MailMarketing
SEND UNLIMITED EMAIL AT A FIXED COST

IMPLEMENTARE L'AUTENTICAZIONE SPF E DKIM

Dopo aver verificato il mittente, è possibile procedere ad una serie di attività per migliorare i tassi di consegna delle tue email.

le guide

1. IMPLEMENTARE SPF/DKIM

Dopo aver verificato il mittente, è possibile procedere ad una serie di attività per migliorare i tassi di consegna delle tue email. Una di queste attività è l'implementazione dell'autenticazione SPF e DKIM.

SPF e DKIM sono protocolli di autenticazione, entrambi basati sul DNS del dominio, che consentono al proprietario del sito di specificare quali server di posta elettronica utilizzano quando inviano email da quel dominio e quindi evitare attività fraudolente di terzi.

L'implementazione di SPF e DKIM consente di aumentare l'affidabilità presso gli Email Service Provider (come Gmail, Hotmail, Yahoo!) , migliorare la sicurezza degli invii e garantire la massima deliverability possibile, sia su IP condivisi che dedicati.

Per una corretta implementazione del SPF e DKIM è consigliabile chiedere supporto a chi gestisce il tuo dominio o al fornitore del servizio di hosting.

2. SPF

Un registro SPF (Sender Policy Framework) è uno standard di autenticazione email che confronta l'indirizzo IP effettivo del mittente dell'email con un elenco di indirizzi IP autorizzati a inviare posta da quel dominio.

Un registro SPF (Sender Policy Framework) è uno standard di autenticazione email che confronta l'indirizzo IP effettivo del mittente dell'email con un elenco di indirizzi IP autorizzati a inviare posta da quel dominio.

In pratica un record SPF elenca i server di posta autorizzati ad inviare email per conto del tuo dominio ed è utilizzato per impedire agli spammer di utilizzare il tuo dominio per l'invio di email non autorizzate mediante una tecnica fraudolenta denominata spoofing

Alcuni destinatari di posta richiedono un record SPF. In questi casi, se non ne aggiungi uno al tuo dominio, i tuoi messaggi possono essere contrassegnati come spam o addirittura essere respinti.

COME CONFIGURARE SPF

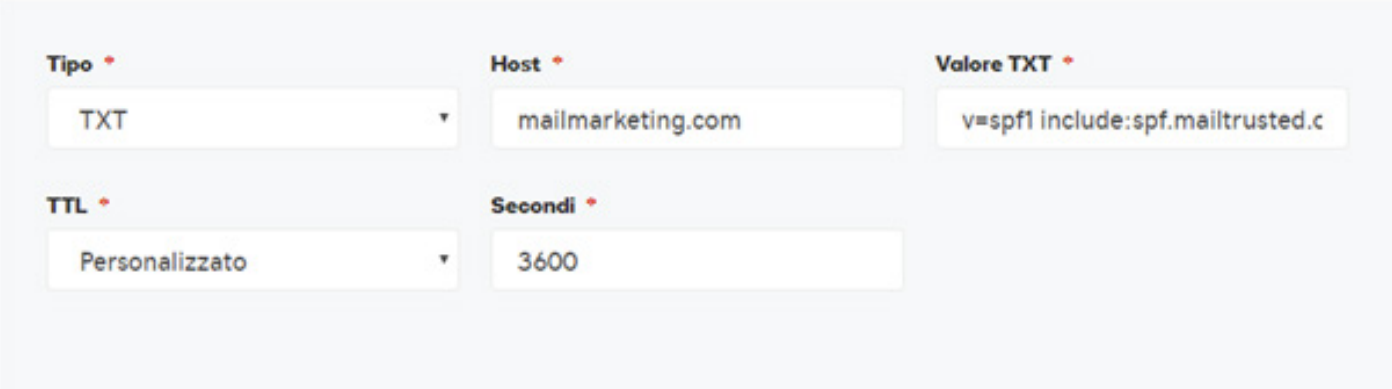
Per configurare SPF deve essere aggiunto/modificato il record dedicato nel DNS del dominio.

