Email Best Practices & Email Warm Up

This guide is designed to give Users everything they to know to avoid the SPAM folder and send emails to their email lists.

This guide is designed to give Users everything they need to know to avoid the SPAM folder and land their emails into the Inbox. Below you will find a detailed guide on how to get sending emails .

Caution: Ignoring this guide can result in emails going to SPAM. We want your emails to arrive in the inbox and not in the SPAM folder. Please learn and apply this guide to your Email Sending Practices.

TABLE OF CONTENTS

Who is this guide for?

While this guide is for anyone sending emails ... It is specifically designed for those utilizing LC Email and LC Email Dedicated Domain Features. Those utilizing a Custom SMTP Provider that is not LC

Email will need to consult their provider. Our team will be limited on how much we can assist in some of the email compliance and best practices as they are not managed by us.

Learn more about the difference between LC Email and Custom SMTP Providers here.

Now that we know who this is for, let's hop into our guide together as we review Email Best Practices and Email Sending Recommendations below. We can't wait to see how this helps you grow your business!

Email Best Practices

Now that your new sending domain is set up, it is critical for you to set yourself up for a successful landing into people’s inboxes and NOT their spam folder. Before you get started sending, ensure you have set up and followed these necessary best practices.

1. Set Up a Dedicated Email Sending Domain

D

What is it? You Sending Domain, is how the internet routes emails. It Rather than sharing the domain provided for all users, a dedicated email domain is a single private domain you use to send and receive emails, when you are using LC Email - you have the ability to create your own dedicated domain. If you are using a non-LC Email (or SMTP Provider) you will not have this ability inapp.

Why it matters? Not having a Dedicated Email Sending Domain often results in your emails going into SPAM despite practices good emailing. When you set up a Dedicated Email Sending Domain, you can gain full control of your reputation and email deliverability. This means you can work your way into all emails going into the inbox while avoiding that SPAM folder.

How to Set it Up? If you haven't already, it is highly recommended to have your own Dedicated Domain for sending emails. To set up your Dedicated Email Sending Domain, check out this step-by-step guide.

```
What if I already have a Dedicated Email Sending
Domain and my Emails are going to SPAM? If this
describes you.
```

D

2. Set Up a Dedicated Sending IP Address

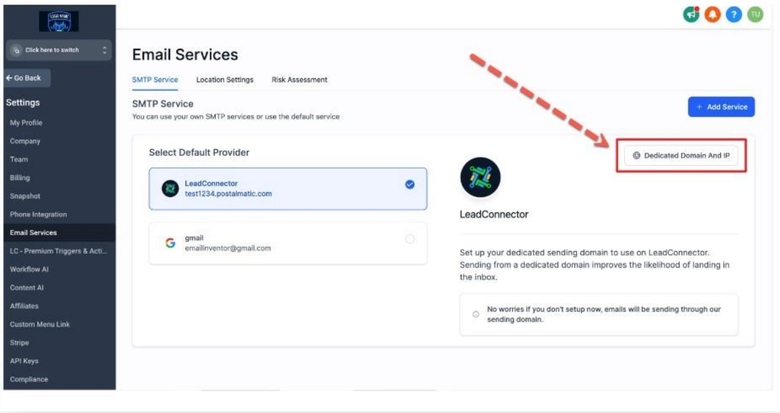
What is it? Dedicated IPs offer a distinct advantage by sending your email messages from a unique, exclusive IP address. Email service providers (ESPs) closely monitor the reputation and behavior of an IP address to determine the deliverability of emails linked to specific domains associated with that IP.

Getting a dedicated IP address provides your organization with exclusive ownership, giving you full control over the management of the email sender's reputation and deliverability tied to that IP. Learn more here:

What is a Dedicated Sending IP Address?

Why it Matters? If you have an LC Email Dedicated Sending Domain (see point 1 above) , you share the same Sending IP Address with all . Mailbox providers give a reputation to IP addresses, so this could negatively impact your sending, especially at high volume. A dedicated sending IP address helps you control more of your email-sending health to build your own IP reputation. This becomes more important when sending high-volume, especially 200k emails or more.

