EBOOK

Autenticazione DMARC: la chiave per migliorare il tasso di recapito delle email

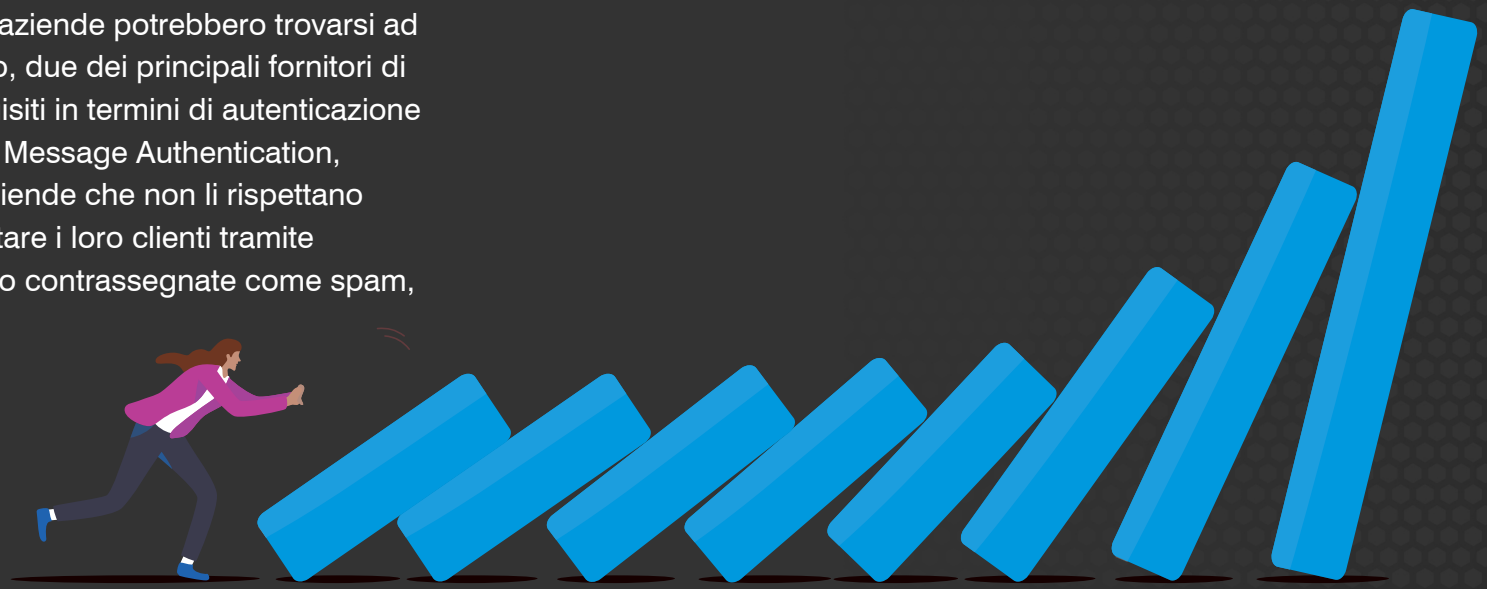
Perché l'autenticazione delle email è fondamentale per raggiungere i potenziali clienti, servire i clienti attuali e proteggere il tuo marchio

proofpoint.

Introduzione: Il giorno dell'autenticazione DMARC è arrivato

Cosa succederebbe se i tuoi clienti smettessero di ricevere le email della tua azienda? Improvvisamente, il tuo canale di marketing più rapido ed efficace non sarebbe più disponibile. I clienti non potrebbero accedere per verificare la loro identità o reimpostare le loro password. Il servizio di assistenza ai clienti sarebbe interrotto.

È proprio questo lo scenario che le aziende potrebbero trovarsi ad affrontare dopo che Google e Yahoo, due dei principali fornitori di email, hanno annunciato nuovi requisiti in termini di autenticazione delle email DMARC (Domain-based Message Authentication, Reporting and Conformance). Le aziende che non li rispettano potrebbero avere problemi a contattare i loro clienti tramite l'email, in quanto le email verrebbero contrassegnate come spam, o addirittura bloccate.



L'obiettivo

L'email è uno dei canali di comunicazione più utilizzati ed efficaci del mondo moderno. Ma deve anche affrontare numerose sfide e minacce da parte dei criminali informatici che sfruttano questo canale per lanciare attacchi di phishing, spoofing e spam.

