Trusting Transactional Email

Best practices for safeguarding user trust and breaking the attack chain

Introduction

Most organisations work to secure email sent and received by their users. But for every email written by a person, at least six more are generated by systems. They're called transactional emails—think password resets, receipts, invoices, one-time passcodes, delivery updates, reminders and the like.

Transactional emails help make modern business possible. They bear the digital imprint of your trusted email domain. And they aren't questioned by most recipients.

Unfortunately, these emails also go largely unsecured. They sit outside your protected email infrastructure (for valid technical and business reasons). So they are prone to being compromised by cyber criminals seeking to exploit your domain—and your users' trust.

What are transactional emails?

Transactional emails are automated messages sent to customers as part of a business routine. Examples include:

- Password-reset emails
- Order confirmations
- Digital receipts
- Follow-up surveys
- One-time login codes

These types of emails are usually triggered by user actions, custom-generated for each recipient and are used for established customer-vendor relationships. This category of email does not include person-to-person or one-to-many emails such as those used in marketing campaigns

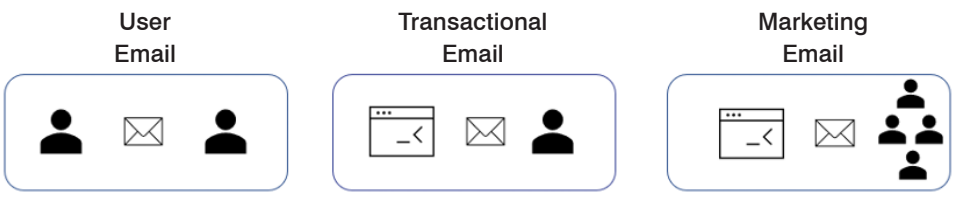

Figure 1: Different types of email.

Headlines from Email Relay Compromises

- **Mailchimp says it was hacked—again** (*TechCrunch,* January 2023)
- **HMRC phishing scam abuses mail service to bypass spam filters** (*BleepingComputer,* December 2020)
- **Sendgrid Under Siege from Hacked Accounts** (*KrebsOnSecurity,* August 2020)
- **Rackspace security vulnerability leaves customers open to cyberattack: SMTP Multipass** (*Hacking,* July 2020)

Email automation service Mailchimp is a case in point. Between April 2022 and January 2023 company suffered three social engineering attacks. Attackers used employee credentials to get into internal support and account admin tools. The breach gave attackers access to email domains owned by Mailchimp customers. Armed with those domains, attackers then targeted people on those firms' email marketing lists.

Some of the breached accounts belonged to Mailchimp customers with hundreds of thousands, or even millions, of email addresses on their rosters. One of the affected customers was WooCommerce, a widely used e-commerce plugin for WordPress with 5 million customers.[1] Another was FanDuel, a popular gambling website.[2]

Why transactional email is a target

It's easy to see why attackers target transactional and other app-generated email:

- They get access to infrastructure built for sending large volumes of email.
- Compromised accounts can send malicious emails through a trusted domain that passes basic security checks. The emails may seem benign to even security-aware recipients.
- These channels are used for routine business and exist outside of the protected email environment, so they often sidestep normal security controls.

Why it often goes unprotected

If transactional email is such a prime target, why do so few organisations secure it?

First, these email channels are often set up outside of organisations' protected email environment, usually for sound technical and business reasons.

Most transactional emails come from one of these three sources:

- Internal on-premises applications
- Internal cloud-hosted applications
- Third-party software-as-a-service (SaaS) partners sending email on your domains' behalf

Companies that still use on-premises email relays for transactional email avoid mixing it with email sent by their users. That's because transactional emails can occur in high volumes. Sending everything through the same relay may drag down sending performance for everyone. And critically, apps tend to send transactional messages in large, sudden bursts—activity that can be misconstrued as spam. A blocklist on an IP address used for mixed user and transactional emails would halt user all outgoing email, grinding most business to a halt.

Many legacy applications were deployed on premises. But more and more often, companies are migrating to web applications and cloud hosting with platform-as-a-service (PaaS) platforms such as Microsoft Azure. In this case, keeping user and transactional email separate remains a best practice for many of the same reasons.

