

Key Email Deliverability Trends for 2025 – A Warmy.io User's Guide

Maintaining strong email deliverability in 2025 is critical for Warmy users aiming to land in the inbox and drive ROI. With stricter standards from inbox providers and evolving regulations, failing to meet new authentication and hygiene requirements risks spam filtering and lost audience trust. This report outlines five key trends for 2025 and offers actionable advice to help you adapt and keep your emails visible and effective.



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



The
Warmy.io team

Table of contents

Page 5: **Stricter Authentication Protocols (SPF, DKIM, DMARC)**

Page 9: **Increased Emphasis on Email List Hygiene**

Page 14: **Growing Integration of AI in Email Marketing and Deliverability Optimization**

Page 20: **Adapting to New Global Privacy and Data Protection Regulations**

Page 26: **Microsoft's New Bulk Sender Requirements (May 2025)**

Page 32: **Conclusion**

Key points or TL:DR

- **Stricter Authentication Requirements:** Major providers now demand SPF, DKIM, and DMARC authentication for better sender verification and security.
- **Enhanced List Hygiene:** Keeping email lists clean and engaged is critical for avoiding spam traps, bounces, and deliverability issues.
- **AI in Email Optimization:** AI tools help personalize content, predict recipient behavior, and streamline warm-up processes, boosting engagement and inbox placement.
- **Privacy and Compliance Focus:** Global data privacy regulations continue to tighten. Explicit consent and clear unsubscribe options are non-negotiable.
- **Microsoft's 2025 Deliverability Changes:** High-volume senders must meet Microsoft's new authentication and hygiene standards to maintain inbox placement.

Stricter Authentication Protocols (SPF, DKIM, DMARC)

What's Happening: Email service providers are aggressively pushing senders to implement proper email authentication protocols. SPF, DKIM, and DMARC – once “best practices” – are now effectively mandatory for anyone sending bulk email in 2025.

Google and Yahoo set the tone in early 2024 by requiring that high-volume senders (those sending >5,000 emails per day to their domains) have these authentication protocols in place, including at least a DMARC record with a policy of p=none. Senders who fail to meet these standards risk seeing their emails deferred or rejected; in fact, Google started bouncing a portion of non-compliant messages in 2024 and gradually increased rejection rates. This industry-wide crackdown continues in 2025.

Adoption of DMARC has surged (an 11% increase was observed in one recent survey after Gmail/Yahoo's changes), and mailbox providers have signaled that basic compliance is only the first step. Yahoo's email product director has stated “the end goal is ideally a policy of p=reject” for DMARC – meaning in the near future, simply having a monitoring (p=none) policy may not be enough. In other words, email providers want to ensure that senders are fully validating their identity and taking responsibility for their mail. New related standards (like BIML for brand logos) also require strict authentication to work, further incentivizing senders to shore up their DNS records.

Why It Matters in 2025: Proper authentication is the foundation of trust between your sending domain and mailbox providers. Without it, your messages are much more likely to be flagged as suspicious or spoofed and sent to spam. Now that giants like Gmail, Yahoo, and Microsoft (more on Microsoft's specific policy later) are enforcing these protocols, failing to configure SPF/DKIM/DMARC will directly hurt your deliverability.

Every legitimate Warmy user should also welcome these changes – they help ensure bad actors and spoofer are filtered out, which in turn means your authenticated, well-configured emails stand a better chance of inbox placement.

In 2025, proper authentication isn't optional: Every sender should use SPF and DKIM, and bulk senders need a DMARC record at least set to p=none to reach inboxes reliably. As providers phase in stricter enforcement, we can expect that moving to a quarantine or reject policy for DMARC will become the new standard for reputable senders.

In short, having these protocols not only prevents others from spoofing your domain – it also serves as a “passport” that convinces mailbox providers you are a responsible sender, improving your reputation and inbox placement odds.

How to Adapt: Make authentication a top priority in your 2025 email strategy. Here are some practical steps for Warmy users:

- **Audit and Update Your DNS Records:** Ensure your domain has a valid SPF record that lists all of your sending servers/IPs, a DKIM key set up for all email streams, and a DMARC record. At minimum, set DMARC to p=none (monitoring) with proper alignment, so you can gather reports – this is now required by major providers. As you gain confidence that all legitimate mail is authenticated, consider moving your DMARC policy to p=quarantine or p=reject to fully prevent unauthorized use of your domain (and to meet the stricter standards that providers hint are coming).
- **Monitor Authentication Results:** Use tools to check that your emails pass SPF and DKIM checks consistently. Warmy’s platform provides insights into sender authentication, including checking your SPF, DKIM, and DMARC configuration, and can guide you on any issues to fix for better deliverability (e.g., if your DKIM signature fails, Warmy can alert you to that). Regularly review DMARC aggregate reports (or use a service to visualize them) to spot any sources failing alignment.
- **Leverage Warmy for Testing:** When warming up a new domain or IP with Warmy, pay attention to the deliverability reports and health checks. Warmy’s system sends emails to a network of test inboxes (across Gmail, Outlook, etc.) and can indicate if your messages are being flagged. If you see authentication-related warnings in Warmy’s dashboard, address them immediately by fixing DNS entries. Warmy even offers free tools like an SPF record generator and DMARC record generator to help you set these up correctly. A fully authenticated warm-up process ensures that once you scale up sending, you won’t hit an authentication roadblock.
- **Stay Ahead of the Curve:** Given that mailbox providers ultimately want strict DMARC enforcement, you can stand out as a reputable sender by moving to a stronger DMARC policy before it’s universally required. This proactive approach not only protects your brand from spoofing but also sends a clear signal to ISPs that you’re a highly trustable sender, potentially boosting your inbox placement.

In summary, 2025 is the year to double-check that every email you send carries the proper “credentials.” With Warmy’s help in monitoring and a solid implementation of SPF, DKIM, and DMARC, you’ll satisfy the stricter authentication demands and keep your sender reputation intact.

Increased Emphasis on Email List Hygiene

What's Happening: As email filters grow smarter, they're looking not just at what you send but whom you send it to and how those recipients react. In 2025, there is a heightened emphasis on email list hygiene – the practice of keeping your contact lists clean, up-to-date, and limited to genuinely engaged recipients. Having a huge email list full of old or unengaged addresses is now a serious liability. In fact, regular email list hygiene ensures you're only reaching interested, valid contacts, which reduces the chances of hitting spam traps. Spam traps (email addresses set up by ISPs or anti-spam entities to catch senders with poor list management) are a major threat: hitting one can severely damage your sender reputation or even get you blocklisted. ISPs have made it clear that senders who don't manage bounces and inactive addresses will suffer. For example, Microsoft's new guidelines explicitly recommend **“remove invalid addresses regularly”** as a best practice to maintain sender quality. Moreover, mailbox providers are increasingly using engagement-based filtering. This means if a large fraction of your list never opens or interacts with your emails, future emails are more likely to be treated as spam. **AI-powered spam filters are looking at engagement metrics to determine placement – a clean, engaged list signals that your emails are wanted and valuable.**

In 2025, we also see more tools and services to help with list hygiene (from email verification services that can scrub out bad addresses, to CRM features that automatically suppress chronically inactive contacts). Email marketers are moving away from the old “batch and blast” mentality. Instead of hoarding every contact they've ever acquired, smart senders now focus on quality: keeping lists lean and full of people who actually want to hear from them. List hygiene isn't a one-time task but an ongoing process: many organizations have adopted rolling sunset policies (where they gradually phase out or try to re-engage inactive subscribers).

Why It Matters in 2025: All the fancy authentication and content optimization in the world won't help if you're sending to bad addresses or people who consider your emails unwanted. Poor list hygiene can lead to high bounce rates (sending to a lot of invalid emails), which ISPs interpret as negligence or spamming. It can also lead to more spam complaints if you keep messaging people who have lost interest or don't remember subscribing. Those signals – bounces and complaints – are tracked in ISP algorithms and can quickly tank your sender reputation.

Conversely, a well-maintained list improves deliverability because: (a) you avoid negative signals like bounces, spam traps, and complaints, and (b) you generate positive signals (opens, replies, clicks from genuinely interested recipients). In 2025's environment, engagement is king. ISPs like Gmail measure your overall campaign engagement rate and may prioritize senders with higher user interaction. A clean list directly contributes to that.

Additionally, new privacy regulations (next section) increasingly require proof of consent – another reason to only keep contacts who have legitimately opted in. Ultimately, sending to fewer, higher-quality contacts is far more effective than blasting to a bloated list full of risks. It not only protects your sender reputation but also boosts your conversion metrics (since you're focusing on people who care).

How to Adapt: Make list hygiene a continuous part of your email workflow. Some recommendations for Warmy users:

- **Verify and Remove Invalid Emails:** Use an email verification tool (many are available, and Warmy users often integrate these in their workflow) to periodically check your list for addresses that have become invalid (e.g., accounts that were deleted or have typos). Removing these addresses will reduce your bounce rate dramatically – studies show that verified email lists can reduce bounce rates by up to 98%. ISPs take notice of bounce rates, so keeping that near zero helps your reputation.
- **Purge Spam Traps and Dormant Contacts:** Spam traps often lurk in older lists or purchased lists (which you should never use). If you haven't emailed a segment of contacts in a long time, don't just fire off a big email blast to them; instead, run those addresses through a verifier first or send a re-confirmation campaign. Remove any addresses that hard-bounce. For contacts who never engage, implement a sunset policy: e.g., if a subscriber hasn't opened or clicked any email in, say, 6 months, consider removing or at least excluding them from future sends. It's better to have a smaller list of people who interact than a large list where many ignore you. This reduces the chance of hitting recycled spam trap addresses (old abandoned emails that turned into traps).
- **Use Double Opt-In for New Subscribers:** Adopting double opt-in (where a new subscriber has to confirm their email address by clicking a link) can drastically improve list quality from the start. It ensures the address is valid and that the person truly wants your emails. Yes, it adds a tiny bit of friction, but that friction keeps out bots, fake sign-ups, and typo'd addresses that could become bounces or traps. In 2025, many businesses have returned to double opt-in as a best practice for building healthy lists, especially in regions with strict consent laws. If you're capturing leads via landing pages or forms, consider enabling double opt-in. Warmy doesn't manage your subscription process, but as a user, you could feed only confirmed addresses into the Warmy warming campaigns or your email campaigns, ensuring you start with a high-quality list.

- **Monitor Engagement and Segment Accordingly:** Keep an eye on engagement metrics (opens, clicks, replies). Most email marketing platforms and Warmy's deliverability insights will tell you how recipients are interacting. Consider segmenting your list by engagement level – for example, “hot” segment (opened or clicked in last 30 days), “warm” (last 31-90 days), “cold” (no interaction in 90+ days). You might send different content or re-engagement campaigns to the cold segment, and if they still don't respond, it's time to stop mailing them. Engagement is now directly tied to deliverability, so sending only to those who want your emails will improve your inbox placement over time.
- **Use Warmy's Insights to Diagnose List Issues:** While Warmy is primarily an automated warm-up and deliverability enhancement tool, it can indirectly help with list hygiene. How? By observing the performance of your warm-up campaigns. For example, if your emails in Warmy's network are landing in spam or getting low engagement, it might be a sign that something in your sending practices needs improvement. Also, Warmy's Email Health Checker and similar features can sometimes flag if your domain or IP reputation is suffering (which can happen if you've been hitting spam traps or high bounces). If you see a sudden reputation drop, investigate your most recent email sends and consider whether list quality issues played a role. In essence, Warmy helps build a strong sender reputation baseline; it's your job to maintain that by not poisoning the well with a dirty list.

By scrubbing out bad contacts, focusing on engaged subscribers, and using tools to automate this process, you'll keep your sender reputation strong and your inbox placement high. Remember, when it comes to email lists in 2025, quality beats quantity every time.

Growing Integration of AI in Email Marketing and Deliverability Optimization

What's Happening: Artificial Intelligence (AI) is revolutionizing how email campaigns are crafted, sent, and optimized. In 2025, more email marketers than ever are leveraging AI-driven tools to boost both campaign performance and deliverability. According to recent industry data, **about 35% of companies are already using AI in their email marketing workflows**, and this number is growing. AI is being integrated in several key areas:

- **Content Creation & Personalization:** Generative AI tools (like GPT-based systems) can now write email copy, subject lines, and even generate entire templates in a human-like way. Marketers use these to brainstorm and produce engaging content faster. More importantly, AI is used to personalize emails at scale – analyzing subscriber data to tailor subject lines, product recommendations, and send times for each recipient. Instead of one-size-fits-all newsletters, AI can help create dynamic content that changes based on the recipient's preferences or past behavior. This level of personalization was cumbersome in the past, but AI makes it much more accessible. The result is emails that feel more relevant to recipients, which increases open and click rates. In fact, studies predict that **60% of B2B marketers will integrate AI-driven personalization into their email strategies by 2025, reflecting how critical this is becoming.**
- **Send-Time Optimization & Predictive Analytics:** AI algorithms can analyze when each individual user is most likely to check their inbox and interact, then schedule emails accordingly for optimal timing. Some email service providers now offer “predictive sending” features where AI looks at a user's past opens to predict the best send time. Additionally, predictive analytics can identify which recipients are most likely to convert or which leads are “hotter,” allowing you to prioritize and target those contacts. Essentially, AI can crunch massive amounts of engagement data to find patterns that humans might miss – for example, it might segment your list automatically based on subtle behavior patterns or predict which subscribers are at risk of disengaging. All of this helps you send smarter campaigns that get better engagement and avoid sending emails to folks who are unlikely to respond.

