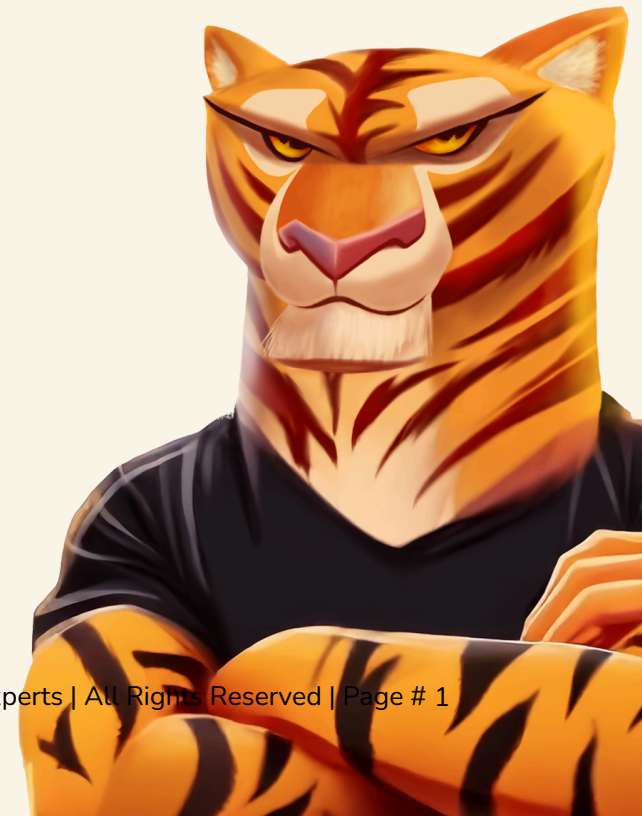
warmy
Email Channel. Reliable.

March 2025

# Understanding ESP Blocks: Causes, Types, and Prevention

Email Service Providers (ESPs) like Gmail, Outlook (Hotmail/Live/MS365), and G Suite (Google Workspace) use sophisticated filters to protect users from spam. For businesses relying on email outreach, it's critical to understand why emails get blocked or sent to spam, how to recognize blocks, and what steps to take to ensure messages reach the inbox.

This report provides an in-depth analysis of ESP blocks – covering their causes, how to identify different block types, ways to alleviate and prevent them, differences among major providers, expert insights, and best practices to maximize deliverability.



# About Warmy and the Research Team

Warmy is the leading email deliverability technology, helping businesses improve their inbox placement, sender reputation, and overall email performance. Powered by AI-driven strategies.

The Warmy Research Team is a dedicated group of email deliverability-certified experts focused on analyzing and optimizing email-sending practices.

Through continuous testing, data-driven insights, and innovative methodologies, they uncover factors that impact deliverability and translate findings into actionable improvements for Warmy's platform. Their expertise helps businesses navigate the complexities of email deliverability with confidence.

**Daniel Shnaider**
Deliverability Expert

**Alexandr Panchenko**
Technical Deliverability Expert

**Vahagn Shirinyan**
Senior Deliverability Expert

**Max Popov**
Senior Deliverability Expert

**Oleksiy Lutskin**
Deliverability Expert

**Artem Klymenko**
Deliverability Expert

**Bohdan Tsapenko**
Head of Research Team

warmy

The Warmy.io team

# Table of contents

# Key points or TL:DR

**Sender Reputation is Paramount:**

- Poor reputation—stemming from new domains or IPs, sudden volume spikes, high bounce rates, and low engagement—remains the leading cause of ESP blocks. Maintaining a positive reputation is crucial for inbox placement.

**Authentication is Essential:**

- Properly configured SPF, DKIM, and DMARC records are non-negotiable. These authentication methods verify your sender identity, dramatically reducing the risk of blocks by ensuring emails are trusted by ESPs.

**Content Matters in Context:**

- While individual “spam trigger” words are less influential on their own, spammy content (excessive links, attachments, and overtly promotional language) combined with other risk factors can elevate your risk of being flagged.

**Volume and Sending Patterns Impact Deliverability:**

- Rapidly ramping up email volume can trigger temporary (soft) or permanent (hard) blocks. A gradual warm-up strategy is recommended to build credibility and avoid triggering ISP thresholds.

**Provider-Specific Differences:**

- Gmail and G Suite emphasize engagement metrics and domain reputation, whereas Outlook/MS365 focuses more on IP reputation and blacklist status. Understanding these nuances allows for tailored strategies based on the target provider.

**Proactive List Hygiene is Critical:**

- Maintaining clean mailing lists by removing invalid addresses and spam traps is essential to keep bounce rates low, thereby protecting your sender’s reputation and overall deliverability.

**Continuous Monitoring and Adaptation:**

- Using tools like Gmail Postmaster Tools and Microsoft SNDS for real-time insights helps detect issues early and adjust practices accordingly, ensuring sustained email deliverability over time.

# Causes of Email Provider Blocks

- **Sender Reputation (Domain/IP)** – ESPs heavily favor senders with good reputations. If your sending IP address or domain has a history of spam or low engagement, providers may block or junk your emails. For example, Gmail may flag messages from a domain with "very low reputation" as suspicious and block them Microsoft's filters likewise block IPs with poor reputation; Outlook might return "550 5.7.1 … blocked using Spamhaus" if your IP or domain appears on a spam blacklist.

- **New domains or IPs** start with no reputation and are especially vulnerable – sudden high-volume sending from a fresh domain often triggers deferrals or blocks until you establish credibility.

- **Lack of Authentication** – Messages that aren't properly authenticated with DNS records are frequently rejected as spam. SPF, DKIM, and DMARC are essential to verify your identity. Gmail now requires senders to authenticate via SPF or DKIM; if you don't, Gmail will block the message as "unauthenticated".

- **Similarly, Outlook/Office365 expects valid SPF (and honors DKIM/DMARC if configured)** – failing these checks can land your email in junk or result in a bounce. Proper DNS MX and reverse-DNS records for your domain are also important so your server isn't seen as suspicious.

- **Spammy Content and Keywords** – The actual content of your email can raise red flags. Excessive use of "spam trigger" keywords (free money, winner, etc.), all-caps subject lines, or overuse of exclamation points used to be common causes of spam filtering. Modern filters take a more holistic approach, but content still matters. As deliverability experts note, today's spam filters consider overall context – "certain words can trigger spam filters, but modern filters are much more sophisticated and take a holistic view of your email content, sender reputation, and engagement".

- **In short,** a few marketing phrases won't kill your campaign if your reputation is strong, but blatantly spammy or deceptive content (like phishing-like text, misleading subject lines, or gibberish) can trip filters. **Links and attachments** are also scrutinized – messages with multiple links or dangerous attachment types can be blocked. It's best to avoid attaching large files or using numerous or URL-shortened links in cold emails, especially from a new sender, as these can appear spammy.

- **Sudden Volume Spikes** – How you ramp up your sending volume matters. Sending too many emails, too quickly (relative to your normal pattern) is a common trigger for ESP rate-limiting. For instance, if a new Gmail account that's meant to send ~500 emails/day suddenly tries to send thousands, Gmail may temporarily defer those emails with an error like "421-4.7.0 [TSS04] Messages from your IP address temporarily deferred due to unexpected volume".

