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.

---

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.