IP Warming

Best Practices:

Before you start the process of warming up your IP or domain, there are some things to prepare so that everything goes smoothly.

1. Make sure your authentication records are correct and in place: Email authentication is crucial to the success of your IP warming efforts, so you need to configure your SPF and DKIM records. For good measure, we recommend that you implement DMARC as well.

2. Check the pointer (PTR) record for your IP: The PTR record points from the IP address to the domain for a reverse DNS (Domain Name System) lookup. When an email is received, the mail server uses the PTR record in the email to check that the sending mail server matches the IP it claims to be using.

The PTR record goes in the reverse DNS zone but, in most cases, your Email Service Provider (ESP) or Internet Service Provider (ISP) will do this for you. You can check if a PTR record has been created with the reverse lookup tool from MXToolBox.

3. Register the IP with mailbox providers' feedback loops: A feedback loop allows senders to receive messages about spam complaints, which are forwarded by the mailbox provider. It's a good idea to set this up when warming your IP, as it will enable you to remove users who complain from your email list, which in turn will increase deliverability. If you're using an ESP, this will be taken care of for you. Check out this list of feedback loops to see which providers offer it.

4. Sign up to Microsoft Smart Network Data Services (SNDS) and Google Postmaster Tools: As well as allowing you to manage feedback loop settings for Outlook and Gmail, SNDS and Postmaster Tools provide detailed IP data which will enable you to monitor IP reputation.

5. Clean your email list: IP warming doesn't only depend on gradually increasing your sending volume. It also depends on engagement from subscribers; ISPs need to know that your list is full of subscribers that opted in, and that you're sending them what you promised.

The best indicators of this are your engagement metrics, like your email open rate and click rate. They also look at whether people delete or move your email to their spam folder. So before you start sending, it's super important to run your email list through an email validation tool. This will remove any nasties that might harm your engagement and sending reputation.

6. Segment your most engaged subscribers: Since engagement is an important part of warming up your IP, it makes sense to start out by sending to your most engaged subscribers. For example, create segments of subscribers who have opened and/or clicked in the last 30, 60, 90 and 180 days.

Begin sending to the subscribers in the 30 day segment, and then gradually add in the lesser engaged ones in the other segments as you progress. Keep each addition to a maximum of 15% of the existing volume, so their effect doesn't outweigh that of the engaged subscribers.

7. Craft engaging content: Take a look at your most successful email campaigns—which ones got the highest open rate and click rate? What do they have in common? Think about the types of content your subscribers like and engage with, and base your emails on this. And remember: When in doubt, just ask! Implement a survey in the newsletter or ask people to reply with their feedback.

8. Allow people to easily unsubscribe: Including an unsubscribe link in your marketing emails is mandatory. But, it will also keep your email list healthy by giving subscribers an alternative to flagging your emails as spam—they can simply opt-out.

You can go a step further and add the List-Unsubscribe header to your email headers. This header signals mailboxes to generate a secondary unsubscribe link and place it at the top of your email, so subscribers don't have to scroll through its contents to find the link.

9. Think about how soft/hard bounces will be handled: If any emails bounce during the IP warm-up process, you'll want to remove them from future sendings to avoid the bounces having an impact on your IP reputation. The best way to do this is to automatically add them to a suppression list.

Recommendations:

There are countless ways you can approach IP warming. These differences are due to numerous factors, such as platform infrastructure, system limitations, or anticipating performance issues – to name a few. And it's because of these differences that the process is fluid and subject to a bit of trial and error – or pivoting when necessary. No matter which approach you choose, there are several must-haves/do's that you should remember before, during, and after the IP warming process.

Allow for consistent sends and growth: Set a regular and consistent email sending schedule.
Your aim here is consistency. You want the ISPs and algorithms to begin seeing a clear impression of who you are as a sender. By remaining steadfast, the algorithms will recognize your sending behavior, follow it, assess the quality of your email stream, and note the engagement/responses from your recipients. A conservative approach to sending might be an ideal way to start. This means you'll want to start with a low volume of emails and then slowly and gradually add to that volume each day. It's important to note you'll want to send to your most engaged (especially recently engaged) subscribers first, as they'll be more likely to engage. Then, as time goes on, you can sprinkle in some lesser-engaged subscribers.

Obtain permission and consent: Whether you're operating with a new IP or a well-seasoned one, you must obtain permission and consent before you send a recipient an email. It's an ISP's job to protect its inbox owners from unwanted and unsolicited emails. So, if you land on their radar with a new IP, and no real sending history or sender reputation, you run the risk of appearing somewhat risky. But if you start by warming up your new IP with a list of unconsenting email addresses? That's a sure-fire way to end up in Spam, get blocked, and preemptively destroy the sender reputation you're trying to build. The foundation of your IP warming process begins with consenting and engaged subscribers/double opt-ins.

Ensure your authentication protocols and sending infrastructures are secure and up to date: Securing your systems is an essential step. That means updating your DNS records, implementing signing with DKIM, passing SPF, and more. A new sending IP or domain doesn't yet have a sending history – you must earn that. Email authentication protocols exist mainly because of deceptive email sending practices. Ensuring your authentication protocols are in place and your sending infrastructures are up-to-date and secure will allow ISPs to distinguish between you (a shiny new legitimate sender) from a more seasoned spam sender.