Imponendo l'autenticazione DMARC ai mittenti che inviano più di 5.000 email al giorno a indirizzi Gmail o Yahoo Mail, i due giganti di Internet mirano a proteggere i loro utenti da email dannose che usurpano l'identità di mittenti o domini affidabili. Queste includono le truffe della violazione dell'email aziendale (BEC, Business Email Compromise) che costano alle aziende miliardi di dollari ogni anno. Le due aziende sperano inoltre di incoraggiare l'adozione di pratiche e standard più sicuri per l'email nel settore. Questi standard includono l'introduzione di semplici opzioni di cancellazione e il rispetto di una soglia di tassi di spam.

Insieme, queste misure mirano a ridurre il volume delle email indesiderate e fraudolente che intasano le caselle email degli utenti e minano la loro fiducia nell'email.

La sfida

Implementare correttamente l'autenticazione DMARC non è un compito facile. Richiede un'attenta configurazione e monitoraggio dei record DNS (Domain Name System), l'allineamento degli identificatori SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail), la verifica delle diverse regole DMARC e l'analisi dei report DMARC.

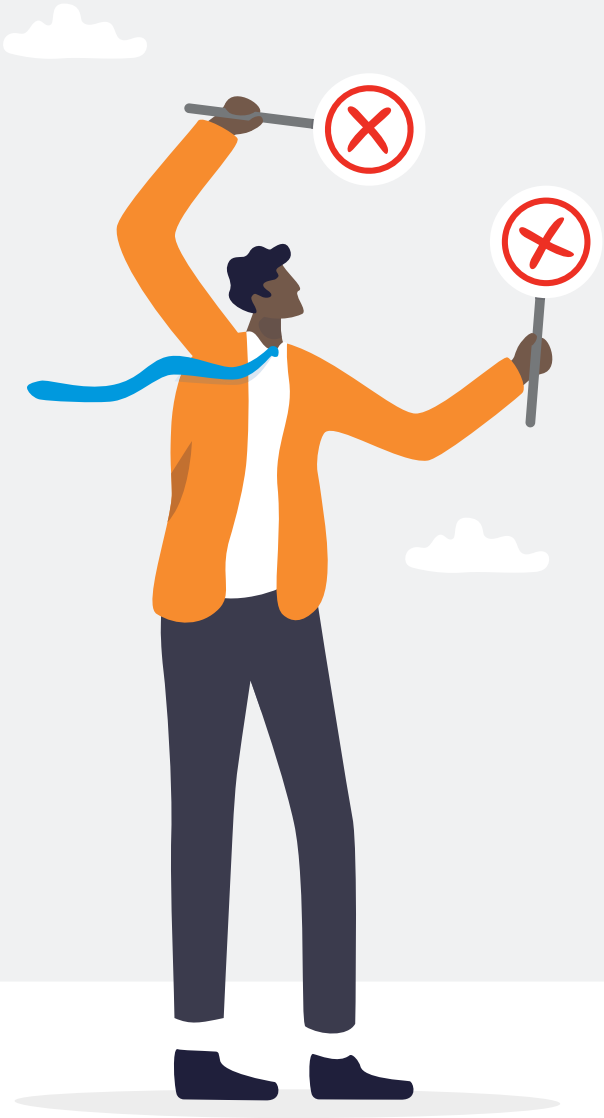
In caso contrario, le email legittime potrebbero essere bloccate o contrassegnate come spam, con ripercussioni negative sui tassi di recapito e sulle prestazioni delle email. Per questo motivo è fondamentale che le aziende che comunicano via email comprendano i vantaggi e le sfide dell'autenticazione DMARC e come implementarla correttamente, prima dell'entrata in vigore dei nuovi requisiti.

Questo eBook spiega come funziona l'autenticazione DMARC, analizza il suo impatto sul recapito delle email e offre una serie di best practice e consigli per ottimizzare i risultati dell'autenticazione DMARC.

SEZIONE 1

L'email, uno strumento fondamentale per le aziende moderne

Nel frenetico mondo digitale attuale, l'email è diventata una parte vitale dell'economia moderna. Dire che le aziende dipendono da essa per mantenere le loro operazioni senza intoppi è un eufemismo. Dalle strategie di marketing al servizio clienti, lo scambio quotidiano di milioni di email riguarda quasi tutti gli aspetti delle attività aziendali.



