PROOFPOINT EMAIL FRAUD DEFENSE

ELIMINATING THE IMPACT OF EMAIL FRAUD
Email fraud is rife—business email compromise (BEC) is costing companies billions, and consumer phishing is at an all-time high. The majority of these email attacks can be prevented.

Leveraging the power of email authentication (SPF, DKIM, and DMARC), Proofpoint Email Fraud Defense protects your organisation from all phishing attacks (including 80% of impostor emails) spoofing trusted domains.

Visibility into who is sending email across your enterprise allows you to authorise all legitimate senders and block fraudulent emails before they reach your employees, business partners, and customers.

When you deploy Email Fraud Defense with our other defenses, you can nullify an entire class of impostor email fraud. Use our solutions to:

• Stop email-based ransomware
• Prevent CEO/CFO wire transfer attacks and W-2 scams
• Block emails spoofing corporate and brand identities before they reach your employees and customers

GRANULAR VISIBILITY
Understand who is sending email across your enterprise.

Email Fraud Defense helps you make sense of email authentication data via a DMARC (Domain-based Message Authentication Reporting & Conformance) reporting interface that renders authentication results for all email traffic coming into, and going out of, your organisation. We interpret that data using automated algorithms that differentiate between anomalies and issues that need attention.

With Email Fraud Defense, you can:

• Monitor all emails (inbound and outbound) from your domains and those of third parties
• Accurately distinguish between legitimate emails and bad emails failing authentication
• Understand the reasons behind each authentication failure

BLOCK EMAIL THREATS AND ELIMINATE RISK
Implement a DMARC “reject” policy without the risk of false positives.

A DMARC “reject” policy is effective; it will block all emails from IPs you have not authorised to send messages from your domain. But implementing DMARC may also result in legitimate inbound email getting blocked. Email Fraud Defense is the only email authentication solution that gets you to a full DMARC implementation faster with less risk.

With Email Fraud Defense, you can:

• Get clear workflow instructions for specific email authentication policy actions
• Configure exceptions, alerts, and rules on your Proofpoint Email Protection gateway for any sender scenario
• Instruct your Proofpoint Email Protection gateway to block impostor email threats before they reach employee and consumer inboxes

GET SUPPORT
Our global team of email experts is here to help.

Getting your legitimate mail streams (as well as those of your vendors and partners) to authenticate correctly without support is hard. Our Professional Services team crafts fully customised project implementation plans, develops a comprehensive risk assessment from start to finish, while providing a trouble-free DMARC implementation and ongoing management.

We will:

• Act as a dedicated extension of your internal teams, analysing email threat data to help you understand the nature of attacks identified
• Provide ongoing support as your business email practices evolve
• Offer continuous monitoring to optimise your DMARC implementation