warmy
Email Channel. Reliable.

April 2025

Bounce-Rate Root-Cause Analysis: Hard vs. Soft Failures Across ESPs

Email bounces occur when a message cannot be delivered and is returned with an error code explaining why. These bounce codes are crucial for understanding deliverability issues. They generally indicate either a soft bounce (temporary failure) or a hard bounce (permanent failure). In this report, we break down common hard vs. soft bounce causes across major email providers – Gmail, Outlook/Hotmail (Microsoft), Yahoo, AOL, Zoho, and others – and provide insights into their root causes and how to mitigate them. The goal is to help email deliverability professionals and marketers reduce bounce rates and ensure their emails reach end users' inboxes.

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

- **Hard vs. Soft Bounces:**
  - Hard bounces (5xx codes): Permanent failures – invalid recipients, policy blocks, failed authentication.
  - Soft bounces (4xx codes): Temporary issues – greylisting, server overload, mailbox full.

- **Gmail (Google):**
  - Hard bounces for invalid users (5.1.1), failed SPF/DKIM/DMARC (5.7.26), and spam rejections (5.7.1).
  - Soft bounces often due to greylisting (4.7.0) or rate-based deferrals.
  - Mitigation: Authenticate fully, warm up IPs/domains, monitor via Postmaster Tools.

- **Outlook / Hotmail (Microsoft):**
  - Uses detailed bounce codes like SC-001 (spam content) and RP-001 (rate limit).
  - Hard bounces for blocklisted IPs or user complaints.
  - Soft bounces from throttling and temporary rejections (421 RP codes).
  - Mitigation: Use SNDS/JMRP, clean lists, throttle volume, fix rDNS/SPF issues.

- **Yahoo / AOL:**
  - Hard bounces include invalid users and policy rejections ([BLXX] blocklists, failed DMARC).
  - Soft bounces often marked as [TS01]/[TS02] (greylisting); [TS03] is a permanent block in disguise.
  - Mitigation: Sign up for Yahoo/AOL feedback loop, reduce complaint rates, monitor for Spamhaus listings.

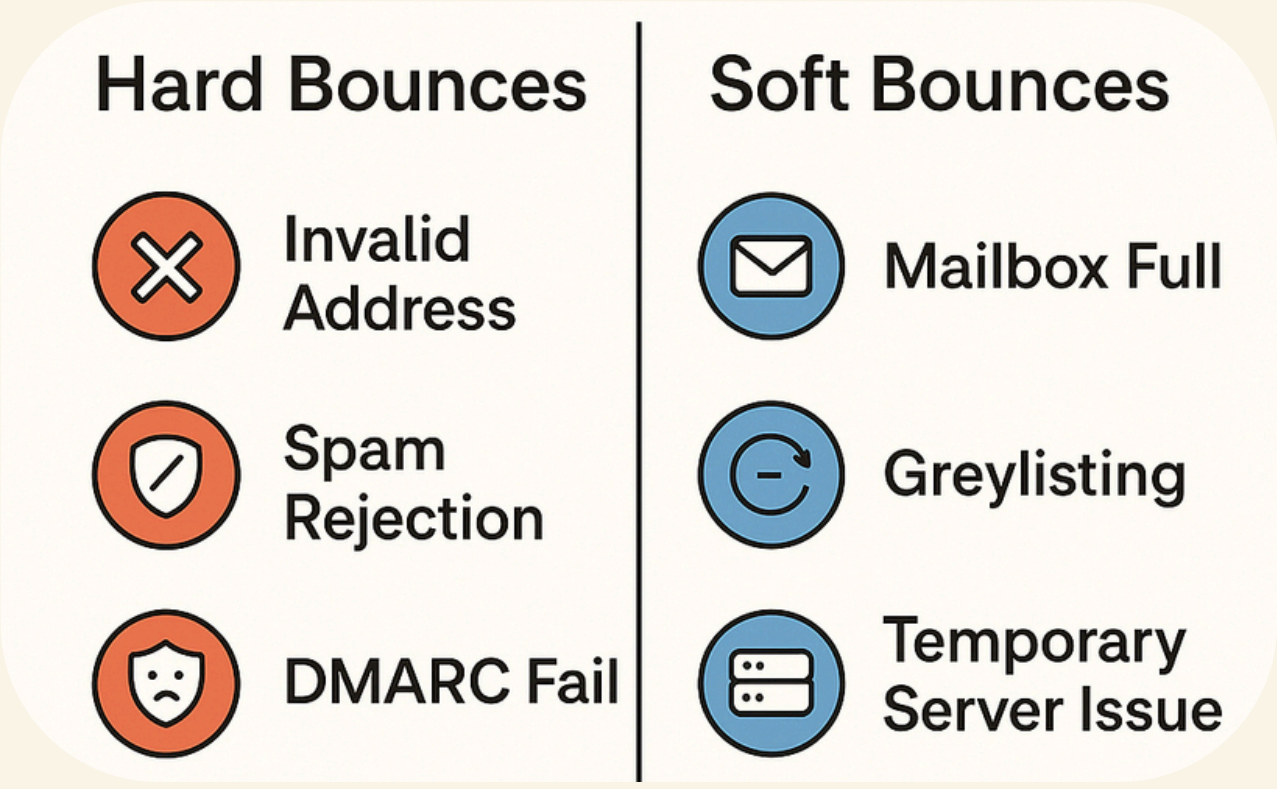
- **Zoho Mail:**
  - Hard bounces for spammy content, blacklisted IPs, or DKIM failures.
  - Soft bounces mostly due to greylisting (451) or mailbox full.
  - Mitigation: Retry after greylisting, authenticate domain, simplify content, and ensure proper DNS.

