Why Emails Get Blocked

A Business Guide to Fixing Delivery Issues

- ***Why Was My Email Blocked?***
- ***Why Did I Not Receive an Email?***

Email delivery can sometimes seem unpredictable. Factors such as spam filtering, email content, and server policies all play a role. Here, we address common concerns such as accountability and outline steps to ensure smooth email communication for your business.

! In 2023, approximately 347 billion emails were sent daily, with 46% identified as spam.

SOURCE: EMAILTOOLTESTER

Who Is Accountable?

Understanding accountability in email delivery is crucial. Here's a simple breakdown:

Sender Accountability

If an email **never reaches** the recipient's system, the issue is typically with the sender. This could be due to:

- Incorrect email configuration
- Spam filtering blocking outgoing messages
- Domain authentication issues (SPF/DKIM failures)
- Email flagged as suspicious

Recipient Accountability

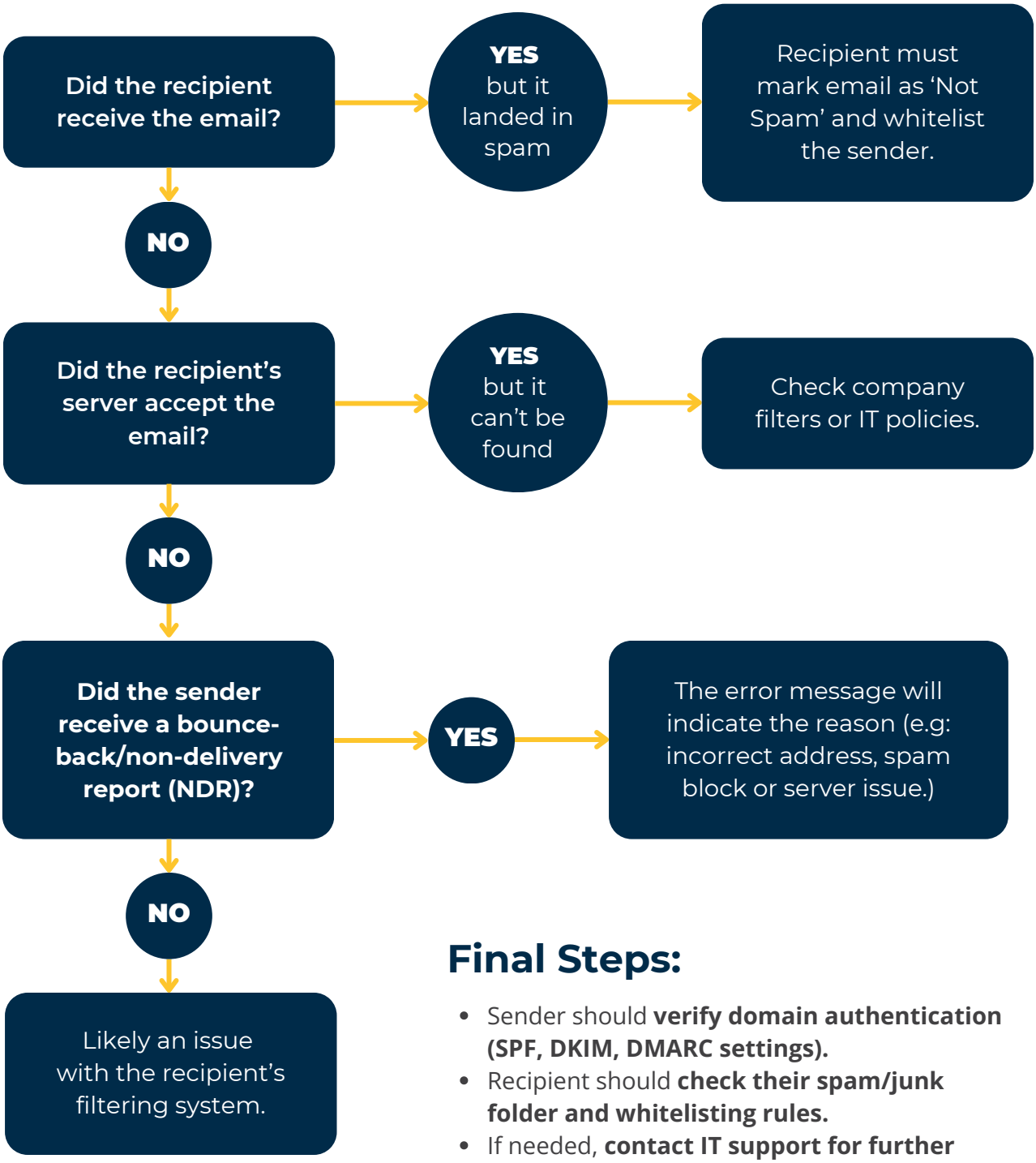
If an email **arrives at the recipient's system but is not delivered to their inbox**, the issue lies with the recipient. This could be due to:

- Spam or junk folder filtering
- Security policies blocking certain emails
- Quota limitations (mailbox full)
- Internal IT restrictions

Email is not always 100% reliable. If a message is critical, **always verify receipt.** If it contains sensitive information (e.g., financial details), **never rely solely on email - always verify via another method.**

Troubleshooting Email Delivery Issues

Here's a quick flowchart to help diagnose the issue:



Final Steps:

- Sender should **verify domain authentication (SPF, DKIM, DMARC settings).**
- Recipient should **check their spam/junk folder and whitelisting rules.**
- If needed, **contact IT support for further investigation.**

Total Group's Role & Limitations

Enterprise Email Systems

- **Total Group provides best-in-class email systems** to ensure reliability and security.