- **AI-Powered Deliverability Tools:** Beyond content and targeting, AI is directly used to improve deliverability. A prime example is the emergence of AI-driven email warm-up and reputation management tools. These tools (including Warmy) simulate human-like interactions to build up your sender reputation automatically. They typically work by sending emails from your account to a network of test inboxes and having those messages be opened, replied to, and marked as “not spam” in a coordinated way. This fools the algorithms (in a legitimate way) into seeing your emails as welcomed by recipients, thus boosting your reputation. For instance, Warmy’s AI engine conducts interactions with real inboxes on your behalf – ensuring your emails are opened, replied to, and even pulled out of spam if they land there, which **“ensures your emails are opened, marked important, and stopped going to spam, significantly boosting your sender reputation”**. In practice, what a tool like Warmy does is automate the warm-up process that used to be manual. They adjust sending volumes, content, and engagement in an intelligent way to gradually earn the trust of ISPs. AI is also used in monitoring: Some deliverability dashboards use machine learning to analyze your campaigns and suggest changes (for example, flagging language that might trigger spam filters or identifying segments of your list that are hurting engagement metrics).
- **AI in Spam Filtering (Defensive AI):** It’s worth noting that ISPs themselves use advanced AI to detect spam or phishing. They analyze email content, sender behavior, and recipient engagement using machine learning models. This means the battle for the inbox is often AI vs AI – with mailbox providers’ AI trying to block unwanted mail and senders’ AI trying to prove their mail is wanted. This dynamic is driving both sides to get more sophisticated. For legitimate senders, the takeaway is that adopting AI tools can help you keep up and ensure your emails don’t get mistakenly caught in the crossfire.

Why It Matters in 2025: The integration of AI can significantly improve your email performance and deliverability, which go hand in hand. Higher engagement from better content and timing leads to better sender reputation (ISPs see that people open and click your emails, which suggests your mail is desired). At the same time, AI-driven warm-up and reputation management can solve technical deliverability challenges that might otherwise require dedicated experts.

For Warmy users specifically, AI is at the core of Warmy's value – it automates the tedious but crucial process of warming up new domains/IPs and maintaining a positive reputation. Users who take advantage of these AI capabilities can focus more on strategy and content while trusting the tool to handle the “behind-the-scenes” inbox placement factors. Additionally, by using AI for personalization, you can greatly increase the relevance of your emails. In 2025, recipients have inboxes full of automated, generic emails (since automation is widespread). AI gives you the power to rise above that noise with highly personalized messaging, which can translate to better engagement and fewer spam complaints.

Also, consider the competitive aspect: if your competitors are using AI to optimize their email programs and you're not, you risk falling behind. An AI-augmented email strategy can yield incremental improvements in deliverability that compound over time – for example, a slightly higher open rate because of smart send-time optimization can lead to a virtuous cycle of improving reputation, leading to even more inbox placement and opens in the future. Essentially, AI can act as a force multiplier for your email program's success.

How to Adapt: Embrace AI thoughtfully as part of your email strategy.

Here are some tips:

- **Use AI for Content and Subject Lines:** Consider using AI writing assistants to generate or refine your email content. For instance, you might use an AI tool to draft 5 versions of a subject line, then pick the best. AI can help you A/B test at scale by providing many variations. Just be sure to review AI-generated content for accuracy and tone – it's there to assist, not fully replace human judgment. Personalized content is key: try feeding the AI with data about your user segments so it can tailor the output (e.g., different product recommendations for different industries). Many Warmy users are cold email senders; if that's you, an AI tool can help you craft messages that sound more individual and less templated, which can improve reply rates and reduce the chance of being flagged as spam.
- **Implement AI-Powered Personalization:** Leverage tools or ESP features that automatically personalize send times, frequencies, or content. For example, you might enable a feature that sends each email at the optimal time for each subscriber (determined by AI analysis of past behavior) – this can lift open rates and is increasingly easy to do with 2025 technology. You can also use AI to analyze which products or topics a user is most interested in (based on clicks or website behavior) and then dynamically change newsletter content to match those interests. The more relevant your emails, the better your engagement and deliverability. If you have a large list, consider an AI segmentation tool that can automatically cluster subscribers into segments you might not have discovered (e.g., an algorithm might find a cohort of users that tend to only open weekend emails, or who prefer a certain type of content).

- **Take Advantage of Warmy's AI for Deliverability:** Warmy is an AI-driven email deliverability platform by design. To benefit, ensure you run your new sending accounts through Warmy's warm-up process. Warmy's AI will gradually increase your sending volume and interact with thousands of other inboxes to build your reputation. For example, Warmy's network will open your emails, mark them as important, reply to some, and move any that go to spam back to the inbox – all actions that signal to providers that your emails are legitimate and wanted. Warmy's dashboard provides real-time insight into how this warm-up is going. By the time Warmy's AI has finished its cycle, your email account or domain will have a much better standing, allowing your real campaigns to hit the inbox rather than spam. This is a clear case where AI directly improves deliverability. If you're already using Warmy, make sure to utilize features like the Email Deliverability Checker and Template Checker – these use AI/ML to analyze your content and technical setup for any red flags. Warmy's AI can also generate suggestions (and even personalized warm-up message content automatically) to continuously keep your sender reputation high.
- **Monitor AI Outcomes and Fine-Tune:** While AI can automate a lot, don't put it entirely on autopilot. Monitor your results and tweak as needed. For example, if you let an AI tool choose send times, periodically check if that's actually improving engagement. If you use AI-generated content, watch your spam complaint rates or replies to ensure the content isn't accidentally offensive or too "bot-like." AI is powerful, but it works best in partnership with human oversight. Keep an eye on Warmy's reports to see the effects of the warm-up. If something looks off (e.g., deliverability doesn't improve as expected), Warmy's support or community might help interpret the AI's data and adjust the strategy. The key is to integrate AI's capabilities with your own expertise about your audience.