Understanding Hard vs. Soft Bounces

Hard bounces are permanent delivery failures. The sender should not retry these, as something fundamental prevented delivery. Typical causes include non-existent addresses, domain name errors, or messages rejected due to policies (e.g., message content or authentication failures). For example, if you send to an address that doesn't exist, you'll get a 5xx error like "550 5.1.1 The email account that you tried to reach does not exist" – a clear hard bounce indicating a permanent failure.

Soft bounces are temporary failures. They suggest the message might be delivered if attempted later. Common reasons are recipient mailbox full, mail server temporarily unavailable or busy, or a message deferral due to suspicious sending behavior (a kind of greylisting). Soft bounces use 4xx status codes. For instance, an error code 421 or 451 indicates a temporary issue (server busy, network error, etc.) that may resolve on retry. Because soft bounces are not final, sending servers will usually retry these for some time.

Every Email Service Provider (ESP) and Internet Service Provider (ISP) may have unique bounce codes and policies, but they usually follow the 4xx = soft, 5xx = hard convention. Below, we analyze bounce failures at specific providers, detailing common hard vs. soft bounce scenarios, along with technical examples and mitigation strategies.



Gmail (Google)

Google’s Gmail (including Google Workspace) is known for providing detailed bounce messages in plain language, often with links to further information. Gmail’s SMTP response codes help pinpoint issues, whether related to invalid recipients, reputation problems, or policy enforcement. Here are common bounce scenarios at Gmail

Hard Bounce Causes at Gmail

- **Invalid Recipient Address (User Unknown)**: Gmail returns a permanent error if the recipient's address does not exist. The typical SMTP reply is 550 5.1.1 – e.g., "The email account that you tried to reach does not exist. Please try double-checking the recipient's email address". This hard bounce indicates the address is invalid or no longer active on Gmail's servers.

- **Message Rejected as Spam/Low Sender Reputation**: Gmail will outright reject messages it deems as spam or from a sender with a very poor reputation. In these cases, you may see a 550 5.7.1 error. For example: "550-5.7.1 Our system has detected that this message is likely unsolicited mail... this message has been blocked". A 5.7.1 permanent rejection means Gmail classified the email as spam and refused delivery (often after repeated issues). This can happen if your sending domain or IP is blacklisted or has built a history of sending unwanted emails.

- **Authentication or DMARC Failures**: Gmail strictly enforces authentication policies. If your email fails SPF/DKIM or violates the recipient domain's DMARC policy, Gmail may bounce it. One example is 550 5.7.26 for DMARC failures: "Unauthenticated email from <domain> is not accepted due to the domain's DMARC policy". This hard bounce occurs when the sending domain has a DMARC p=reject policy and the message isn't properly authenticated, so Gmail refuses it. Similarly, Gmail might issue 5.7.26 or related codes if SPF or DKIM checks hard-fail.

- **Message Size or Other Policy Blocks**: Gmail imposes message size limits (e.g., ~25MB for attachments). Exceeding these or other Google policy limits (such as too many recipients in one email) can result in a hard bounce (e.g., 552 5.3.4 Message size exceeds limit). These are less common but represent permanent rejections until the content is adjusted.

Soft Bounce Causes at Gmail

- **Greylisting / Suspicious Traffic Temporary Block**: Gmail sometimes defers messages from new or suspect senders using 4xx codes – effectively a temporary block. A common soft bounce is 421 4.7.0. For example: “421-4.7.0 Our system has detected an unusual rate of unsolicited mail originating from your IP address... mail from your IP has been temporarily blocked”. This is Gmail’s way of saying “slow down” – it views your sending behavior as suspicious (low reputation, high volume spike, etc.) and is temporarily refusing email. The mail server will typically retry later. If the issue is not resolved (e.g., you continue sending high volumes), repeated soft bounces might turn into a hard bounce (5xx). In practice, this Gmail greylisting is a protective measure to see if the sender improves or persists.

- **Temporary Authentication or Encryption Issues**: Gmail might defer a message if there’s a transient issue with authentication lookup or encryption. For instance, a 421 4.7.0 could also appear if “message does not have authentication information or fails to pass authentication checks”. Gmail could treat it as a temporary error if it expects you to fix SPF/DKIM and retry. Another scenario: if Gmail requires TLS encryption for a certain recipient domain and your server didn’t use it, you might get a soft bounce like “TLS required for RCPT domain, closing connection” – indicating you should retry with a secure connection.