Uno strumento di marketing essenziale

I team di marketing fanno ampio uso dell'email come principale vettore di comunicazione per le loro campagne. La usano per inviare offerte, notizie e contenuti ai clienti potenziali ed esistenti, per stimolare il coinvolgimento e le vendite.

Un vettore di comunicazione per le transazioni

Per i clienti, la possibilità di reimpostare le password o di ricevere codici di accesso unici via email è fondamentale. Senza queste email transazionali, non potrebbero accedere ai servizi o fare affari con la tua azienda.

Un pilastro del servizio clienti

Le conferme d'ordine, le ricevute digitali e i sondaggi di follow-up inviati via email contribuiscono notevolmente a migliorare l'esperienza post-acquisto. Queste email non sono solo attese, ma richieste dai clienti come elemento fondamentale del servizio clienti.

E l'obiettivo principale dei criminali informatici

Senza un servizio email affidabile, molti aspetti delle attività si fermerebbero completamente. Purtroppo, l'email è diventata anche un obiettivo primario per i criminali informatici che cercano di sfruttare il tuo dominio e la fiducia dei tuoi utenti.

SEZIONE 2

Perché implementare l'autenticazione DMARC?

La violazione dell'email aziendale (BEC) è una delle forme più comuni e costose di frode via email (In questi attacchi, i truffatori si spacciano per mittenti affidabili utilizzando indirizzi email violati o simili). Secondo l'FBI, le truffe BEC costeranno alle aziende 51 miliardi di dollari tra il 2013 e il 2022[1]. Inoltre, secondo le nostre ricerche, più di tre aziende su quattro sono state vittime di almeno un tentativo di attacco BEC nel 2022[2].

In risposta alla crescente minaccia della frode via email, nel 2012 un consorzio di 20 aziende, tra cui Google, Yahoo, Microsoft e Facebook, ha creato lo standard DMARC, un protocollo aperto di autenticazione email che protegge l'email a livello di dominio. Questo protocollo si basa sugli standard SPF e DKIM, che verificano l'identità del mittente e l'integrità dell'email.

1 FBI, "Business Email Compromise: The $50 Billion Scam." (Violazione dell'email aziendale: una truffa da 50 miliardi di dollari), giugno 2023.
2 Proofpoint, "State of the Phish", marzo 2023.

Le truffe BEC sono costate alle aziende 51 miliardi di dollari

tra il 2013 e il 2022.

Più di 3 aziende su 4

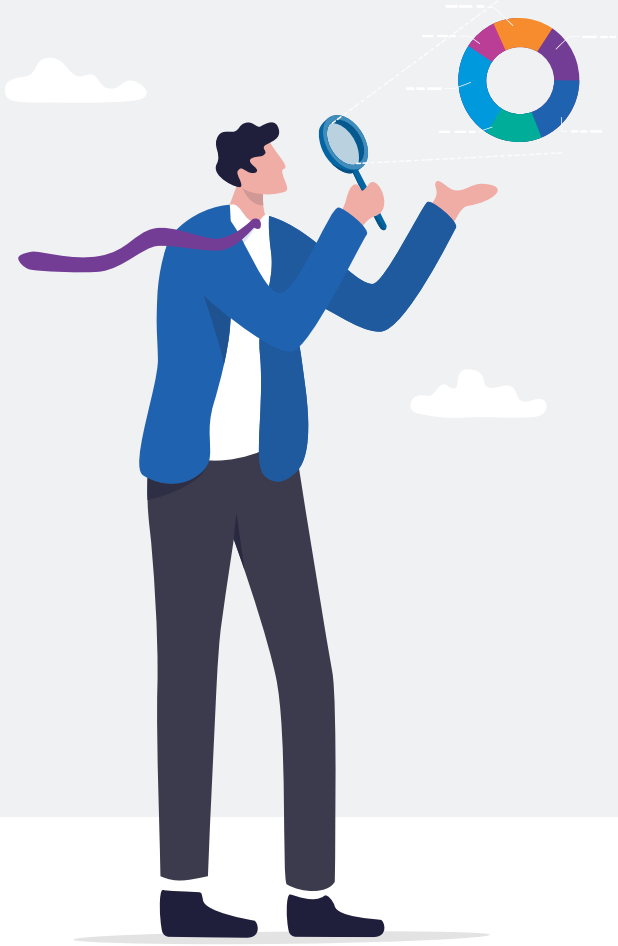
sono state vittime di almeno un tentativo di attacco BEC nel 2022.

