Issue Solved: Mail server Misconfiguration

Mail server misconfiguration is also known by the email spoofing. It is like forging the email address of someone. By spoofing, the original identity of the email sender can be kept hidden from the email recipient.

The mail server misconfiguration settings may affect your email communications to your recipient so, we decide to give a simple configuration settings about the issue.

Follow these step by step instructions to solve the issue quickly.

Causes Of Email Spoofing

- Domain not listed in the SPF record
- Missed DMARC protocol
- Affect your email communication
- Cannot update or configure your email
- reduce the usage of the server

Steps To Solve The Issue

- Use top-level domain while sending email
- Update your DNS system
- Check if your email include the SPF and DMARC records

- Configure your email server settings
- Keep your server up to date
- The impact of email spoofing problems is such that anyone can share fake messages using a company's email. As a result, the company might lose its reputation.
- The other method to prevent the **mail server misconfiguration** problem is DKIM (Domain Key Identified Mail). This uses a cryptographic key that helps to validate the incoming messages.
- This method is commonly referred to as a replay attack.

We hope the above steps solve your problem if you want tech support please click the below read more button.
Read More