-your-email-reputation/
[3] Contact us: https://250ok.com/contact/

figure 1.2 DomainKeys Identified Mail (DKIM)



DKIM Key Rotation

The security community recommends regularly changing the encrypted tokens of your DKIM records to enhance the security of your authentication configuration. The typical schedule for rotation is at least once every 12 months.

There are multiples ways to achieve rotation, but the two most common are:

1

Publish a completely new selector for DKIM and run the old and new in parallel while you update your systems configuration to utilize the new selector keys.

2

Change the published token data in the public key and update to a new private key on an existing selector.

Pitfalls/Warnings

Some ISPs monitor reputation on multiple values beyond just IP or domain reputation, including things like a DKIM selector. Be aware, changing your selector may impact your delivery at some ISPs. Keep this in mind and consider some additional testing as you determine the best path for your rotation schedule. A complete change of a DKIM selector may require additional domain reputation warm-up and increased monitoring of delivery during the transition period.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a sender-published policy for email messages that fail authentication, helping to prevent spoofing, where a bad actor impersonates your brand to spread viruses or scam recipients.

Most ESPs will set up your account with SPF and DKIM. DMARC is often an added measure of protection, but worth inquiring about if you do not have the internal resources to make it a reality.

DMARC is important when you consider something called "alignment." Domain alignment means the sending domain matches a prescribed authentication. For DKIM, this means the sending domain used to create the signature (and provided through the d= parameter), should match the "from" header. For SPF, this is the domain in the RFC5321.MailFrom (MAIL FROM) portion of SMTP, the RFC5321.EHLO/HELO domain, or both. These could be different, and usually are not visible to the recipient.

Here's an example of how DMARC comes into play when looking at alignment-related passes or failures:

SPF Pass = DMARC Pass
DKIM Pass = DMARC Pass
SPF Pass + DKIM Pass = DMARC Pass
SPF Fail + DKIM Pass = DMARC Pass
SPF Pass + DKIM Fail = DARMC Pass
SPF Fail + DKIM Fail = DMARC Fail

> The vision driving DMARC was senders and receivers working together to protect recipients.

Paul Midgen

Co-author of the original DMARC specification, former Hotmail senior program manager, and 250ok advisor

Brand Indicators for Message Identification (BIMI)

currently in beta

Brand Indicators for Message Identification (BIMI) is an emerging email standard operating in a limited beta with Oath (AOL, Verizon, and Yahoo), intended to incorporate a brand's image alongside their "from" address in recipient's inboxes when the message passes DMARC validation and is of solid reputation. To accomplish this, the sending domain must use SPF, DKIM, DMARC with a reject policy (p=reject), and publish a BIMI record within their DNS pointing to a hosted image of their chosen logo. At publication time this standard is in beta with Oath's email platforms, but here's an example of what it looks like[4].

IPs

An Internet Protocol (IP) address is a number assigned to any device connected to the Internet. When sending email, ISPs use your individual IP address to identify you and your server. With the limited number of IPv4 addresses, IPv6 was created to help make additional "space" in the virtual rolodex of the internet. While the majority of mail is still sent over IPv4, the transition to IPv6 is underway.

Shared vs. Dedicated IPs

You can use different IP categories when you send marketing email. The shared IP environment includes a series of IPs used to send mail from a group of unrelated organizations called the "shared IP pool." This is considered the entry-level space used by most ESPs. Talk to your ESP about this configuration, as each has their own qualifications and requirements for configuring dedicated IP addresses for commercial and transactional use.

Though it tends to weaken email performance for the highest quality senders, it will improve performance for less stellar senders. That is not to say, though, that you can abuse email without repercussions on a shared IP. ESPs are now extremely skilled at sniffing out abusive senders and even predicting unacceptable behavior before it's conducted, so we suggest you don't try to play games.

Here's our bottom line on shared IPs: If you send on a small scale, send irregularly, or simply don't send email that often, the standard shared IP environment at most top-level ESPs may be beneficial. When mailing via a shared IP, sending with a unique DKIM selector and key will further help differentiate your emails from those senders utilizing the same IPs for sending mail.

Let's say you send a large volume of email and the success of your business depends on impeccable deliverability: you'll want to take a look at a dedicated IP. Dedicated IPs are the

[4] Source: s.250ok.com/BIMI

gold-standard approach when you have the means and need to invest in the success of your email program. This dedicated IP is exclusive to your business, allowing you to define the characteristics of the mail sent over your IP without influence from any other senders. It will paint the most accurate depiction of your mailing practices, and give you complete control over your reputation.

Unfortunately, we cannot share this information without a very important caveat. If your ESP has senders of marginal or poor reputation with dedicated IPs, even if it's a relatively small group of clients, the entire IP range could be flagged by a blacklist provider. If your IP lands within the range, you're going to be lumped in with the bad actors. Our advice is to split your transactional mail (receipts) and bulk mail (e-newsletters) across two IPs, preferably in different network ranges. Of course, scale appropriately based on the complexity of your email program. Talk to your ESP, as they may have policies and rules in place for brands interested in a dedicated IP or remaining in a shared environment.

Commercial vs. Transactional IPs

Like we just mentioned, it's a good idea to always split dramatically different kinds of email communication onto different IPs. In particular, you'll want to keep your transactional messaging, where people receive receipts, tracking information, password resets, and the like, separate from messages more likely to be caught or flagged as spam. The physical separation of transactional email should also include a different subdomain, or as many as necessary for each type of transactional mail (receipts, system messages, shipping notices) to help distinguish between various communications. There are a few key reasons why this should be done:

1

TIME SENSITIVITY

You need a password reset now and not in an hour. If you've just sent a large marketing communication, rate limits could impact your ability to deliver time-sensitive communications.

2

REPUTATION PROTECTION

If your marketing communication generated a higher than expected number of bounces or complaints, your IP's reputation may decrease and delivery of important emails may end up routed to the junk folder.

