LUXSCI®

Best Practices for Ensuring Deliverability, Scalability, and Reliability When Sending Large Quantities of Email

Secure email specialists LuxSci give you a rundown on how to improve your approach to bulk sending.

If your organization sends large quantities of email, then deliverability, scalability and reliability are especially important. Any issues or inefficiencies become magnified by the scale of the operation, resulting in serious business costs or a measurable lack of effectiveness.

Thankfully, there are several helpful strategies your business can follow to ensure that deliverability, scalability and reliability are maximized.

Manage Your Email Lists

Why bother sending emails to people who don't want them, or those who no longer exist? All it does is decrease your deliverability rate and reputation. To boost its efficiency, your organization's email list needs to be culled back to only those people who have opted in – those that specifically want its marketing messages.

If possible, your company should strip out any recipients who have marked its emails as spam. It also needs to follow the CAN SPAM Act guidelines and include information about why the recipients are getting your email, how they can unsubscribe, and quickly remove any recipients who request to be taken off the list.

Your business should also exclude those addresses that fail to deliver or are invalid. The rate of emails sent to invalid addresses is often monitored by email providers. If your organization sends too many, it could end up with a temporary or permanent suspension.

Organizations can use MXToolbox to see if their servers are on any blacklists. If they are, they can contact the provider and find out why, and also try to remove the listing.

If your organization sends too many emails to invalid addresses, it could end up with a temporary or permanent suspension.

Strategies for Sending Emails at Scale

It's important to understand the potential constraints that come with various bulk email strategies. If your organization sends out its emails from a shared server or service, its performance will be limited by the other users. These users could also damage the IP reputation, which will reduce your deliverability rate as well.

Servers can also fail. Your organization's transactional emails can be blocked if your server ends up on blacklists. Thankfully, there are strategies that can reduce the impact of these issues.

Use Multiple Dedicated Servers

The best approach is to use multiple dedicated servers to take care of your company's email needs. This means that your company doesn't have to share the server with other users who could create performance problems. It also helps with scalability, because it's easy to increase the storage space and power of a dedicated servers alongside the needs of your business.

By setting up dedicated servers, your organization has complete control of the outbound email security, reputation, and throughput. No one else is using the servers, so there aren't any other parties that can introduce problems.

Introducing multiple dedicated servers allows your company to separate its transactional and marketing emails and to scale each set of messages separately. This is important, because if both types are sent from the same server, any deliverability issues affecting your marketing emails (e.g, because they were marked as spam by recipients) will also affect your transactional emails. This can cause huge problems to your organization's relationships with its customers.

This setup also ensures that you have a fail-safe. If one server crashes or its IP reputation is harmed, your company can quickly switch over to another server and continue sending emails in a reliable manner.

By setting up dedicated servers, your organization has complete control of the security, reputation management and other aspects.

Warm Up Your Servers

If you suddenly start to send out large numbers of emails from your server, ISPs will get suspicious and flag your email as spam. It's best to start slow and send out a few thousand at a time, slowly ramping up over several weeks. This activity pattern won't be identified as spam, allowing your organization to eventually send its required number of emails without being blocked.

Set Up SPF and DKIM

ISPs have to contend with spam that comes from forged email addresses. If messages sent from your servers can prove that they are legitimate, it can increase the likelihood of delivery to Inbox. Your organization can show the validity of its servers by setting up email authentication measures like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

Getting the Most Out of Your Bulk Email

The costs add up quickly when you send a massive number of emails. This is why it's so important for the entire setup to be as efficient as possible. By following the suggestions we have covered above, you will improve the deliverability, scalability and reliability of your organization's bulk email system, increasing its overall effectiveness and setting your business up for growth.

LUXSCI®

Have Additional Questions? We're Happy to Help!

Call: **+1 800-441-6612**

Email: **sales@luxsci.com**

Web: **luxsci.com**

Solutions to Ensure Your Private Information Stays Private:

- Secure Email
- Secure Websites
- Secure Web & PDF Forms
- Secure Text
- Secure Chat
- Secure Email Marketing
- Secure Video

LuxSci is your trusted leader for secure email, data and communication solutions. LuxSci helps ensure that "what's private stays private." Find out why LuxSci is the go-to source by the nation's most influential institutions in healthcare, finance and government for comprehensive, flexible, and easy-to-use secure solutions.