

How Can Phishing Impact Your Marketing Emails?



Introduction

Phishing is one of the main factors that hurt **email deliverability** today. Even with zero malicious intent, your systeme.io campaigns can be **interpreted as phishing** by Gmail, Outlook, and Yahoo—then blocked, spam-foldered, or used to damage your **sender reputation** (help article [11133](#)).

Why Phishing Logic Hits Your Newsletters

Providers may:

- **Block** delivery
- Route to **spam**
- Collect **spam reports**
- Lower **domain trust** for all future sends

That can move you to a **higher-risk pool** in systeme.io ([4472](#)). In severe cases, domains or IPs can be **blacklisted or suspended** ([11133](#)).

Marketing Practices Often Flagged as Phishing

1. Ambiguous sender names

Risky: "Customer Service," "Urgent Support," "Account Security," "Notification" **without your brand**. Better: **Your Brand – Customer Service** (11133).

2. Clickbait subjects

Risky examples: "URGENT: Your account will be suspended," "You've won a gift," "Immediate action required." They mimic phishing and drive complaints ([363](#)).

3. Rotating links / dynamic redirects

Multi-hop or per-click redirects are prohibited and look fraudulent ([3730](#)).

4. Content vs destination mismatch

One promise in the email, another domain on the link—filters treat that like credential theft ([4247](#)). Send from you@yourbrand.com → link to **yourbrand.com** (3730).

Consequences for Your Campaigns

- **Short term:** spam folder, collapsed opens, higher spam rate, possible send pauses ([227](#))
- **Long term:** Gmail reputation loss ([11171](#)), sub-20% opens ([157](#)), brand distrust

How to Avoid Being Flagged

- **Transparency:** branded sender, honest subject, body matches CTA (11133)
- **Identity:** logo, consistent design, visible unsubscribe
- **Technical trust:** SPF/DKIM/DMARC + live site ([316](#)); opt-in only ([11009](#))
- **Links:** same root domain; no blacklisted or cloaked URLs (3730)
- **Monitor:** Email → Statistics; Postmaster ([2243](#)); re-engage inactives ([11010](#))

Frequently Asked Questions

Can honest marketing look like phishing?

Yes—filters read patterns, not intent (11133).

Link rules?

Match sending domain; avoid forbidden redirects (3730).

Already in spam?

Fix transparency, authentication, list hygiene, and watch Postmaster.

Related Resources

- [How Spam Filters Work \(10452\)](#)
- [Which Links Are Not Allowed \(3730\)](#)
- [Why Emails End Up in Spam \(2923\)](#)

On [systeme.io](#), market with **clarity and consistent domains** so anti-phishing systems work for you—not against you (11133).

Last updated: July 4, 2026