Cloud VPS Servers

My Emails are Bounced Due to Blacklist, What Can I Do?

What is RBL?

RBL is a short form of Real time Black List

RBL is a basically block list that mail servers uses to reject mails from IP addresses which has a history of spamming.

RBL is also known as DNSBL as DNS is used to determine whether an IP is blacklisted.

One of the important points about RBL is that your email will not be rejected just because your ISP IP address or your email server IP address is listed in an RBL. There are many many RBLs in this world and your IP being listed in one of them for any reason will not make your mail bouncing. Your email will be affected if and only if one of the email servers involved(either email server of your email address or email server of recipient email address) is using the RBL that lists your IP address.

How to check whether an IP is blacklisted?

Common method is to use an online blacklist checker.

Eg: http://mxtoolbox.com/blacklists.aspx

Actual method that mail servers use to check whether an IP is blacklisted is to use DNS as given below.

```
==========================================
dig txt "Reversed IP".sbl-xbl.spamhaus.org +short
==========================================
```

If the IP is 192.168.56.47, we need to run DNS query as "dig txt 47.56.168.192.sbl-xbl.spamhaus.org +short"

Eg:

```
================================================
sherin@mypc ~/ $ dig txt 47.56.168.192.sbl-xbl.spamhaus.org +short

"http://www.spamhaus.org/query/bl?ip=192.168.56.47"
================================================
```

What are the possible scenarios?

1. ISP IP address is blacklisted

In this case, your email will not leave "Outbox" of your mail client(Eg: Outlook) and your email will be immediately rejected.

Your ISP allocates you a dynamic IP address in most cases. This means that every time you connects to internet, you will get a random IP address. This means that you are likely to get an IP with spam history before.

If your desktop computer has a virus, it may be sending spam. In that case, you need to fix the issue with your computer.

If you get an IP with spam history when you connect to internet, and this IP address is blacklisted in a particular RBL, and if this RBL is enabled in mail server of your email address or mail server of recipient email server, your email will be rejected

Solutions

1. Get a new IP address from your ISP. Simply disconnecting and reconnecting may help you to get a new IP address. You may also contact your ISP for assistance regarding this.

2. If your email address is hosted in a VPS server or dedicated server, you will be able to remove the RBL that lists your ISP IP address. If you need assistance regarding this, please contact Bytehouse 24x7 Technical Support

3. You maybe able to send email from webmail of the email address. This will help you send emails without the effect of ISP IP address blacklist on email.

4. In some cases, you may contact mail server administrator of recipient email address, if recipient mail server is rejecting emails due to blacklist added.

5. In some cases, your ISP might have asked to add all of its IP addresses to add a blacklist. Spamhaus Policy Blacklist(PBL) is an example for this. If your ISP follows this practice, you can send emails in following ways

1. Ensure that pbl.spamhaus.org is not enabled in the email server of your email address
2. Use ISP provided SMTP server to send emails instead of using actual mail server of your email address
3. Use webmail to send emails.

2. IP address of the mail server of your email address is blacklisted

In this case, your email will leave "Outbox" of your mail client(Eg: Outlook) and your email will NOT be immediately rejected. However, the recipient email server will reject your email and you will get a bounce email.

In this case, your email server might be sending spam emails. So, reason for spamming need to be found and fixed.

Spamming can happen due to various reasons given below.
1. Password of one the email addresses in server is compromised and hackers are using it to send spam
2. Hackers found a way to misuse an email script in one of the websites in server to send spam without knowledge or permission of website owner
3. Hackers managed to gain access to server due to a security vulnerability and utilising this access to send spam.

If you are unable to find reason for spamming and fixing it, please contact Bytehouse 24x7 Technical Support

Once the spamming is fixed, you can contact blacklisting agency to delist the IP address. Please note that all the RBLs does not provide option to delist an IP address. Some blacklists are fully automated, in such blacklists spamming IP addresses are added & removed automatically. Further, there are some blacklists which charge your for removal! These are RBLs are unlikely to be used in any common mail servers. In almost all cases, you can ignore listing of your IP addresses in such blacklists.

Common delisting URLs are given below.

http://cbl.abuseat.org/lookup.cgi
http://www.spamhaus.org/lookup/

Very Important Note: You should NOT request an IP delisting unless you are 100% sure that NO spam is being sent from the IP address.

3. Virtual Block Lists, Temporary Block Lists, Rate Limiting & Reputation.

There are mail servers like Gmail which wont use any common RBL, but still effectively blocking spamming IP addresses. These mail servers will monitor mail traffic and if they see suspiciously large mail traffic from any IP address, they will refuse to accept email from such server until malicious email traffic is stopped.

If you experience such an issue of gmail blocking your emails, you need to do following.

1. Check whether your server is sending spam emails. If your server is sending spam, stop it fully. For any assistance, please contact Bytehouse 24x7 Technical Support

2. Remove all email forwarders to gmail. Gmail does not like email forwarder to Gmail! You can use Gmail mail fetcher instead of a forwarder.

Finally there are mail server Reputation services. These services rates your server as good, bad, neutral etc. We wont be able to influence these ratings by any means.

If your mail server or mail server IP address or domain or email address is very fresh and does not have a history of previous emails, you are likely to get a "neutral" rating. While neutral rating is not bad, your emails might still be treated as suspicious until a good reputation is built based on email pattern from your mail server or mail server IP address or domain or email address.

If your mail server IP address happened to got a bad reputation due to spamming, you need to fix the spamming issue and patiently wait until good reputation is built again.

If IP reputation or blacklist is causing all the trouble, why not change my IP address?

If your IP got blacklisted due to spamming from your server, an IP change is unlikely to help as the new IP addresses can get easily identified as the new IP address of the old spamming server. So, recommended solution is to fix spamming & patiently wait until IP address is delisted from blacklist & good reputation is built. This may be a difficult as business depends on email. If your IP got blacklisted, and you are unable to send email, you may temporarily send emails using an ISP SMTP server or using a service like gmail until the issue is resolved.

Unique solution ID: #1196
Author: Sherin George
Last update: 2016-06-09 01:21