








Bolster AI Customer Abuse Mailbox



Bolster Customer Abuse Mailbox helps enterprise brands like yours quickly detect and stop phishing and impersonation scams. Using AI and crowd-sourced reports from your customers, we automate the detection and remediation process, keeping your brand safe while saving your team time and resources.

Why You Need Customer Abuse Mailbox

Phishing Threats Are Costly

-  Major brands are receiving upwards of **30,000 customer-reported phishing emails** per month on average.
-  Manual reviews of emails take upwards of 6 mins per email.
-  **2 out of 3 emails** are false positive, creating a lot of noise and increasing the tier 1 triage costs.
-  Manual Process can take **weeks** per takedown, leading to lost customer trust and increased operational costs.
-  A phishing report from 1 customer can uncover campaigns targeting tens of thousands or more, revealing widespread threats that impact the broader customer base.

The Impact

-  **15%** of scammed customers do not renew their services
-  **30%** create costly support tickets at ~\$5 per ticket
-  Account takeover scams can cost companies upward **\$500** per user

How It Works

1 AI-Powered Detection

Analyzes customer-reported emails for phishing by detecting intent, brand impersonation through logos, suspicious links, sender details, and malware in attachments.

2 Automated Takedowns

Bolster's AI agents + SOC team handle threats end-to-end, reducing response times from days to hours.

3 Customer Communication

Automatically informs customers about threat resolutions, building trust and engagement.



1. Scammer sends fake emails to customers

2. Customers report scam emails to brand's mailbox

3. Emails are automatically forwarded to Bolster

4. Bolster reviews all emails to identify true positives and begins takedowns



Bolster AI Customer Abuse Mailbox

Key Benefits

- ✓ **Protect Your Customers**
Stop phishing scams, protect your customers, and safeguard your reputation.
- ✓ **Automate Your Defense**
AI and SOC teams collaborate to handle thousands of phishing reports efficiently.
- ✓ **Build Customer Loyalty**
Show customers their safety is your priority, strengthening trust and retention.
- ✓ **Save Time and Costs**
Cut manual processing by 50%, freeing up your team to focus on strategic priorities.

What Makes Bolster Different

- 🔗 **Crowd-Sourced Model**
Engage your customers to report phishing, creating a broader security net.
- 👍 **True Positive Insights**
Our solution helps you focus on the real threats that need action while eliminating the time wasted on reviewing positives.
- 🌐 **Global Reach**
Handles complex takedowns across multiple countries in just hours.
- 💡 **Scalable Solution**
Designed for enterprises processing tens of thousands of phishing reports monthly.

Manual Triage vs. Bolster

Process	Manual Triage	 With Bolster
Average Time to Review Email for Scam	6 mins	5 seconds
Average Time per Takedown	2 weeks+	80% are taken down within 72 hours
True Positives Handled	Limited by capacity	Scalable to thousands monthly
False Positives Reviewed	2 out of 3 emails (wasted time)	Automated filtering
Customer Communication	Delayed or inconsistent	Automated in real-time

Proven Results



99.999%
detection accuracy rate



Hours vs. Days
Threats neutralized within hours



98.6% Manual Reduction
Easing Internal team workloads



Ready to Strengthen Your Brand's Defense?

Contact us today to see how Bolster Customer Abuse Mailbox can protect your business, save time, and build customer trust.

[Request a Demo](#)