- **Recipient Mailbox Full or System Busy**: Although Gmail’s storage is large, a recipient’s mailbox quota being full can cause a bounce. Gmail typically sends a 452 or 552 error for mailbox full (exact wording might be “Mailbox full”). This is usually treated as a soft bounce because if the user clears space, future emails can go through. Likewise, a Gmail server downtime or overload can trigger a 421 4.4.5 or 451 temporary failure (e.g., “Temporary server problem. Try again later”). These indicate Gmail couldn’t deliver to the user at that moment, but the address itself is valid.

Mitigation & Optimization for Gmail

Maintaining a good sender reputation is key. To avoid Gmail bounces, use proper email authentication – set up SPF, DKIM, and DMARC correctly. This prevents Gmail from rejecting your mail as unauthenticated. Senders should also warm up new domains/IPs by gradually increasing volume.

Sudden large send spikes can trigger Gmail's temp blocks for "unusual rate of mail". Monitor Gmail-specific feedback: Google's Postmaster Tools provides data on domain reputation, spam rate, etc., so you can catch issues early. Always cleanse your mailing lists (remove invalid addresses) to avoid hard bounces for nonexistent users. If you receive a 4.7.0 deferral, slow your sending and improve your content/reputation before retrying – continuing to push during a temporary block can lead to a 5.7.1 permanent block.

Ensure your content isn't triggering spam filters: avoid known spam phrases, excessive links, or other issues Gmail flags. If Gmail bounces cite a specific reason (e.g., DMARC), follow the included link or guidance (Gmail often links to support articles in bounce messages) to resolve the issue. Over time, maintaining low complaint rates and engaging content will improve Gmail inbox placement and reduce bounces.

Outlook/Hotmail (Microsoft)

Microsoft's email ecosystem (Outlook.com, Hotmail, Live, MSN, and Office 365) has its own set of bounce codes and policies. Microsoft uses enhanced SMTP status codes with abbreviations like SC, STO, SNP, DY, OU, etc., to indicate specific block reasons on Outlook.com (consumer) mail servers. They also employ throttling for volume management. Below are common Outlook/Hotmail bounce scenarios

Hard Bounce Causes at Outlook/Hotmail

- **Unknown User or Mailbox Not Found**: As with any ISP, sending to a non-existent @outlook.com or @hotmail.com address results in a hard bounce (typically 550 5.1.1 User unknown or similar). The NDR (non-delivery report) might say the recipient was not found on the server. These are permanent – the sender must remove or correct the address.

- **Policy Blocks – Spam Content or Reputation**: Outlook.com rejects emails that violate its anti-spam or security policies. A common bounce is 550 5.7.1 with additional codes. For example, error 550 SC-001 means “Mail rejected by Outlook.com for policy reasons. Reasons for rejection may be related to content with spam-like characteristics or IP/domain reputation.”. This indicates Microsoft’s filters blocked the message, possibly due to suspicious content or a poor sender reputation. Similarly, 550 OU-002 is a policy block for spam-like content or reputation issues. These are hard bounces; the mail system will not retry.

- **IP Address Blocked or Blacklisted**: Microsoft will bounce if your sending IP is on a blocklist or has violated sending rules. For instance, 550 SC-004: “Mail rejected… A block has been placed against your IP address because we have received complaints concerning mail from that IP”. This is a direct block due to spam complaints. Another example is 550 OU-001, which specifically notes a Spamhaus listing: *“Mail rejected… For more information about this block and to request removal, please go to: http://www.spamhaus.org. In short, if your IP is on a known spam blocklist or Microsoft’s internal blacklist, Outlook.com will hard-bounce your emails.

- **Domain Authentication Issues (SPF/DKIM)**: If you send from a domain that fails Microsoft's SenderID/SPF checks, you might see an NDR like "550 5.7.1 … Sender ID validation failure". This is less common since SPF has mostly replaced Sender ID, but it highlights that authentication issues can cause rejection. Nowadays, Office365/Exchange might bounce messages that fail their anti-spoofing policies (especially if the receiving domain has strict DMARC). These bounces typically have 550 5.7.x codes indicating authentication failure.

- **Prohibited Sender Sources**: Outlook.com refuses mail from certain IP ranges by policy. 550 DY-001 exemplifies this: "We generally do not accept email from dynamic IPs". If you attempt to send directly from a residential/dynamic IP address, Microsoft will hard-bounce it, treating it as a policy refusal. Similarly, 550 DY-002 means your server might be compromised or sending spam (hence blocked). These are permanent until you send from a reputable static mail server.

- **Namespace Mining Protection**: Outlook.com uses "namespace mining" detection – if a sender tries many email addresses (likely guessing usernames), the system blocks them. The code 550 SC-002 indicates "IP has exhibited namespace mining behavior". Essentially, too many unknown recipients triggered a block. This is a hard bounce scenario until the behavior is corrected.

Soft Bounce Causes at Outlook/Hotmail

- **Rate Limiting & Throttling**: Microsoft often temp-fails excessive traffic to protect its system. Errors like 421 RP-001 / RP-002 / RP-003 are used for rate limiting. For example, “421 RP-001: The mail server IP connecting to Outlook.com has exceeded the rate limit”. In other documentation, RP-001 is described as “Messages from IP temporarily deferred due to user complaints or sending limits”. These 4XX codes mean “try again later, but send slower.” Outlook will defer connections if you send too many emails in a short time or if recipients are marking them as spam at a high rate. This is a soft bounce — the sending server will retry and should also slow its pace.

