What is Email Backscatter and How to Prevent It

https://campus.barracuda.com/doc/98219781/

Email backscatter is unwanted email that occurs when a spam or phishing email is sent with a spoofed sender address. When the email cannot be delivered, a bounce message is generated and sent to the recipient of the spoofed message. The bounce message appears as if it was sent by the original sender's email server, which can result in increased spam traffic and harm the reputation of the email server.

To limit email backscatter, do the following:

1. Implement authentication mechanisms such as SPF, DKIM, and DMARC to validate the source of incoming emails and prevent email spoofing.
2. Configure your email server to reject emails that contain invalid or suspicious header information.
3. Use regular expressions to identify and block emails with subject lines or message content that are indicative of backscatter. For example,
   - `(?:delivery.status.notification|returned.mail.?:.unreachable.recipients|undelivered.mail)`
   - `(?:returned.mail.?:.see.(the.)?transcript|message.you.sent.blocked.by.our.bulk.email.filter)`
   - `(?:undeliverable.?:|undelivered.mail.returned.to.sender|mail.delivery.failed:.returning.message)`
4. Monitor your email logs for signs of backscatter, such as a sudden increase in the volume of bounce messages received, receipt of bounce messages from unfamiliar or unexpected domains or email addresses, or receipt of bounce messages with unusual or suspicious content.

By taking these steps, you can reduce the risk of email backscatter and protect your email server and users from unwanted and potentially harmful emails.

Set Content Policies

In Email Gateway Defense, you can set content policies to help identify and block emails that are indicative of backscatter. Go to **Inbound settings > Content policies**; using the **Message Content Filter** section, create three new policies blocking on **Subject**.

For examples of regular expressions to identify and block emails with subject lines or message content that are indicative of backscatter, see *Step 3* above.

(?:delivery.status.notification|returned.mail...	🚫 Block	Subject
(?:returned.mail.?:.see.(the.)?transcript|m...	🚫 Block	Subject
(?:undeliverable.?:|undelivered.mail.returne...	🚫 Block	Subject

Example of Email Backscatter

Figures

1. contentPoliciesBackscatter.png
2. backScatterExample.png