PROOFPOINT EMAIL FRAUD DEFENSE

EMAIL IS THE NO. 1 THREAT VECTOR IN THE ENTERPRISE

- BEC has cost companies over $5.3 billion since January 2013.[1]
- 30% of recipients open phishing messages, and 12% click on attachments.[2]
- Domain spoofing makes up the majority of all email fraud and can be prevented through email authentication.[3]

BENEFITS

- Stop email fraud and phishing attacks before they reach the inbox.
- Gain full visibility and control of the email sent from your organization.
- Implement email authentication quickly and confidently on your domains and gateway.
- Extend protection to your customers and partners.

Proofpoint Email Fraud Defense protects your employees, customers, and business partners from cyber criminals who spoof trusted email domains. It makes email authentication easy and reliable so you can stop email fraud before it reaches the inbox.

Email Fraud Defense blocks socially engineered attacks such as business email compromise (BEC) and consumer phishing. These attacks shift constantly, and they target people, not your infrastructure. That makes email fraud hard to stop with traditional security tools. Cyber criminals posing as colleagues, partners and vendors simply lure money and valuable information away from victims—no malware or exploit needed.

Email Fraud Defense stops these attacks using DMARC (Domain-based Message Authentication, Reporting and Conformance) authentication. The industry-standard protocol ensures that email is really from who it says it's from. DMARC authentication makes email trustworthy. It ensures that attackers aren't impersonating your organization. Using Email Fraud Defense also stops spoofed email from entering your environment—even email from other organizations.

With Email Fraud Defense, you can prevent entire categories of email fraud. And you get full visibility into the authentication status of email sent to and from your organization. Email Fraud Defense gives you the confidence that you're blocking fraudulent email and letting legitimate senders through.

PROTECT YOUR EMPLOYEES, CUSTOMERS, AND BUSINESS PARTNERS

Employees, outside email service providers, and partners send email on your behalf every day. Cyber criminals take on these trusted identities to defraud recipients through BEC and credential phishing.

Get visibility into your entire email ecosystem. You can see what email passes authentication, what email fails, and why. You'll know whether legitimate email that should have passed failed—and how to fix it.

[1] FBI. "Business E-Mail Compromise/E-Mail Account Compromise: the 5 Billion Dollar Scam." May 2017.
[2] Verizon. "2016 Data Breach Investigations Report." April 2016.
[3] Proofpoint. "The Human Factor 2017." June 2017.

Email Fraud Defense helps you account for and verify all email coming into and sent out from your organization. This 360-degree visibility helps you authorize all legitimate email sent on your behalf and block fraudulent messages before they reach the inbox.

- Stop email fraud targeting your employees, customers, and partners.
- Maintain the trust people place on your email communications.
- Get a complete view into all email coming into, and sent out from your organization.

SIMPLIFY EMAIL AUTHENTICATION WITHOUT BLOCKING LEGITIMATE EMAIL

Identifying and authenticating the legitimate email sent to your employees, customers, and partners, empowers you to block all unauthorized email.

But authentication enforcement can't be automated. And it requires deep expertise. Enforcing DMARC can be difficult. Often, it leads to legitimate email being blocked, disrupting business.

Email Fraud Defense gives you the tools and services you need to deploy DMARC authentication quickly and confidently.

- Automate the identification of legitimate email sent on your behalf.
- Understand the reasons behind—and learn how to fix—each authentication failure.
- Get ongoing guidance and support from our professional services team to deploy email authentication efficiently on your domains and gateway.

ENRICH YOUR INVESTMENT IN PROOFPOINT EMAIL PROTECTION FOR GREATER SECURITY AND FLEXIBILITY

Having visibility and control of the email sent to your employees can help you prevent email fraud. With Email Fraud Defense, you can quickly and safely configure Email Protection to enforce authentication on all incoming email.

For added protection, use the flexibility of Proofpoint Email Protection to configure overrides for legitimate email that fails authentication. That means you can enforce authentication more quickly on all other messages. Add Email Protection's Impostor Classifier to Email Fraud Defense for a multi-layered approach to protect against every type of impostor email attack.

- Prevent BEC and phishing attacks that target your employees.
- Account for and authorize all email sent to your organization faster with visibility and control.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.