IPv4 vs. IPv6

Most email is still sent over IPv4, however new IPs are being made available in the IPv6 namespace and should be utilized for sending email only after publishing all standard email authentication solutions for your domains. Otherwise, you may find email delivery harder to accomplish at production levels. Be advised, not all mail servers are currently accepting mail over IPv6, so you should ensure an alternate IPv4 address is available to send mail. IPv4 has approximately 4.3 billion available addresses, which has reached near total saturation. IPv6 has exponentially more numbers than IPv4, with more than 340+ undecillion (a 39 digit-long number) addresses available.

Inbox vs. Tabs

As more emails providers implement a tabbed interface, like Gmail, there are regular conversations about how to move your messages to a specific tab or the primary tab. Here is a little inside secret: The tabs are part of the inbox, and people continue to check for emails in the other tabs. Also many of the commonly used email programs (e.g., Outlook, Thunderbird, iPhone mail) all ignore the tab locations and show the messages in the chronological order that they we were received in. So before you invest the time in trying to change the placement of your emails, understand how your subscribers are reading your messages. We get into this a little deeper on our blog[5].

[5] Source: http://s.250ok.com/PromoTab

CHAPTER 04

REPUTATION

Building Reputation

Your reputation is directly related to your business practices and how your subscribers interact (or don't interact) with your mail, very similar to your personal reputation. If you behave poorly and people are bothered by your behavior, you negatively impact your reputation. When it comes to your email, you can expect to see your inbox placement tank in tandem. So how do you protect and strengthen your reputation? There are a few best practices to follow right out of the gate.

Reputation starts with data collection and the practices used from the beginning of your email program. You can have a recipient truly wanting to receive and engage with your email but if you don't collect valid information (i.e., they've entered a typo address), you may encounter reputation issues down the road. To add insult to injury, you've also missed an opportunity for future interactions (and transactions) with that errantly-added recipient. Always send a confirmation email requiring recipient action before committing that address to your list.

Sending an introduction email in addition to a subscription confirmation is always a smart idea, and really, we'd recommend a welcome series to ease your recipients into ongoing communication with you. There are a variety of ways to improve acquisition hygiene ranging from web-form best practices to vendor-based solutions. Talk to your deliverability guru to find the best fit for you.

Reputation also includes targeting, content, and frequency with which you contact your subscribers. When investigating any reputation issue, be sure to look at a wide range of data points to determine the scope of the impact. Is it limited to a small number of domains, a specific real-time block list (RBL), or a general issue impacting delivery across your entire email program? As part of this investigation, be sure to look at the information based on the sources of the addresses and where these subscribers became part of your lists. By looking at your data with a source-view, you can see if you have a bad source impacting your reputation and email delivery. Other metrics to review are complaints and bounces by collection source.

Always use your own lists. Even if a consumer double-opts-in to a list you purchased, they still aren't likely to recognize where your email came from (a simple rule is that consent cannot be bought and sold). Sending unexpected emails significantly increases the probability of those people marking your messages as spam. This practice is also a violation of most large scale ESPs and can result in termination of your account.

It’s important to remember ISPs can choose what to accept or reject, and they want to protect their users from spammers who just want to make a quick buck and then disappear, so the onus is on you to make it clear you are not one of those spammers.

IP vs. Domain Reputation: Understanding the Differences

We’re going to say this very loud for the people way in the back: *Your domain is your identity.*

Say it with us this time: My domain is my identity.

This domain is what your customers, *your email recipients*, believe they can trust. It is your job to protect that trust. Otherwise, the best discount you offer within an email won’t do a dang thing—they aren’t opening your email. Your domain will also be integral in detecting phishing attempts and spam trap hits.

Domain reputation is important to understand, as it will be tied to a name that will be consistent regardless of where the messages originate. This has a much wider impact on email delivery than IP reputation, because it is significantly harder to change your company’s domain than it is to change the IP addresses you are sending email from.

IP Reputation-Building vs. IP Warming: Which is Right for You?

Spam filters are sensitive. They notice when you change IP addresses or domains, or implement new authentication policies. In a very real sense, you look like a different sender, so naturally, they’ll be suspicious of you until you again prove you intend to be a responsible sender. You could easily be blocked (where your email is flatly denied) for abusive practices when you’re simply doing the same thing you’ve always done, just from a different IP.

How do you win back their affection? By “warming” your IP or domain by starting with small email distributions and working up to full volume over time. How? We’ll tackle that in the next section.

A caveat: What one ISP wants to see can be significantly different from another. The experience and industry connections necessary to stay up-to-date on these topics are accumulated over years, so it’s critically important to consult with an expert before doing anything that might accidentally corrupt your reputation with your first campaign.

We also have some bad news about changing IPs. If your new IP had spammers on it, you're probably starting out at a disadvantage with ESPs. Likewise, if your previous IP was being abused by a spammer, traces of that abuse, although not yours, may stick to your domain.

IP/Domain Warm-Up: How?

Start with just a few dozen messages sent to each ISP. Be sure you're sending to users who are most likely to engage with the message. To do that, use recent open and click data to identify your most interactive users. Then, send more the next day and so on until you've worked up to your target volume. This could happen as quickly as five days to one week, or can be a months-long process. The key is to establish your reputation as a welcomed sender, through a reasonable amount of emails to people who want to hear from you.

Maintaining Reputation

Your reputation is the most important factor in your ability to deliver mail, but the path to a clean reputation isn't always clear. Once you've done all you can to set yourself up for success, you must continually monitor your reputation to maintain and improve email deliverability.

Here are a few things to do to keep yourself in check:

1 **Proactively monitor blacklists**

ISPs and filtering companies commonly use third-party blacklists to filter mail and identify messages from senders with poor reputation. Like the name implies, being blacklisted is a major hit on your reputation and will adversely affect your deliverability. Avoid at all costs.

2 **Set up authentication records to protect your brand from phishing**

Authentication records essentially tell mailboxes your message is authentic and is not harmful. Implementing DKIM and SPF authentication dramatically helps your deliverability by confirming mail came from where it says it came from, and thus, isn't phishy. To really cover all your authentication bases, add a DMARC policy for the greatest level of protection for both your brand and your email recipients.

