DMARC Checker

A cosa serve il DMARC Checker

Il DMARC Checker legge il record DMARC di un dominio e mostra se è stato pubblicato correttamente. Vedi se il dominio è protetto, se la sintassi è valida e che cosa significa ogni tag del record. Il Checker propone anche suggerimenti per migliorare il record.

Controllare un dominio

1. Apri **Controlli** nel menu e scegli **DMARC Checker**.
2. Inserisci il nome del dominio nel campo **Dominio**, per esempio `example.org`.
3. Fai clic su **Controllare**.

Basta il nome del dominio: il record lo cerca il Checker stesso, sotto `_dmarc` seguito dal dominio, per esempio `_dmarc.example.org`.

Leggere il risultato

- **Stato DMARC.** Prima di tutto trovi la conclusione. Se la policy è quarantine o reject, vedi che il dominio è protetto. Se la policy è `none`, il Checker ti dice che il dominio non è protetto e suggerisce di passare a quarantine o reject. Se non esiste alcun record, il Checker segnala che non è stato trovato nessun record DMARC.
- **DNS TXT.** Il nome con cui è stato trovato il record, di solito `_dmarc` seguito dal tuo dominio. Se vedi **DNS TXT via CNAME**, quel nome rimanda tramite un CNAME a un'altra posizione in cui è ospitato il record, e il Checker mostra anche quella posizione.
- **Il tuo record DMARC.** Il record così com'è ora nel DNS, con un messaggio che indica se la sintassi è valida. Il pulsante **DIG** mostra la risposta DNS grezza.
- **Suggerimenti per il record.** Sotto il record il Checker elenca ciò che si può migliorare. Un suggerimento non rende il record non valido: un dominio può quindi essere protetto e avere comunque dei suggerimenti.
- **Tag DMARC rilevati.** Una tabella con ogni tag del tuo record, il suo valore e una spiegazione. È un modo rapido per verificare che il record faccia ciò che intendi.
- **Tag DMARC predefiniti.** I tag che non compaiono nel tuo record, con il valore che i riceventi assumono al loro posto: `fo` (0), `rf` (afrf) e `ri` (86400).

Suggerimenti frequenti

- **Il record non ha il tag `rua`.** Senza `rua` non ricevi report DMARC, quindi non puoi vedere chi invia posta a nome del tuo dominio. Aggiungi un indirizzo `rua`. Se gestisci il record dalla piattaforma, lo fai in Gestore DMARC.
- **La policy è impostata su none.** I messaggi che non superano il controllo DMARC vengono comunque consegnati. Va bene finché stai ancora raccogliendo informazioni, ma non offre alcuna protezione. Quando tutti i tuoi mittenti legittimi sono configurati correttamente puoi passare a

quarantine e poi a reject. Come fare lo spiegano le linee guida DMARC.

- **Un indirizzo di report non verificato nel tag `ruf`.** Hai chiesto di inviare i report a un indirizzo di un altro dominio. Quest'altro dominio deve autorizzarlo con un record DNS. Senza, molti riceventi non inviano i report.
- **Un tag non viene riconosciuto.** Il Checker segnala un tag che non riconosce. Non significa sempre che qualcosa non vada: `np`, `t` e `psd` fanno parte dello standard DMARC attuale (RFC 9989), quindi un record che li usa è valido, anche se il Checker non li conosce ancora. I riceventi che implementano lo standard attuale tengono conto di questi tag. Quelli che non conoscono un tag lo ignorano, e il record continua a funzionare.

> **Protetto non significa configurato correttamente**
>
> Il Checker mostra ciò che è pubblicato nel DNS. I tuoi report mostrano se la tua posta legittima supera davvero il controllo DMARC. Parti dai report aggregati.

Come proseguire

- SPF Checker
- DKIM Checker
- Gestore DMARC
- Linee guida DMARC