Order confirmation email that customers receive has "noreply@shopfactory.com" email in the FROM field

Elenor A. - 2025-05-09 - Order Management

Mail servers have spam filter settings or spam control measures so when order confirmation emails are not accepted by the recipient's mail service, they bounce back to our system and the system retries sending them several times, as is normal practice in those situations, until after a while they get deleted automatically by the email system as not deliverable.

However, while we constantly monitor spam prevention systems, it is impossible to always guarantee the delivery of emails, as spam prevention systems constantly evolve.

You can enable "Use my email address as sender" setting in https://app.santu.com/buynow/store

But you will need to contact your Mail Provider first to update the SPF records for you.

Contact your Mail Provider with the following information:

Configure your SPF record to allow Santu.com to send email on your behalf

SPF stands for Sender Policy Framework. This is a technical method of preventing unauthorized senders from forging your email address, or spoofing. Spoofing is a practice used by spammers and email abusers that alters the email header so that an email message appears to come from a source other than the one actually sending it.

The Sender Policy Framework protects your sender address by validating the sending server to confirm that email messages that appear come from you are authorized. Whether you send email through Santu, or not, you will benefit from setting up SPF records. An increasing number of ISPs (Internet Service Providers) require SPF records be published under your domain name in order to accept your email. Adding the SPF record can dramatically improve email deliverability because it allows you to control which servers send email using your sender address. It is a way of stating who you are and designating who is allowed to send emails with your from address.

To maximize email deliverability, you should add a SPF record for Santu.com, indicating our servers are authorized to send email from your sender address.

This is the optimal SPF record to use:

v=spf1 a mx ip4:54.194.8.133 ip4:54.72.67.76 ip4:54.76.107.13 include:yourdomain.com ~all

The Santu checkout product servers are as follows:

54.194.8.133 (app01.3d3.com)

54.72.67.76 (app02.3d3.com)

54.76.107.13(app03.3d3.com)

"MX" tells the web to all your domain's own mx servers to send email with your from address

"ip4:thisIP" tells the web to allow thisIP to send email with your from address

"include:yourdomain.com" tells the web to allow yourdomain to send email with your from address

"~all" Indicates that emails that do not comply with the SPF rules are suspicious, but do not need to be rejected immediately. Often used when testing an SPF record or in situations where you are not yet sure of all the allowed senders.

Here are links to instructions from a couple of well-known domain registrars. You can also contact your domain registrar directly to request assistance.

GoDaddy (https://ph.godaddy.com/help/manage-dns-records-680)

Network Solutions (http://www.networksolutions.com/support/how-to-manage-advanced-dns-records/)