Your status as a phishing target doesn't rely on the size of your mailing list or your budget. If you send email, you're at risk. To protect yourself, use a monitoring tool (like 250ok Reputation) to identify unauthorized mailings or phishing attempts, and actually pinpoint where the email is coming from.

3 Proactively monitor spam traps to identify sloppy sending

If you're hitting spam traps, you're dinging your reputation. Keep an eye on spam traps to make sure your lists are clean, meaning they aren't chock-full of fake or inactive email addresses. (Read a little further for a spam trap 101.)

By using a tool like 250ok Reputation[6], you can monitor your IP addresses and domains to see if you're regularly hitting traps. You'll also see if your authentication records are failing, signaling a major authentication issue. From there, you can take appropriate corrective action to protect your reputation.

4 Clean your mailing list(s) regularly

If you're bouncing mail or hitting spam traps, it's probably a sign you need to clean your mailing list. People change their email addresses. A lot. Remove email addresses inactive for a year.

Suppression lists

Typically there are a few different types of suppression lists, or lists of email addresses you should never send to, that a company needs to understand: An internal do-not-send list, an ESP's suppression list, and potentially a third-party suppression list an organization may need to apply. But how are these lists different?

- **Internal:** Over time, your organization is going to have a number of users who requested you stop sending them emails, but these users may still be active on your website. These addresses should be added to an internally managed suppression list for future marketing communications and can usually be used across all of your marketing channels.

- **ESP:** Most ESPs can impose a global suppression list across all of their clients. These typically include role accounts (e.g., abuse@, info@, postmaster@), domains or users that have requested full suppression from future communications, or in some cases domains, domains the ESP identified should no longer be mailed to. This last classification could be due to a domain's retirement or frequent typos (i.e., @home.com, or @gmail.ca).

- **Third-party:** Occasionally, if you're working with a third party, they may supply a suppression file of individuals who requested they cease receiving emails from the brand, or where there may be a legal requirement to suppress some addresses, like Michigan's child protection registry.

[6] 250ok Reputation: http://250ok.com/tour/reputation/

There are other simple measures you can take to maintain a clean mailing list:

- Only send mail to customers who opt in (confirmed opt-ins preferred)
- Never buy or rent mailing lists
- Provide an obvious unsubscribe link in your email footer
- Immediately unsubscribe customers upon request
- Build a solid collection practice based on opt-in consent (legally required in some jurisdictions)

Spam Trap Deep-Dive

A trap (or spam trap) is an email address that should exist on exactly zero customer lists. Yes, zero, meaning absolutely none. Trap Network Operators (TNO) such as SORBS, Spamhaus, Proofpoint, and others acquire trap addresses a few different ways:

1. **Recycled:** These addresses used to belong to a real human, but are now inactive for a certain period of time. Once inactive, they were reclaimed by the domain owner and then conditioned according to a certain specification to allow it to be re-entered into the world as a trap.

2. **Pristine:** These brand-new addresses have never been seen, and were created by TNOs specifically to catch bad emailers who use bulk email automaters that do things like guess email addresses. What do we mean by that? Think of a common name, misspell it by one or two letters and tack @gmail.com to the end of it.

3. **Typo:** an address that may have been easily mistyped and isn't validated for accuracy (**gmail.com** vs. **gmaill.com**)

Messages received by a trap (also called trap hits) are processed to extract certain metadata:

- Sending identities (e.g., “from” domain and IP)
- Associated infrastructure (e.g., compromised DNS servers, other MXs)
- Message content (e.g., link hosts, content signatures)

This information is how senders get added to blacklists, which, as we reviewed, are used by domain owners to filter messages.

The great thing about a trap hit from a traditional TNO is it's an almost perfect signal a sender has list acquisition and/or hygiene issues. The quality of that signal is *completely unrelated to the number of trap hits, only the frequency*. Recycled traps indicate a sender is purchasing old data or not paying attention to engagement metrics.

Pristine and typo traps are a little different. Pristine addresses do not sign up to lists. When they receive mail from brands, trap networks often assume the address was acquired as part of a purchased list. Typo hits are a little similar, but are better indicators that the sender simply isn't good about list hygiene and sends to every single address they have, whether they're valid, ill-begotten, or otherwise.

Spam Traps vs. Sensor Networks

There are two key types of spam trap "networks," or groups of spam traps with a stated intent: Reputation-impacting and informational (sensor networks).

What's the difference? Well, a reputation-based spam trap network is often used by an ISP, anti-spam vendor or RBL provider to review the mailing practices of the sender whose email their networks are receiving. These types of traps can have a wide range of impact on your ability to deliver emails to your subscribers, ranging from little-to-no noticeable impact to a significant multi-domain block of your emails.

The role of a sensor network, like the proprietary network operated by 250ok as part of 250ok Reputation, is to provide the domain owner or ESP a view of non-reputation-impacting trap data, because if you're hitting traps on a sensor network, you're hitting spam traps—count on it. By allowing senders to proactively identify issues with their lists and take the required steps to change their behavior, valuable reputation measurement and repair becomes possible before a reputation disaster. Unfortunately, many novice senders don't dig into trap network data until they have a deliverability issue on their hands. Our advice: Be proactive, not reactive.

> **The effort of the sender should not be in removing the one spam trap, but finding out how the address got onto the list in the first place. Whether you're using sensor or trap network, any hit is indicative of an underlying list hygiene issue.**

Sridhar Chandran

250ok solutions architect and former AOL postmaster

CHAPTER 05

ANTI-SPAM PROVIDERS

Barracuda

Barracuda is a commercial anti-spam solution offering both cloud and on-premises installation designed to incorporate anti-spam and real-time threat intelligence from a global network of customer feedback. Barracuda's solutions operate on both content and IP-based filtering for messages sent to their devices. Domain administrators are able to toggle the aggressiveness of their instance to levels in-line with corporate policies and needs.