- **ESPs** interpret sudden surges as a sign of a possible spam outbreak or compromised account. Unusual traffic patterns without a sending history will cause blocks until the sender "cools off." Always increase the volume gradually (a process known as warming up) to build trust. Many providers have explicit limits for new senders – e.g. a brand-new Gmail may only allow ~20 emails/hour initially. Exceeding these limits can get the account flagged or disabled for 24 hours.

- **Low Engagement & Spam Complaints** – ESPs like Gmail and Outlook monitor how recipients interact with your messages. If too many users delete your emails without reading or mark them as spam, your sender's reputation suffers. Gmail, in particular, uses engagement metrics (opens, replies, spam reports) as a major factor in deliverability. They advise bulk senders to keep spam complaint rates under 0.3% – that's no more than 3 complaints per 1,000 emails. Exceeding that can quickly lead to Gmail throttling or spam-foldering your messages.

- **Microsoft** has similar thresholds; one industry source notes that as little as 0.5% of users marking mail as spam can degrade your ability to reach Outlook inboxes. On the flip side, positive engagement (opens, clicks, replies) boosts reputation. A "poor reply rate" – i.e. almost no one ever replies to your outreach – is a red flag in cold emailing, whereas senders "that have plenty of replies have no issues with spam".

- **In short,** emails that generate no engagement and occasional complaints will be seen as unwelcome. List quality is crucial here: sending to unengaged or uninterested recipients (or non-opt-in contacts) will drive up spam complaints and blocks.

- **Bad Mailing Lists (Bounces and Spam Traps)** – Mailing to invalid or stale addresses can get you blocked. High bounce rates, especially many "user not found" hard bounces, suggest poor list hygiene. ISPs interpret a high invalid address rate as indicative of spamming or email harvesting. ("Normal" unknown-user bounce rates are under 2–3% for clean lists.) Worse, you might hit spam traps – inactive addresses used by anti-spam services to catch senders who don't clean their lists. Hitting traps or too many unknown users can land your IP/domain on blocklists.

- **Spamhaus**, one of the most widely used spam blocklists, explicitly lists senders of "unsolicited bulk email" and those caught by spam traps. If your domain or IP gets on a blacklist like Spamhaus or Barracuda, many providers will outright reject your emails. In fact, "Spamhaus's blocklists are widely used... If you end up on one, your email deliverability will be hit hard". This is why maintaining a clean list of valid, engaged contacts is vital – it prevents blocks due to excessive bounces or blacklistings.

- **Other factors** can contribute as well. Misconfigured technical headers (like missing a legitimate "From" address or improper HELO/EHLO identification) might cause certain strict servers to refuse email. Using a domain name similar to a known spammy domain can also bias filters against you (ESP filters sometimes group lookalike domains or factor in domain history).

In sum, spam filters assign risk scores to a combination of factors – hitting one or two triggers (e.g. a couple of "spammy" words, or a small volume spike) likely won't cause a block on their own, but multiple risk factors together will tip the balance. The most dangerous signals are those tied to user harm and fraud (high spam reports, forged identity, malware), which ESPs punish swiftly, whereas minor content issues carry less weight. Understanding these factors that lead to blocks helps in proactively avoiding them.

# Types of Blocks

Not all email blocks are the same. Mail providers may temporarily defer your messages or permanently reject them, depending on the severity of the issue. It's important to distinguish these outcomes and read bounce messages to diagnose the cause.

- **Temporary vs. Permanent Blocks**: A temporary block means the provider is currently deferring your emails but might accept them later once conditions improve. These often manifest as SMTP 4XX status codes (in the 400s range). For example, Gmail might respond with a 421 4.7.28 error for a temp block: "Our system has detected an unusual rate of unsolicited mail… mail sent from your IP has been temporarily rate limited". That 4.7.28 code indicates Gmail is throttling you (soft bounce) rather than outright banning – the server may retry later. Temporary blocks (also called soft bounces) often result from things like sending too fast, hitting rate limits, or a mild reputation issue that might recover (ESP might be saying "slow down" or "clean up your act" but not permanently rejecting you yet).

By contrast, a permanent block is a hard rejection (SMTP 5XX codes) – the provider refuses to deliver the message as is, and will not automatically retry. A common permanent bounce is 550 5.7.1 which often denotes a policy block or spam rejection. For instance, Outlook might return "550 5.7.606 Access denied, banned sending IP" or "550 5.7.1 Service unavailable, client host blocked using Spamhaus" when your IP is on a blacklist. A 550 error from Gmail saying "likely unsolicited mail… message has been blocked" is similarly a firm rejection.

In short: **4.X.X** codes = temporary issue (you may retry), **5.X.X** codes = permanent failure (you must address the problem before sending again).

- **Bounce Message Clues**: The bounce-back message (Non-Delivery Report) often contains text explaining the reason for the block. It may explicitly mention words like “temporarily deferred” or “permanently rejected” and sometimes a URL for more information. For example, Yahoo deferrals include links to their postmaster page and phrases like “temporarily deferred due to user complaints”.

Gmail rejections might reference their help center (“...visit Why has Gmail blocked my messages? - Gmail Help for more information” in the bounce).

Microsoft’s errors often include codes like 5.7.0–5.7.999 with subcodes; e.g., 5.7.606 or 5.7.511 often indicate the sender is blocked due to reputation or a blacklist and will point to a delisting page (such as the sender.office.com removal form).

Always read the bounce detail: it may say “message content rejected” (pointing to a spam content filter), “IP blocked” (reputation issue), “policy violation,” “blacklist,” “over quota” (recipient mailbox full), etc. Sometimes the message is generic (“Message blocked” with no detail), in which case you have to investigate other factors (checking your reputation, authentication, etc.). SMTP reply codes are standardized to a degree – any 4.2.X or 4.7.X usually means a temporary deferral, often for volume or suspicion, whereas 5.1.X might mean addressing issues (invalid recipient, etc.) and 5.7.X specifically relates to security or policy (spam, auth failures, etc.) in many systems.

- **Reputation-Based Blocks**: Many blocks are triggered by sender reputation metrics. A few scenarios: if your IP or domain is on a known blacklist, the receiving server might reject it with a message referencing that list (as shown with Spamhaus above). If your recent sending to that provider has generated a lot of user spam complaints or low engagement, you may see "421 try again later" style throttling as a warning, escalating to "550 spam rejected" if you don't improve.

**Gmail Postmaster Tools** categorize domain reputation as High, Medium, Low, or Bad – a "Bad" reputation will result in many of your messages being spam-foldered or blocked outright.

**Outlook's Smart Network Data Services (SNDS)** similarly gives insight into IP reputation at Outlook.com; if it shows a poor color rating, you can expect blocks or junking until it improves.

---

- **Volume-based blocks are related** – if you exceed a provider's implicit thresholds for an unfamiliar sender, you'll get temp failures. Hotmail/Outlook.com historically limited new IPs to around 10,000 emails/day until its reputation improved. During that "probation," they would delay excess emails. So, a sudden spike might manifest as a 4XX refusal that later goes away once volume is reduced or spread out.

