proofpoint

# PROOFPOINT EMAIL FRAUD DEFENSE

## EMAIL IS THE NO. 1 THREAT VECTOR FOR THE ENTERPRISE

- 30% of recipients open phishing messages and 12% click on attachments[1]
- Business email compromise (BEC), or impostor email scams, have cost companies over $3.1 billion since January 2015[2]
- Nearly 2/3rds of all impostor emails spoof trusted domains and can be blocked before reaching the inbox[3]

## FEATURES

- Granular visibility across your email ecosystem
- Real-time identification of emails failing authentication
- Dynamic configuration of exceptions, alerts, and rules

## BENEFITS

- Block BEC or impostor emails spoofing your domains before they reach the inbox
- Block wire transfer fraud, W-2 breaches, and ransomware infections
- Alleviate board concerns and mitigate risk of exposure by preventing corporate identity theft
- Extend protection to your customers and partners

[1] "2016 Data Breach Investigation Report" April, 2016
[2] Business Email Compromise: The 3.1 Billion Dollar Scam" June, 2016
[3] Proofpoint 2017

Email fraud is rife. Impostor email is costing companies billions and consumer phishing is at an all-time high. These attacks are highly targeted and constantly shift in approach, creating a successful avenue for cybercriminals to lure money and valuable information away from organisations.

Authenticating email (DMARC, SPF, DKIM) can prevent the most common form of email fraud—domain spoofing. It is common practice to authenticate users, websites, and resources to protect critical information and as the number one threat vector, email must be authenticated as well. But enforcing authentication can be difficult and may result in blocking legitimate email, potentially disrupting your business.

## ELIMINATE THE IMPACT OF EMAIL FRAUD

Proofpoint Email Fraud Defense protects your organisation from all phishing and impostor attacks that spoof your domains. Visibility into who is sending email on your behalf 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 solutions, you can nullify an entire class of impostor email fraud.

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

## GRANULAR VISIBILITY

Email Fraud Defense gives you visibility across your email ecosystem by not only analysing and interpreting DMARC reports, but enriching them with robust message samples. Understand who is sending email on your behalf with a full view into the email traffic coming into, and going out of your organisation. Gain insights into authentication failures and differentiate between anomalies and real issues that need attention.

- Monitor all emails sent using your domains (whether they're sent from you, or by third parties)
- Accurately distinguish between legitimate emails and bad emails failing authentication
- Understand the reasons behind—and learn how to fix—each authentication failure

## IMPLEMENT AUTHENTICATION WITH CONFIDENCE

By leveraging the power of DMARC to identify and authenticate legitimate email sent from your domains, Email Fraud Defense works to block all unauthorised messages. Plus, you get clear workflow instructions for how to

fix authentication failures, should they occur. Email Fraud Defense is the only solution that gives you the tools and services you need to implement authentication quickly and confidently.

- Authorise all legitimate email sent from your domains
- Understand the authentication posture of your third-party email senders
- Fix authentication issues of legitimate traffic sent from your organisation

## GAIN CONTROL WITH POLICY ENFORCEMENT

Block all fraudulent emails without risk by applying authentication policies. Email Fraud Defense gives you the confidence to implement a DMARC 'reject' policy, stopping all unauthorised messages sent from your domain, before they reach your employees, partners, and customers. With the Proofpoint Email Protection gateway, you can configure exceptions, alerts, and rules for any sender scenario and block all incoming domain-spoofing emails that fail authentication.

- Get clear workflow instructions for specific email authentication policy actions
- Enable recipients to authenticate valid email from you
- Instruct your Proofpoint Email Protection gateway to block impostor email threats before they reach employees

## PEACE OF MIND WITH MANAGED SERVICES

Authenticating your mail streams correctly—including those of your vendors and partners—is difficult. Our Professional Services team helps you reduce the risk of blocking legitimate mail. Additionally, you gain fully customised project execution plans, a comprehensive risk assessment, and trouble-free implementation and ongoing management of DMARC. We offer:

- A dedicated extension of your internal teams to help you identify legitimate email streams
- Ongoing support as your business email practices evolve
- Continuous monitoring to optimise your DMARC implementation