OVERCOMING THE CHALLENGES OF B2B EMAIL DELIVERABILITY

Written by Laura Atkins
Deliverability Consultant & Owner of Word to the Wise

SPARKPOST
Table of Contents

01  What Works for Consumer Email Doesn’t Always Work for Business Email

02  The Consumer Inbox

03  The Business Inbox

07  Data & Monitoring

08  Improving Business Delivery

11  Conclusion
What Works for Consumer Email Doesn’t Always Work for Business Email

The explosion of online marketing has created a host of specialist fields in the last 10 to 20 years; email deliverability is one of them. But even those of us who’ve been around since the beginning often struggle with achieving marketing goals when sending business-to-business (B2B) email. It’s easy to assume we’re simply doing things the right way and to double down on the wrong thing. We know the advice is good – we see it work every day in consumer email programs. We tweak our programs and apply the standard recommendations but still don’t get the results we expect.

The reason so many folks struggle with B2B delivery is this: business filters are substantively different than consumer filters. The good news is that by understanding business filters and how they differ from consumer filters in goals and processes, we can improve the deliverability of B2B mail.

Achieving high deliverability is crucial for the success of email marketing programs, and most marketers are familiar with the basics of deliverability. In order to reach the inbox, you need a high reputation. And in order to get a high reputation, you need good engagement. This is all true… in the consumer space.

Email in the business space is different from email in the consumer space. In the consumer context, email is a tool – but it’s a personal tool. In a business context, email is a work tool. These distinct contexts don’t just affect how users interact with mail, they affect how the filters and email providers interact with mail.

In this guide we’ll explore:

- The differences between business and consumer inboxes
- What does and does not affect how filters act on mail
- Metrics and tools to use when monitoring business delivery
- Actionable strategies to improve business delivery
The **Consumer Inbox**

Consumers use email in many ways: leisure activities, reconnecting with friends, shopping, and a host of others. They expect that their mailbox will contain mail they want, and the mail will be safe. The consumer mailbox providers, like Google, Microsoft, and Verizon Media Group know this. They focus on providing a happy and safe email experience for their users. They curate an inbox containing mail the user wants while removing harmful mail or mail the user doesn’t seem interested in.

Because every user is unique and interacts with email differently, the providers have a big challenge on their hands. Part of the solution involves instrumenting the inbox and monitoring user interaction with messages. Mailbox providers invest considerable time and money into systems enabling them to monitor and measure user interaction with email. Some interactions, like reading or replying to email, are positive and drive reputation up. Other interactions, like deleting or marking as spam, are negative and drive reputation down. These measurements feed into and tune the filters. While these interactions are for each recipient, they do affect overall reputation. If too many users interact negatively with mail then the overall reputation decreases and deliverability falls.

Much of the standard deliverability advice works in this context. By getting users to interact with email in ways that increase positive signals and decrease negative signals, we improve reputation and delivery. We have standard tools that let us monitor how users are interacting with messages. Open tracking and click tracking are by no means perfect, but they do give senders insight into which users are engaged and which aren’t. Many consumer mailbox providers have feedback loops (FBLs) that share direct negative feedback with senders. Outlook and Gmail both provide platforms where senders can monitor their deliverability and see how their mail is performing.

In the consumer space, both senders and receivers work together on behalf of their mutual customers to ensure users get the mail they want. As deliverability experts, we know how to send wanted mail and effectively reach the consumer inbox.
The Business Inbox

Business email exists in a different context than consumer mail. At work, email is a tool for employees and their employers. Some business users utilize their inbox as a to-do list. Some use productivity hacks like ‘inbox zero’ to keep their inboxes clean and facilitate their day-to-day work. There are some email addresses that don’t go to just one person, they go to many people inside the company or even into a CRM or ticketing system. Email isn’t a fun leisure activity in the business space, it’s part of the job.

Business users don’t really own their email address. Employees don’t take their company email address with them when they move to a new employer. The business owns the address and the account and all the email in it.

Security is a much higher priority for business users than consumers. We all know that many of the breaches over the last decade have started with a malicious email. Keeping malicious email out of the network is crucial to the overall success and bottom line of the business. In fact, many business filters are not stand-alone products. They’re a part of an overall security system including firewalls, traffic monitoring, and other security tools. Email filters are one layer in a comprehensive security system.

These contextual differences affect how the filters work for businesses. Business filters do not focus on wanted email. Instead, the filters place business needs first. The overarching business need is security. In the business context, the risks of letting in a malicious email outweigh the problems of blocking a few wanted emails.

By default, business filters focus on minimizing false negatives; they would rather block a safe email than let in a malicious email. However, they also provide extensive and granular controls that let the business modify and adjust filters as needed. This is evident when you compare the controls offered to hosted customers by Google and Microsoft. Consumers have a small level of control over their inbox, mostly blocking mail or overriding the decision to put mail into the spam folder. Business users can block and unblock mail at the mail server.