---

- **Blacklist Correlations**: ESPs often rely on third-party blacklists and their own internal lists. We mentioned Spamhaus; another common one is Barracuda. Microsoft specifically is known to use Spamhaus data and also have ties with Barracuda's blocklist for Office 365. If you see an error referencing Barracuda (for example, a bounce that says your message was blocked by "Barracuda Email Security" or a code pointing to their site), it means your sender info matched a pattern they block. Google's consumer Gmail doesn't publicly admit using third-party blacklists, but if your sending domain/IP is on a major blacklist, all providers (Google included) might treat your mail suspiciously. In the Warmy community notes, it's observed that Gmail block incidents can correlate with Spamhaus/Barracuda listings.

- **Reputation-Based Blocks**: Many blocks are triggered by sender reputation metrics. A few scenarios: if your IP or domain is on a known blacklist, the receiving server might reject it with a message referencing that list (as shown with Spamhaus above). If your recent sending to that provider has generated a lot of user spam complaints or low engagement, you may see "421 try again later" style throttling as a warning, escalating to "550 spam rejected" if you don't improve.

**Gmail Postmaster Tools** categorize domain reputation as High, Medium, Low, or Bad – a "Bad" reputation will result in many of your messages being spam-foldered or blocked outright.

**Outlook's Smart Network Data Services (SNDS)** similarly gives insight into IP reputation at Outlook.com; if it shows a poor color rating, you can expect blocks or junking until it improves.

---

- **Volume-based blocks are related** – if you exceed a provider's implicit thresholds for an unfamiliar sender, you'll get temp failures. Hotmail/Outlook.com historically limited new IPs to around 10,000 emails/day until its reputation improved. During that "probation," they would delay excess emails. So, a sudden spike might manifest as a 4XX refusal that later goes away once volume is reduced or spread out.

---

- **Blacklist Correlations**: ESPs often rely on third-party blacklists and their own internal lists. We mentioned Spamhaus; another common one is Barracuda. Microsoft specifically is known to use Spamhaus data and also have ties with Barracuda's blocklist for Office 365. If you see an error referencing Barracuda (for example, a bounce that says your message was blocked by "Barracuda Email Security" or a code pointing to their site), it means your sender info matched a pattern they block. Google's consumer Gmail doesn't publicly admit using third-party blacklists, but if your sending domain/IP is on a major blacklist, all providers (Google included) might treat your mail suspiciously. In the Warmy community notes, it's observed that Gmail block incidents can correlate with Spamhaus/Barracuda listings.

# Identifying the Block Type

To summarize, when you receive a bounce or notice emails aren't arriving:

- **Check the SMTP code** (4xx vs 5xx) to see if it's temporary or permanent. A soft bounce (4xx) suggests you should slow down and retry later, whereas a hard bounce (5xx) means you must change something before resending.

- **Read the message text** for clues: look for words like "deferred," "temporarily," "permanently," "blocked," "spam," "reputation," "blacklist," etc.

- **Examine any included links or references**. ESPs sometimes include links to their postmaster support pages or error code explanations. For instance, Yahoo's bounce might point you to postmaster.yahooinc.com/error-codes for the code TSS04 (their throttling code). Gmail often cites a help article number (e.g., 188131 or 2451690) that corresponds to Gmail's guidelines or DMARC info.

- **Look at which provider is blocking** – if all bounces are from, say, Gmail recipients, then focus on Gmail-specific causes (your domain's Gmail reputation, Google's sending limits, etc.). If it's across multiple ISPs, the issue may be broader (your domain on a blacklist, or content that many filters flag).

By identifying the nature of the block, you can decide on the next steps: whether it's a waiting game (temporary throttling) or requires immediate fixes (authentication, contacting a blacklist, list cleanup). The bounce codes are essentially diagnostic signals that, when interpreted correctly, point to the root cause of the block.

# How to Alleviate and Prevent Blocks

Preventing email blocks (and spam folder placement) requires a combination of good sending practices, technical setup, and proactive reputation management. Here are key strategies to alleviate an ongoing block and prevent future issues:

## Warm Up Your Domain And IP

If you're starting with a new email domain or IP address, don't blast out emails at full volume on day one. ISPs need to see a history of responsible sending. Begin with a low send volume and gradually increase it over days or weeks. This warm-up period lets you build a positive reputation (through consistent delivery and hopefully some engagement) without tripping alarms.

For example, when warming a new IP for Outlook.com, one recommendation was to start around 2,000 messages, then double each day as long as no blocks occur. If you hit a deferral (like an Outlook error saying you've reached a limit), slow down until it clears.

Gmail likewise should be ramped up carefully; one guideline is to keep it to a few hundred a day initially. In fact, Gmail defines bulk senders as anyone sending over 5,000/day and will be especially watchful as you approach that.

Using a tool like Warmy can automate this process – they send gradual test emails and even generate positive interactions (replies, opens) to train mailbox providers that your address is legitimate. Warming can take a couple of weeks of gradually increasing send counts.

The key is consistency: don't go from 50 emails one day to 5,000 the next. Increase in measured steps and monitor for any soft bounces or warnings. This approach will prevent many volume-related blocks.

## Implement Proper Email Authentication (SPF, DKIM, DMARC)

**SPF (Sender Policy Framework)** specifies which mail servers are allowed to send on behalf of your domain.

**DKIM (DomainKeys Identified Mail)** adds a cryptographic signature to your email headers, which receiving servers verify using your public DNS key, ensuring the message wasn't tampered with and is truly from your domain.

**DMARC** builds on SPF/DKIM by telling receivers how to handle messages that fail those checks and providing you with reports.

Having all three in place is now an industry standard best practice – Google and Yahoo's new guidelines (2024) mandate DKIM, SPF, and a DMARC policy for senders at scale. Without these, your emails are more likely to be mistrusted or outright refused. For instance, Gmail will reject unauthenticated mail with a 5.7.26 error ("The sender must authenticate with at least one of SPF or DKIM").

Ensure your SPF record isn't too broad (it should include all your sending services' IPs) and doesn't exceed DNS lookup limits. Configure DKIM on your sending platform (many email services handle this for you by giving you a DKIM key to publish in DNS). Finally, set a DMARC policy (start with "p=none" for monitoring, then move to "quarantine" or "reject" as you gain confidence) – this not only protects your brand from spoofing, but also signals to receivers that you're a legitimate sender in control of your domain. Proper authentication boosts your credibility and is often the first thing to fix if you're experiencing deliverability issues.

# Optimize Email Content

Crafting your email content to avoid spam triggers can significantly help inbox placement. While, as noted, content is not the sole determinant, it still plays a role.

- **Avoid obvious spam tropes**: excessive use of all-caps, "$$$ MAKE MONEY!!!", too many emojis, or words like "Viagra" (unless that's legitimately your product!) will trip filters or at least look unprofessional. Modern filters use advanced algorithms – for example, Outlook's SmartScreen filter uses machine learning and customer feedback to evaluate content's spam probability. This means it's not just specific words, but the overall pattern and similarity to known spam that matters. To be safe:

- **Use a natural, professional tone in your emails**. If it's a cold outreach, personalize it so it doesn't read like a mass mail.

- **Include text that is unique to each recipient** (merging in their name, company, or details) – not only does this help engagement, it also differentiates the content. Spam filters notice when you send the exact same text to hundreds of people; using some dynamic fields or Spintax (spinning text) can make each email slightly different, which Warmy recommends to improve deliverability.

