

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

CAPITOLO 1. IMPLEMENTARE L'AUTENTICAZIONE SPF E DKIM	3
CAPITOLO 2. SPF	5
- COME CONFIGURARE SPF	6
CAPITOLO 3. DKIM	8
- COME CONFIGURARE DKIM	9
CAPITOLO 4. DKIM	11
- COME CONFIGURARE DMARC	12
CAPITOLO 5. VERIFICA DELLA CORRETTA IMPOSTAZIONE SPF/DKIM	13

1. IMPLEMENTARE SPF, DKIM E DMARC

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, DKIM e DMARC

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



The image shows a form for configuring a DNS record. It has five fields arranged in two rows. The first row contains 'Tipo' (TXT), 'Host' (mailmarketing.com), and 'Valore TXT' (v=spf1 include:spf.mailtrusted.c). The second row contains 'TTL' (Personalizzato) and 'Secondi' (3600). Each field has a small red asterisk next to its label.

Tipo *	Host *	Valore TXT *
TXT	mailmarketing.com	v=spf1 include:spf.mailtrusted.c
TTL *	Secondi *	
Personalizzato	3600	

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.

DKIM (DomainKeys Identified Mail) utilizza la crittografia a chiave pubblica per controllare la posta elettronica e per consentire al destinatario di verificare che le intestazioni e il contenuto delle email non siano stati modificati durante il transito.

L'autenticazione DKIM si divide in due fasi: quella della firma e della verifica.

Nel caso in cui l'hash generato corrisponda alla firma DKIM decrittografata, l'e-mail passa il controllo DKIM: questo vuol dire che l'email proviene dal mittente dichiarato nell'header e che non è stata modificata durante il trasporto.

Come per SPF, anche DKIM costituisce parte integrante nell'implementazione di DMARC

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-DCBiQKBgQDXEbvzRtmqiOfbmkxvjt2YTVMgC1Q5qtiNbdCOnkPQF-DEYh5noE/mEhRVpfpdKRJshEHXZ9U3vms3YwBg1hhMtoLsucLzYzTV-6gj7laY9UIYHsHIXVmTtiNmiTYs99JZCXiWQGcKz0BwhHx0Ifwam+U-7SNIW+2o+bJnd2Y+ZYwIDAQAB

Per il sottodominio 'sign._domainkey.'

Come da esempio:

Type ▾	Host ▾	TXT Value ▾
TXT ▾	sign._domainkey.mailmarketing	v=DKIM1; k=rsa; p=MIGfMAOG
TTL ▾	Seconds ▾	
1 Hour ▾	3600	

4. DMARC

DMARC (Domain -based Message Authentication, Reporting, and Conformance) è un metodo standard per l'autenticazione delle email, che serve ad impedire che gli hacker falsifichino l'indirizzo nell'intestazione dell'organizzazione e del dominio.

DMARC (Domain-based Message Authentication, Reporting and Conformance) è uno standard di posta elettronica che ha la finalità innanzitutto di confermare l'identità del mittente, utilizzando SPF e DKIM, di cui abbiamo parlato sopra; in secondo luogo di indicare al servizio di posta elettronica del destinatario che cosa fare con le e-mail che non hanno superato il controllo. Infine, ha lo scopo di chiedere ai servizi di posta elettronica dei destinatari di fornire report sulla provenienza dell'email.

Il principale vantaggio del DMARC è quello di offrire protezione da attacchi fraudolenti, migliorando di conseguenza fiducia nelle e-mail inviate dal proprio indirizzo di posta elettronica.

COME CONFIGURARE DMARC

Aggiungi un record nella configurazione del tuo DNS, in modo simile al DKIM.

Nello specifico andrà aggiunto un record con:

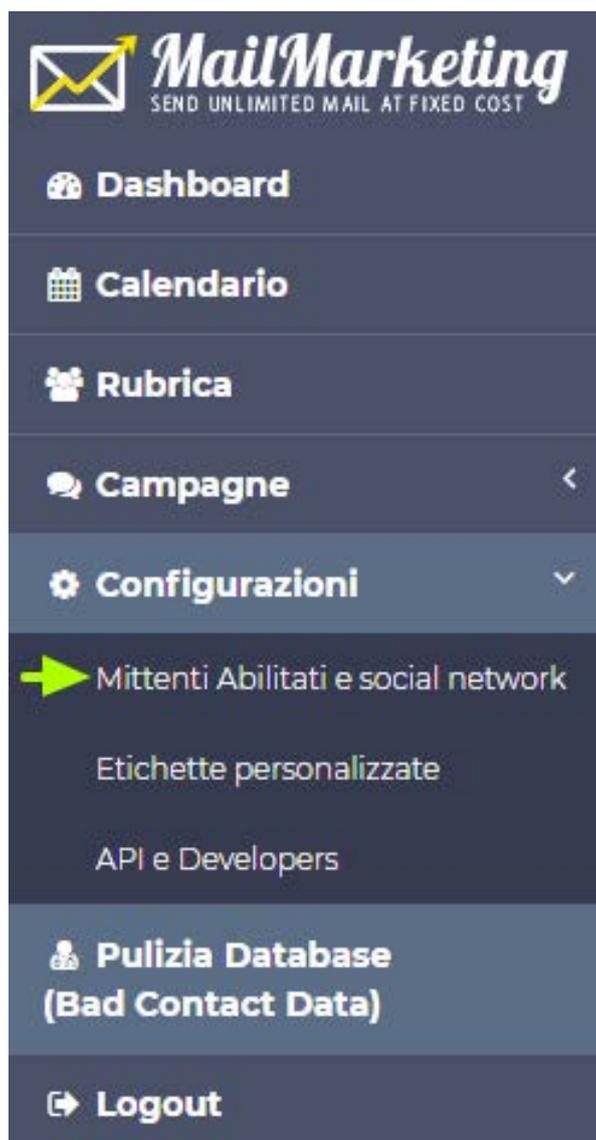
- TIPO: TXT
- HOST: `_dmarc.nomedominio.com` (ad esempio `_dmarc.mailmarketing.com`)
- DATA: `v=DMARC1; p=none`

5. VERIFICA

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

Dopo 24 ore dall'aggiunta del record SPF, DKIM e DMARC 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, DKIM, DMARC cambieranno lo stato da rosso a verde.



Prima dell'implementazione

Email registrata	Descrizione	Verifica mittente	Record SPF <small>INFO</small>	Record DKIM <small>INFO</small>	Record DMARC <small>INFO</small>	Azioni
a.rossi@email.com	Antonio Rossi	✓ VERIFICATO	✓	✓	✓	AZIONI ▾

Implementazione effettuata con successo

Email registrata	Descrizione	Verifica mittente	Record SPF <small>INFO</small>	Record DKIM <small>INFO</small>	Record DMARC <small>INFO</small>	Azioni
a.rossi@email.com	Antonio Rossi	✓ 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