How to Set it Up? While everyone can benefit from a Dedicated Sending IP, businesses sending more than 200,000 emails a week will benefit the most from this service. To set up and learn more about Dedicated Sending IP Address, check out this guide.



Email Services

SMTP Service

You can use your own SMTP services or use the default service

Select Default Provider

LeadConnector test1234.postalmatic.com ✓

gmail emailinventor@gmail.com ○

Set up your dedicated sending domain to use on LeadConnector. Sending from a dedicated domain improves the likelihood of landing in the inbox.

No worries if you don't setup now, emails will be sending through our sending domain.

What are the Costs? $59 per month per IP. The amount is billed to the Agency Billing Card on file. The agency can set up rebilling to cover this cost by rebilling the client this amount. Learn more about the pricing here.

Additional Resources:
Reserve DNS (rDNS) Set Up, Fixing "Reverse DNS does not match SMTP Banner"

3. Enable Email Validation

What is it? Email Validation will check if the email you are sending is valid or not. Sending to an invalid email can negatively impact your email deliverability.

Why it matters? If you send emails that do not exist or are not valid, it harms your domain reputation leading to poor email deliverability. Meaning emails will go to spam or not be accepted into the mailbox at all.

How to enable it? We’ve actually made it as easy as possible to validate your emails, it is a setting in your Sub-Accounts Settings.

1. Enabling Email Verification for the Sub-Account
    1. Sub-Account View > Business Profile > Scroll to the “Verify Email Address when the first email is sent to a new contact” > check box.
    2. Email Validation every 90 days

1. Agency View > Sub-accounts > Click on the sub-account name > Scroll down to “Enable Re-validation for 90 days”.

Learn more here: How to enable and rebill LC Email Validation.

What are the Costs?

We charge $2.5 for 1000 Email Validations for all the plans at a lower cost than most major providers compared to $12/1000 with MailGun, which is 79% Cheaper. See How to enable and rebill LC Email Validation.

4. Add Your DMARC Record

What is it? A DMARC Record provides instructions to receiving servers about how to handle incoming mail. In order to get delivered, messages need to pass DKIM and SPF alignment checks according to the requirements set by the DMARC policy. Messages that do not pass DMARC checks can be

D

rejected, reported back to the domain owner, or placed in the spam folder.

Why Add it? Not having a DMARC Record can negatively impact your domain reputation and email deliverability. Often, mailbox providers count it against you when DMARC Records are not set up properly - resulting in emails going to SPAM.

How to Add it? To add a DMARC record, you must log into your DNS provider and add the following TXT record below.

To confirm your DMARC Record is applied correctly, you can use this DMARC Checker.

Additional Resources for DMARC:

Email Authentication - DMARC

Add your DMARC Record

DMARC Reports

5. Use the Proper “From Email”

What is it? The “From Email” is the email a recipient will see when receiving an email. For example, your Sending Domain might be “mail. l.com” however, you can send your From Email as “test@.com.” or as “test@mail.com.”

Why it matters? Using a “from email” that does not match the primary domain you are sending from can result in poor email deliverability.

How to Set It Up?

Use a From Email on the same organizational domain as your dedicated sending domain.

If your dedicated sending domain is a subdomain (e.g., mail..com), you can use either name@.com or name@mail..com. Deliverability is the same when SPF, DKIM, and DMARC are set up correctly.

D

Do not use a From Email on a different organizational domain (e.g.,

name@otherbrand.com) if your sending domain is .com.

Examples

Sending domain: replies.company.com → Valid
From: sender@company.com or sender@replies.company.com

Sending domain: mail.gohighlevel.com → Valid From: highly-test@.com or someone@mail..com

Invalid: Sending domain mail..com with From user@otherbrand.com

See more information here: [Masking Sender Emails - From Name & Address]()

6. Add Unsubscribe Links

What is it? An unsubscribe link allows your users to “unsubscribe” from receiving emails from you in the future.

Why it Matters? Not having an unsubscribe link will severely harm your email deliverability rates.

How to Set It Up? We make it as easy as possible to add an unsubscribe link all of your emails. Within the email builder, our “Footer” Element. Be sure to use this or edit and create your own.