- **Temporary Server or Network Issues**: Occasionally, Outlook’s servers might respond with a 451 or 4.4.0 error indicating a transient issue (e.g., “server busy” or routing problem). For instance, “451 4.7.500 Server busy. Please try again later” is a known Outlook.com deferral during high load. These are soft bounces resolved by retrying after some time.

- **Transient Spam Filter Deferral**: In some cases, Outlook might initially deflect mail it’s unsure about. Rather than an outright 550, it might issue a 421 4.7.0 with a generic message about temporary rejection. If your message content trips some filters but not enough for a permanent block, Outlook could soft-bounce it (hoping your mail server retries later, and if reputation improves or the spam spike subsides, the mail might then pass). This behavior is not well-documented publicly, but senders observe it in the form of “temporary rejection” NDRs without permanent block codes.

- **Deferred for Suspected Open Relay or Bounce Backlog**: Microsoft’s error codes like 451 4.7.1 or 451 4.7.0 might appear if your sending pattern looks like an open relay or you have too many previous bounces. (Outlook might penalize IPs that attempt delivery to many invalid Hotmail addresses by temporarily deferring additional attempts, as a mitigation for dictionary attacks.) These soft bounces serve as a warning; continued issues may escalate to a block (SC-002 as mentioned).

Mitigation & Optimization for Outlook/Hotmail

Managing Microsoft-specific deliverability requires both technical setup and sending practices. First, ensure proper DNS setup: a valid reverse DNS (PTR) is mandatory (Outlook may outright reject mail from IPs without rDNS). Set up SPF and DKIM for your domain, and consider enabling DMARC to show you're a legitimate sender. Monitor your IP and domain reputation via Microsoft's free tools: sign up for SNDS (Smart Network Data Services) to see your IP's status and complaint rates, and enroll in Microsoft's JMRP (Junk Mail Reporting Program) to receive feedback loop reports when users mark your emails as spam. High complaint rates will lead to blocks, so use that data to prune unengaged or unhappy recipients. If you encounter a block (5.7.1 with SC or OU codes), use the Outlook Delist Portal at sender.office.com to request removal after you've addressed the cause. For example, if you got an SC-004 due to complaints, ensure you remove those complainants and send only to willing recipients before requesting delisting. Sending volume control is crucial: adhere to ramp-up schedules and avoid large, sudden blasts to Outlook addresses. If you see 421 deferrals (soft bounces) like RP-001, throttle your send rate and spread out your mailings. Also, avoid sending emails to many invalid addresses at Outlook – maintain list hygiene to prevent "namespace mining" blocks (SC-002). Content-wise, Outlook's filters may be sensitive; ensure your emails don't contain obvious spam triggers or malicious links. By following Outlook/Hotmail's postmaster guidelines and steadily building a good sending history, you can minimize both hard and soft bounces.

Yahoo Mail

Yahoo Mail (including AOL and Verizon domains under the Yahoo umbrella) provides detailed SMTP bounce codes via its Yahoo Mail Sender Hub. Yahoo's bounce messages often include bracketed codes like [TS01] or [BLxx] that indicate specific issues. We will focus on Yahoo-specific behaviors, though note that AOL Mail's bounce logic has converged with Yahoo's since their infrastructure merged under Verizon Media.

Hard Bounce Causes at Yahoo

- **Invalid Recipient Address**: If the Yahoo address doesn't exist, you'll get a hard bounce. Yahoo's servers might respond with an error like 554 delivery error: dd This user doesn't have a http://yahoo.com account. In the Yahoo SMTP code list, a bounce for a nonexistent user is shown as: "554 ... [BODY] The Yahoo account that you're trying to send to doesn't exist". This is a definitive hard bounce – the sender should stop sending to that address.

- **Policy Rejections (Content or Sender Behavior)**: Yahoo will permanently reject emails that violate its policies or appear highly suspicious. These typically return a 5XX code. For example, 554 5.7.9 means "Message not accepted for policy reasons" – Yahoo could not verify the sender as legitimate, or the content triggered Yahoo's filters. Likewise, a generic 554 Message not allowed indicates Yahoo classified the content or sending pattern as objectionable (spam or potentially malicious). These are hard bounces; Yahoo advises not to retry such messages.

- **Authentication Failures**: Yahoo, like Gmail, enforces authentication. If your email fails DKIM or DMARC in a way that conflicts with the sender domain's policy, Yahoo may bounce it. Yahoo's documentation notes that they will reject messages that fail DKIM when the domain has specified that all mail must be DKIM-signed. For example, if your domain's DKIM is set up incorrectly and Yahoo can't verify the signature, you could get a 5xx bounce requiring you to fix your DKIM. Similarly, failing DMARC (when the domain policy is reject) will cause a hard bounce at Yahoo. These typically manifest as 554 or 553 errors indicating an authentication failure.