I principali vantaggi degli standard SPF, DKIM e DMARC sono i seguenti:

	Descrizione	Vantaggio
SPF	Record DNS che specifica gli indirizzi IP autorizzati a inviare email da un dominio.	Impedisce l'uso non autorizzato di un dominio da parte di spammer o ladri d'identità.
DKIM	Firma digitale integrata nell'intestazione dell'email che dimostra che il messaggio è stato inviato dal proprietario del dominio e che non è stato alterato durante il transito.	Garantisce l'autenticità e l'integrità del messaggio.
DMARC	Record DNS che definisce come interpretare i risultati SPF e DKIM e quali azioni intraprendere se i controlli di autenticazione di un'email falliscono.	Consente ai proprietari di domini di monitorare e controllare come i loro domini vengono utilizzati nelle comunicazioni email.

DMARC è la prima e unica tecnologia ampiamente distribuita in grado di rendere affidabile il dominio di invio delle email (quello che gli utenti vedono nei loro client email). Utilizzando DMARC, i proprietari di domini possono evitare che i loro domini vengano sfruttati in attacchi di phishing o di furto di identità contro i loro clienti, collaboratori e partner.

Purtroppo, l'adozione dell'autenticazione DMARC è lenta e non uniforme. Per accelerare l'adozione e migliorare la protezione dell'email, Google e Yahoo hanno annunciato alla fine del 2023 che le email non conformi agli standard SPF, DKIM e DMARC potrebbero essere bloccate o inviate direttamente alla cartella della posta indesiderata. Gli standard più severi si applicano ai mittenti che inviano più di 5.000 email al giorno a indirizzi Gmail o Yahoo Mail.



In aggiunta a questi incentivi dettati dal mercato, nuove regole stanno aumentando la pressione sulle aziende affinché implementino l'autenticazione DMARC. Dall'inizio del 2025, la versione 4.0 dello standard PCI DSS richiederà l'introduzione di meccanismi contro il phishing, il che significa che i revisori potrebbero penalizzare le aziende che non hanno adottato l'autenticazione DMARC.

Obblighi regionali rafforzeranno ulteriormente il requisito della conformità DMARC. In Giappone, ad esempio, le norme Unified Standards for Cyber Security Measures for Government Agencies richiedono che tutte le organizzazioni pubbliche implementino una regola di rifiuto o messa in quarantena DMARC entro luglio 2024. Le autorità giapponesi stanno inoltre facendo pressione affinché tutte le società emittenti di carte di credito implementino una regola di rifiuto DMARC entro febbraio 2024.