In the business space, filters focus on the needs of the business over the wants of the individual recipient. The different context means what works to achieve high deliverability in the consumer space doesn’t always work for businesses.

Marketers moving from consumer marketing to business focused marketing often struggle with the different email context and experience deliverability challenges. Understanding the specifics of business filters will help marketers improve deliverability to business users.
Business Filters are a Paid Product

Most consumers use free webmail addresses, still others use addresses bundled in with their broadband connectivity. That’s not the case for business mail. Most businesses pay for their email, either through buying software, appliances, or hosted services. Several different companies provide business filtering software and appliances. Being a paid product has a direct impact on the filters and how they work.

Consumer providers make their money selling advertising access to the end user or selling broadband access directly to the consumer. Filters are not a selling point for email, they’re simply expected. People don’t pick an email address based on the spam filtering.

In the business space, however, spam and incoming email filtering are a selling point. Businesses choose their mail platforms based in part on the filtering: how they work, how effective they are, and how easy they are to use.

The Business Owns The Mailbox

When someone claims an email address for personal use, they become the owner of that address. They give that address out and use it for their own purposes. In a business context people don’t claim an address. The employer assigns an address to an employee, who uses it to facilitate the employer’s business.

As with consumer filters business filters act on behalf of the owner. But the ultimate owner is the business, not the person using that email address. When filtering, the mailbox provider acts on behalf of the mailbox owner and prioritizes the business needs and wants over those of the individual employee.

Business filters provide a significant amount of control over incoming mail to their customers. Customers can allow or deny mail based on any number of conditions to ensure that they get the mail they need. This does make it more challenging to troubleshoot business delivery problems. Sometimes it’s not clear whether the delivery failure is the decision of the filtering provider or the business itself. When the filter is business specific there are few avenues for appeal.

Filters don’t have Access to User Activity or Engagement

In the consumer space, the free webmail providers control both the email filters and the email client. The tight integration between filter and client allows the provider to measure engagement. Data gathered from monitoring user behavior feeds back into the filter and improves the accuracy and specificity of the filter. The tight integration necessary to allow the use of engagement in filtering is only possible because the provider owns the email client and the email server.
With an exception I’ll discuss in a moment, business filters and the email client are separate. Filters accept an email, decide where it should go, and deliver it to the appropriate mailbox. Employees access mail through company supplied email clients. Filters don’t have the access to measure engagement, such as opens or clicks.

The exception is Google and Microsoft. Both companies sell businesses hosted email services. Employees often access email through the same web-based email client that consumers do. The tight integration between email filter and email client are there, but the engagement of the end user isn’t as important in filtering as it is for consumer mail.

**Same Filters, Different Priorities**

In fact, Microsoft and Google provide us some of the clearest examples of how business filters are different from consumer filters. These companies each use the same filtering engine for their consumer mail and business mail. Still, we regularly see mail that delivers fine to the consumer domains and not the hosted domains or vice versa. There are a couple reasons for this difference including the de-emphasis on wanted mail and extra control over delivery granted to the domain owner.

Additionally, Microsoft and Google do not share business data back with the sender. Neither Microsoft Smart Network Data Services nor Google Postmaster tools include data from the hosted domains. Both tools only include information about the free domains. Business users can report spam to both companies through use of the this-is-spam button, but the company does not share this data through their feedback loop.

**Filters are Active**

In the consumer space, the filters are relatively passive. They typically don’t do anything more than scan the mail, add some tracking headers, and deliver the message to the user. But business filters regularly and actively interact with email as it comes in over SMTP. These actions affect not only email delivery, but they also potentially affect sender reporting and tracking.

We’ve all had to address cases where email filters have followed every link in our email. Business filters are more likely to do this than consumer filters. For performance and privacy reasons, filters are selective in following links in normal email. If, however, there is something more suspicious about an email stream or there is evidence of a broader security event, then the filters aggressively check links. When the risk is losing money or having a network breach, spending a few extra seconds to check mail is well worth it.

*Engagement isn’t as important in business filtering as consumer email.*
Business filters sometimes inject text into the body of the emails as well. These messages warn the user that the mail came from an outside source or external sender. Warnings like these demonstrate just how important security is in the business space. In the consumer space, an email provider may put warnings on a message through the web interface, but they do not add text into the body of a message.

**Limited Insight by Senders**

Part of standard deliverability advice is to monitor user activity through a host of tools, including complaints, opens, and clicks. Business filters often interfere with these tools.

For instance, many business users have a this-is-spam button, just like consumers do. The data when a user hits this button often goes back to the filter and affects reputation and future delivery. Many consumer providers share this data with the sender through FBLs. In the business space, however, there are no FBLs. Even providers that host both consumer and business mail do not share FBL data from their business customers.

