MAILING PLAN GUIDELINES
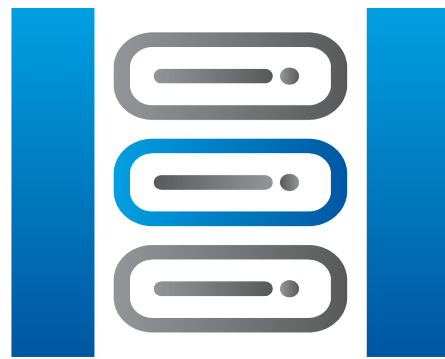
HostStage

TABLE OF CONTENTS

INTRODUCTION

HostStage offers the possibility to run email marketing campaigns through your own infrastructure.

Whether it is a newsletter, opt-in mailing, or auto responder set ups, the mailing plan is the ideal solution for you.

You are being given a CentOS 6 64 Bits Virtual private servers, on which you can configure your MTA (mail transporter agents: Postfix, Exim, Power MTA …).

Along with your VPS, you're being given a set of IPs, at the best market pricing for emailing activities: they are meant to rotate according to your mailing process.

Throughout this guide, we will cover the ideal mailing setups, its limitations and practical advices.

CONFIGURATION

a. rDNS / PTR Records

As you may know, the IPs need to resolve to a domain/subdomain to increase their authority and legitimacy. At HostStage, you have access in your client area to an interface allowing you to manage and set your rDNS; you would just need to create a DNS A entry from your domain/subdomain name to your IP address.

Basically, the domain needs to resolve to your IP which will enable you to set your PTR records.

The propagation should be almost immediate.

b. Mail Transporter Agent

For you to be able to send emails, you need to configure SMTP server through a mail transporter agent. You are free to choose and configure the MTA of your choice, or even run your automated deployment script.

Your MTA will define whether you can rotate IPs: for instance, Exim will not be able to easily do it. But it would be perfect in an auto responder setup since you can easily assign a domain to an IP.

For more information about your MTA, please refer to their User Guides.

c. DKIM

DKIM is a DNS side authentication of domain ownership. It is basically a string of characters which needs to be set on your DNS server (self-hosted on the VPS or domain registrar.)

If you're using an auto installer, the DKIM setup will be configured for you.

d. SPF Records

SPF records are a DNS entry defining the IPs allowed to send emails. Setting it up will increase the inboxing rate.

It is also meant to be done either on the VPS DNS server or the domain registrar.

e. DMARC

It means Domain Based Message Authentification Reporting.

It is also a DNS entry allowing you to register and authenfy your domain to as an email sender one. It is a sign of trust and shall increase the inboxing rate.

f. FBL – Feedback Loop

A FBL allows the ISP to forward the complains of their users directly to a complain email you would have set up. It is warmly recommended to centralize the complains to remove the receiver's emails from all your mailing list.

Here are a short list of ISP allowing you to set a feedback loop:

    1) Yahoo: http://feedbackloop.yahoo.net

    2) Hotmail: https://support.msn.com/eform.aspx?productKey=edfsjmrpp&ct =eformts

    3) AOL : http://postmaster.aol.com/Postmaster.FeedbackLoop.php

g. Public WHOIS

By using a domain with a public Whois you would increase the trust signal of our algorithm while using a private Whois would increase the score given.

h. Proper Headers

Using properly constructed headers which identify your email routes, the date, the subject.

They are used by some ISPs to route the mails to the users inbox.

Therefore, a simple PHP mail integration would have high chances to be flagged as spam.

LIMITATIONS

While we are a mailing compliant company without any defined hourly mailing rate, we do not allow spam on our network, nor IP hopping.

Therefore, we have deployed an algorithm which would analyze your mailing pattern in order to avoid IP blacklisting.

The algorithm lies on several parameters and can lead to an SMTP port block. Those parameters are:

a. Bounce back emails

if your mailing lists aren't qualitative, it will generate a lot of bounce back and will trigger our algorithm which will block your SMTP port and blacklist your IPs: a pre-screening process of your lists is warmly recommended (double opt in …).

b. Content / Link or Image ratio

Our algorithm analyzes your email content in order to allocate a quality score based on a ratio between html links, and image content.

If the quality score is too low, it will trigger the SMTP port block.

You can refer the SpamAssassin content checker in order to have an idea of the quality score. The quality score also relies on the niche you're covering in your campaigns and it will be greatly diminished if the content deals with the niches: gambling, adult, loans, pharma.

You should opt for sub divided images rather than just one.

Avoid to use JavaScript which would have a negative impact on your spam score.

Phishing and Virus Spreading are strictly forbidden and will trigger the permanent a SMTP port block.

c. Rates

The spam score will have a direct impact on the hourly rate while there isn't any one defined by default.

d. MTA setup

As covered previously DKIM SPF, FBLs setups have a direct impact on your quality score

PRACTICAL ADVICES

1 – **Do not scrap your list**

Scrapping lists are just illegal, because the emails are not opt-in, and you are exposed to RBL spam traps which will instantly blacklist your IPS. Some websites are posting hundreds of thousands Spam Traps.

http://www.projecthoneypot.org/statistics.php

2 – IP warm up

We always recommend to warm up your IPS through highly selective lists in order to optimize the inboxing rate in the long term, and to increase your sender score at

http://www.senderscore.com

3 – Work on your emails templates.

It is very important to dedicate the necessary time to your email content in order to your quality score which would also affect your inboxing rate

HostStage

MADE BY IMER FOR IMER

http:// www.host-stage.net