- **Sender Reputation Blocks (Spamhaus, etc.)**: Yahoo uses external blacklists as well. A common hard bounce is 553 5.7.1 [BLXX] Connections not accepted from IP addresses on Spamhaus PBL. “[BLXX]” is a code for a blocklist hit. In this case, Yahoo rejected the email because the sending IP is on a Spamhaus blocklist (PBL in this example, meaning it’s a blocked ISP range). Until the IP is removed from the blacklist or you switch to a different IP, these bounces will persist. Yahoo recommends checking your IP status on Spamhaus if you see a [BL] code.

- **Excessive Invalid Recipients (List Hygiene Issues)**: Yahoo’s servers can issue permanent errors if your sending behavior shows a pattern of many invalid addresses. For instance, Yahoo’s bounce codes include “554 5.4.5 [internal] too many invalid recipients” (which might appear if you repeatedly send to addresses that don’t exist at Yahoo). In practice, Yahoo might first temp-fail excessive invalids (see VS1 codes in soft bounces), but if the problem continues, your IP/domain could be deprioritized or blocked. Essentially, poor list hygiene leading to a lot of Yahoo bounces can itself trigger a broader hard bounce block.

Soft Bounce Causes at Yahoo

- **Transient Deferral – "Yahoo TS Codes"**: Yahoo uses 421 4.7.0 errors with codes like [TS01], [TS02], [TS03] to indicate temporary deferrals for suspected spam or high volume. For example: "421 4.7.0 [TS01] Messages from x.x.x.x temporarily deferred due to user complaints – 4.16.55". TS01 and TS02 both mean Yahoo is seeing unusual traffic or complaints from your IP and is temporarily deferring your messages. These are classic soft bounces (Yahoo is effectively greylisting you for the moment). TS03, however, is special: "421 4.7.1 [TS03] Messages from x.x.x.x permanently deferred. Retrying will NOT succeed". Although TS03 is presented with a 4.7.1 code, Yahoo explicitly says it's a permanent block on that sender (due to a high volume of what appears to be unsolicited mail). In other words, TS03 is Yahoo's way of telling you that further retries are futile until you resolve the underlying issue (it's essentially a hard bounce disguised as a 4xx). Generally, if you hit TS01 or TS02 deferrals, you should slow down and improve your sending practices before it escalates to TS03.

- **Temporary Server/System Issues**: Yahoo may send a 451 error if their mail system is having issues processing mail. One example from Yahoo's docs: "451 Resources temporarily not available – Please try again later [numeric code]". This indicates Yahoo's servers were too busy or encountered a temporary error during the connection. It's not about your message or reputation – just a technical hiccup on their side. The sending server will attempt retries later, and these usually succeed once the condition clears.

- **Greylisting for New Senders**: Yahoo (and AOL, as part of the same group) can employ a greylisting-like tactic, especially for new IPs or domains. They may initially defer messages from an unknown sender to see if the sender retries properly. If you're sending to Yahoo addresses from a brand-new IP or domain, expect a few 421 deferrals at first. This soft bounce will resolve if your mail server retries after a few minutes. Consistent retry behavior signals to Yahoo that your server is legitimate (spammers often won't bother retrying after a deferral). Thus, these greylist deferrals are temporary by design.

- **Too Many Recipients or Message Frequency (Temporary)**: Yahoo's SMTP may return a 4xx if you try to send too many messages in one connection or too many recipients in one go. Their guidelines mention rate limiting. For instance, error 451 4.7.0 [GL01] (generic greylisting) or 421 4.7.0 [RL02] (rate limit) could be used. These mean "slow down, you're sending too fast." They are soft bounces – a hint to reduce your sending rate to Yahoo.

Mitigation & Optimization for Yahoo

When dealing with Yahoo bounces, first categorize whether it's a temporary deferral or a permanent rejection. For soft bounces like TS01/TS02 deferrals, do not panic – these often clear up if you reduce volume and maintain consistent sending. Space out your emails to Yahoo users and gradually increase volume. If you encounter TS03 (or if TS01 deferrals persist), you likely need to pause sends and evaluate: check your complaint rates (are Yahoo users marking your emails as spam?), and possibly use Yahoo's support channels. Yahoo's error messages often include a link or suggestion, such as submitting your IP for review. Indeed, Yahoo provides a form for senders to request removal of a block or to check status. Use those resources if needed.

Always remove invalid Yahoo addresses from your list after a hard bounce. Yahoo explicitly advises senders not to resend to addresses that bounced with 5xx errors. Continuing to send to bad addresses can get your IP flagged (Yahoo's 451 VS1-MF error warns of "excessive unknown recipients"). So, good list hygiene is crucial. Ensure your emails pass DKIM and SPF alignment – Yahoo will reject if authentication fails under certain policies. Monitor your sending IP against blacklists like Spamhaus; if you hit a [BLXX] bounce, immediately check Spamhaus and request delisting. To reduce complaints, send only to users who have engaged or signed up (Yahoo deferrals often correlate with high complaint rates or spam folder placement). It's also wise to sign up for the Yahoo Feedback Loop (now part of Verizon Media's FBL, covering Yahoo/AOL) so you get reports when Yahoo users mark your messages as spam. Those recipients should be suppressed to protect your sender reputation.

Finally, be aware that Yahoo's filtering sometimes acts in concert with AOL (since they share infrastructure). Success with Yahoo generally translates to success with AOL, and vice versa – so the best practices below for AOL will complement your Yahoo strategy.

