proofpoint.

EMAIL FRAUD DEFENSE DI PROOFPOINT

LA POSTA ELETTRONICA È IL PRIMO VETTORE DI MINACCE IN AZIENDA

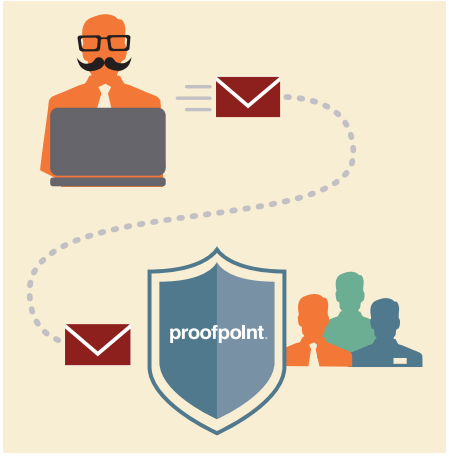
- Le truffe BEC sono costate alle aziende oltre $5,3 miliardi dal gennaio 2013.[1]
- Il 30% dei destinatari apre i messaggi di phishing e il 12% fa clic sugli allegati.[2]
- Lo spoofing del dominio costituisce la maggioranza di tutte le frodi per e-mail e può essere prevenuto tramite l'autenticazione delle e-mail.[3]

VANTAGGI

- Fermate le frodi per e-mail e gli attacchi di phishing prima che raggiungano la posta in arrivo.
- Ottenete completa visibilità e controllo delle e-mail inviate dalla vostra azienda.
- Implementate l'autenticazione e-mail in modo rapido e sicuro su domini e gateway.
- Estendete la protezione a clienti e partner.

[1] FBI. "Compromissione delle e-mail aziendali/ Compromissione dell'account di posta elettronica: la truffa da 5 miliardi di dollari." Maggio 2017.
[2] Verizon. "2016 Data Breach Investigations Report." Aprile 2016.
[3] Proofpoint. "The Human Factor 2017." Giugno 2017.

Email Fraud Defense di Proofpoint protegge i vostri dipendenti, clienti e partner aziendali dai criminali informatici che falsificano domini e-mail affidabili. Questo strumento consente un'autenticazione semplice e affidabile permettendo di fermare le frodi per e-mail prima che raggiungano la posta in arrivo.



Email Fraud Defense blocca gli attacchi progettati socialmente come la compromissione della corrispondenza digitale aziendale (BEC) e il phishing dei consumatori. Questi attacchi mutano continuamente e anziché rivolgersi all'infrastruttura, sono diretti alle persone. Questo rende le frodi per e-mail difficili da fermare con gli strumenti di sicurezza tradizionali. I criminali informatici che si fanno passare per colleghi, partner e fornitori convincono le vittime a consegnare loro denaro e informazioni preziose, senza bisogno di usare malware o exploit.

Email Fraud Defense ferma questi attacchi utilizzando l'autenticazione DMARC (Domain-based Message Authentication, Reporting and Conformance). Il protocollo standard del settore assicura che l'e-mail provenga realmente da chi l'ha inviata. L'autenticazione DMARC rende le e-mail affidabili. Assicura che gli aggressori non si spaccino per la vostra azienda. Email Fraud Defense impedisce inoltre alle e-mail falsificate di entrare nel vostro ambiente, perfino quelle provenienti da altre aziende.

Con Email Fraud Defense, potete prevenire intere categorie di frodi per e-mail, e ottenete completa visibilità dello stato di autenticazione delle e-mail inviate e ricevute dalla vostra azienda. Con Email Fraud Defense avete la sicurezza di bloccare le e-mail fraudolente e di lasciar entrare i mittenti legittimi.

PROTEGGETE DIPENDENTI, CLIENTI E PARTNER AZIENDALI

Dipendenti, fornitori di servizi di posta elettronica esterni e partner inviano e-mail per contro della vostra azienda ogni giorno. I criminali informatici si appropriano di queste identità affidabili per derubare i destinatari tramite BEC e phishing delle credenziali.

Ottenete visibilità dell'intero ecosistema di posta elettronica. Potete vedere quali e-mail superano l'autenticazione, quali no e perché. Saprete se l'e-mail legittima che avrebbe dovuto superare l'autenticazione non l'ha fatto e come risolvere questo problema.

Email Fraud Defense aiuta a tenere conto e verificare tutte le e-mail ricevute e inviate dalla vostra azienda. Questa visibilità a 360 gradi vi consente di autorizzare tutte le e-mail legittime inviate per vostro conto e di bloccare i messaggi fraudolenti prima che raggiungano la posta in arrivo.

- Impedite alle frodi per e-mail di mirare ai vostri dipendenti, clienti e partner.
- Conservate la fiducia che gli altri ripongono nelle vostre comunicazioni per e-mail.
- Ottenete una visione completa di tutte le e-mail inviate e ricevute dalla vostra azienda.

SEMPLIFICATE L'AUTENTICAZIONE E-MAIL SENZA BLOCCARE I MESSAGGI LEGITTIMI

L'identificazione e l'autenticazione delle e-mail legittime inviate ai dipendenti, ai clienti e ai partner, vi consentono di bloccare tutte le e-mail non autorizzate.

Tuttavia applicare l'autenticazione non può essere un processo automatizzato e richiede un'esperienza approfondita. L'applicazione del DMARC può essere ardua. Spesso, causa il blocco delle e-mail legittime, con interruzione dell'attività.

Email Fraud Defense fornisce gli strumenti e i servizi necessari per implementare in modo rapido e sicuro l'autenticazione DMARC.

- Automatizzate l'identificazione delle e-mail inviate per vostro conto.
- Comprendete i motivi che stanno dietro ogni errore di autenticazione e imparate a risolverli.
- Ottenete guida e supporto continui dal nostro team di servizi professionali per implementare in modo efficiente sui vostri domini e gateway l'autenticazione delle e-mail.

ARRICCHITE IL VOSTRO INVESTIMENTO NELLA EMAIL PROTECTION DI PROOFPOINT PER UNA MAGGIORE SICUREZZA E FLESSIBILITÀ.

Avere visibilità e controllo delle e-mail inviate ai vostri dipendenti può aiutarvi a prevenire le frodi per e-mail. Con Email Fraud Defense, potete configurare in modo rapido e sicuro Email Protection per applicare l'autenticazione su tutte le e-mail in arrivo.

Per una maggiore protezione, utilizzate la flessibiltà di Email Protection di Proofpoint per configurare gli override per le e-mail legittime che non superano l'autenticazione. Ciò significa che potete applicare l'autenticazione più rapidamente su tutti gli altri messaggi. Aggiungete Impostor Classifier di Email Protection a Email Fraud Defense per un approccio a più strati per proteggervi contro ogni tipo di attacco e-mail fraudolento.

- Prevenite gli attacchi phishing e BEC rivolti ai vostri dipendenti.
- Tenete in considerazione e autorizzate tutte le e-mail ricevute dalla vostra azienda in modo più rapido con visibilità e controllo.