1. Accedi al tuo Hosting Web

2. Vai nella sezione dedicata ai DNS

3. Aggiungi un nuovo record SPF con le seguenti informazioni:
   - **TIPO DI RECORD**: *TXT*
   - **HOST**: *nome del vostro dominio (es. mailmarketing.com)*
   - **VALORE**: *v=spf1 include:spf.mailtrusted.org ~all*

Come da esempio



Il codice SPF è disponibile nella sezione Gestione Mittenti in Mittenti Abilitati - Configurazioni cliccando sull'icona rossa presente nella colonna "Record spf".

Per aggiungere un record TXT, devi accedere al tuo host di dominio, che in genere corrisponde al servizio presso cui hai acquistato il nome di dominio. Se non sei sicuro di quale sia il tuo host, puoi identificarlo tramite i dati di fatturazione o tramite i sistemi di whois.

Per ulteriori informazioni sulla creazione di record TXT, contatta il team di assistenza dell'host.

Una volta che avrai inserito il nuovo record SPF nel DNS del tuo dominio, torna sulla pagina Gestione Mittenti, aggiorna e il colore dell'icona del record SPF passerà da rosso a verde.

3. DKIM

DKIM (Domain Keys Identified Mail) è un altro metodo di autenticazione ed è utilizzato dai provider di servizi email per determinare l'identità e per stabilire la reputazione e l'affidabilità di un mittente.

Un registro SPF (Sender Policy Framework) è uno standard di autenticazione email che confronta l'indirizzo IP effettivo del mittente dell'email con un elenco di indirizzi IP autorizzati a inviare posta da quel dominio.

In pratica un record SPF elenca i server di posta autorizzati ad inviare email per conto del tuo dominio ed è utilizzato per impedire agli spammer di utilizzare il tuo dominio per l'invio di email non autorizzate mediante una tecnica fraudolenta denominata spoofing

Alcuni destinatari di posta richiedono un record SPF.

In questi casi, se non ne aggiungi uno al tuo dominio, i tuoi messaggi possono essere contrassegnati come spam o addirittura essere respinti.

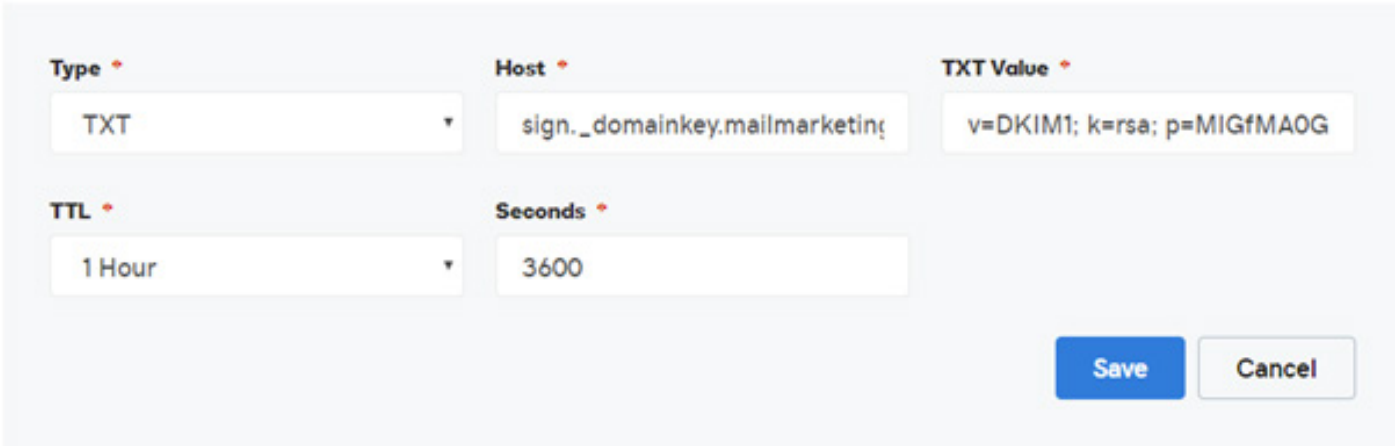
COME CONFIGURARE DKIM

Aggiungi un record nella configurazione del tuo DNS con i seguenti valori

- **TYPE**: TXT
- **HOST**: sign._domainkey. nome_del_tuo_dominio (ad esempio sign._domainkey. mailmarketing.com)
- **DATA**: v=DKIM1; k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNA-DCBiQKBgQDXEbvzRtmqiOfbmkxvjxt2YTVMgC1Q5qtiNbdCOnkPQF-DEYh5noE/mEhRVpfpdKRJshEHXZ9U3vms3YwBg1hhMtoLsucILzyzTV-6gj7IaY9UlYHsHlXVmTtiNmiTYs99JZCXiWQGcKz0BwhHx0Ifwam+U-7SNIW+2o+bJnd2Y+ZYwIDAQAB