We don’t just have to deal with a lack of data from business filters. Some filters actively modify the data we can collect. A significant part of the protection offered by business filters is against phishing and intrusions. Anti-phishing filters regularly examine links in emails, including triggering opens and possibly unsubscribes. Some filters go so far as to rewrite any links in the emails and force outgoing interactions through proxy machines controlled by the filtering company. These actions have consequences for how we measure and evaluate the success of our marketing programs. We can’t stop the filters from interacting with our mail in this way, but we can minimize their impact on how we work.

The good news is, we can improve delivery at business domains and reach the inbox.

*In the business space, there are no feedback loops.*
Standard deliverability advice leverages data from consumer ISPs and filters. Smart senders use opens, clicks, and complaints as proxies for how effectively their mail is reaching the inbox. Deliverability professionals monitor ISP provided websites, like Google Postmaster Tools (GPT) and Microsoft Smart Network Data Services (SNDS), for delivery and blocking information.

For businesses, we simply don’t have access to the same data. In fact, neither GPT nor SNDS include data from their hosted domains. The information on those sites is only for the consumer domains. Likewise, the Microsoft FBL and the Google spam complaint metrics are only for the consumer domains. Filtering companies don’t offer FBLs, even while they’re collecting complaints from their customers and using that data themselves. Deliverability professionals lack insight into how the ISPs and filters judge the sender.

Even more challenging for the deliverability expert, business filters interact with email in ways that change open and click data. Filters that follow every URL in a message change click and open data. We can’t be sure that every open or click is the result of a user action. Some appliances and business rules block loading of open pixels from the user. The result is a situation where we don’t know how a specific user is engaging with our mail. Sometimes an open or click happens without their interaction. Other times, they are opening mail, but the filters block recording of that action.

In the business space, standard deliverability metrics are full of noisy data, so how should senders evaluate the success of their mail programs?

**Use Trending Data**

The best way to minimize the effect of business filters is to monitor trends over time instead of looking at data for every send. This essentially factors out the effect of the filters from our data. We can look at improvements or failures without having to worry about the actions of specific filters or the activities of specific addresses. Trends let us see what is normal for a particular audience or mail stream, and act when that normal changes.

**Use Monitoring Tools**

Deliverability monitoring tools, like SparkPost’s Inbox Tracker, let senders see how the filters judge email. The Inbox Tracker reputation score is a great way to understand how the filters see a mailstream. In fact, Inbox Tracker features an array of comprehensive deliverability intelligence such as inbox placement, inactive subscriber rates, campaign details showing subscriber metrics and engagement, complaint, blocklist, trap monitors and DKIM and SPF monitoring.
Throughout this document we’ve talked about how delivery to business domains is different. That means that the standard deliverability advice given to B2C marketers doesn’t always work. The good news is that we still do have ways to improve delivery.

**Engagement Matters**

Because business filters interact in ways that change engagement numbers and sometimes block actual interactions, we can’t treat engagement numbers as absolutes. That doesn’t make them useless, however. Trending data tells us whether delivery is getting better or worse. When deliverability trends down, that’s the time to reevaluate your program and look at your segmentation and your target market. Removing disengaged recipients — whether that be due to mail going to their spam folder or a career change — can improve delivery over the long term.

Every target market has its own benchmarks for when to re-engage with or let go of a recipient. One of the factors for a benchmark is how frequently employees move and change jobs in your target audience. If, for instance, the average person on your list spends 2 to 3 years in a job, how relevant is your mail going to be four years later? What are the chances that the person may have a new focus, even if they stay at the same company and have kept the same email address?

Removing disengaged recipients can improve delivery.

Understanding your audience lets you prune lists to the users who are more likely getting your mail and less likely to complain about your mail to their filter provider. Even in the absence of complaint or open data, you can make sensible decisions about your recipient life cycle and who should continue to receive mail.

**Relevancy Matters**

In the business space, relevancy is slightly more complicated than in the consumer space. An employee wants email relevant to their job. Relevant email makes their job easier or helps their career in some way. There’s a different tolerance for commercial mail. Consumers might flag email and go back to it in the evening or on a weekend, but that may not happen as regularly in a business context.

Providing employees with relevant email that helps them do their job improves delivery. This is mail they want, and if they don’t get it, they are likely to investigate why they aren’t receiving it. Having the employee on your side means when filters break, the employee becomes your best advocate internally. Employees do have input into filters. When filters mistakenly block or spam folder email, there are paths for employees to change that. If your mail actively helps the employee do their job, they are more inclined to report the error to the right people.
Engage Outside of Email

Successful businesses engage with their customers through channels other than email. These channels are a great way to engage users with email. Not only can companies monitor for reports but they can encourage recipients to look for messages that may end up in the spam folder. Most business email clients will adapt to recipients marking mail as not spam. This is even more true when the filters are G Suite and Office365. Getting the recipient to mark mail as not spam is still one of the most effective ways to improve delivery.