- **Limit the number of links and avoid risky links**. Don't include dozens of URLs or link to known blacklisted domains. A good rule is no more than one link in a cold email (e.g. maybe a link to your company site or a calendar invite).

If you must include a link, make sure the domain of that link has a good reputation (if you're using a link tracker or URL shortener, be cautious – some spam filters flag those). Similarly, be careful with attachments – sending an unexpected attachment (especially .zip, .exe, etc.) to cold contacts is a fast track to spam. If you need to send a file, consider linking to it instead, or wait until the recipient engages.

- **Provide an unsubscribe option for bulk mail**. If you're sending marketing emails (even cold B2B outreach in some cases), including an unsubscribe link is legally required in many jurisdictions (CAN-SPAM, GDPR). But beyond legality, it's a pressure relief valve: it gives uninterested recipients a way out other than marking you as spam. Notably, Gmail and Yahoo now require a working unsubscribe method for large senders.

There is a nuance: one internal guide noted that unsubscribe links can slightly lower deliverability because it's an extra link (and a clear sign of bulk mail), but they "help reduce the risk of your emails being marked as spam.".

On balance, it's better to include the unsubscribe for outreach at scale – it's better to lose a prospect via an unsubscribe than to have them hit "Report Spam," which hurts you with the entire ISP.

- **Keep HTML simple (or use plain text)**. Messages that are plain-text or lightly formatted generally have fewer deliverability issues than complex HTML emails. Many cold emailers stick to a plain text format (possibly with a simple signature) to mimic a one-to-one email. If you do use HTML, avoid things like large images (especially as the only content), heavy use of different fonts/colors, or code errors. A good practice is to make sure your email looks like something a person crafted, not a flashy newsletter. Warmy's guide suggests using more text than images and even delaying adding any image (like a signature logo) until later emails in a sequence. This reduces the chance of spam filters flagging corporate newsletter-style templates in a cold outreach scenario.

## Follow Sending Best Practices

- **Send at a reasonable pace**. Do not hit the SMTP servers with too many connections or messages at once. For Outlook.com, Microsoft specifies no more than 500 simultaneous SMTP connections – most small senders won't hit that, but it illustrates that blasting out email without pacing can get you blocked. Use your sending software's throttling settings if available (e.g., send X emails per minute).

- **Respect provider-specific limits**. Every provider has sending limits, especially for individual accounts. Gmail's free accounts typically allow up to ~500 recipients per day; Google Workspace (paid G Suite) allows more (varies by plan, often 2,000). Outlook.com free accounts are around 300/day. Sending significantly more via those accounts will result in blocks. Even via SMTP relays or ESPs, if you're hitting one recipient domain too hard (hundreds of messages to Gmail in a minute), Gmail might start deferring you. So spread out sends over time.

As a guideline, Warmy suggests if sending directly from an inbox (like Gmail or Outlook), limit to 50–100 emails per day per inbox, distributed evenly throughout the day. This aligns with the idea of slow and steady output rather than big bursts.

- **Maintain a healthy mailing list**. List hygiene is critical. Remove addresses that consistently bounce (especially hard bounces). Remove or suppress users who never engage after a few attempts – continuing to send to unresponsive addresses can hurt your metrics. A high "unknown user" bounce rate will get Microsoft to think you're a list-bomber (they note that a high rate looks like email address harvesting behavior). They advise keeping unknown user rates under 2-3%.

Also, keep an eye out for typo domains (like gmial.com) which could be spam traps or just invalid. Use email verification tools to scrub your list periodically; this prevents bounces and can even catch spam traps or emails known to complain.

- **Honor unsubscribes and complaints**. If someone asks to be removed or hits “unsubscribe,” make sure they are taken off your send list promptly. Microsoft’s guidance through their feedback loop program is that you absolutely must not continue sending to people who complained.

Continuing to email users who marked you as spam will very quickly tank your reputation with that provider. Use Feedback Loop (FBL) services where available: for Outlook.com, you can sign up for Microsoft’s Junk Email Reporting Program (JMRP) to receive spam complaint reports.

Yahoo/AOL (now Verizon Media) also offer FBLs for qualified senders. Gmail doesn’t offer individual FBL, but their Postmaster Tools will show aggregate spam report rates.

- **Monitor engagement and prune inactive contacts**. This is more applicable for marketing/newsletter senders, but even in sales outreach, it can help to remove or reduce emailing those who never respond. Mailbox providers like Gmail track if a recipient consistently ignores your emails – if a large fraction of your list never opens or clicks, over time Gmail’s algorithm might start placing your mails in spam for those users (or generally lower your sender reputation). Thus, it can boost deliverability to periodically sunset or “cool off” inactive recipients.

Sending a re-engagement email (“Hey, haven’t heard from you, should I stop emailing?”) and then removing non-responders can keep your list full of people who engage, thereby improving your reputation metrics.

# Responding to a Block

What if you're already blocked? Here are steps to alleviate and recover:

- **Stop and Analyze**: The first step is to analyze which of the above issues is present. Check your authentication, send volume, content, list, and see what likely went wrong (e.g., did you send a campaign that triggered a spam trap hit or a lot of complaints?). It's crucial to fix the root cause before trying to send more, otherwise you'll get blocked again.

- **Wait if Temporary**: If it's a temporary block (4XX errors), pausing sending to that domain for a day or two can help. ISPs often lift temp throttles after 24-72 hours of reduced activity. Use this time to implement improvements (e.g., lower your send rate, authenticate your domain, etc.), because if you resume without changes, you might escalate to a permanent block.

- **Reduce Volume and Frequency**: Back off the number of emails to that provider. If you were sending 1,000/day to Gmail when you got blocked, try sending a much smaller amount (say 100/day) once you resume, then slowly ramp back up. As noted in a Gmail context: "if blocked, reduce the volume to at least the level before the block" and probably even lower. This shows the ISP that you got the message and are behaving more cautiously.

- **Change Up Your Content**: Spam filters remember patterns. If a particular email content got flagged as spam, don't keep sending the exact same text. "Spam filters have a tendency to remember emails that were marked as spam. Rewriting emails after falling in spam helps.".

Consider tweaking your template – change the subject line, and phrasing, remove or alter links – so that when you attempt again, it's not an identical retry of the blocked message.

- **Check and Fix DNS/Auth issues**: Make sure your SPF, DKIM, etc. are all correct (use tools like MXToolbox or Gmail's Postmaster Tools to verify). If you find an issue (e.g., your SPF was missing an entry and causing "SPF fail" at receivers), fix it before attempting to resend.

# Use Provider Postmaster Support

Some providers have support channels for senders:

- **Google/Gmail**: Gmail doesn't have traditional support for senders unless you're a Gmail Workspace customer. However, you can use Gmail Postmaster Tools to monitor your status. If you see "Bad" domain reputation there, you know you need to drastically cut back and improve engagement.

Gmail's philosophy is generally to let reputation recover naturally over time with better practices; there isn't a form to fill out to be "unblocked" (their old mitigation form is only for rare cases and requires consistently good history afterward). So with Gmail, focus on slowly rebuilding your reputation (stop the bad sends, maybe send only to your most engaged contacts for a while, etc.).