AOL Mail

AOL Mail is now under the same umbrella as Yahoo (both owned by Verizon Media, now Yahoo Inc.). In recent years, AOL's bounce codes and filtering policies have largely aligned with Yahoo's. However, there are still some AOL-specific codes and legacy behaviors worth noting. AOL addresses use the @aol.com domain (and related domains like @verizon.net in some cases). Here's what to expect from AOL bounce replies

Hard Bounce Causes at AOL

- **Non-Existent Address**: If the recipient's AOL address is invalid (for example, the user left AOL or the address is typed wrong), you'll get a hard bounce. AOL's classic message for this was "550 5.1.1 User unknown" or sometimes a code 521 5.2.1 with a message indicating the service will not accept the message. In some instances, AOL used 521 5.2.1 : AOL will not accept delivery of this message even for certain policy blocks, which can be confusing. For a pure unknown user, expect a permanent failure – the address should be removed from your list.

- **DMARC Policy Rejection**: AOL was one of the early adopters of enforcing DMARC on inbound mail. If you send on behalf of a domain with a p=reject DMARC policy and the alignment fails, AOL will bounce it. A real example: "521 5.2.1 : (DMARC) This message failed DMARC Evaluation and is being refused". This bounce (521 code) came because an email purportedly from a http://Yahoo.com address failed DMARC when delivered to an AOL recipient (a known scenario when forwarding emails). AOL treats DMARC failures as a permanent reject when the domain owner requests it. The solution is to ensure DMARC alignment or avoid scenarios (like unauthenticated forwarding) that trigger these.

- **IP Blocked for Spam/Other Policy**: AOL, like Yahoo, will block senders for spam-like activity. AOL's NDRs historically had codes like 554 5.7.1 with messages such as "Your IP has been blocked" or "Email rejected due to policy requirements". One snippet from AOL's postmaster info: "554 mtain-dc03.r1000.mx.aol.com ESMTP not accepting connections", which indicates AOL's server outright refused the connection, likely because the sender was blocked. Another common AOL-specific code was CON:B1 or similar, embedded in a 5XX message, meaning the IP is on AOL's internal blocklist due to spam complaints. These are hard bounces – no immediate retry will succeed. The sender must investigate why the block occurred (e.g., heavy spam complaints from AOL users or hitting a spam trap).

- **Dynamic/Residential IP or rDNS issues**: AOL historically was strict about requiring proper reverse DNS and not accepting mail from dynamically assigned IP ranges. If you attempt to send from such an IP, AOL could bounce with a message similar to the Outlook DY-001. For example, “554 5.7.1 AOL will not accept delivery from this IP” if the IP appears residential or has no rDNS. This is a permanent policy block.

- **User Complaint or Spamhaus Listings**: If your IP is listed on a major blacklist or has many AOL user complaints, AOL may block you. AOL’s system might respond with 554 5.2.1 with a reference to their own URL or say “blocked for abuse”. Although the exact text can vary, any 554 from AOL with wording about “not accepting delivery” or referencing spam indicates a hard bounce that needs sender action (like cleaning up complaints or delisting IP).

Soft Bounce Causes at AOL

- **Greylisting/Deferral (Transient)**: AOL can temporarily defer messages, much like Yahoo does. In fact, since the Verizon merger, AOL often returns the same 421 4.7.0 [TS01] or [TS02] deferral codes as Yahoo. So if you send to AOL triggers a soft bounce with TS01, it means AOL is temporarily deferring due to suspicious volume or content (user complaints, etc.), just as described in the Yahoo section. You might also see a generic "421 Service unavailable – try again later" from an AOL mx server, which is a soft bounce indicating the service can't take your message right now (either due to load or greylisting you).

- **DNS or Routing Glitches**: Sometimes, an AOL mail server might respond with a 4xx if it can't properly route the message internally or if there's a transient DNS issue. This is uncommon, but a "451 please try again" from AOL should be treated as a temporary problem. Your server will retry and likely succeed once the issue is resolved.

- **Recipient Mailbox Full**: If an AOL user's mailbox is over quota, AOL will usually send a bounce. It might be a 421 (temporary) or a 552 (permanent) depending on how AOL treats full mailboxes (some ISPs use 5.x.x but still expect you to retry later after the user clears space – effectively a soft issue). If you see an AOL bounce about "mailbox full" or "space unavailable," treat it as a soft bounce. You might try re-sending after some time; however, if the condition persists for many days, the mailbox might be abandoned.

- **Spam Filter Deferred (Trial)**: AOL could initially accept a message but then decide to defer similar messages for a short time if it sees borderline spam behavior. This is more speculative, but akin to Yahoo's behavior. Practically, if you get a 421 from AOL mentioning something like "temporarily deferred", the best approach is to slow down and monitor – it's not an outright block yet.

Mitigation & Optimization for AOL

Because Yahoo and AOL share backend systems now, many of the Yahoo best practices apply to AOL as well. Keep your sending reputation healthy: low complaints, authenticated emails, and clean lists. If you encounter a hard bounce from AOL referencing DMARC (521 5.2.1), it's telling you the sender's domain policy is rejecting your mail – ensure you're not spoofing addresses without alignment. For example, if you forward emails, implement SRS (Sender Rewriting Scheme) so forwarded mail passes SPF/DMARC and doesn't bounce at AOL for policy reasons.