Minimize Cold Business Email

Let’s be frank, no one reallylikes cold business email, and much of it is outright spam. Still, sales organizations use cold email to prospect for customers. This cold email can have deliverability effects. Some sales organizations go so far as to use different domains, IP addresses, and other infrastructure to minimize the negative impact on email deliverability. The filters are aware of these tactics, and companies aggressively sending cold email do experience delivery problems – even for their opt-in email on different domains and IP addresses.

One solution is to not use prospecting tools completely. Instead, focus on getting direct permission from the recipient and send them relevant content. However, some organizations refuse to give up prospecting, even when it’s damaging deliverability of other email.

Another solution is to actively engage with the sales teams and ensure the prospecting mail is a small fraction of the overall mail sent by the company. This requires coordination and discussion between the marketing, deliverability, and sales teams. While I don’t have exact recommendations for fractions, keeping prospecting mail minimal means few complaints compared to overall send volume and less risk to the overall program. A smaller portion of the total volume sent means it can have less of a negative impact on deliverability.

Part of the calculation should be a clear accounting of the net revenue related to email marketing and email prospecting. This accounting should consider both the revenue generated by the program and the costs associated with deliverability issues.

Recently, we’re seeing cold email impacting overall reputation and email delivery for the opt-in email streams, even in cases where the infrastructures are separate. Marketers need to take a holistic approach to email and look at every source of email from the company, especially when the delivery problems seem to happen overnight. Often these problems have nothing to do with the opt-in mailstreams but are directly tied to the cold marketing.

Ensure prospecting mail is a small fraction of the overall mail sent.
Improving Business Delivery (CONTINUED)

Keep Your Data Clean

Data hygiene is crucial to deliverability, including in the B2B space. Removing addresses that aren’t in active use improves deliverability, even for business filters. Bounce handling and removing dead addresses is easy, but not every dead address bounces.

In a business context, we know that employees move on and jobs change. When employees move to a new company, they leave their email address behind. Businesses get to decide what to do with email to that address. Sometimes the business chooses to forward mail to a manager, peer, or replacement employee; and sometimes they choose to just leave the address active but unmonitored. The best way to address this issue is to make it simple for the new recipient to opt-out of mail.

Another way to keep data accurate is giving recipients an easy way to change their email address. Recipients making lateral moves may still want your mail at their new address-- ensuring a simple process for them to update their subscription keeps the subscriber and improves delivery.

Running regular re-engagement and “sign of life” campaigns is another way to keep data clean. As every industry is different, there are no hard and fast rules about how often to run these campaigns. Exact and correct timing depends on how often job changes happen in the target industry and field. One way my clients have successfully identified the ideal time to manage re-engagement campaigns is to look at engagement stats segmented by original subscription date. We then create re-engagement campaigns targeted to these segments.

Give recipients an easy way to change their email address.
Conclusion

Email marketing in the B2B space is much more challenging than email marketing in the consumer space. Businesses use filters tailored to a different audience and designed to meet different needs.

• Email is a business tool. Effective marketing programs focus on content relevant to employees and their employers.

• Business filters focus on security first and foremost. They will interact with and modify messages, including rewriting links and inserting text to protect the business. This leads to a host of challenges for marketers. We know metrics like opens and clicks are inaccurate, and instead of basing decisions on raw open and click rates, we need to use trending data.

• Business filters don’t monitor individual user engagement, and we can’t manipulate them as easily as consumer filters. We must focus on actively sending mail users have asked for and that helps them in their work.

Standard deliverability advice works with consumer marketing programs but doesn’t always apply to business marketing programs. B2B marketing programs challenge us to approach deliverability problems with creativity and innovative thinking.

About The Author

Laura Atkins, Deliverability Consultant & Owner of Word to the Wise. Laura has over fifteen years worth of experience in helping companies mitigate and manage mailing risks, respond to spam complaints and interact more effectively with ISPs. She works with clients to define email-related goals and to identify and implement policy and procedural changes that further those goals. She regularly helps to mediate client delivery and blocking issues with anti-spam blacklists and internet service providers.

Before founding Word to the Wise, Laura led the outsourced abuse desk group for the Mail Abuse Prevention System (the industry’s first anti-spam blacklist). In this role, she advised ISPs on the most effective ways to manage their customers and complaints about their customers behavior.

With her background in molecular biology, Laura is well suited to investigating and troubleshooting complex processes from scientific and analytical perspectives, allowing her to expertly investigate and resolve email delivery problems for a variety of types of email senders. Laura writes and speaks frequently for industry publications, events, and educational offerings.