Cloudmark

Cloudmark is a commercial anti-spam solution owned by Proofpoint that uses digital fingerprinting technologies to determine the likelihood of future messages being part of the same email campaign. The result of a digital fingerprint of a message will likely route mail into a quarantine or spam folder, and in some cases may result in rate limiting or blocking of emails. This application is favored by enterprise organizations and ISPs alike.

Spamhaus

Comprised of an international team of spam researchers, Spamhaus developed several different types of block lists, like non-mailing policy blocks, bot traffic, exploited or compromised hosts, commercial spam sources by IP or domain, and the ROKSO (Registry of Known Spam Operations). Spamhaus' listing-impact on emails covers approximately three billion email accounts worldwide and will result in about 40-50% of email traffic being blocked from delivering… and that's us being conservative.

SpamAssassin

SpamAssassin is the most widely used open-source, anti-spam solution in the world, due to the user's ability to customize the software for their specific network's needs and priorities. The open-source nature of this solution allows a vast community of individuals to build or customize their own rules to better combat various forms of abusive content. This approach is heavily focused on both a set of rules maintained by the user community combining content and statistical matching (using a series of scores that are given both positive and negative weightings against each message) to determine the likelihood of a message being spam. The resulting score will determine the delivery location of the message. By default, less than five points will deliver to an inbox, five to 10 points will result in a quarantine/spam folder placement, and more than 10 will result in a message rejection or deletion.

SURBL

SURBL is a collection of lists of Uniform Resource Identifier (URI) hosts, typically website domains, that appear in unsolicited messages. These lists are mainly trap-driven or reports from trusted network partners, which are then evaluated for inclusion in one of their RBLs. SURBL focuses on several areas including abusive domains, phishing sites, malware links, and compromised sites used to hide spam links unknown to the site owner. By looking at URLs instead of message source (IP address), services like SURBL can detect spam campaigns across multiple sources when they are promoting the same destination URL.

CHAPTER 06

LEGISLATION

According to *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*[7], researchers found 86% of test subjects spent less than one minute reading terms of service, and a staggering 97% spent less than five minutes. Additionally, less than 2% noticed that by agreeing to the terms of services, they were actually "providing a first-born child" as payment for access to the test application.

If we heard it once during the Cambridge Analytica/ Facebook debacle, we heard it a million times: **"If you aren't paying for a product (or service), you are the product."**

There's a growing demand for data privacy and protection across the globe, and in response, we're seeing not just more stringent spam policies, but best practice development to better secure personal data shared online.

CAN-SPAM

The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act is a law setting rules for commercial email in the United States. This includes establishing requirements for commercial messages, giving recipients the option to stop receiving your email, and sets meaningful penalties for violations. These rules don't only apply to bulk email either, so even if you're sending marketing mail on a small scale, it needs to comply with the law.

Many of the rules laid out by CAN-SPAM are common sense practices, like avoiding being misleading in subject lines or content, clearly identifying the email is advertising, and so on. But it also includes some fine print information you might not consider necessary, like telling recipients where your business is located. You must always include an unsubscribe option and you must always (yes, always) honor those requests, lest you be subject to a hefty fine.

> **Since inception, the running joke among many in the email community is the CAN-SPAM Act does just that; it provides a set of guidelines which inform mailers how they (legally) 'can spam.'**

Greg Kraios

250ok founder and CEO

[7] Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465#%23

Canada’s Anti-Spam Legislation (CASL)

The Federal Anti-Spam Task Force (FAST-F) held several meetings over the course of a year and produced a highly-regarded document titled “Stopping Spam: Creating a Stronger, Safer Internet” in 2005. Many of the recommendations from this initial document went on to become the foundation of CASL, passed in 2010. After finally becoming law, a couple years passed before the regulations from the various enforcement agencies finalized, leading to a 2014 enforcement date. Today, infringements and “undertakings” roll in, penalizing businesses who use deceptive or simply unclear practices when emailing Canadians.

- Applies to commercial email
- Excludes “Transactional” messages such as welcome or confirmation emails
- Subscribers can receive commercial messages without prior consent
- Fines up to $16,000 USD per violation
- Must clearly identify the sender
- Must contain an unsubscribe mechanism

- Applies to commercial email, SMS, social media, instant message, and voice
- Includes “Transactional” messages such as welcome or confirmation emails
- Subscribers must give consent to receive commercial messages
- Fines up to $10 million CAD for corporations and up to $1 million CAD for individuals, imprisonment, liability of the business owner if employees fail to comply
- Must clearly identify the sender
- Must contain an unsubscribe mechanism

General Data Protection Regulation (GDPR)

GDPR is the new EU privacy regulation related to data protection laws replacing the existing Data Protection Directive (95/46/EC) and adding additional requirements for organizations. GDPR limits the amount of consumer data collected, the length of time it may be stored, and how it can be used. The data protection regimen extends the scope of the existing data protection laws to include all companies, even those outside of the EU if they process the data of EU residents. Now that GDPR is fully activated, companies or organizations not in compliance could be the target of significant fines.

We cannot stress this enough: GDPR focuses on the personal data of EU residents, not the geographical location of the organization. Companies not located in the EU but handle and process the personal data of EU residents are expected to comply with the legislation. This could also cover a company that manages or processes the data of a third party operating within the EU.

Put plainly, if you email someone who resides in the EU, you have to comply with GDPR. Period.

To effectively send email marketing communications under GDPR, you will need to collect “a freely given, specific, informed and unambiguous consent” (Article 7) or be able to prove a “lawful reason” for processing (Article 6). To achieve compliance, you must adopt new practices:

1. Use opt-in permission rules when collecting data.
2. Ensure you have strong proof-of-consent management systems.
3. Provide tools or contacts through which consumers can request their personal information be removed from your systems.
4. Maintain proper documentation showing the “lawfulness of processing” each record.

Some consultants recommend using a confirmed opt-in to align with the enhanced permission requirements under GDPR. Also, make it clear, easy, and foolproof to unsubscribe to your emails, and honor the unsubscribe request promptly.