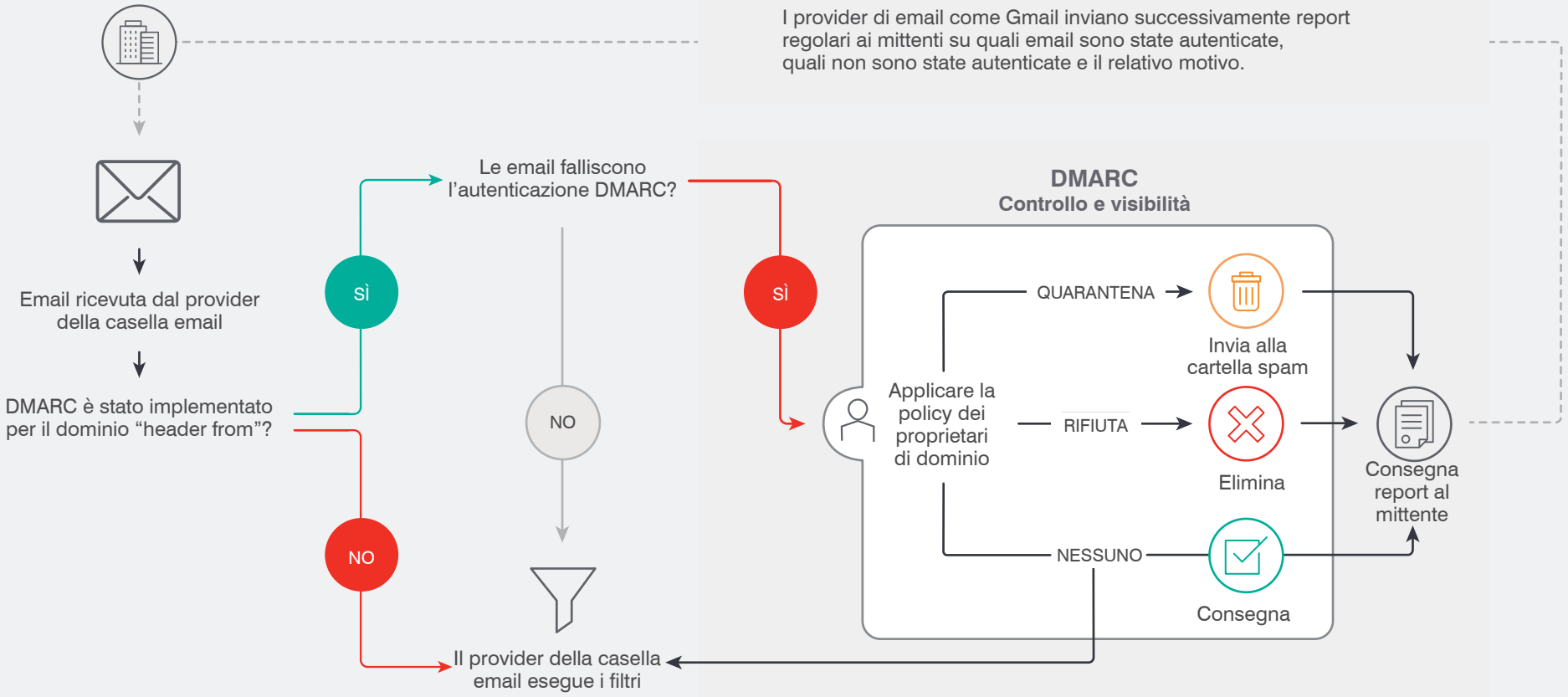
Funzionamento dell'autenticazione DMARC

Tutte le aziende che utilizzano l'email come strumento di comunicazione essenziale devono capire cos'è l'autenticazione DMARC e come implementarla correttamente.

DMARC funziona autenticando i messaggi legittimi per i propri domini di invio delle email. A tal fine, controlla se le email rispettano due standard esistenti: SPF e DKIM.

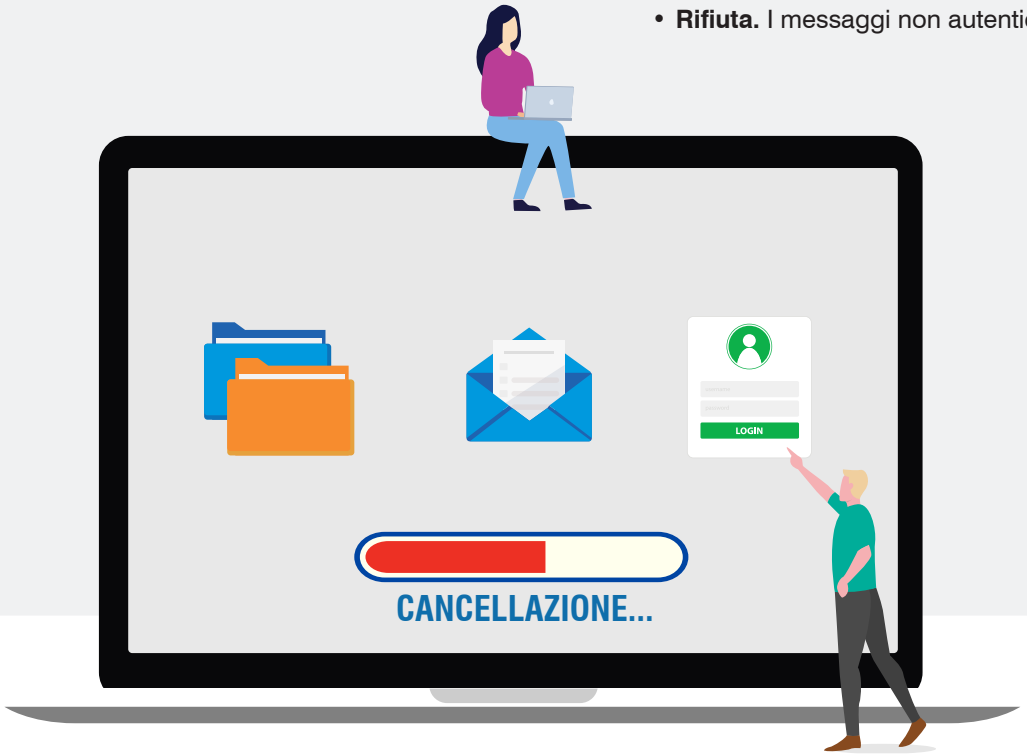
SPF verifica che l'email provenga da un indirizzo IP autorizzato dal proprietario del dominio, mentre DKIM assicura che il messaggio abbia una firma digitale valida corrispondente alla chiave pubblica del proprietario del dominio.