Adapting to New Global Privacy and Data Protection Regulations

What's Happening: The regulatory landscape around data privacy and electronic communications continues to tighten worldwide, and 2025 is seeing significant new developments. In recent years, laws like the EU's GDPR (General Data Protection Regulation) and California's CCPA/CPRA (California Consumer Privacy Act / California Privacy Rights Act) have set high standards for user consent and data protection in marketing – including email marketing. Now, more regions are following suit with their own regulations, creating a global patchwork of rules that email senders must navigate. For example, **momentum for stricter privacy laws accelerated in the U.S.: five new state privacy laws took effect on Jan 1, 2025, with three more coming into force later in the year.** These include states like Delaware, Iowa, Indiana, etc., each with their own requirements for how businesses handle personal data and marketing communications. Other countries around the world (such as Brazil with LGPD, Canada with updated CASL guidance, and India with its new Personal Data Protection Act) are likewise enforcing tougher rules on email consent and data usage.

Key themes of these regulations include: **requiring clear consent from users to receive marketing emails, giving users the right to easily opt out or unsubscribe, limiting data retention, and penalizing misleading or excessive emailing.** GDPR, for instance, mandates opt-in consent for marketing emails in most cases (especially to individuals in Europe) and heavy fines for non-compliance. The newer laws often mirror these principles. Microsoft's own move to enforce unsubscribe links and consent (as mentioned in their bulk sender guidelines) aligns with the regulatory push that marketing emails must respect user choice. In 2025, we're also seeing increased enforcement – regulators are not shy about issuing fines or warnings to companies that send spam or misuse email data. Even if you are not directly governed by some of these laws, big email providers often implement policies that effectively enforce these principles broadly. For instance, Google's bulk sender guidelines require honoring unsubscribe requests within 2 days, which is essentially a reflection of good practice and regulatory expectations.

Why It Matters in 2025: For email marketers, adapting to privacy regulations isn't just about avoiding legal trouble (though that's a huge motivator – fines for GDPR violations can reach into the millions). It's also about maintaining deliverability and customer trust. If you're sending emails to people who haven't given explicit permission, you're far more likely to be reported as spam. Spam complaints directly harm your sender reputation and deliverability. Conversely, emailing only people who have consented and who expect your emails means fewer complaints and higher engagement – exactly what ISPs want to see for good inbox placement.

From a legal standpoint, regulations can dictate certain practices that influence your deliverability. For example, laws often require an unsubscribe mechanism in every marketing email (CAN-SPAM in the US, CASL in Canada, GDPR in EU all have this requirement). If you fail to include an easy unsubscribe link, not only are you breaking the law, but you also risk recipients marking you as spam because they can't find a proper way to opt out. Another example: GDPR gives individuals the right to access or delete their data. If a user in the EU flags your emails as unwanted and invokes their rights, you could face compliance headaches if you haven't managed your list hygiene and records properly. Essentially, good deliverability and legal compliance go hand in hand – both require sending relevant emails to people who want them, and respecting those who don't.

In 2025, with privacy laws multiplying, email senders must be more careful about how they collect and use email addresses. You might need to implement region-specific rules (e.g., double opt-in for EU subscribers if not already, or honoring “Do Not Sell” or global unsubscribe lists for certain jurisdictions). It adds complexity, but ignoring it can lead to severe outcomes beyond just spam folders. It's also a brand reputation issue: consumers are more aware of privacy and can lose trust in a company that spams or misuses their email. On the flip side, demonstrating respect for user privacy can improve your brand image and email engagement; subscribers who know you value their consent are more likely to remain subscribed and interact with your emails.

How to Adapt: Make compliance and respect for user privacy a fundamental part of your email strategy. Here's how Warmy users (and all email senders) can adapt to the evolving privacy landscape:

- **Ensure Proper Opt-In Practices:** If you haven't already, switch to an opt-in (preferably double opt-in) model for email list building. This means only emailing people who have actively signed up and confirmed their email addresses. Avoid purchasing lists or scraping contacts – those tactics not only violate most laws but also yield very poor deliverability (since the recipients are cold and often mark such emails as spam). If you operate internationally, be aware of the strictest requirements: for example, in the EU, you generally need explicit consent before emailing someone marketing content (the days of pre-checked subscribe boxes are gone). Double opt-in, as mentioned, can help provide proof of consent which is useful under laws like GDPR. Warmy's platform might not directly handle your sign-ups, but as a user you should feed Warmy only contacts that have legitimately opted in. Notably, Warmy's Cold Outreach Laws resource is available to users – use such resources to educate yourself on legal requirements in different regions.
- **Include Clear Unsubscribe Options in Every Email:** This is non-negotiable. Every marketing or bulk email you send should have a visible, easy way for the recipient to unsubscribe or opt out. Many laws require it (CAN-SPAM, CASL, GDPR, etc.), and Gmail/Yahoo will penalize senders who don't include one-click unsubscribe links. Make sure the unsubscribe process is smooth – ideally one click, no login required, and honor the removal quickly. Google expects unsub requests to be processed within 2 days (and legally CAN-SPAM says within 10 days). If you're using an email service provider, this is usually built-in. If you're sending cold emails manually, you still need to include an unsubscribe notice (even just a line like “If you don't wish to hear from us, let us know or click here”). Not only does this keep you compliant, it also reduces spam complaints because people have a proper avenue to opt out. Microsoft explicitly calls for “functional unsubscribe links” in their 2025 sender guidelines, showing how this overlaps with deliverability best practices.

- **Manage Your Data and Respect User Rights:** Develop a habit of maintaining records of consent – for example, keep track of when and how each subscriber joined your list. In case of an inquiry or audit (especially under laws like GDPR), you should be able to show that a user opted in. Also, be prepared to delete or stop emailing someone if they request it (GDPR “right to be forgotten” or similar rights in other laws). From a deliverability perspective, if someone asks to be removed or unsubscribed, do it promptly – sending email to people who explicitly said they don’t want it is a sure way to generate spam complaints or even have them report you to authorities. Many Warmy users might be in B2B sales or outreach, which sometimes operates in a gray area of cold emailing. If that’s your use case, **research the specific laws for B2B communication** in your target country – some places allow B2B cold emails with certain conditions (e.g., you must include an unsubscribe and your company address), while others treat them the same as consumer spam. Warmy’s service will help you with technical deliverability, but it’s up to you to ensure you’re not violating any solicitation laws in the process.
- **Stay Informed on New Regulations:** Make it a point to periodically check for updates on email and data protection laws in the regions where your contacts live. 2025 introduced many new rules (like those new U.S. state laws). These laws can affect things like whether you can use emails collected from third parties, how you must structure your privacy policy, etc. Subscribing to industry blogs or using resources (many email service providers publish compliance guides) can keep you updated. Warmy’s blog or knowledge base might also cover deliverability in context of laws (for example, they might publish articles on how GDPR affects cold emailing, etc.). Taking the time to read those can save you from deliverability nightmares later. Remember, compliance isn’t a one-time project – it’s ongoing, just like list hygiene.

- **Align Your Email Strategy with Privacy-Friendly Principles:**

Ultimately, adopting a privacy-first mindset tends to naturally improve deliverability. Practices like only emailing interested users, providing value in your content, and giving users control result in a healthier sender-recipient relationship. Try to segment users by the level of consent or preferences they've given. For instance, if someone only agreed to receive your monthly newsletter, don't suddenly start sending them daily promo emails. If you allow people to set preferences (frequency, topics of interest), honor those. Not only will this keep you compliant with consent requirements, it will also lead to higher engagement (since you're sending what the user expects).

Warmy's Role: Warmy is an ally in deliverability, but it doesn't override laws. Use Warmy's deliverability boosts in conjunction with a strong compliance foundation. For example, Warmy can help you land in the inbox by improving your technical reputation, but if you were to use that power to send spammy or non-compliant emails, you'd still get in trouble (and likely damage the reputation Warmy helped build).

However, one indirect way Warmy helps with compliance is by improving your email placement such that you can be more confident that when you send a confirmation email or re-permission email (common tactics to ensure compliance), it will reach the inbox. This helps in onboarding subscribers legally. Also, by monitoring Warmy's reports and inbox placement, you can catch if perhaps a particular campaign resulted in issues – which might hint at a compliance problem (e.g., if a certain segment caused a spike in spam flags, maybe those contacts didn't truly opt in). In summary, use Warmy's technology hand-in-hand with a responsible email strategy that respects user privacy. That combination will keep your sending domain in the good graces of both the law and the inbox algorithms.

Microsoft's New Bulk Sender Requirements (May 2025)

What's Happening: In a major move this year, Microsoft has announced upcoming changes to its Outlook email platform (covering addresses like outlook.com , hotmail.com, live.com, and other consumer Microsoft email services) that will affect bulk senders.