Per il sottodominio 'sign._domainkey.'

Come da esempio

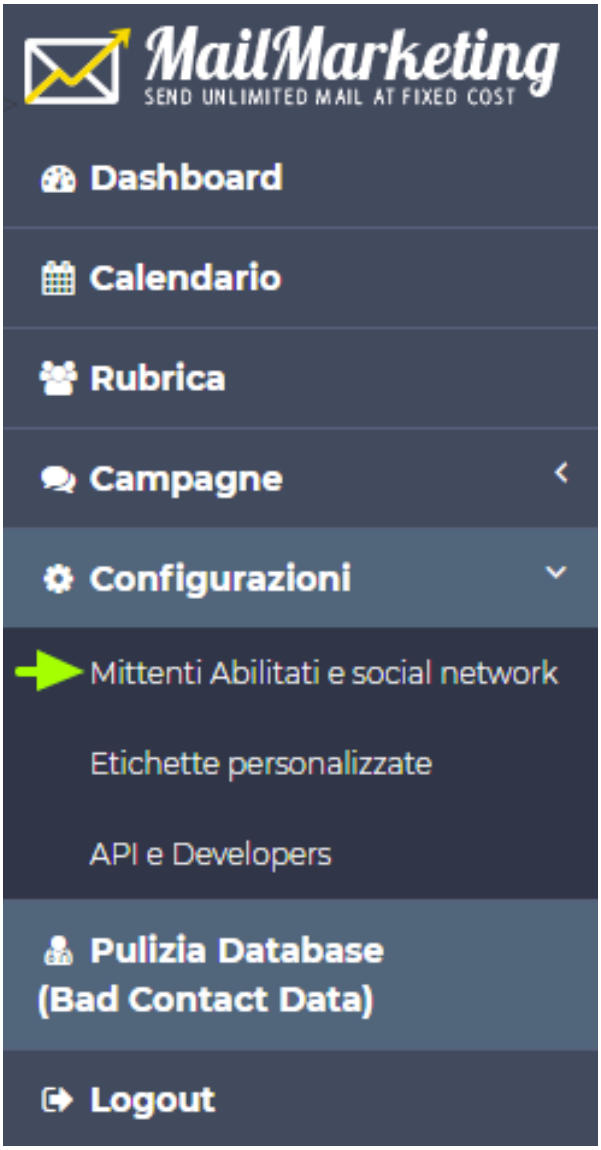


4. VERIFICA

Dopo 24 ore potrai verificare la corretta impostazione del Record SPD e DKIM nen DNS

Dopo 24 ore dall'aggiunta del record SPF e DKIM nei DNS del tuo dominio potrai verificare se la configurazione è avvenuta con successo direttamente nella sezione di Mittenti Abilitati e Social Network

Nel caso SPF e DKIM siano stati configurati con successo, le icone presenti nel record SPF e DKIM cambieranno lo stato da rosso a verde.



Prima dell'implementazione

Email registrata	Descrizione	Verifica mittente	Record spf	Record dkim	Azioni
info@mailmarketing.com	Mail Marketing	✔ VERIFICATO	!	!	AZIONI

Implementazione effettuata con successo

Email registrata	Descrizione	Verifica mittente	Record spf	Record dkim	Azioni
info@mailmarketing.com	Mail Marketing	✔ VERIFICATO	✔	✔	AZIONI

TI È STATA UTILE QUESTA GUIDA?

Scopri di persona come sfruttare il potenziale delle email
grazie a una **soluzione su misura per te**.

www.mailmarketing.com

MailMarketing
SEND UNLIMITED EMAIL AT A FIXED COST