You have two options, you can use the default unsubscribe link we have automatically set up for you or you can create your own!

1. Default Unsubscribe Link Set Up

    1. If you are using LC Email, it’s quick and easy to use our default unsubscribe links.

    2. This will not work for non-LC Emails. Refer to the next point for non-LC Email users.

2. Custom Unsubscribe Link Set Up

    1. Make the best possible unsubscribe link and process, giving you full control, get started here with this

       Custom Unsubscribe Link Set Up Help Doc above.

7. Use Double Opt-In

What is it? A Double Opt-In is when you ask subscribers to opt-in twice. For example, they fill out a form and then “verify” their email address by clicking a link to “Verify” their email. Only after someone has double opted-in will you start sending them emails. This is in contrast to a single opt-in which will start sending emails to recipients right after the first opt-in.

Why it Matters? Double opt-ins are highly beneficial to your domain reputation and email deliverability. This is because users have double opt-in to receive emails from you. Think about it… the act of a recipient receiving their first email from you, then opening, and clicking on a link within this email looks really good for your domain. In addition, it ensures your list knows and wants to receive emails from you. Which is invaluable when list building.

How to Set It Up? To set up a Double Opt-In Email Flow, we must do some quick building in

HighLevel. See the how to build a Double OptIn Flow here: How To Build A Double Opt-In Flow.

8. Stop Sending to Unengaged Emails

What is it? As simple as it sounds… When sending to your email list, do not send to unengaged emails. Meaning if they do not take the action to open or perform the next step in your campaign stop sending to them.

Why does it matter? When you send to a more engaged group of people, your emails go into the inbox more often. Whereas fewer open or links clicked (engagement) will result in emails going to spam.

How do I do this? If you have been sending to the same person who has taken no action for weeks, send to them less frequently or not at all.

While it hurts to trim the list, it’ll hurt more to ruin your email deliverability due to unengaged recipients. It just isn’t worth it and there are no hard feelings for users not wanting to engage with you. Focus your efforts on those that ARE engaging with you.

> It is better to stop sending to an unengaged recipient than it is to have them "unsubscribe" or "mark as SPAM."

9. Send Regularly…. Just Not Too Regularly

What is it? Another large factor in your sending domain's reputation is how often you send emails. If you only send out an email blast to your list once a month or once every couple of weeks - it can negatively impact your reputation. In contrast, if you send it every day or multiple times a day, it is just as bad. Especially if in the past you didn’t send it like this.

Why does it matter? Thus, it is important to consider how often you send. When someone has opted in and is engaging (opening emails, clicking on links in those emails), then you can send a bit more. But after they are not engaged, slow it down to weekly. And as covered above, if users are unengaged, stop sending them all together. How often you send and how engaged your recipients are can play a huge role in ensuring emails arrive in the inbox.

1

How do I do this? There are many opinions out there on how often to send and when to send. In general, we've found success in only sending to opt-in (preferably double opt-in) recipients. After they have signed up we send them about an email a day for the first 5 days, then we slow down to a couple a week. This is until they take the action we want. If they take no action after 20 days, we only send weekly emails until we have another planned promotion.

Our Recommendations:

1. If someone has opted in (preferably a Double Opt-In) you can send to them daily for a brief time to convert them…

    1. If after a week or two of no engagement, slow the sending down to them to a weekly cadence.

    2. If they are not engaged for a longer time, say two months of weekly emails, stop sending them all together.

2. You can send out special promotions or offers as you have them

    1. Just consider how often this is and keep them shorter.

    2. It's important to send fewer than to oversend.

    3. In addition, it's important to stop sending to unengaged recipients, remember the above...

```
It is better to stop sending to an unengaged
recipient than it is to have them "unsubscribe" or
"mark as SPAM."
```

