Proofpoint Impersonation Protection

Protect your communications with trusted partners, customers and suppliers

Key Benefits

- Protect your trusted business communications from impersonation threats
- Prevent you and your brand from impersonation abuse
- Detect and defend against risky suppliers, including compromised supplier accounts
- Secure your user and application emails so they can be trusted

Most organizations rely on email to do business. But attackers have figured out how to hijack your trusted business communications. They can impersonate you, your brand or your business partners. According to the FBI, impersonation attacks such as business email compromise (BEC) have cost businesses more than $2.7 billion. And the cost of a data breach that involved a compromised vendor was nearly $5 million.[1]

Tactics such as spoofed domains, lookalike domains and compromised supplier accounts are often used jointly in impersonation attacks. You must protect your communications with trusted partners, customers and suppliers against these threats. Proofpoint can help you mitigate the risk. We authenticate your user and application email and defend against compromised supplier accounts.

Proofpoint takes a holistic multilayered approach to protect you and your brand from impersonation abuse. We identify your risky suppliers. We detect potentially compromised supplier accounts as well as lookalikes of your suppliers' domains. We also secure both your user and application email so they can be trusted.

Protect You and Your Brand from Impersonation Abuse

One of the most common impersonation tactics is domain spoofing. Without the right security controls in place, attackers can easily steal your trusted domains. This allows them to target your customers, partners and even your employees. Email authentication is the most effective way to stop it. Proofpoint Impersonation

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

1 IBM. *Cost of a Data Breach Report*. 2023.

Protection implements DMARC to help you authenticate both your user and application emails. We simplify DMARC implementation by guiding you through each step of your rollout. Our experts will work with you to identify your legitimate senders. They will also ensure that all of your email—including those from third-party authorized senders—authenticate properly.

Integration with Proofpoint Threat Protection allows you to enforce DMARC authentication for inbound messages with confidence. It adds a security layer to prevent inbound threats that spoof your trusted domains. It also lets you override DMARC policies without blocking legitimate email or compromising security with safelisting. This integration gives you visibility into both inbound and outbound email traffic. You can see all the emails sent that use your trusted domains, including those sent by third parties.

Defend Against Compromised Supplier Accounts

Attackers have turned the supply chain into another threat vector. They often use compromised supplier accounts to hijack email communications between you and your business partners. Emails from compromised suppliers do not always carry malicious payloads and will pass authentication. This makes them hard to detect. And they often result in huge financial loss, data extortion or ransomware attack.

Proofpoint Impersonation Protection helps you detect and defend against risky suppliers, including compromised supplier accounts. It uses behavioral AI, machine learning and threat intelligence derived from across our large customer footprint to proactively uncover potentially compromised supplier accounts. It includes adaptive controls, such as automatic isolation of URLs from compromised supplier accounts, to mitigate your exposure. Integration with Proofpoint Threat Protection and context around sender-recipient relationships streamline third party incident response and investigation.

Uncover Malicious Lookalikes

Another common tactic is to fool recipients with lookalike domains. This is where attackers register domain names that closely resemble a legitimate brand or entity. Lookalike domain spoofing is used in attacks such as credential phishing, BEC and even telephone-oriented attack delivery (TOAD).