Send low-risk and relevant content your subscribers will engage with: Of course, you always want to ensure your email marketing content is appealing and relevant, but this is especially important during the IP warm-up process. You don't want to change things up too much or introduce something entirely new when you're not sure how your recipients might react. Instead, think about sending some type of incentive or promo code – something your recipients will likely be more than happy to receive and engage with. Or, if it's time for you to circulate the next subscriber newsletter – or some other regular, expected email – this can also work. Familiarity, on some level, is key here. To summarize, aim to send relevant and engaging content during this process.

Monitor your email performance metrics: Paying close attention to the feedback during every step of this process can help to provide you with some crucial insights into your progress. Make a point to monitor your metrics daily, if possible. Signing up for feedback loops can also help. Remove recipients who aren't engaging with your emails during this warm-

up period, so you don't risk a user complaint or block. Here are some of the metrics you'll want to pay careful attention to during this warm-up period:

- Email bounce rate
- Spam rate/user complaints
- Engagement rates–open, click-throughs
- Blocklist inclusions
- Track email authentication failures

Resist the temptation to send a high email volume too quickly: Depending on your time constraints, maybe a conservative approach won't work for you. While IP warming is a fluid process, you also need to exercise patience and resist sending a high email volume before you've warmed up. Remember, it's called warming your IP, not scalding your IP. On average, the IP warming process can take around 4 to 6 weeks – if everything aligns, of course. But if you experience warming issues, limitations with targeting or scheduling, it could take 90 days or more. There's always room to pivot if necessary, but remember, slow and steady will likely win the warm-up race. When in doubt, it's always best practice to seek the advice of an email deliverability consultant who can help you with the IP warming process.

Don't forget about prioritizing your email hygiene practices: It's one thing to start "fresh" with a new sending IP. But if you're warming it up with an unverified email list, you'll take a significant risk at showing the algorithms that you're sending to invalid or valid but unconsenting, or unengaged recipients. The problem with that? You risk email bounces, spam complaints, and damaging your IP reputation and your sender reputation before you've even built them. It's critical to only use a clean email list or database all the time – not just when you're warming up a sending IP. A two-step approach to email verification can help you sort out your lists straight away, and more importantly, show the ISPs that you're a trustworthy sender, worthy of reaching the inbox.

Frequently Asked Questions:

What is IP warming?

IP warming is the process of "warming up" a dedicated IP address by gradually increasing the number of emails sent over a 4-6 week period. This involves sending emails to a small amount of engaged subscribers, increasing the sending volume by a little each day. This allows senders to build a good sending reputation and lets ISPs recognize them as legitimate, not spammers. IP warming is all about building trust between your new sending IP and an Internet Service Provider (ISP). You want to build a strong reputation, slowly, steadily, and consistently.

A cold start isn't the best way of starting off with a new email sender identity. By forgoing warming up a new sending IP, you could risk significant consequences on your delivery, deliverability, and ROI.

Internet Protocol (IP) warming is the process of slowly, methodically, and constantly increasing your email sending volume for a new or otherwise dedicated IP address.

Why is IP warming needed?

When looking for potential spammers, ISPs use sending volume as an indicator. This is because spammers tend to use new IP addresses to quickly send out high volumes of unsolicited emails.

By gradually increasing your sending volume, thus "warming up" your IP, you signal to ISPs that you're a credible sender. Warming up your IP will help to build a good sender reputation, which is key for optimal email deliverability.

Sending high volumes of mail from a "cold" IP can hurt your sending reputation, especially if engagement for this mail is poor (bounces, marking as spam, etc.). For this reason, it's safer to "warm" an IP with smaller volumes of mail and target users with a history of positive engagement (clicks, opens, etc.).

Do I need to warm up my IP?

Every IP used for sending emails needs to be warmed up, but whether you need to carry out IP warming depends on whether you're using a shared IP or dedicated IP. Dedicated IPs come with no sender reputation, so if you're using one, then it needs to be warmed up.

If there has been no sending activity for your dedicated IP for 30 days or more, you may also need to carry out IP warming. The same applies to email sending domains. If your email sending domain is new, you'll need to carry out email warming in the same way as an IP.

Finally, if you plan to dramatically ramp up your sending volume, this should be done gradually rather than all at once.

Why IP warming is a must for sender reputation and deliverability?

While domain and IP warming takes time, it's the only way to show ISPs that your new IP isn't being used for spam. It'll result in a better sender reputation, and more emails reaching the inbox.

Just remember to be patient, keep monitoring your progress and keep sending! Setbacks and deliverability issues are common in the early days of IP warming, but don't let it discourage you. Before you know it, your email will be warmed up and you can crack on with sending your awesome campaigns!

How often is my sender reputation evaluated?

Sender reputation is evaluated based on a 30-day rolling calendar. If you've decreased your sending volume over the last 30 days, your IP will need to be rewarmed by following the IP warmup schedule.

When can I send mail to my less engaged audience?

Send a win-back campaign after IP warmup is complete. Consider sending a campaign with a special promo or CTA before adding these emails back into the distribution list (for example: "It's been a while. Do you still want to hear from us?"). If users still do not engage, remove them from all future marketing mailings. Continually targeting this population can cause negative engagement, which may impact your engaged users from receiving your emails in the future.