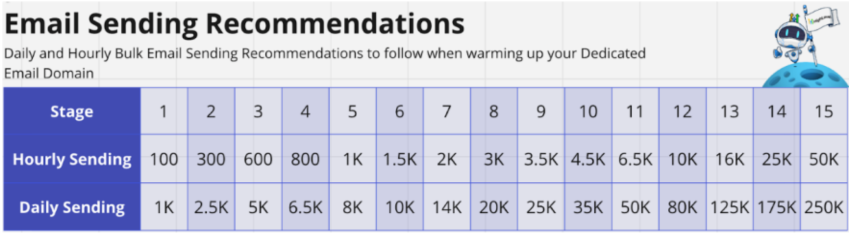
Email Warm Up

Mailbox providers will often SPAM emails from new dedicated email domains. This makes sense because anyone can make a new sending domain (like a spammer for example) and get sending. Utilizing the Email Best Practices

above and the Email Sending Recommendations below will greatly improve your chances of landing in the inbox and converting those leads!

Email Sending Recommendations

When sending your first emails to warm up your domain, you should only send to emails that have opted-in. Further, you need to follow the “Email Sending Recommendations” below to ensure you aren’t sending too many emails within a single day or hour.



Email Sending Recommendations

Daily and Hourly Bulk Email Sending Recommendations to follow when warming up your Dedicated Email Domain

Stage	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hourly Sending	100	300	600	800	1K	1.5K	2K	3K	3.5K	4.5K	6.5K	10K	16K	25K	50K
Daily Sending	1K	2.5K	5K	6.5K	8K	10K	14K	20K	25K	35K	50K	80K	125K	175K	250K

What this reveals is how many emails you can send within a single day or a single hour. So for the first emails I send, I should send no more than 100 per hour and 1,000 in that day. When I go to send my next emails, I move into stage two. In stage two, I can now send 300 per hour with a total of 2,500 emails in a day. It’s important to remember the stage isn’t just how long you’ve had the domain, it is the current stage or time in which you go to send emails.

Learn How to Send Emails in Drip Mode? (Daily and Hourly Sending)

Pro Tips for Sending Your First Warm-Up Emails

- Follow the Email Best Practices above
- Follow the Email Sending Recommendations above
- Send fewer emails per day or hour if you can at the beginning
- Send to only opted-in emails with higher chances of engagement

  - Cold emailing, or emailing to people who haven’t opted-in, needs to go through a list-cleaning process. It is not recommended to do cold emailing during the early processes of warm-up. Cold emailing tends to result in poor email deliverability. Learn more about Cold Emailing below.

- Keep the content of your emails short and to the point

- Do not use a Public Link Shortener like bit.ly or tiny.url

Email Tools

Are you wanting to test, track, or monitor your email domain? Below you will find a number of powerful tools for troubleshooting and monitoring your email sending and health.

Test the Spammyness of Your Emails

The content of your email can impact it’s deliverability. For example, too much text or using a URL shortener can greatly impact how mailbox providers rate your emails. If an email seems to “SPAM”-like, the mailbox provider will SPAM the email.

Did you know you can see how “spammy” your emails are by utilizing this free tool… https://www.mail-tester.com/

1. Copy the email provided

2. Create a new contact with this new email address you copied

3. Send your email to this new contact email address

4. Navigate back to Mail-Tester and click “Then check my score”

5. Review the score and make adjustments

If you are worried or seeing emails go to SPAM this can be a helpful tool in seeing if your content is to blame. Make adjustments based on the feedback you receive.

Review Your “Email Health Report”

To quickly check for errors in your domain, such as if it is blacklisted, missing a DMARC, etc, you can paste your sending domain into this “Email Health Report,” see

https://mxtoolbox.com/emailhealth. This will show any number of potential issues with your domain. A great place to begin with troubleshooting or checking your domain reputation.

Advanced: Use Postmaster Tools to monitor outgoing email

Utilizing the information of every Google mailbox user you send to from your domain… the Google Postmaster tool will monitor and return valuable information on how your ongoing emails are doing. Complete with:

1. Spam rate
2. IP Reputation
3. Domain Reputation
4. Feedback Loop
5. Authentication

D

6. Encryption

7. Delivery errors

This information is invaluable when trying to see what is impacting your sending email deliverability. Just use the tool to add a record to your sending domain to see how you are doing today!