- **Microsoft (Outlook/Hotmail/Office 365)**: Microsoft has a few tools. For Outlook.com (consumer), the Outlook.com  Deliverability Support form is available if you're following best practices and are still blocked – you can reach out and ask for guidance or unblocking. More directly, they have the delist portal at sender.office.com for Office 365/IP blocks.

If you get a bounce with a URL to that portal, go there, enter the blocked IP, and request delisting. This usually sends a verification email to you and if your IP isn't a known repeat spam offender, they often remove the block within 24 hours. Additionally, sign up for SNDS (Smart Network Data Services) if you send high volumes to Outlook – SNDS will tell you if Microsoft is seeing spam coming from your IP, and whether you're on their internal block lists.

- **Yahoo/AOL**: Yahoo (now under Verizon Media) has a support site for senders (Mail ) and a form for Yahoo Mail filtering issues. They also offer a feedback loop for complaints (through the Yahoo CFL program). If you find your emails to Yahoo are bouncing with a specific code, consult their SMTP error code page for what it means. For instance, a 421 4.7.0 [TSS04] from Yahoo is a temp block that usually clears in a few hours if no further spam is seen – continuing to resend during that window won't help.

- **Other Providers**: Many smaller providers or corporate mail servers might use spam firewalls like Barracuda, Proofpoint, or Mimecast. If a bounce points to those, you may need to contact the recipient's email admin to get unblocked or follow the instructions in the bounce (Barracuda sometimes provides a link to request removal if you believe it's an error). Public blacklists like Spamhaus we discussed; others include SpamCop, SORBS, etc., which have their own removal processes.

---

Additional methods include:

- **Investigating Blacklists**: If the bounce or your mail logs hint at a blacklist (mention of Spamhaus, Barracuda, etc.), go to those blacklist websites and look up your IP and domain. If listed, follow their delisting procedures. Spamhaus, for example, has lookup and removal request forms.

Resolve the cause first – e.g., if you got listed due to a compromised account sending spam, secure it; if it was due to hitting a spam trap, improve your list acquisition – then request delisting. Many blacklists will remove first-time offenders or accidental listings once you show the problem is fixed. Being delisted can take anywhere from hours to a couple of days, but it's crucial because as long as you're on a major blacklist, big ISPs will likely continue to block you.

- **Rotate to a New Sending Domain/IP (Last Resort)**: If a block is permanent and intractable, or your domain reputation is severely damaged, you may need to switch to a new domain or IP. The Warmy team notes, “If the block is permanent, you gotta buy a new mailbox” – essentially, you may need to retire the burned email/account and start fresh.

Similarly, some opt to move to a new sending domain if the old one is poisoned. Caution: This is a last resort because if you don’t fix the underlying issues, the new domain will likely get the same treatment.

But in cases where, say, your domain was unknowingly used by spammers in the past or your IP is on dozens of blocklists, starting anew (and then practicing good warm-up and hygiene) might be the quickest path. When you do this, consider adding new domains/inboxes and spreading out emails between them to “reduce pressure from any one mailbox”. This way, even if one gets blocked, it doesn’t halt all your outreach at once. Domain and inbox rotation is a common cold email strategy to mitigate risk – just be sure each new sender's identity also follows all best practices.

---

In summary, preventing blocks is about building and maintaining a good reputation – through authentication, responsible sending rates, clean lists, and engaging content – and promptly addressing any problems that do arise (temporary throttles, spam complaints, etc.). If you do this, you maximize your chances of landing in the inbox instead of the spam folder.

# Comparison of Email Providers' Filtering (Gmail vs. Outlook/Office365 vs. G Suite)

Every email provider has its own algorithms and policies for filtering spam and blocking senders. Here's how our key players stack up and differ:

## Gmail / Google Workspace (G Suite)

**Reputation and Engagement Focus**: Gmail is known for its sophisticated, engagement-based filtering. It uses hundreds of signals, but a standout is how users interact with your emails.

---

**User behavior heavily influences Gmail's spam filters**. If many recipients read and reply to your messages, you're more likely to reach the inbox. Conversely, if your emails are frequently deleted without being read or marked as spam, Gmail will start routing future emails to spam automatically for many users. This learning is largely automated and personalized; one user's spam is not necessarily spam for another if their engagement differs. (This is why sometimes one person sees your email in the inbox and another finds it in Gmail's spam folder.)

---

**Bulk Sender Guidelines**: Gmail's official guidelines for bulk senders (recently enforced more strictly) include three main requirements: **authenticate your emails with DKIM/SPF/DMARC, include a one-click unsubscribe, and keep spam complaint rates under 0.3%.**
If you fail these, Gmail may start deferring or blocking your mail. Initially, you might see 4XX deferrals (temporary), but continued non-compliance or high spam rates will result in 5XX rejections or spam placement. Google defines high-volume senders as >5,000 emails per day. Smaller senders have a bit more leeway but are still subject to the same principles.

---

**Throttle Limits**: Gmail (for Google Workspace accounts) typically allows a certain number of recipients per day (e.g., 2,000 for paid accounts, 500 for free Gmail). New accounts or domains might be implicitly limited to much less until reputation is established. Gmail will temporarily block sending (with a "you have reached a limit" error or a "421" deferral) if you go over their thresholds. They also have per-message recipient limits (like 100 recipients max on a free Gmail, which is not usually relevant to cold email since you'd send it individually).

**Filtering Mechanism**: Gmail's filters are largely machine-learning driven. They look at content, sender reputation (both IP and domain), authentication, and user feedback. Gmail does not offer a traditional feedback loop for spam complaints, but senders can use Google Postmaster Tools to see metrics on their domain: it shows **Domain Reputation, IP Reputation, Spam Rate, Feedback Loop (FBL) spam%, and more**. For instance, if your domain reputation is "Low" or "Bad" in Postmaster Tools, that explains inboxing problems – you'd need to improve it by reducing spam complaints and sending to more engaged users. Gmail also classifies mail by categories (Primary, Promotions, Updates, etc.) – while not a "block," landing in Promotions vs. Primary tab is another aspect of Gmail deliverability that marketers consider, though it's more about content/formatting than fundamental blocking.

---

**Recovery from Gmail Blocks**: Gmail doesn't have a manual unblocking support, so you must correct issues and slowly rebuild reputation. They will typically stop blocking once your sender reputation improves (which could take days or weeks of changed sending behavior). Severe issues like repeated phishing/spam might cause longer-term blocks; in extreme cases Google can blacklist a domain across all Gmail (rare, and usually tied to egregious spam or malicious content). Also, Gmail's system tends to "forget" or forgive reputation issues after a period of good sending – e.g., if you had a bad run but then stop sending for a while and come back with better practices, you might find deliverability gradually improves after 1-2 months, as long as users aren't still complaining.

---

**G Suite vs Gmail**: Google Workspace (formerly G Suite) addresses (yourname@yourcompany.com hosted on Gmail) use the same filtering algorithms as @gmail.com addresses for incoming mail. The difference is, a G Suite organization admin can set custom spam policies for their users or whitelist certain senders. From the sender's perspective, emailing a G Suite user is like emailing Gmail, unless that company has special rules. So, you can consider Gmail and G Suite as one category in terms of how they will treat your emails (the spam filtering logic is very similar).