Other Policies Worldwide

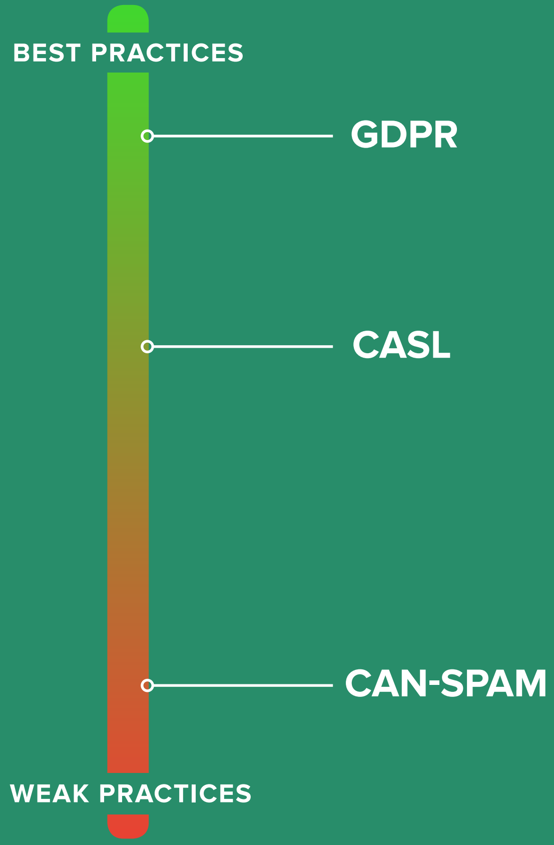
While other global policies are less known or rarely included in marketing discussions, there is more legislation you need to be aware of if you email to areas outside North America and the European Union.

For a deeper dive into policies by country, check out this comprehensive guidebook[8] from the Email Experience Council (eec).

[8] Source: S.250ok.com/EECguide

EMAIL LEGISLATION

Legislation ranges from making sure marketers are being cognizant and responsible with recipients' personal data, to simply making sure advertisers aren't outright lying in their emails. Different countries prioritize different things, so if you want to understand how particular legislation falls on a scale from encouraging really great emails to just making sure emails aren't pieces of misleading garbage, check out the scale to the right.



CHAPTER 07

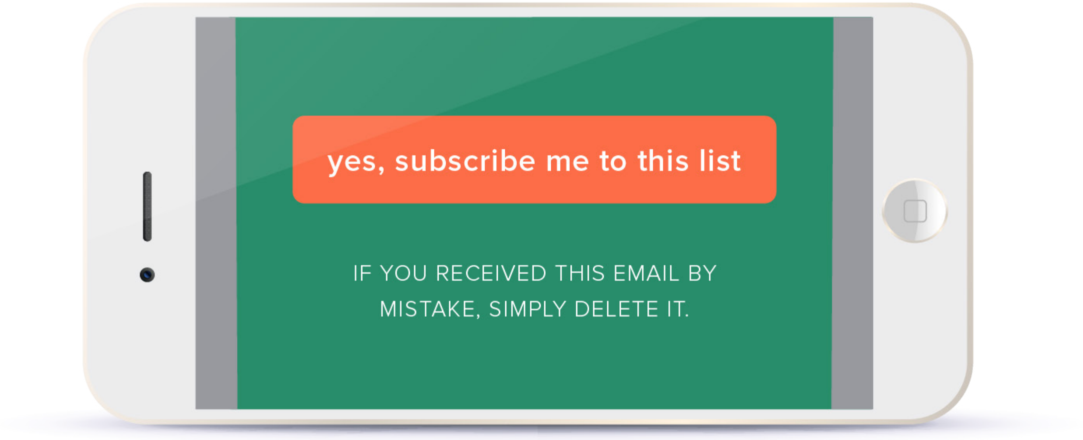
MARKETING EMAIL BEST PRACTICES

FOR REPUTATION AND RECIPIENT SATISFACTION

Single Opt-In vs. Confirmed Opt-In

In most instances, entering an email address and selecting to opt-in to the email list is probably enough. But we'd recommend moving away from this kind of single opt-in and making your best practice and standard a confirmed opt-in (also known as double opt-in, as shown in figure 1.4). What does that mean? After your recipient enters their email address, send them a welcome email asking them to complete one more step—usually clicking a link to confirm their intention to subscribe to your email list. While some may not take that step, those that do are a more qualified recipient, and are likely less prone to mark your emails as spam and interact/open them on an ongoing basis. Plus, as legislation moves towards needing records of clear intent and full comprehension of what "consent" means, having this extra step will be an asset if ever needed.

figure 1.4 Confirmed Opt-in



IF YOU RECEIVED THIS EMAIL BY MISTAKE, SIMPLY DELETE IT.

Welcome Emails

Most marketing email programs offer some kind of incentive to entice a consumer to opt-in. Of course, if you'd offered a discount or other premium, the first email you send to that recipient should be what you've promised (unless you took our advice about confirmed opt-in!) and it should be relatively soon. We looked at how e-retailers collected list sign-ups in 2017, and of the retailers studied, 73% sent their welcome email within 24 hours of sign-up.