Effective May 5, 2025, Microsoft will require any domain sending high volumes of email to Outlook.com recipients (over 5,000 emails per day) to fully comply with email authentication best practices – namely having valid SPF, DKIM, and DMARC records. This policy mirrors similar standards Google and Yahoo put in place in 2024, signaling an industry-wide consensus that authentication is a must for large-scale senders. Under Microsoft's new rules, if you send more than 5,000 emails per day to Microsoft's mail domains and your emails fail authentication checks (meaning SPF doesn't pass, or DKIM doesn't verify, or you lack a proper DMARC record aligned with your domain), Microsoft will start redirecting your messages to the Junk folder. **After May 5, 2025, any high-volume email from a non-compliant domain will initially go to spam (junk) instead of the inbox.** Microsoft is giving senders a grace period to fix issues, but they have also warned that in the future (at a date to be announced) they plan to outright reject emails from domains that remain non-compliant. In short, Microsoft is raising the bar: to reach the inbox on Outlook/Hotmail, you now must authenticate your emails properly – otherwise, your deliverability to Microsoft addresses will plummet.

Additionally, Microsoft's announcement included several "hygiene" and best-practice recommendations, reinforcing other trends we've discussed. They emphasized things like using a consistent, valid **From address** that can receive replies (no more no-reply@ senders for bulk mail), providing a clear **unsubscribe link** in every message, and doing proper **bounce management and list hygiene** (removing invalid addresses, etc.). They even note that if senders don't follow these practices, Outlook "reserves the right to take negative action, including filtering or blocking" such mail. This is a strong statement – it shows Microsoft is actively policing sender behavior in a way perhaps more visible than before. Many of these things were always recommended, but now they are becoming requirements for those who send a lot of email to Microsoft users.

Why It Matters: If a portion of your audience or customers uses Microsoft email (Outlook, Hotmail, MSN, Live addresses), this change directly impacts you. Many B2C senders in particular have sizable Outlook/Hotmail segments. Even in B2B, you might have small businesses or individuals using those addresses. For Warmy users who engage in cold outreach, consider how many leads or prospects might have signed up for something using a Hotmail address – quite a few, likely. Therefore, not meeting Microsoft’s requirements could mean a chunk of your emails start going to spam folders after May 2025, hurting your engagement and conversion opportunities. Moreover, Microsoft’s stance is another confirmation that **full email authentication is now table stakes across all major providers**. Gmail and Yahoo were first, now Microsoft has joined – so virtually every large mailbox provider is on the same page. If you haven’t fixed your SPF/DKIM/DMARC by now, this is basically an ultimatum.

For those who do comply, there’s an upside: this change will help filter out truly fraudulent or low-effort spam from Outlook inboxes, potentially improving overall inbox placement for legitimate senders. It levels the playing field in a sense – everyone sending mass emails to Microsoft must adhere to the same standards, which favors those who are already following best practices.

It’s also worth noting that Microsoft’s focus on things like unsubscribe links and list hygiene in the same breath means they might also incorporate those factors into filtering decisions. This implies that even if your authentication is fine, if you’re spamming Outlook users with emails they didn’t ask for (causing lots of complaints or no engagement), Microsoft could still throttle or filter you under these “hygiene” grounds. So, it ties back to the importance of the previous trends: good list hygiene and respecting user preferences will be crucial to stay in Microsoft’s good graces. Essentially, Microsoft is codifying into policy what deliverability experts have been saying for years – authenticate your mail, send wanted emails, or suffer consequences.

How to Adapt: If you're a Warmy user (or any sender) who sends significant volume to Microsoft email users, you should take immediate steps to align with these requirements:

- **Implement SPF, DKIM, and DMARC (if not already):** This is non-negotiable. Ensure your sending domains have a correct SPF record listing all sending IPs (and that you're not accidentally sending from servers not in SPF). Set up DKIM signing on all outgoing emails – typically this means adding a DKIM public key in DNS and enabling signing in your email platform. Finally, publish a DMARC record for your domain. Microsoft's minimum ask is *p=none* (monitoring) with alignment to SPF or DKIM, but if you can, set *p=quarantine* or *p=reject* once you're confident; though *none* will satisfy the requirement, a stricter policy offers extra protection and might boost trust. Use tools to test your emails – for example, send a test to a Gmail or Outlook address and check the email headers to see if SPF and DKIM both show “pass”. Warmy can help here: when you send warm-up emails, Warmy's reports will often indicate whether your messages passed SPF/DKIM checks. Address any failures now, before May arrives.
- **Follow Microsoft's Sender Best Practices:** Make sure you have a valid From address that looks professional and can receive email. Avoid using weird domains or subdomains that don't match your branding – Microsoft (and other providers) prefer alignment (the From domain matching the authenticated domain). Ensure every email includes an unsubscribe link that actually works. If you're using Warmy to send warm-up emails, this might not apply (those are system emails), but for your actual marketing or outreach emails, double-check this element. Also, practice good bounce management – if you send an email that bounces (say, to an invalid Hotmail address), remove it from your list so you don't keep sending to it. Warmy's system, when warming, will handle fake addresses in its network, but in your real sends, your email software should handle bounces automatically – just verify that it's doing so. Microsoft explicitly calls out removing invalids to reduce “wasted messages” and spam complaints, which suggests they monitor if you keep sending to dead addresses (a sign of list negligence). So keep that list clean (tying back to Trend #2).