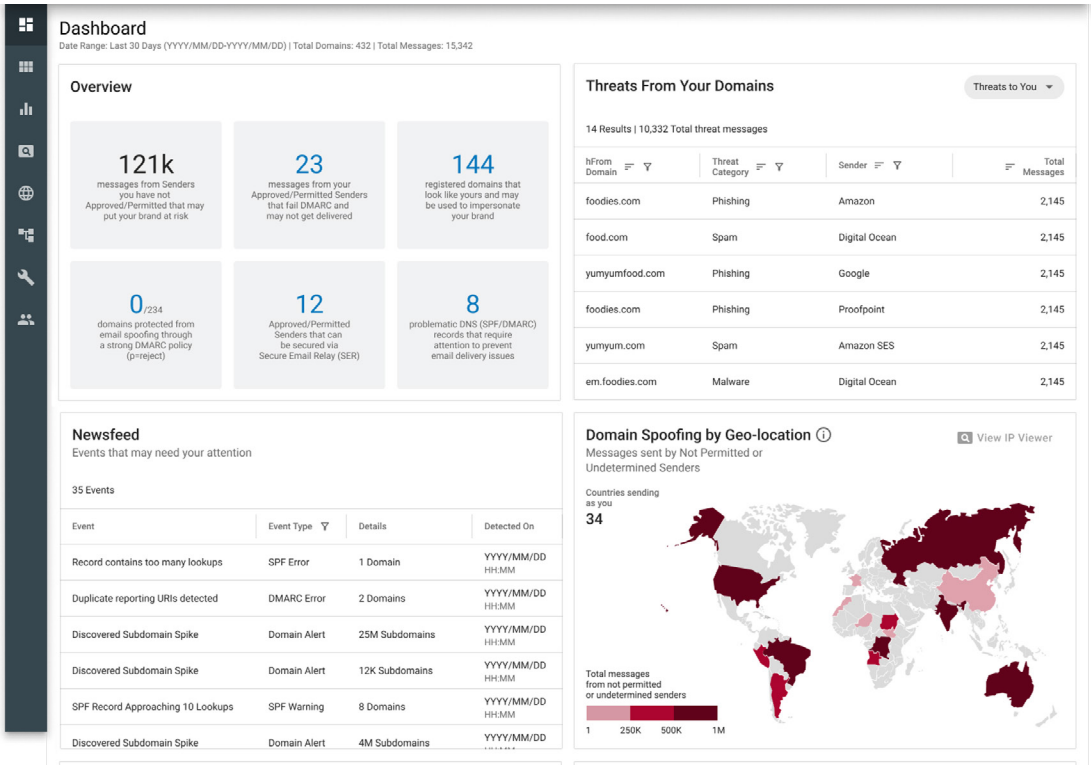

Figure 1: Proofpoint gives you visibility into domain spoofing threats, malicious lookalikes of your domains, as well as emails being sent using your trusted domains.

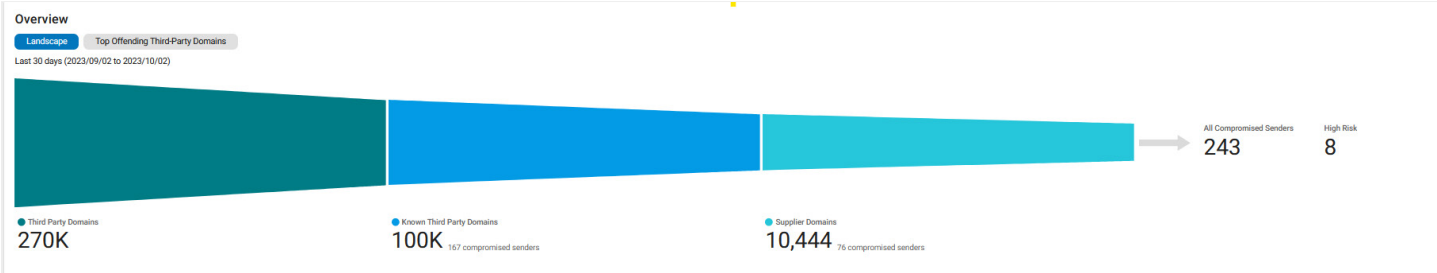

Figure 2: Proofpoint detects potentially compromised third party accounts that you do business with and provides you visibility into high-risk suppliers.

Proofpoint helps you uncover malicious lookalikes of your trusted domains. We dynamically detect newly registered domains that pose as your brand in email attacks or phishing websites. We provide a complete view of suspicious domains. We also help you detect malicious lookalikes of your suppliers' domains. By revealing the message volume and the messages delivered from the lookalikes of your suppliers' domain, we enable you to proactively address high-risk suppliers who may be impersonated.

Secure Application Emails Sent As You

Emails sent "as you" can come from third party applications that you do not control. Organizations might use Workday to send their employees payroll-related email, for example. And they might use Salesforce to send their customers newsletters. Without any control, this could leave application emails that use your trusted domains vulnerable. Once a third-party application or a SaaS partner is compromised, attackers can inject malware into transactional emails that can seem to come from you. Worst of all, these contaminated transactional emails could pass email authentication.

Proofpoint Impersonation Protection secures your application emails as well as the ones sent on your behalf. We bring our security and compliance controls to bear on transactional emails that use your trusted domains. We authenticate these emails and apply our industry-leading threat detection to spot malware or threats. This ensures that your customers, business partners and employees only receive authentic, clean application emails from you. It also gives you centralized control over transactional emails from third-party applications and SaaS partners. You can shut down malicious application email traffic from compromised third-party partners using your domains at any time.

LEARN MORE

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