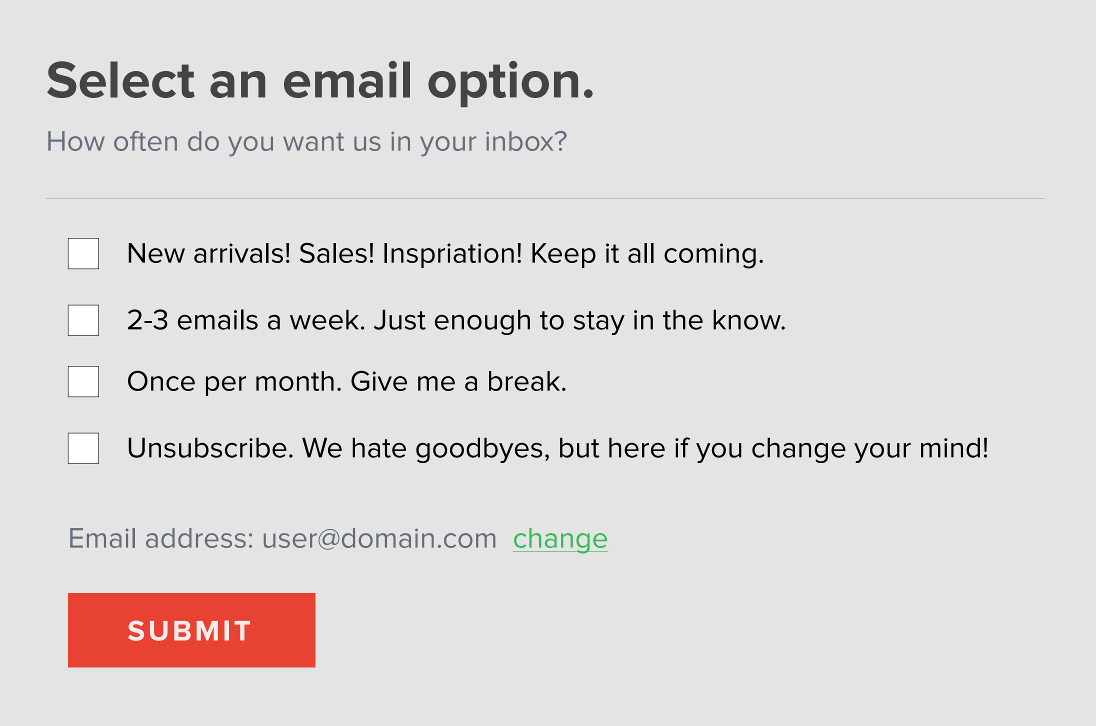
However, we have a better idea. Why not transition to a welcome email series? This is the perfect opportunity to educate new subscribers about your brand or loyalty program. You can break them up into logical, manageable chunks as to not overwhelm them with information. Try dedicated emails for account management tips, FAQs, loyalty program rules or guidelines, and more.

Don't forget—if you're emailing recipients in the EU, you should likely send an email covering their data rights.

Preference Centers

When collecting information about subscribers, it's common to ask just a few questions (figure 1.5) to get the users consent and then request they file all their communications preferences and additional personal details in a "Preference Center." These can be built to manage user profiles and communication needs, which could include address, frequency of communication, newsletter selection, and other relevant information. It's easiest to prompt users to do this during the welcome email series, at the bottom of each email as part of the unsubscribe process, or after a significant change in an email program.

figure 1.5 Preference Center



Select an email option.

How often do you want us in your inbox?

□ New arrivals! Sales! Inspriation! Keep it all coming.

□ 2-3 emails a week. Just enough to stay in the know.

□ Once per month. Give me a break.

□ Unsubscribe. We hate goodbyes, but here if you change your mind!

Email address: user@domain.com change

CHAPTER 08

HOW TO CREATE RELEVANT, EFFECTIVE EMAIL

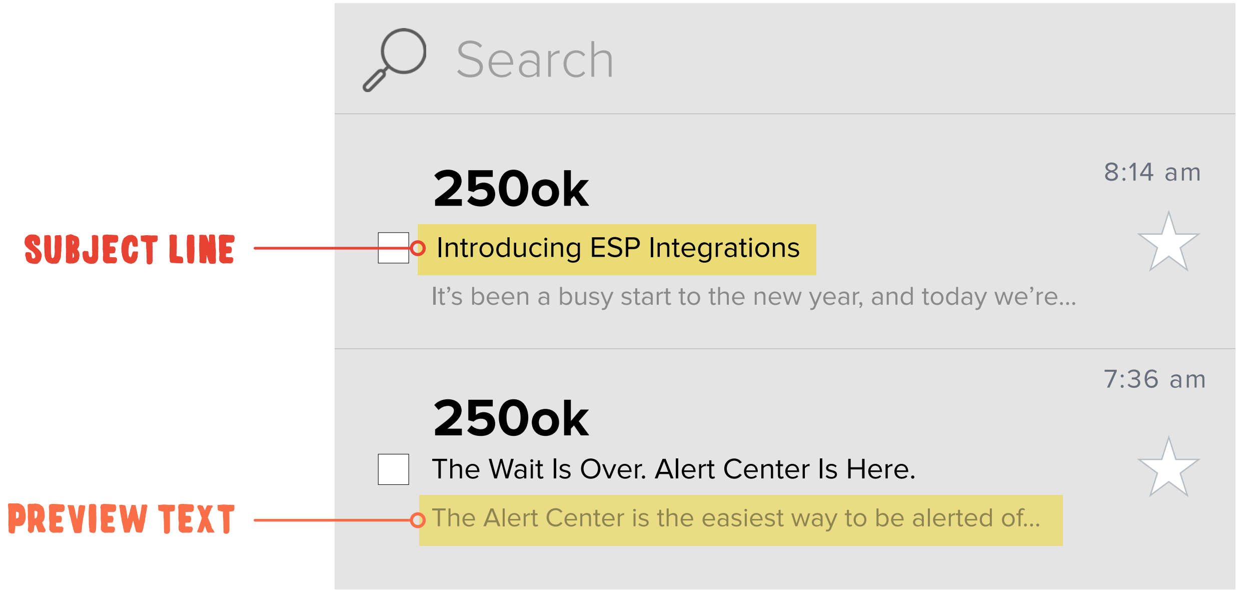
Building an email isn't rocket science, but it can sure feel like it. Your goal is to increase open rates, engagement, and conversions. But...are you making it easy for customers to engage within the inbox? Design plays a major role in how people interact with your email. Not all subscribers engage with the same methods, but there are a few imperative practices to follow when designing your campaign.