Se uno di questi controlli fallisce, l'email viene considerata non autenticata e potenzialmente fraudolenta.


I provider di email come Gmail inviano successivamente report regolari ai mittenti su quali email sono state autenticate, quali non sono state autenticate e il relativo motivo.
Email ricevuta dal provider della casella email
DMARC è stato implementato per il dominio “header from”?
SÌ
NO
Le email falliscono l’autenticazione DMARC?
NO
SÌ
DMARC
Controllo e visibilità
Applicare la policy dei proprietari di dominio
QUARANTENA
Invia alla cartella spam
RIFIUTA
Elimina
NESSUNO
Consegna
Consegna report al mittente
Il provider della casella email esegue i filtri

Tramite un parametro esplicito, DMARC indica anche ai provider email come gestire i messaggi rifiutati dal processo di autenticazione. Questi messaggi possono essere inviati a una cartella della posta indesiderata o immediatamente rifiutati. Sono disponibili le tre opzioni seguenti:

- **Nessuna azione.** Non viene intrapresa alcuna azione sui messaggi non autenticati. Il proprietario del dominio può comunque ricevere segnalazioni sull'uso del suo dominio nelle email.
- **Quarantena.** I messaggi non autenticati vengono contrassegnati come spam e inviati a una cartella di posta indesiderata. I destinatari possono esaminare i messaggi di spam, ma raramente lo fanno.
- **Rifiuta.** I messaggi non autenticati vengono bloccati e rispediti al mittente. Il destinatario non li vede mai.



SEZIONE 3

Vantaggi dell'autenticazione DMARC

DMARC offre numerosi vantaggi alle aziende che utilizzano l'email come strumento di comunicazione essenziale. Eccone alcuni.

Aumento della percentuale di recapito e dell'engagement delle email

Garantendo che solo le email legittime e autenticate provenienti dal tuo dominio raggiungano la casella email del destinatario, DMARC riduce il rischio che il tuo messaggio venga contrassegnato come spam o filtrato dai provider email. Ciò migliora la reputazione e le prestazioni delle tue email, aumentando la probabilità che i tuoi messaggi vengano aperti, letti e gestiti dal tuo pubblico di riferimento.

Questo vantaggio dell'autenticazione DMARC è particolarmente essenziale per le email transazionali.

Garantisce che le tue attività non vengano interrotte da email non consegnate o non prioritarie.

Maggiore protezione di collaboratori, partner commerciali, privati e brand

DMARC neutralizza un'intera classe di email fraudolente prima che raggiungano i tuoi collaboratori, i tuoi partner e i tuoi clienti. Prevenendo gli attacchi di phishing e spoofing che utilizzano il tuo dominio per ingannare o danneggiare i tuoi interlocutori, DMARC favorisce la fiducia e la fedeltà verso il tuo brand. Inoltre, riduce il rischio di violazione dei dati, perdite finanziarie e altri problemi legali.

Visibilità del panorama delle minacce contro l'email

Non puoi controllare ciò che non riesci a vedere. L'autenticazione DMARC ti dà visibilità immediata sulle minacce che colpiscono la tua azienda. Fondamentalmente, rileva gli attacchi di phishing e spoofing dei domini che mettono a rischio la reputazione dei tuoi clienti e del tuo brand. Grazie a report regolari sulle fonti e sui volumi di email non autenticate che utilizzano il tuo dominio, puoi identificare e neutralizzare potenziali vulnerabilità e criminali informatici.