# Outlook.com/Hotmail and Office 365

**IP Reputation Emphasis**: Microsoft's email ecosystem (this includes Outlook.com, Hotmail, Live mail for consumers, and Exchange Online in Office 365 for businesses) places significant weight on IP reputation. They have long provided the SNDS tool which shows senders their IP's "color" status (Green/Yellow/Red) based on complaint rates and spam hits to spam traps. If you're sending via a dedicated IP and that IP is new or has sent high spam, Microsoft may junk or block your mail regardless of domain.

That said, domain reputation is not ignored – it's increasingly considered, especially for Office 365 which has advanced anti-spoofing (they use DKIM/DMARC too). But many Outlook/Office365 bounce messages refer to IP-based blocking. For example, "5.7.606 Access denied, banned sending IP" indicates Microsoft outright blocked the IP (could be via their internal blacklist or a third-party like Spamhaus).

**New IPs** sending to Outlook addresses will be throttled at first (like Gmail, they don't trust new senders immediately). As noted earlier, Microsoft will accept about 10k messages/day from a new IP and defer the rest, gradually increasing acceptance as your IP proves trustworthy.

---

**Spam Complaint Handling**: Outlook provides the JMRP (Junk Mail Reporting Program) complaint feedback loop to ESPs and senders, wherein when a user clicks "Report Junk" on an Microsoft Outlook (formerly Hotmail): Free email and calendar | Microsoft 365 email, you can get a copy of that complaint (if you've registered). They expect senders to promptly remove those users from the list. Microsoft's tolerance for complaints is low; a 0.5% spam complaint rate can impact deliverability (for major senders, even lower is ideal).

They also measure something called **SRD (Sender Reputation Data)** which is essentially a panel of users' feedback used to rate senders. If your emails are often marked as junk by this panel, it weighs heavily.

**Content Filtering**: Microsoft uses a system formerly known as SmartScreen (and now integrated into Exchange Online Protection for Office 365). It uses machine learning trained on billions of messages, plus user submissions of phishing/spam. Content that resembles known spam or contains malware/phishing triggers will be filtered.

Microsoft's filters tend to be slightly more permissive about marketing content (they might not spam-folder you just for saying "Free offer" if your reputation is okay), but they will absolutely block mails that fail authentication or appear to be spoofed. Interestingly, Microsoft still mentions Sender ID (an offshoot of SPF) in some docs, though **Sender ID** is legacy now – practically, just ensure SPF passes and consider DKIM a must for Office365 too (modern Exchange does check DKIM if available).

---

**Blacklists and Outlook**: Microsoft often references third-party blocklists in their bounce codes. Spamhaus hits are common – "Service unavailable, client blocked using Spamhaus". They also use their own internal IP blocklist (sometimes called the Outlook/Exchange IP Reputation list). If you're on a Spamhaus list, Outlook mail will almost certainly hard bounce until you're delisted.

Likewise, **Office 365** uses additional services (like Proofpoint's URIBL for malicious URLs, etc.). Office 365 admins (the recipients' admins) can also have custom block/allow lists, so occasionally a block might be due to an individual company policy.

# Differences between Outlook.com vs Office 365

Essentially those 2 share the same filtering backbone in many ways, but there are a few differences:

- **Outlook.com** has static rules suitable for consumer inboxes and uses things like the Microsoft Services Agreement and Anti-Spam Policy to decide on blocking mass mail. It also limits each account (if you're sending from an @outlook.com address) to a certain number of emails/day and will temporarily block your sending if it suspects you're a spammer using a hacked account.

- **Office 365** gives each enterprise admin control. By default, EOP (Exchange Online Protection) will filter spam with its default policies, but admins can tweak thresholds and block/allow lists for their domain. As a sender, this means if you're emailing corporate addresses on Office 365, you might encounter variability – one company might have very strict settings, another might allow more through. However, the baseline EOP does leverage things like the Microsoft 365 IP Reputation and known bad senders lists. Office 365 also uses Azure sentinel and ML for detecting phishing – if your email looks phishy (e.g., pretending to be a CEO, or contains a suspicious link), it might be quarantined even if your domain/IP is fine.

---

**Postmaster Tools**: Microsoft doesn't have a single equivalent to Gmail Postmaster for domain reputation, but they offer SNDS for IP reputation monitoring and Office 365 Enhanced Spam Feedback for organizations (which is more for recipient admins). They also encourage using DKIM and DMARC to improve deliverability for custom domains in Office 365 – in fact, Microsoft 365 will display a trusted sender mark (via BIMI, etc.) if you have these in place and a good reputation.

# GSuite (Google Workspace) vs. Gmail

As mentioned, G Suite uses Gmail's filtering algorithms. One small difference: if you are sending from a G Suite address, Google imposes outbound sending limits and will temporarily disable your account from sending if you exceed them or trip filters (to protect their IPs).

Those sending limits are similar (500/day for new accounts, up to 2,000/day for established ones). If you're blocked from sending externally, G Suite admin might see an alert like "Google has temporarily restricted user's account for sending". The remedies internally are similar (wait 24 hours, reduce volume, etc.).

For incoming mail to G Suite users, G Suite admins can whitelist your domain/IP if there's a consistent problem (which is something not possible with consumer Gmail). But as a sender, you can't rely on all your recipients doing that – you should still follow Gmail's general rules.

# Summary

- **Gmail/G Suite**: Very sensitive to engagement and authenticity. Requires authentication and low complaints. More likely to throttle (soft block) first. Hard to get direct support; you must align to their best practices.

- **Outlook/MS365**: Very sensitive to sender reputation (IP especially) and list quality. Tends to outright block if reputation is bad (hard bounces). Has avenues for remediation (delist request). Also requires good list hygiene (few bounces) and compliance with spam laws (unsub, etc.).

- **Both Gmail and Outlook** rely on big data and user feedback. Neither will let a high-volume spam campaign through for long. But Gmail might "learn" a bit faster from individual user signals, whereas Outlook might apply more static rules combined with user complaints.

- Both providers (and others like Yahoo) now strongly enforce having proper **DKIM/SPF** and **low spam rates**. As one deliverability expert quipped, these "new" requirements are not really new – they've been recommended for years, but now Gmail/Yahoo/Outlook are enforcing them strictly due to increased spam.

Understanding these differences can help you tweak your approach depending on which domain you're targeting. For example, you might notice your emails do fine in Outlook but go to Gmail spam – that could indicate your content is getting caught by Gmail's algorithm (maybe too promotional and not enough engagement), whereas Outlook's more rule-based filter passed it. Or vice versa: good Gmail inboxing but Outlook keeps bouncing – maybe your IP is on a blacklist or you have too many bounces. Always examine your delivery statistics by provider; you may need to adjust volume or practices specifically for one or the other.

# Insights from Industry Experts and Blogs

Industry experts and email deliverability blogs provide valuable insights (and sometimes differing opinions) on how to maximize inbox placement and avoid blocks. Here are some key takeaways:

- **Reputation Trumps Content (Mostly)**: A common theme is that sender reputation and engagement metrics outweigh specific "spam words" in modern spam filtering. As the EmailConsul blog noted, the idea that using a single spam keyword will automatically get you blocked is a **myth** – "content doesn't factor into spam filtering decisions as heavily as it once did". Instead, filters look holistically at the sender's history.