Subject Lines and Preview Text

Whoever said, "Don't judge a book by its cover," hasn't met email subject lines. According to Consumer Pulse, 47% of email recipients decide whether or not to open an email based on subject line alone. Don't let your subject line stand in the way of engagement. The greatest email is worthless if it doesn't get opened. Keep it simple, short, and relevant. Know your audience and appeal to them. Explore using emojis every now and then, but test the subject line in preview before sending—not all email clients support emojis.

Preview text adds valuable context to your subject line and can help your open rate. Subject line and preview text should work together and be accessible for all subscribers (figure 1.6). Use this space to clue in your customer to why the email is useful to them. Preview text is pulled from the first few lines of text within an email. Avoid the default preheader showing ("*Is this email not working correctly? View in browser*") by hiding preview text[9] in the body of your campaign. When hidden, there is no limit on the length of preview text. Go ahead and write out a full preview. Those who use email readers like Apple's Siri appreciate the extra content.

figure 1.6 Subject Line and Preview Text



8:14 am
250ok
□ Introducing ESP Integrations
It's been a busy start to the new year, and today we're...

7:36 am
250ok
□ The Wait Is Over. Alert Center Is Here.
The Alert Center is the easiest way to be alerted of...

[9] Source: https://litmus.com/blog/the-ultimate-guide-to-preview-text-support

Email Framework

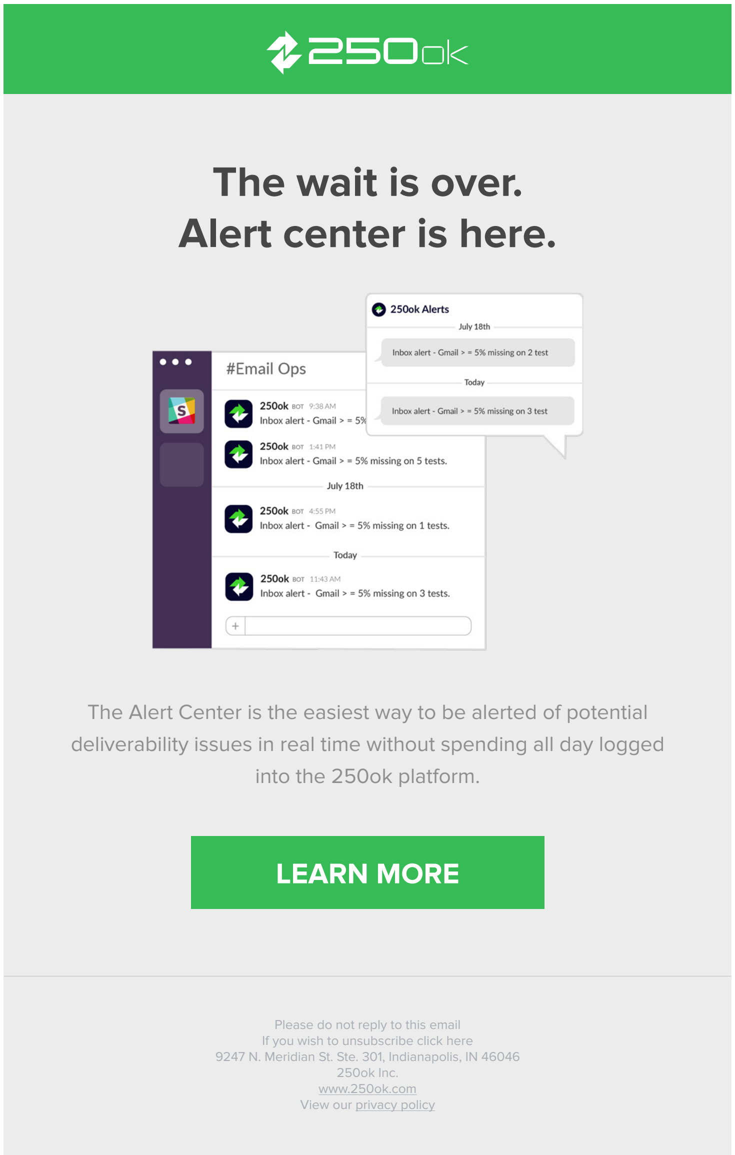
Are you making engagement easy? In order to gain clicks from your audience, make it as simple as possible for them to do so. Framing your campaign to fit within an email client's preview window will lower the risk of losing a subscriber to scrolling. And yes, this includes mobile and tablet readers. More than 60% of users are opening on mobile, so build a responsive email to give your subscribers a clear view of your campaign regardless of the device. Use a single column design to not only make it easy to optimize for mobile, but for readers to scan material efficiently. If you use email programs with a pre-built template, many of these framework concerns are addressed. Take advantage of their preview mode to be sure its optimizing properly.

Content Hierarchy

How are you structuring your content to reach engagement? Placing a bold phrase or compelling image at the top of the email will entice the subscriber to actually scroll. Below, use additional content to describe your purpose. Give the audience a clear idea what to do next. Whether they skimmed or read the email, a defined, well-positioned call-to-action (CTA) button will help them decided. By creating an unambiguous hierarchy, you're leading readers to an enticing link to click.

Email length is not an issue when hierarchy is in place. Group information into sections to create clear resting points in between. Subscribers will scroll if the content is relevant. Stay cautious of your email's size in bytes, though—going over 100kb will clip your email with clients like Gmail.

figure 1.7 Email Example



250ok

The wait is over.
Alert center is here.

250ok Alerts

July 18th

Inbox alert - Gmail > = 5% missing on 2 test

Today

Inbox alert - Gmail > = 5% missing on 3 test

#Email Ops

250ok BOT 9:38 AM
Inbox alert - Gmail > = 5%

250ok BOT 1:41 PM
Inbox alert - Gmail > = 5% missing on 5 tests.

July 18th

250ok BOT 4:55 PM
Inbox alert - Gmail > = 5% missing on 1 tests.

Today

250ok BOT 11:43 AM
Inbox alert - Gmail > = 5% missing on 3 tests.

The Alert Center is the easiest way to be alerted of potential deliverability issues in real time without spending all day logged into the 250ok platform.