*Please note: it can take up to two days or more for Google to get the data for some of your reports. Refresh your page and clear the cache or use an incognito window to ensure it is not a caching issue.

See more information on how to use the Google Postmaster Tool here.

Troubleshooting

Remember there are many reasons why emails can go to spam. For example, did you know using URL shorteners results in a much higher chance of going to SPAM? Email sending can be a complicated process. Which is why following the guide was created. As you review why emails are going to spam, you can follow this guide above as well as review the questions below.

In the event of your emails going to SPAM, it’s best to check the following:

1. Check how long you have been sending emails?

    1. Remember, it can take up to 4 weeks for a domain to be warmed up.

    2. If it is less than four weeks, stay focused on the Email Best Practices & Email Sending Recommendations noted above.

    3. In addition, use our “Email Tools” section above to monitor and improve your email sending.

2. Check Your MX Records

    1. Confirm your MX records are installed correctly.

    2. See the Review Your “Email Health Report” section above.

3. Ensure Your DMARC is Set Up

    1. Confirm your DMARC records are installed correctly.

    2. See the Add Your DMARC Record section above.

4. Reach out to Support
    1. If after confirming the top three steps (and the content above), you still need assistance - reach out to Support for further assistance.

Frequently Asked Questions

Q. What about Cold Email Outreach?

Cold emailing means contacting people who haven’t opted in—and it’s generally not recommended, especially for new domains. If you do it, make sure to validate emails, enable bounce protection, and avoid using your main domain. It’s best to use a separate sub-account and domain to protect your reputation.

Cold Email Outreach Pro Tips:

- Validate emails and filter out bad addresses
- Send small batches and drip slowly
- Warm up your domain first
- Don’t use your primary sending domain
-

Use cold email tools to qualify leads before importing them into HighLevel Third-Party Cold Email Services:

Tools like instantly.ai or smartlead.ai can help with cold outreach. Once leads engage, you can move them. (These tools aren’t affiliated with us.)

Q. What if I already have a Dedicated Email Sending Domain and my Emails are going to SPAM?

That’s normal in the beginning. If your domain is already warmed up and emails are still going to spam, it’s better to set up a new sub-domain than trying to fix the current one.

Q. What happens if my IP is blacklisted?

If you IP is blacklisted, reach out to support.
Click here for details on how to reach support.

D

Q. Should I Share the Same Dedicated Sending Domain Across Multiple Sub-Accounts or My Entire Agency?

No, don’t share domains across sub-accounts. Each one should have its own dedicated domain to keep deliverability strong and avoid cross-account issues.

Q. What is Email Warm Up?

It’s the process of gradually increasing your email sending volume to build a good reputation with inbox providers. This helps your emails avoid spam folders.

Q. What is Email Deliverability?

It’s your ability to land emails in the inbox instead of spam. It’s influenced by sender reputation, list health, content quality, and engagement.

Q. What is Domain Reputation?

It’s how mailbox providers rate your domain’s trustworthiness. A strong reputation gets you to the inbox—poor reputation means spam filters.

Q. How Long Until a Domain is Warmed Up?

Usually around 4 weeks. Stick to the best practices and monitor performance to make sure your domain builds a healthy reputation.

Q. What happens if I want to send more than the recommended amount?
Sending too much too soon can hurt your domain’s reputation and even get you blacklisted. Always follow the volume guidelines to stay safe.

Q. What are the Differences Between LC Email and a Custom SMTP Provider?

LC Email gives you built-in tools and better deliverability support. With Custom SMTP, you’re responsible for setup and troubleshooting, and our ability to assist is limited.

Q. What is a Dedicated Domain?

A dedicated domain gives you control over your email reputation by keeping your sending activity separate from others. This improves inbox placement.

Q. How to Send Emails in Drip Mode? (Hourly and Daily Sending)

Use Bulk Actions or Workflows to stagger your email sends. This helps maintain a good sender reputation by avoiding volume spikes.

Q. What is an Email Bounce?

A bounce happens when your email can’t be delivered.

-
- Hard Bounce: Invalid or non-existent address

Soft Bounce: Temporary issue like a full inbox or server delay