Riduzione dei costi del servizio clienti

Bloccando le email fraudolente che usurpano il tuo dominio, DMARC riduce il numero di reclami, richieste e controversie dei clienti che devi gestire. In questo modo, risparmi denaro e tempo prezioso per le operazioni di assistenza clienti. Migliorano anche la soddisfazione e la fidelizzazione dei clienti.

Riduzione dei costi di neutralizzazione degli attacchi di phishing

Secondo l'Internet Crime Complaint Center (IC3) dell'FBI, il phishing costerà ai marchi 6,9 miliardi di dollari nel 2021[3]. DMARC riduce i costi associati a frodi, rimborsi e neutralizzazione degli attacchi di phishing. Prevenendo gli attacchi BEC che utilizzano indirizzi email contraffatti per indurre i tuoi collaboratori o partner a trasferire fondi o divulgare informazioni sensibili, DMARC ti protegge da perdite finanziarie e danni alla reputazione causati da queste truffe.

3 FBI, Internet Crime Report (Report sui crimini di Internet) 2021, aprile 2022.

SEZIONE 4

Come garantire che le tue email vengano recapitate nella casella email dei tuoi clienti

Sono molti i fattori che possono determinare se la tua email viene inviata alla casella di posta in arrivo o alla cartella Posta indesiderata. Tuttavia, ecco un elenco di requisiti minimi per garantire che le tue email importanti non finiscano nella cartella Posta indesiderata.

Implementazione delle policy DMARC

Per definizione, questo richiede anche l'implementazione dei metodi di autenticazione SPF e DKIM. Affinché l'email sia convalidata dal processo di autenticazione DMARC, l'intestazione "Da:" deve essere allineata al dominio SPF o DKIM (In altre parole, l'intestazione deve corrispondere al dominio aziendale o condividerlo). Inoltre, non devi impersonare Gmail nelle intestazioni "Da:". Tutte le email che affermano di provenire da Gmail saranno automaticamente contrassegnate come spam o rifiutate.

Record DNS inversi e di inoltro validi

I record DNS sono utilizzati per mappare i nomi di dominio agli indirizzi IP e viceversa. I record DNS di inoltro (come i record A o CNAME) mappano i nomi di dominio agli indirizzi IP. I record DNS inversi (come i record PTR) mappano gli indirizzi IP ai nomi di dominio. Disporre di record DNS di inoltro e inversi validi aiuta i provider email a verificare l'identità e la reputazione del tuo server di posta per evitare attacchi di spoofing e phishing.

Mantenimento dei tassi di spam segnalati al di sotto dello 0,3%

Il servizio Gmail Postmaster Tools ti consente di monitorare e analizzare le prestazioni e il tasso di recapito delle tue email su Gmail. Il tasso di spam è uno degli indicatori misurati dal servizio. Corrisponde alla percentuale delle tue email contrassegnate come spam dagli utenti. Un tasso di spam elevato può compromettere la reputazione delle tue email e far sì che i tuoi messaggi vengano filtrati da Gmail. Un tasso di segnalazione dello 0,3% è la soglia oltre la quale Gmail considera le email come spam.

Formato dei messaggi conforme allo standard RFC 5322

Lo standard RFC 5322 è un documento che definisce il formato e la sintassi standard delle email. Stabilisce le regole e le convenzioni per la struttura e il contenuto delle intestazioni e dei corpi delle email, come data, oggetto, mittente, destinatario e identificatore del messaggio.

Rispettando lo standard RFC 5322, puoi garantire che le tue email siano conformi ai protocolli email e possano essere elaborate e visualizzate correttamente dai provider email e dai clienti.

Opzione di disiscrizione in un clic

Per rispettare le leggi e le normative sull'email marketing, come il CAN-SPAM Act o il GDPR, devi offrire ai tuoi abbonati un modo chiaro e semplice per cancellarsi dalla tua mailing list.

Una buona pratica consiste nell'includere un link o un tasto di cancellazione con un solo clic nel piè di pagina delle tue email, in modo che gli abbonati possano cancellarsi dalla tua mailing list senza dover inserire il loro indirizzo email o accedere al tuo sito web. Questo approccio ti permette di rispettare le preferenze e la riservatezza dei tuoi abbonati, ma riduce anche il rischio che le tue email vengano contrassegnate come spam o segnalate come abusive.