LEARN MORE

Please do not reply to this email
If you wish to unsubscribe click here
9247 N. Meridian St. Ste. 301, Indianapolis, IN 46046
250ok Inc.
www.250ok.com
View our privacy policy

Personalization

Campaigns sent to segmented lists and contain relevant information increases open rates by 20-40%. Subscribers are more likely to engage with relevant content. Focus on gender, location, and age to personalize the email experience. Tactics like abandoned cart and purchase history are deliberate reminders for the reader to return to what feels familiar. So instead of sending one campaign to everyone, you should segment your lists and send relevant content and offers to each unique audience.

Visual Accessibility

Not all viewers and email clients will allow downloadable images. If you rely on images to communicate your campaign, some subscriber might miss out. Going image-only on a campaign can drain users' data plans and exclude the visually impaired. As backup, include descriptive alt-text for each image. The industry recommendation is 60:40 text-to-image ratio for good reason.

Finding the right font to work across all email clients may be a struggle. Only a small number are universally considered email-safe: Arial, Georgia, Century Gothic, Helvetica, to name a few. If your brand favors a font considered noncompliant, find a fallback to ensure the integrity of your design.

Stay on Brand

Your subscriber needs to know the campaign is coming from you. Coordinate your email to the company brand—colors, fonts, logo, and voice should match across all other customer touchpoints. Staying on-brand strengthens your credibility, creating a level of trust between you and the subscriber. The safer your audience feels, the better chance you have of gaining a click-through.

Testing

The anxiety of sending an email to hundreds, thousands, or hundreds of thousands of people is often a lot for people to handle. But don't worry, there are several tools to help alleviate this stress and anxiety before you press the send button. First, you should use a design testing tool, like 250ok Design[10], to help you understand how your messages will appear in dozens of email clients without having to maintain accounts, phones, or multiple versions of Outlook on your desktop. The second tool is 250ok Inbox[11], a seed-based testing platform used to evaluate how a message should deliver to consumers at the tested domains. Using these tools to predict your campaigns behavior before sending emails to your live audience can greatly help reduce that post-send anxiety.

[10] 250ok Design: https://250ok.com/tour/design/

[11] 250ok Inbox: https://250ok.com/tour/inbox/

CHAPTER 09

SUMMARY

This is a lot of information. It can be confusing, and when you're dealing with budgets and success, it can be downright scary. But we hope the information we covered in this guide helps you cut through the wilderness that is email, and helps you feel at least a little more knowledgeable and confident in your ability to email responsibly. Undoubtedly, there are complexities and nuance that have no place in a primer to get you simply up-to-speed on deliverability, but that's why we're here. To help you help your email. If you have questions, want more assistance in setting yourself up for success, or have deliverability issues you need help resolving, don't hesitate to reach out to us.

CHAPTER 10

APPENDIX

Acceptance rate: The percentage of emails in a campaign that pass mail server filters without being blocked or marked as spam.

Deliverability: The ability or inability to deliver email to a specific inbox.

Confirmed or double opt-in: Same as a single opt-in but with the addition of a confirmation step.

Email blacklists: Lists created to identify “known” spammer IPs and domains. It is common practice for internet service providers (ISPs) to blacklist the IPs and domains of suspected spammers.

Email blocking: Occurs when the receiving email server blocks incoming mail. Mail services (AOL, Gmail, Yahoo, etc.) will often block email from reaching the inbox when the sender is a suspected spammer.

Hard bounce: The permanent delivery failure of an email for a number of reasons, most commonly a non-existent email address.

Open rate: The percentage of opened emails in an email campaign.

Preheader: Text that appears visually above the header in the email body.

Preview Text: The short summary text that immediately follows the subject line when viewing an email in an inbox. Copy is pulled from the first few lines of email body text.

Single opt-in: An individual adding their email address to a mailing list usually by filling out a web form without a subsequent confirmation step.

Soft bounce: Delivery failure isn't permanent and is caused by a temporary issue.

Spam: Email sent to a recipient who did not consent to be emailed.

Spam report: Report of an email being marked as spam, accurately or not.

Spam trap: Email recognized by a server as going to an invalid address, which is automatically reported as spam.

CHAPTER 11

ABOUT

Matthew Vernhout (CIPP/C)

Director of Privacy, 250ok

Matthew Vernhout is the Director of Privacy at 250ok and is a Certified International Privacy Professional (Canada) with nearly two decades of experience in email marketing. He actively shares his expertise on industry trends, serving as director at large of the Coalition Against Unsolicited Commercial Email (CAUCE), vice chair of the Email Experience Council's (eec) Advocacy Subcommittee, and senior administrator of the Email Marketing Gurus group. He is a trusted industry thought-leader, speaking frequently at email marketing and technology conferences around the globe. Matthew has contributed to several benchmark publications during his career including *DMARC Adoptions Among e-Retailers*, *eec Global Email Marketing Compliance Guide*, *The Impact of CASL on Email Marketing*, and more.

Tim Moore

SVP of Customers Solutions, 250ok

Tim is the Senior Vice President of Customer Solutions at 250ok and an email deliverability expert. He became the “Swiss army knife” of the deliverability world through combined experiences at a traditional ESP (Oracle Marketing Cloud), a cloud-based ESP (Message Bus), and a third-party vendor (Return Path).

Alex Eilmann

Designer, 250ok

Alexandra is the Designer at 250ok. She joined the company in its infancy, acquiring creative and email design best practices by being the driving force behind 250ok’s evolving visual brand.

Sloan Simmons

Solutions Consultant, 250ok

Sloan is a Solutions Consultant at 250ok, where he serves as a go-to resource for customers and employees alike. With more than five years of deliverability and email privacy experience, including direct knowledge from Marketo, he provides expert insight on optimizing and improving email programs across the globe.

250ok

250ok focuses on advanced email analytics, insight and deliverability technology to power a large and growing number of enterprise email programs ranging from clients like eHarmony, Pinterest, and Furniture Row who depend on 250ok to cut through big data noise and provide actionable, real-time analytics to maximize email performance.

For more information, visit 250ok.com.