If your IP is blocked (e.g., a 554 with AOL refusing connection), use AOL's postmaster support. AOL used to have a dedicated http://postmaster.aol.com site and contact for senders. Now, Verizon Media has a support page for both Yahoo and AOL senders (the Yahoo Sender Hub). You can find AOL's specific error code definitions there or contact their postmaster team to request unblocking once you've fixed the issue. Joining the AOL Feedback Loop is recommended (if separate from Yahoo's, ensure you have both), so you get notified of AOL user spam complaints. Removing complainers will help prevent blocks.

When you see temporary deferrals from AOL, treat them similarly to Yahoo's: pause or slow your send, and resume gradually. Consistency and patience are key – AOL's servers will lift temporary deferrals after a cooling-off period if no further bad signals are seen. Lastly, ensure your DNS and server configuration are solid for AOL: have correct reverse DNS, and ideally send from an IP with a positive history (AOL still values IP reputation significantly). By aligning your practices with Yahoo/AOL guidelines and quickly reacting to any AOL-specific bounce messages, you can keep your AOL deliverability strong.

Zoho Mail

Zoho Mail is a smaller but notable provider (popular especially for business domains and users of the Zoho CRM suite). Zoho's bounce behaviors combine standard SMTP codes with its own filtering rules. They also employ techniques like greylisting for unknown senders. If your audience includes addresses hosted at Zoho (e.g., user@zohomail.com or businesses using Zoho to host their domain email), consider the following bounce scenarios

Hard Bounce Causes at Zoho

- **Unknown User / No Mailbox**: Like all providers, Zoho will issue a hard bounce if the recipient address is not valid on their system. The SMTP response will be 550 5.1.1 “Recipient address rejected: User unknown in virtual mailbox table”. This message explicitly tells you the user does not exist on Zoho’s mail server. It’s a permanent failure – no amount of retrying will help. The sender should remove or correct the address.

- **Spam Content Rejection**: Zoho operates spam filters that can outright reject an email deemed highly suspicious or malicious. In such cases, you might get a bounce like 554 5.7.1 “Email cannot be delivered. Reason: Email detected as Spam by spam filters.”. This indicates Zoho’s filters blocked the message during SMTP (rather than accepting and junking it). It’s a hard bounce because the email was refused. Potential causes include sending from a known spammy IP, having malware links or phish-like content, or failing certain fraud checks. Notably, the example above was a user’s own notification email being blocked by Zoho – showing that even legitimate mail can be mistaken as spam if it trips the filters.

- **Failed IP Reputation or Blacklist**: If your IP is on a major blacklist that Zoho uses, your mails could be bounced. For instance, if Spamhaus or SpamCop lists your IP, Zoho may reject the connection with a 550 error mentioning “probable spam source” (though we don’t have the exact text, this is a typical scenario). Similarly, if the sending IP has no proper reverse DNS or has a history of spam, Zoho might hard-bounce messages from it with a message about “policy rejection”.

- **Attachment or Virus Policy**: Zoho may block emails containing certain attachment types or viruses. In such cases, you’d see a 5xx error referencing a virus or disallowed file. For example, an error like “552 5.2.0 Rejected – Virus detected” could appear if your message has a virus. This is a permanent rejection until the content is cleaned.

Soft Bounce Causes at Zoho

- **Greylisting (451 Temporarily Deferred)**: Zoho Mail is known to employ greylisting for unfamiliar senders. If your mail server has never sent to Zoho before, the first attempt may get a 451 4.7.1 “Greylisted, try again after some time”. This is a soft bounce by design – your server should retry after a delay. The example from Zoho’s forum shows Zoho greylisted emails forwarded from another domain, prompting the sender to retry later. After a successful retry (usually after a few minutes), Zoho will accept future emails from that sender more readily. Greylisting is temporary and automatically lifts after the sender proves itself by retrying.

- **Recipient Mailbox Full**: If a Zoho Mail user’s storage is full, Zoho might respond with a 450 or 552 indicating the mailbox is over quota. Often, a mailbox full is treated as a temporary issue (450 4.2.2) because the user could free up space. The bounce might say “User’s mailbox is full” or “Quota exceeded.” You, as the sender, can try again later, but it’s wise to notify the recipient through another channel if possible, so they can clear space. Until they do, further emails will bounce.

- **Temporary System Issue or DNS error**: Zoho could send a soft bounce if, for example, it’s unable to route your message internally due to a transient error, or if there’s a DNS resolution issue with the recipient’s domain (in case of hosting multiple domains). A generic 421 4.3.0 Temporary error from Zoho would fall here. These are rare and usually resolve quickly.

- **Anti-Spam Threshold Deferral**: In cases where your email is borderline spammy but not a clear reject, Zoho might initially accept and then bounce with a transient error. Or they might slow down acceptance of your messages (temporarily deferring some). If, for instance, you send a burst of emails to Zoho users and some look suspicious, Zoho might start issuing 421 deferrals to throttle you. This soft bounce signals you to slow down and maybe review your content for spam triggers.

