What are the five pillars of Deliverability?

Deployteq - Suzanne Martens - 2023-11-30 - Comments (0) - Deliverability

To ensure that an email is delivered successfully, it's essential to understand the 5 pillars of deliverability:

1. Strategy
2. Database quality
3. Content
4. Authentication
5. IP-reputation

Strategy

Mail frequency, relevance, call to action. Make sure you have a strategy ready for these three topics that fits your own practice.

The ideal mail frequency does not exist and varies significantly by industry. While a website with daily deals can send an email every day that gets opened, a daily email from an insurer might not be appreciated. Therefore, determine the appropriate mail frequency for your industry and remain critical.

Relevance is crucial. Send emails that are relevant to the recipient, as more activity in relevant emails (opens, clicks) contributes to a better reputation.

For example, a liquor store traditionally sends a lot of information about wines. However, some customers prefer whiskey. Ensure that customers who never drink wine receive enough other relevant content about whiskey.

Once the email is opened, provide a clear call to action. Is it clear what your email aims to achieve? Do the links motivate clicks? A good call to action encourages more interaction in your emails, benefiting your reputation.

Database Quality

The quality of your customer database directly influences your reputation with the mailbox provider. Qualify the database quality in two ways:

- Are the email addresses correct?
- What activity do the email addresses show?

To minimize the chance of incorrect email addresses (and thus bounces) in your database:

- Avoid importing old data files, especially those older than one year. When in doubt, contact us.
- Ensure correct input. If many bounces occur due to new registrations, consider double-entry of email addresses on the signup form and include only matches in your database.
- Use tools like BriteVerify or Kickbox to assess the quality of entered email addresses before sending.

Implement a double opt-in to confirm registrations through a confirmation email link. This not only reduces the number of email addresses but also provides additional commitment and engagement, contributing positively to your reputation.

Frequently email and maintain database quality.

The second aspect is the activity of your email addresses, also known as engagement. The more opens/clicks after sending an email, the better. Set up campaigns to reactivate inactive email addresses or, if unsuccessful, reduce or stop emailing them.

Content

Adhere to the following requirements for email content to avoid being blocked by the mailbox provider:

- Keep the email size reasonable. We recommend a maximum of 101 kB of code, including images, up to a total message size of 250 kB.
- Always include a text version with partially the same content, including the organization's name, email title, the top article, and information and links from the footer. Include an unsubscribe link!
- Include your physical address in the footer of your template.
- Place the unsubscribe link in the header of your template to prevent people from unsubscribing through a spam complaint.

- Avoid words like 'free' and 'win,' and minimize the use of uppercase letters.
- Use a good subject line that entices recipients to open the email. Avoid words like 'free' and 'win' and make it fit the recipient. Our built-in subject line optimizer can help.

Always check your content with the free service EmailAnalyzer: https://analyze.email/. If your email scores below 9, continue refining the content and test it again.

Authentication

The goal is to make your email look as legitimate and trustworthy as possible. Authenticate yourself as a good and reliable sender. Authentication includes SPF, DKIM & DMARC.

- SPF (Sender Policy Framework): Confirms permission to send emails on behalf of the domain.
- DKIM (DomainKeys Identified Mail): Validates the authenticity of emails through the DNS.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): A measure to prevent phishing by combining well-set SPF and DKIM. DMARC checks if the 'header from' field matches the SPF record and includes the DKIM signature.

IP Reputation

Whether your email ends up in the inbox, spam folder, or is blocked altogether largely depends on your IP reputation, also known as the 'Sender Score.' It's a rating of your mail server on a scale of 0-100, generated by an algorithm that looks at statistics from the past 30 days across various email clients and recipients. Factors include:

- Number of people opening your email.
- Number of responses to the email.
- How many times the email is marked as spam.
- How many times the email is moved to another folder.
- How many times the email is forwarded to another.
- How many times the email is deleted before being opened.

Maintaining a high IP reputation is our core business, so you don't need to worry. We actively monitor and take appropriate action if necessary.