SEZIONE 5

Cosa accade in caso di mancata conformità

L'autenticazione delle email non è solo una questione di sicurezza, ma anche di prestazioni e soddisfazione dei clienti. Se non rispetti i requisiti di autenticazione delle email stabiliti da Google e Yahoo, i tuoi messaggi potrebbero essere bloccati o inviati direttamente alla cartella Posta indesiderata, con gravi conseguenze per la tua attività.

Ecco alcuni esempi delle potenziali ripercussioni.

Riduzione dell'efficacia dei tuoi sforzi di marketing

Se le tue campagne email non sono autenticate, potrebbero essere filtrate da Gmail o Yahoo Mail. Il tuo pubblico di riferimento potrebbe non ricevere mai le tue offerte, notizie o contenuti. Di conseguenza, i tassi di apertura, i tassi di clic, le conversioni e le vendite derivanti dalle tue attività di email marketing si ridurranno.

Interruzione dell'attività e perdite commerciali

Se i tuoi clienti non ricevono le tue comunicazioni strategiche, non possono fare affari con te. Potrebbero non essere in grado di connettersi, reimpostare la password, confermare il loro ordine, ricevere le ricevute o accedere all'assistenza, il che potrebbe confonderli, frustrarli e infastidirli. Molti di loro potrebbero abbandonare i tuoi servizi e rivolgersi alla concorrenza.

Indebolimento della soddisfazione dei clienti e della reputazione del brand

Oggi, i clienti si aspettano di ricevere email di follow-up, conferme d'ordine, notifiche di consegna e altro ancora.

Se le tue email non sono autenticate, potrebbero essere perse o ignorate dai tuoi clienti. Potrebbero percepire il tuo brand come poco professionale, inaffidabile o non degno di fiducia, Questo potrebbe offuscare l'immagine del tuo marchio e aumentare la fuga dei clienti.

Come Proofpoint può aiutarti

Il rispetto dei nuovi requisiti in materia di autenticazione delle email può migliorare le tue attività di marketing digitale, garantire la soddisfazione dei tuoi clienti e proteggere il tuo brand. Ecco solo alcuni dei modi in cui Proofpoint può aiutarti a implementare l'autenticazione DMARC per garantire che le tue email importanti raggiungano i tuoi clienti e i clienti potenziali.

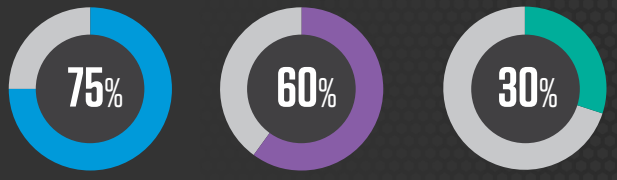
- **Proofpoint Email Fraud Defense (EFD)** ti permette di parlare con consulenti esperti che ti accompagneranno in ogni fase del tuo percorso DMARC, per aiutarti a garantire tassi di consegna delle email e protezione dell'email ottimali.
- **I servizi SPF, DKIM e DMARC in hosting** possono semplificare le attività di configurazione e manutenzione per garantire che i tuoi messaggi siano convalidati attraverso il processo di autenticazione. Questi servizi possono anche aiutarti a aggirare restrizioni come i limiti di ricerca DNS (10) per SPF o i requisiti di rotazione delle chiavi per DKIM.
- **Proofpoint Secure Email Relay** può garantire che le email transazionali (quelle inviate da applicazioni o partner di terze parti per conto dell'azienda) siano state firmate con DKIM per ottenere più rapidamente l'allineamento DMARC. Questo servizio può anche fornire una visibilità e un controllo granulari sul tuo traffico di email transazionali, per aiutarti a identificare e risolvere qualsiasi problema che possa influire sul tasso di consegna o sulle prestazioni delle tue email.

Perché Proofpoint

Ogni giorno, analizziamo oltre:

2,6 MLD DI EMAIL	**49 MLD** DI URL	**1,9 MLD** DI ALLEGATI
1,7 MLD DI MESSAGGI MOBILE	**430 MIO** DI DOMINI WEB	**143.000** ACCOUNT SOCIAL MEDIA

Le nostre soluzioni sono state adottate da oltre:



8.000 GRANDI AZIENDE

200.000 PICCOLE IMPRESE

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui il 75% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.