Mitigation & Optimization for Zoho

To successfully reach Zoho inboxes, be prepared for the greylisting mechanism. Ensure your mail server is configured to retry emails after a temporary 4xx – most are by default. Don't panic if you see a "451 Greylisted" bounce; simply allow the server to retry (Zoho usually accepts on the second attempt). Implementing proper SPF and DKIM for your domain can sometimes shorten the greylisting period, since Zoho might be more lenient if the sender is authenticated. In the forum case, the sender noted SPF/DKIM failures were "accepted" eventually, implying that even if your first attempt fails auth, Zoho will still allow a retry via greylisting. Nonetheless, having correct SPF/DKIM may improve your trust score.

For spam filter bounces (554 5.7.1), analyze your email content and sending IP. If you believe it's a false positive, you may need to reach out to Zoho support to whitelist your sending address or at least provide guidance. Meanwhile, check common spam triggers: avoid sending emails that are purely image-based, have phishing-like links, or overly promotional language. If your legitimate emails are blocked, consider sending a test message to a Zoho address with simpler content to see if it passes – that can identify if content was the issue.

Maintain a good sending reputation: while Zoho is smaller, it still uses data from DNSBLs and likely keeps an internal reputation score. So, keep your complaint rates low and avoid being listed on popular blacklists. If you do get a bounce referencing a blacklist (Spamhaus, etc.), take immediate action to remove your IP/domain from it.

List hygiene matters for Zoho too – sending to a lot of invalid Zoho addresses will trigger greylisting or worse. So, remove hard-bounced addresses promptly. If you suspect a particular user's mailbox is full or inactive (repeated soft bounces over days), you might suppress that address until you hear they've resolved the issue.

Zoho doesn't have as extensive a postmaster site as Gmail or Microsoft, but they do have support forums and a "Zoho Cares" support channel. If you consistently face bounce issues with Zoho that you can't resolve (e.g., your IP gets blocked erroneously), you may contact their support with the bounce details for resolution. Overall, by following standard good sending practices – authentication, prudent sending pace, clean lists, and good content – you can minimize bounces from Zoho addresses.

Conclusion: Best Practices to Reduce Bounce Rates

Across all ESPs/ISPs, the root causes of bounces often fall into a few categories: invalid addresses, recipient mailbox issues, message content/reputation problems, and technical authentication or policy enforcement. To keep your bounce rate low and your deliverability high, consider these best practices

- **Maintain Pristine Email Lists**: Remove or correct invalid addresses immediately after a hard bounce (5xx user unknown). Implement double opt-in and periodic list cleaning to avoid sending to dead addresses. This prevents not only hard bounces but also protects your sender reputation (sending to many invalid users can look like “namespace mining” to providers like Outlook).

- **Send Opt-In, Relevant Content**: High engagement and low complaints are the goal. Only send to users who have opted in, and honor unsubscribe requests promptly. Emails that generate spam complaints will lead to blocks (e.g. Yahoo/Yahoo’s TS01 deferrals or Outlook’s SC-004 complaint-based block). By sending relevant content at a reasonable frequency, you reduce the risk of recipients hitting “Report Spam,” which directly reduces both soft and hard bounces due to reputation.

- **Implement Proper Authentication (SPF, DKIM, DMARC)**: All major ISPs now check SPF/DKIM on inbound mail. Failing these can cause bounces – Gmail 5.7.26 for DMARC, or Gmail’s 4.7.0 temp-fail for missing auth, or Yahoo rejecting for failed DKIM. Ensure your sending domains have SPF records authorizing your mail server IPs, DKIM signatures on all outgoing mail, and a DMARC policy (even p=none for reporting). This not only prevents authentication-related bounces but also boosts your credibility with receivers.

- **Warm Up New IPs and Domains**: If you start sending from a new IP or domain, ramp up volume gradually. Many providers will soft-bounce or throttle large bursts from a new sender (Gmail’s “unusual rate” 4.7.0 deferrals, Outlook’s rate-limit 421s). Begin with smaller sends and build up as engagement allows. Warming up helps establish a positive sender reputation and avoids triggering greylisting or spam blocks early on.

- **Monitor Sender Reputation & Feedback**: Use tools provided by the mailbox providers – e.g., Google Postmaster Tools for Gmail, SNDS for Outlook, Verizon Media Postmaster for Yahoo/AOL – to keep an eye on your IP/domain reputation, spam complaint rates, and any error trends. Also, sign up for feedback loops (FBLs) where available (e.g., Yahoo/AOL, Microsoft’s JMRP) so you get notified of spam complaints. By quickly removing complainers and adjusting your content strategy, you prevent minor issues from escalating into blocks and bounces.

By implementing the strategies above, you address the root causes of both hard and soft bounces. The result: a healthier sender reputation, improved inbox placement, and ultimately more of your emails reaching their intended recipients. In the ever-evolving landscape of email deliverability, staying proactive about bounce management across different ESPs will give you a significant advantage. Keep learning each provider's nuances, adapt your practices accordingly, and your bounce rates will remain as low as possible while engagement soars.

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