That said, experts agree **you still shouldn't ignore content quality**. As one put it: avoid spammy language, but remember it's "just one piece of the puzzle" – focus on creating value for the reader and driving positive engagement. In practical terms, this means if you maintain a good reputation (low complaints, authenticated domain, etc.), you can use a marketing phrase here or there without issue, whereas a pristine email with perfect content could still go to spam if sent from a blacklisted IP.

- **Engagement is Critical**: Many experts highlight how **user engagement signals (opens, clicks, replies)** now feed into filtering algorithms. For example, a Validity (ReturnPath) study might show that high read rates correlate with inbox placement. In Litmus's 2024 panel with Gmail and Yahoo representatives, they emphasized keeping spam complaint rates under 0.1% ideally.

If you can get users to interact (say, by writing compelling, personalized emails that solicit a response), you greatly improve deliverability. On the other hand, continuing to send to people who never engage drags you down. **Trimming inactive subscribers** is a widely recommended practice – letting uninterested people go can boost your overall open rates and reputation. Experts note that an unsubscribe is not a bad outcome; it's better than being marked spam.

- **Warming Up is Worth the Effort**: Industry blogs (and tools like Warmy, etc.) consistently advise warming up new email accounts and IPs. While it can be tedious to gradually ramp up, the consensus is that it significantly improves initial deliverability and helps avoid the dreaded first-impression spam block. Some experts describe warm-up as "building your sender reputation equity" – akin to not asking a mail server to deliver 5,000 emails for you when it's never seen traffic from you before. Many blogs, including Warmy's own, provide warm-up schedules (e.g., start with a handful of emails, then double daily) and emphasize sending to highly engaged contacts first to accumulate positive signals.

The community also often mentions using **warm-up networks** (where accounts automatically send and reply to each other's emails) to game engagement – while not officially endorsed by ESPs, these have become popular to "train" algorithms that your emails get replies.

---

- **Blacklist Monitoring**: Experts advise keeping an eye on your status with major blacklists (Spamhaus, Barracuda, etc.) because getting listed will cause multi-ISP blocks. There's consensus that if you do get blacklisted, you should pause emailing and investigate immediately. **Don't try to plow through a blocklist** – you'll just get more bounces and dig a deeper hole. Instead, resolve the issue (clean the list, tighten opt-in, etc.) then request delisting.

A point of debate sometimes is whether a small sender needs to actively monitor blacklists; some say yes, use a monitoring tool (many ESPs do this for you), others say if you practice proper hygiene you shouldn't normally end up on one. But as Kickbox's blog noted, even "smart email senders" can occasionally end up on Spamhaus by accident, so having a plan for blacklist checks is wise.

- **Conflicting Opinions on Content vs. Unsubscribe Links**: Some cold email practitioners argue that including an unsubscribe link in a one-to-one outreach email can hurt deliverability (since it flags the email as promotional). Others point out that not including it risks more spam reports. We see this conflict even in Warmy's materials: they note unsubscribe links can lower deliverability slightly but are "mandatory for bulk senders" and help prevent spam reports.

The resolution of this conflict in practice is usually: if you're sending at scale, include the unsubscribe (and comply with laws); if you're sending very personal-looking one-to-one emails in small batches, you might omit it to appear more like a personal email – but then you must be extremely careful to whom you send to avoid complaints. Industry consensus leans towards erring on the side of transparency and giving recipients an opt-out.

---

- **Role of "Spam Words" and Tools**: Many blogs debunk the overemphasis on spam keywords, yet they still advise avoiding egregious spammy phrases. Tools that check spam score (e.g., Mail-Tester, GlockApps) often flag certain words or a lack of plain-text part, etc. Experts say these can be useful for catching obvious issues, but passing a spam-score test doesn't guarantee inboxing – your reputation and engagement are the trump cards. In short, "Avoid spam trigger words whenever possible… but focus on your sender reputation and engagement.".

- **Domain Reputation vs. IP Reputation**: There has been a shift in email industry discussions toward domain reputation (especially with the rise of IPv6 and senders moving across IPs).

Gmail led this change: they give strong weight to domain reputation. Outlook historically was IP-based but is also incorporating domain more now (especially with DKIM and DMARC data). For senders, this means you can't just hop IPs to evade a bad rep – your sending domain carries a history too.

Some experts warn about **domain aging** – e.g., don't buy a brand new domain and immediately send thousands of emails; if possible, use a domain that's been around and build it up. Warmy's blog mentions domain age as one factor in reputation (an older domain tends to be more trusted). If you must use a new domain (for branding reasons), warm it extra slowly and consider using a subdomain of an established domain if appropriate

---

- **Watch Out for Spam Traps**: A repeated expert warning is to never purchase email lists and to regularly clean old addresses. Spamhaus and others use recycled old addresses as traps – if you keep emailing an address that's been dead for a year, it could become a trap. Use double opt-in for signups to ensure validity, and deploy email verification on any old list before mailing. As a rule of thumb, any campaign yielding hard bounce rates above a few percent is a sign you need to clean your data – continuing to send to those bounces can get your IP blocklisted.

- **Testing and Monitoring**: Industry pros encourage regular testing of your emails. This includes testing how your email renders (to ensure no broken code that might hit filters) and sending to seed accounts (test addresses in Gmail, Outlook, Yahoo, etc.) to see where it lands – using tools like GlockApps or Mailinator seeds.

If you notice, say, seeds going to Gmail spam, you can adjust before a full send. Also, keep an eye on metrics: sudden drops in open rates could indicate a delivery issue (if your tracking is accurate).

Services like Warmy and others even provide deliverability scores by sending emails and measuring if they hit inbox or spam. These can be useful, though experts sometimes debate their accuracy. Regardless, continuous monitoring of your sender reputation (via Postmaster Tools for Gmail, SNDS for Microsoft, etc.) and performance is recommended so you can catch problems early.

---

In summary, experts across the board stress proactive best practices – don't wait for a block to happen. Build a solid foundation (warm-up, authenticate, quality content, clean lists, engagement) so that you avoid triggering ISP defenses in the first place. And if you do slip up, take corrective action swiftly. While some nuances are debated, the core principles of good email sending are widely agreed upon.

# Recommendations for Warmy Users to Maximize Deliverability

- **Always Warm Up New Inboxes and Domains:** Before you start sending outreach campaigns from a new email address, run it through Warmy's warm-up sequence or a similar warm-up routine. Warmy recommends warming up for about 2 weeks with gradually increasing volumes and even automated positive engagements (replies).

This trains mailbox providers to view your mailbox as a legitimate, active participant in email conversations. During warm-up, Warmy's AI will adjust sending and reply rates to build reputation safely. Only after this warm-up phase should you ramp toward your actual outreach volume.

---

- **Use Multiple Inboxes and Domains for Scale**: If you need to send a high volume of cold emails, don't put all that volume on a single email address or domain. Spread it out. For example, instead of sending 500 emails/day from one address, you might send 50/day from 10 addresses (across a couple of domains). Warmy suggests setting up 4–5 inboxes per domain and leveraging multiple domains for large-scale outreach.