Support Scope

- We assist with **email setup, SPF/DKIM configurations, and troubleshooting within our systems.**
- **We cannot control external systems** or third-party email provider rules.

Understanding Delivery Challenges

Spam Filters and Opt-In Requirements

- Spam filters are designed to block **unsolicited bulk emails.**
- Ensure recipients have **explicitly opted in** to receive emails to avoid deliverability issues.

Email Delivery Statistics

- Over **300 billion** emails are sent daily, but only about **100 billion are actually delivered and opened.**
- Email filtering is **highly stringent**, and proper setup is essential for successful delivery.

Server & Routing Variations

- Emails **pass through multiple servers**, each with **unique filtering rules that change in real-time.**
- Identical emails **sent at different times may have different outcomes** due to routing decisions.

Technical Essentials for Delivery

SPF (Sender Policy Framework)

- Ensures your **domain is authorized** to send emails.
- Prevents **spoofing** and improves trustworthiness.

DKIM (DomainKeys Identified Mail)

- Authenticates the **sender's domain** and **digitally signs** emails.
- Helps prevent email tampering in transit.

Email Content and Formatting

- Plain-text emails are **less likely to be flagged as spam.**
- **Avoid** complex formatting, excessive links, and **large attachments** to improve deliverability.

Practical Tips for Users

Basic Tests for Sending and Receiving Emails

Receiving Issues?
Ask the sender to send a **plain-text email** to test deliverability.

Sending Issues?
Ensure emails follow **proper formatting** and are sent in **plain text** if problems arise.

Attachments and Formatting

Formatting
Use **widely compatible formats** (e.g., PDFs or ZIP files under 5MB).

File Size
Verify that the recipient's **system allows large attachments** or specific file types.

! Approximately **1 in 6** legitimate, permission-based emails fail to reach the inbox.

SOURCE: 2023 EMAIL DELIVERABILITY BENCHMARK REPORT BY VALIDITY

Common Obstacles and Solutions

Non-Delivery Reports (NDRs)

- NDRs (bounce-backs) are now **rare** due to spammers misusing them.
- **Do not rely on NDRs** for confirmation - always verify delivery manually if critical.

Out of Office Replies

- **Limit automatic replies** as spammers use them to confirm active addresses.
- If necessary, **enable auto-replies only for internal contacts.**

Mail Encryption

- For **sensitive content,** use **encrypted email services** to secure messages during transmission.
- This is **crucial for financial, legal, or confidential data.**

! A bounce rate below 2% is considered normal, while rates between 2% and 5% are seen as warning levels, and **above 5% is critical.**

SOURCE: MICROSOFT

Recommended User Actions

Whitelist Trusted Senders
Add important contacts to **prevent emails from being marked as spam.**

Monitor Spam Folders
Regularly **check spam folders** for misplaced emails and **report incorrect spam markings.**

Use Plain Text for Troubleshooting
When encountering issues, simplify emails by **sending plain text with no attachments.**

Email delivery involves **multiple factors**, and accountability is **split between the sender and recipient.** By following best practices and leveraging **Total Group's expertise**, businesses can ensure more **reliable email communication.**

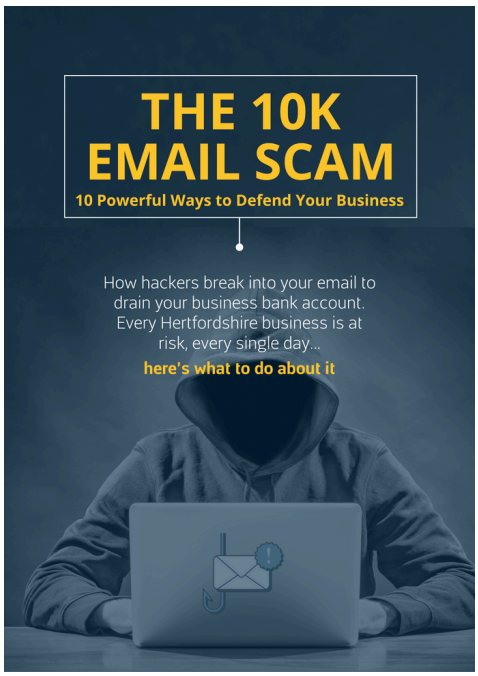
If you have any questions or need support, **we're here to help.**

Resources & Support

Your emails are one of your business's most valuable assets - but they can also be a target for fraud.

Our **10k Email Scam Guide** breaks down how businesses unknowingly expose themselves to risks and what simple steps you can take to keep your emails secure and your business protected.

Download Email Hijack Guide



IT SIMPLIFIED.
CYBERSECURITY
AMPLIFIED.

TOTAL GROUP
BETTER BUSINESS IT

Need Assistance?

Call **0333 567 9891**

IT Support Panel

Online Login: Sign in with Microsoft