# Top 10 tips to secure your email server

www.vircom.com/top-10-tips-to-secure-your-email-server/

1. Configure mail relay options carefully to **avoid being an Open Relay**

It's very important to configure your *mail relay* parameter to be very restrictive. All mail servers have this option, where you can specify which domains or IP addresses your mail server will relay mail for. In other words, this parameter specifies for whom your SMTP protocol should forward mail. Misconfiguration of this option can harm you because spammers can use your mail server (and network resources) as a gateway for spamming others, resulting in your getting blacklisted.

2. Set up **SMTP authentication** to control user access

SMTP Authentication forces the people who use your server to obtain permission to send mail by first supplying a username and password. This helps to prevent open relay and abuse of your server. If configured the right way, only known accounts can use your servers SMTP to send email. This configuration is highly recommended when your mail server has a routed IP address.

3. **Limit connections** to protect your server against DoS attacks

The number of connections to your SMTP server should be limited. These parameters depend on the specifications of the server hardware (memory, NIC bandwidth, CPU, etc.) and its nominal load per day. The main parameters used to handle connection limits include: total number of connections, total number of simultaneous connections, and maximum connection rate. To maintain optimal values for these parameters may require refinement over time.

This could be very helpful to mitigate spam floods and DoS attacks that target your network infrastructure.

4. Activate **Reverse DNS** to block bogus senders

Most messaging systems use DNS lookups to verify the existence of the senders email domain before accepting a message. A reverse lookup is also an interesting option for fighting off bogus mail senders. Once Reverse DNS Lookup is activated, your SMTP verifies that the senders IP address matches both the host and domain names that were submitted by the SMTP client in the EHLO/HELO command.

This is very valuable for blocking messages that fail the address matching test.

5. Use **DNSBL servers** to fight incoming email abuse

One of the most important configurations for protecting your email server is to use DNS-based blacklists. Checking if the sender domain or IP is known by DNSBL servers world-wide (e.g., Spamhaus, etc.), could cut down substantially the amount of received spam. Activating this option and using a maximum number of DNSBL servers will greatly reduce the impact of unsolicited incoming email.

DNSBL servers list all known spammers IPs and domains for this purpose.

6. **Activate SPF** to prevent spoofed sources

Sender Policy Framework (SPF) is a method used to prevent spoofed sender addresses. Nowadays, nearly all abusive email messages carry fake sender addresses. The SPF check ensures that the sending MTA is allowed to send mail on behalf of the senders domain name. When SPF is activated on your server, the sending servers MX record (the DNS Mail Exchange record) is validated before message transmission takes place.

7. **Enable SURBL** to verify message content

SURBL (Spam URI Real-time Block Lists) detects unwanted email based on invalid or malicious links within a message. Having a SURBL filter helps to protect users from malware and phishing attacks. At present, not all mail servers support SURBL. But if your messaging server does support it, activating it will increase your server security, as well as the security of your entire network since more than 50% of Internet security threats come from email content.

8. **Maintain local IP blacklists** to block spammers

Having a local IP blacklist on your email server is very important for countering specific spammers who only target you. Maintenance of the list can take resources and time, but it brings real added-value. The result is a speedy and reliable way to stop unwanted Internet connections from bothering your messaging system.

9. **Encrypt POP3 and IMAP authentication** for privacy concerns

POP3 and IMAP connections were not originally built with safety in mind. As a result, they are often used without strong authentication. This is a big weakness since users passwords are transmitted in clear text through your mail server, thus making them easily accessible to hackers and people with malicious intent. SSLTLS is the best known and easiest way to implement strong authentication; it is widely used and considered reliable enough.

10. Have at least **2 MX records** for failover

This is the last, but not least, important tip. Having a failover configuration is very important for availability. Having one MX record is never adequate for ensuring a continuous flow of mail to a given domain, which is why it’s strongly recommended to set up at least 2 MXs for each domain. The first one is set as the primary, and the secondary is used if the primary goes down for any reason. This configuration is done on the DNS Zone level.