This "rotation" strategy reduces the load and risk on any one sender. It also means if one gets a temporary block, your whole operation isn't stalled. Make sure each of those inboxes is properly warmed up and managed. Monitor each one's reputation (Warmy can help with inbox health monitoring). Also, periodically "refresh" low-performing domains – if one domain starts to struggle with deliverability despite best practices, consider resting it and using a new domain for a while.

- **Ensure Flawless Email Authentication**: For every domain you send from, set up SPF, DKIM, and DMARC before sending any cold emails. Warmy's deliverability guide emphasizes that SPF/DKIM are non-negotiable – without them, your emails might be assumed forged and rejected. After adding the DNS records, use Warmy's or other tools' tests to verify they're passing.

Also, keep an eye on DMARC reports (Warmy or other services can send you these) to catch any authentication failures. Solid authentication will significantly improve your chances with providers like Gmail and Office 365 which otherwise might drop unauthenticated messages.

---

- **Gradually Increase Sending Volume (Even After Warm-up)**: Don't go from zero to max even after the initial warm-up period. If you warmed to, say, 40 emails/day during warm-up, don't jump straight to 500. Step up by, for example, doubling every few days and see how deliverability holds. Warmy's AI can continue to guide sending rates. Warmy advises aiming for a steady increase and even varying the volume a bit (not sending the exact same count every single day, which can look automated).

Also, maintain consistent sending patterns – randomness within a range is fine, but don't disappear for a week and then send a huge batch; consistency builds the sender's reputation.

- **Prioritize Quality of Prospects and Data Hygiene**: The easiest way to get flagged as spam is to send emails to people who absolutely don't want them or to bad addresses. Build your prospect list carefully. Avoid scraping indiscriminately or buying lists – those addresses often include spam traps or uninterested recipients. Use Warmy's **email validation tool** (or another verifier) on any list to remove invalid addresses before you send. This will keep your bounce rates low (remember, high bounce rates hurt your domain reputation).

Also, if you notice certain segments of your list are performing poorly (no opens, high bounce or complaint), stop sending to them. **List hygiene is an ongoing process**. Warmy suggests keeping a 'Do Not Contact' list of people who opted out or complained, and scrubbing that against your sends to ensure you don't accidentally re-send to them. Every email you don't send to an uninterested or bad address is a win for your sender's reputation.

---

- **Aim for Replies and Engagement**: In cold B2B outreach, a reply from the recipient is gold – not only for your sales pipeline, but for deliverability. A reply tells Gmail/Outlook that the recipient found the email valuable enough to respond, which typically whitelists that thread going forward. Warmy's advice is to **"prioritize aiming for a reply rather than a click"**.

In practical terms, this means designing your outreach emails to prompt a response (e.g., ask a direct question or offer something that encourages them to write back) rather than just dropping a link hoping for a click. It also means avoiding CTA links in your first cold email if possible – a link click is nice, but a reply is a stronger positive signal. And certainly don't ask for sensitive info or anything that might make a recipient uncomfortable; you want genuine engagement, not spam flags.

- **Personalize and Vary Your Email Content**: Use personalization tokens and even dynamic content syntax (Spintax) to make each email unique. Warmy suggests that **unique emails are more likely to be delivered**.

This prevents spam filters from seeing a large batch of near-identical messages. At a minimum, include the recipient's name and perhaps their company or a detail in the body. Better, write a couple of variant opening lines or subject lines and alternate them. Warmy's guide mentions using Spintax – e.g., have a few interchangeable phrases in your template that the system can rotate, so each send has slight wording differences.

Also, absolutely personalize the subject line – it should not be generic marketing speak, but something relevant to the recipient (while still not looking spammy). A/B test different subject approaches (Warmy's platform or others can help with this) to see what gets more opens – higher open rates will feed back into better reputation.

---

- **Keep Emails Short, Plain, and Human-like**: Generally, cold outreach emails perform best when they look like a personal email from one person to another. So, **write in plain text (or light HTML) format, with a simple signature**. At Warmy we note that plain text emails have higher deliverability than heavy HTML.

Even if you compose in a rich editor, don't overdo formatting – a mostly text email with perhaps one hyperlink and your email signature image (if needed) is enough. They even suggest minimizing images (including email signature logos), especially in initial emails. Too many images or fancy HTML can trigger promotional filters. A good rule: if your email wouldn't look out of place forwarded from a colleague, it's probably fine.

Also, keep it concise – long emails can get clipped (Gmail clips messages >102KB, which can hide the unsubscribe link – a potential compliance issue), and prospects may not read a wall of text from a stranger anyway. A few short paragraphs or a handful of bullet points is plenty.

- **Monitor Your Sending and Adjust**: Use Warmy's analytics and any available ESP feedback to keep an eye on deliverability. Warmy's dashboard can show you if emails start landing in spam during warm-up (by sending to their network of inboxes).

Even during normal sending, watch your open rates by domain (if you notice, for example, 0% opens for all Outlook recipients, something might be wrong with Outlook delivery). If you see a problem, **act quickly** – don't keep sending and hoping it fixes itself. Pause or slow down and diagnose (authentication issues? content? a particular campaign got high complaints?).

Warmy provides some guidance and support in such cases as well, but it's ultimately on you to adjust your sending practice.

---

- **Use Domain and Inbox Rotation Wisely**: If you do hit a block, you might be tempted to swap in a new domain immediately. This can work in the short term (and Warmy suggests having extra domains/mailboxes ready), but remember to fix what went wrong so the new domain doesn't suffer the same fate.

Use new domains as part of a diversification strategy, not as throwaways for spam. Ideally, each domain you use should be treated with care and warmed and built up. Rotating among multiple domains can also help avoid hitting provider-specific volume caps. For example, if you need to send 1,000 emails to Gmail addresses in a day, splitting that across 5 different Gmail accounts (on possibly different domains) means each account sends 200 – which might fly under Gmail's radar whereas 1,000 from one account might trigger throttling. This is essentially what Warmy's mailbox calculator aims to figure out.

- **Stay Updated on ESP Policy Changes**: Email providers constantly tweak their algorithms and policies (e.g., Gmail's 2024 enforcement of existing guidelines). Warmy's blog and industry newsletters (like Litmus, Validity, etc.) often share updates when Gmail or Microsoft make changes that senders should know about. As a Warmy user, keep an eye on those resources. For instance, Gmail's recent emphasis on list-unsubscribe headers might mean you decide to include an unsubscribe link in all your cold outreach going forward, even if previously you did not. Adapting quickly to these changes can save you from blocks

---

Following these recommendations will help you maintain high deliverability. In essence, think like the email providers: demonstrate that you're a responsible sender with genuine intent to reach people who might want to hear from you. Use Warmy's tools as an aid – to warm up, monitor, and adjust – but also cultivate good sending habits (good data, good content, gradual growth). By doing so, you greatly increase the chances that your next outreach campaign lands in the inbox and not the spam folder, avoiding those costly ESP blocks that stymie your efforts.

# Auto All-In-One Tool For Email Deliverability To Make Your Email Channel Reliable

We are passionate about solving email deliverability challenges and making email a reliable channel for every business

**325+**
Years Of Combined Email Deliverability Expertise

**9 countries**
Home To Our Talented Team

**95+**
Countries Have Daily Active Users In Warmy