A growing number of transactional messages are sent on a company's behalf from third-party SaaS apps such as Salesforce, ServiceNow and Workday. Adding third-party SaaS apps that use shared sending IPs into your Sender Policy Framework (SPF) record adds another layer of risk and can tarnish your brand. These vendors tend to have a business model focused on reliably delivering email—not safeguarding it.

1 Zack Whittaker (*TechCrunch*). "Mailchimp says it was hacked — again." January 2023.
2 Lawrence Abrams (*Bleeping Computer*). "FanDuel warns of data breach after customer info stolen in vendor hack." January 2023.

Equal Protection: A Three-Step Plan to Secure Transactional Email

Setting up the right environment for sending and managing transactional emails in a secure manner is critical. Here are some of the key factors and best practices that you should consider when creating and maintaining your transactional email environment.

Step 1: Establish centralised visibility and control

Securing transactional email starts with centralised visibility and control over both internal apps and any third parties sending on your behalf. Sources should be approved and validated. To that end, we strongly recommend using a secure connection (such as SMTP authentication) between sources and your sending environment.

Reduce the risk of someone spoofing your domain by allowing only a very limited set of sending IP addresses in your SPF record. Sending traffic from dedicated IP addresses shrinks this risk even further.

Step 2: Scan messages before sending

Every message sent from your domain reflects on your company. Scanning messages for spam or malware is a vital step toward ensuring that no one is exploiting customers or business partners in your name. Applying data loss prevention (DLP) rules or encryption is even better, especially if you're dealing with financial, healthcare or other personally identifiable information (PII).

By using these features, you demonstrate your commitment to security and privacy, building trust with customers and partners.

Step 3: Sign messages with Domain Keys Identified Mail (DKIM)

Sign all outbound messages using the Domain Keys Identified Mail (DKIM) protocol. It's one of the best things you can do to ensure the security and authenticity of email sent under your domain. Beyond preventing spoofing, phishing, and spamming, DKIM can improve your sender reputation and deliverability.

If you're using a third-party SaaS partner that lacks DKIM, procure or build an environment to take in these messages and add DKIM signing before sending. DMARC (Domain-Based Message Authentication, Reporting and Conformance), which builds on SPF and DKIM, has become a critical part of protecting brands.

How Proofpoint Secure Email Relay Can Help

Proofpoint Secure Email Relay creates a separate and equally protected sending environment for transactional emails. The solution offers a range of benefits to multiple teams. Here are just a few:

Messaging teams

With Proofpoint Secure Email Relay, messaging teams can ensure that messages are delivered without worrying about external factors that might compromise them.

Application traffic won't harm the reputation of your sending IPs. And if an issue occurs with an app, it won't affect user-generated or marketing emails. Your brand reputation is isolated from any issues that stem from third-party partners sending from your domains.

Proofpoint Secure Email Relay not only helps deliverability, but it can also safeguard the reputation of your domain and brand.

Security teams

For security teams, Proofpoint Secure Email Relay reduces the risks that stem from an overly permissive SPF record. (Too many IP addresses in your SPF record may expose your domain to spoofing and phishing attacks.)

Centralised control also lets security teams turn off apps, such as third-party apps sending on your behalf, if they become suspect. This is especially important for third-party SaaS providers that use shared IP addresses and are ripe for abuse.

With Proofpoint Secure Email Relay, you can ensure that only legitimate and trusted senders can use your domain name, protecting your domain and the people who trust it.

Infrastructure teams

As a cloud-based service, Proofpoint Secure Email Relay ends the need for maintaining on-premises infrastructure and simplifies the email delivery process. You can be sure that your emails reach your customers reliably—and securely.

It also enables developers in your organisation to send transactional emails from the apps they create. Developers have a standardised way of securing transactional email, reducing use of unapproved tools that may or may not be secure.

Next Steps: Learn More

Proofpoint is an industry leader in email security. We have the resources, technology and expertise to help you separate and protect your transactional emails. The process is faster and more cost-effective than you might think. With Proofpoint Secure Email Relay, you'll be up and running in no time.

Learn more about how Proofpoint Secure Email Relay can help secure your transactional email at: **https://www.proofpoint.com/uk/products/email-security-and-protection/secure-email-relay**.

LEARN MORE

For more information, visit **proofpoint.com**.