

How to Avoid Content Filters in Email Marketing

Last Modified on 09/11/2025 12:06 pm MST

This article applies to:

[Pro](#)

[Max](#)

[Max Classic](#)

You've built a great marketing email — compelling subject line, persuasive copy, strong call-to-action — and you're ready to launch. But instead of landing in the inbox, it ends up in spam, junk, or worse — dropped entirely.

You've likely been stopped by a **content (spam) filter**.

What Is a Content Filter?

Content filters are used by inbox providers (e.g., Gmail, Outlook, Yahoo) to screen incoming messages for signs of spam, phishing, or other abusive behavior **before** they reach a user's inbox.

They evaluate:

- Subject lines and body content
- Engagement history
- Sender reputation and domain health
- Link reputationFormatting and structure

If your email fails these checks, it may be junked, bounced, or blocked — even if the recipient expects it.

Why Emails Get Filtered

Inbox providers continuously refine their filtering logic based on **user behavior**. If recipients ignore, delete, or mark your emails as spam, future emails from your domain are more likely to be filtered — even for other recipients who want them.

Best Practices to Avoid Content Filters

Avoid High-Risk Industry Content

Certain industries (e.g., affiliate marketing, adult services, payday loans, crypto) have **high spam complaint rates**. To protect platform-wide deliverability, **Keap does not support** email sending for [these industries](#).

Monitor Domain Health

Your domain reputation affects whether your emails get delivered. Think of it like a **credit score** for email. Poor practices = poor score = more filtering.

How to check:

- Go to hetrixtools.com → Click **Blacklist Monitor** → Enter your domain

If **listed**, follow the de-listing instructions before sending.

Check Link Health

All links in your email — even legit ones — are scanned by filters. Bad links = red flags.

Best practices:

- Avoid shortened URLs (e.g., bit.ly, tinyurl)
- Use full, branded URLs
- Ensure all links resolve properly and lead to secure (HTTPS) pages
- Run link checks via hetrixtools.com

Watch for Spam Trigger Words

Certain keywords are frequently associated with spam and can raise your filtering risk — even in legitimate emails.

Common triggers include:

- Free / Free money / Free quote
- Cash / \$\$\$
- Instant access
- Great offer
- Risk-free / No obligation
- Stock pics

For more, see: [Glock Apps Email Spam Words](#)

Unsubscribe Link Must Be Easy to Find

Hiding or obscuring your opt-out link can cause recipients to mark your message as spam.

Do:

- Place the unsubscribe link clearly in the footer
- Use standard font size and spacing
- Honor unsubscribe requests promptly

Optimize Formatting

Poor formatting can make your email look suspicious.

Best practices:

- Maintain a text-to-image ratio of **80:20**

- Avoid sending image-only emails
- Don't use excessive formatting (ALL CAPS, bright red text, oversized fonts)
- Use consistent branding and structure across emails

Always Test Before You Send

Testing reveals how your email may be scored by spam filters.

Recommended tools:

- mail-tester.com: Scores your email and provides recommendations

Final Tips

Following these practices won't guarantee 100% inbox placement — no one can promise that — but they'll significantly reduce your risk of content-based filtering.

TL;DR – Quick Checklist:

- ✓ Monitor domain and link health
- ✓ Avoid high-risk content and spammy language
- ✓ Keep your formatting clean
- ✓ Make unsubscribe links obvious
- ✓ Test every campaign before launch

Looking for extra help?

If you'd like professional guidance with your email practices or recommended tools to improve your email practices and deliverability, check out these trusted partners:

- Email Deliverability specialist training, consulting and software
 - [EmailSmart](#)
 - List Cleaning
 - [SpamClean](#)
 - [Klean13](#)
 - [ListDefender](#)
 - Form Security
 - [Spamkill](#)
-