- **Monitor Your Outlook/Hotmail Deliverability:** After May 2025, pay attention to your metrics specifically for Outlook/Hotmail addresses. If you see a sudden drop in opens or clicks from those domains, it could be a sign your mail is going to junk due to non-compliance. Use Microsoft's own tools: **Smart Network Data Services (SNDS)** and **Microsoft's Delivery Support** (some use the O365 deliverability insights) can give data on your sending to Outlook.com. Also, Microsoft accounts should generate DMARC aggregate reports if you have a DMARC record with a reporting address; those reports will show your authentication pass/fail rates at Outlook. If you detect issues, act quickly – fix DNS records or consult resources to troubleshoot. **Warmy's Deliverability Insights** feature might also shed light by testing various providers. For instance, Warmy might simulate sends to Outlook as part of its warm-up; if Warmy indicates your Outlook inbox placement is poor, that's a red flag to investigate.
- **Leverage Warmy for Smooth Transition:** Warmy's warm-up is not only for new domains; you can use it if you suspect your domain's reputation needs repair. If you discover that your emails to Microsoft are going to spam because you missed something, after fixing the authentication, consider running a targeted warm-up focusing on Outlook addresses. Warmy's network includes Outlook/Hotmail inboxes, so it can specifically help improve your standing with Microsoft. Basically, Warmy will engage with your emails from those Outlook accounts in the network, signaling to Microsoft that your domain is legitimate and emails are welcomed. This can help pull you out of the junk folder faster. Think of it as a rehabilitation process if you got on Microsoft's bad side. Of course, Warmy works best if you've corrected the root issues (like adding that DMARC record or including an unsubscribe link).

- **Keep an Eye on the Future:** Microsoft has only announced the first phase (junking non-compliant mail). They will move to full rejections later on. This gives you an incentive to not just meet the bare minimum but exceed it. Don't wait for the reject phase to implement things like `p=reject` DMARC or other improvements. Also, anticipate that Microsoft may extend similar policies to Office 365 enterprise email in the future (if not already indirectly happening). The general direction is clear: any big mail provider is going to demand authentication and good practices, or they won't deliver your mail. By embracing this now, you future-proof your program.

In summary, Microsoft's 2025 changes essentially enforce many deliverability best practices under threat of spam-folder placement. By authenticating your emails and following sending protocols, you can continue reaching Outlook/Hotmail users. Warmy users should treat this as an opportunity: if you've already been using Warmy's AI warm-ups and deliverability tools, you likely have SPF/DKIM in place (since Warmy setup guides prompt those) and a good reputation to build on. Make any necessary tweaks now, and you'll navigate Microsoft's new rules with ease – and probably see better results across the board as the overall email ecosystem becomes more trustworthy.

Conclusion

Email deliverability in 2025 is being shaped by tighter standards and smarter technology, all aimed at ensuring that only wanted, trustworthy emails reach user inboxes. For Warmy users – who are already proactive about deliverability – these trends validate the importance of what you’re doing and provide a roadmap for where to focus next. By implementing stricter **authentication protocols**, you satisfy mailbox providers’ requirements and protect your sender identity. By maintaining **pristine email lists and high engagement**, you tell those providers that your emails deserve to be seen. Embracing AI tools can give you a competitive edge, helping you fine-tune both your outreach strategy and your sender reputation in ways that simply weren’t possible before. Adhering to **privacy regulations** isn’t just about avoiding fines; it’s about respecting subscribers – which naturally leads to better deliverability outcomes (since happy subscribers don’t mark you as spam). And finally, adapting to specific changes like **Microsoft’s new bulk sender rules** ensures no segment of your audience is left behind due to technicalities you can control.

As you implement these strategies, remember that Warmy is there to assist you. Warmy’s AI-driven warm-up and deliverability monitoring features are aligned with these trends – they help you with authentication checks, engagement simulation, and feedback on how providers view your emails. But the real magic lies in combining Warmy’s capabilities with sound sending practices on your part. Think of it as a partnership: Warmy provides the deliverability muscle, and you provide the thoughtful strategy (clean lists, good content, lawful compliance) – together, that’s a winning formula for hitting the inbox consistently in 2025.

In the ever-evolving battle for attention in the inbox, those who stay informed and adaptable will thrive. Use the trends and tips in this report as a checklist for your email program. If you cover all these bases, you can be confident that your emails will not only reach recipients but also resonate with them. Here’s to making 2025 your best year yet for email performance – with your messages landing front and center where they belong, and generating the engagement and results you need.



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

