Secuenza

Guida al recapito: SPF, DKIM e DMARC

Che le tue email arrivino nella posta in arrivo dipende da due cose: che i provider possano verificare che sei davvero tu e che la tua casella abbia una buona reputazione. Questa guida spiega i tre record che lo dimostrano, come si impostano presso i provider più comuni e quali abitudini proteggono la reputazione.

Perché è importante

Gmail, Yahoo e Outlook.com chiedono a chi invia spesso di avere **SPF, DKIM e DMARC** sul proprio dominio, di permettere di disiscriversi da ogni email con un clic e che quasi nessuno la segnali come spam. Senza questi record, di solito le tue email finiscono nello spam o non arrivano proprio.

Secuenza invia dalla tua casella, quindi è il tuo provider di posta a firmare (o no) ogni email. Quello che devi fare è pubblicare nel DNS del tuo dominio i dati che lo confermano.

Prima di cominciare: dov'è il tuo DNS

Il DNS del tuo dominio si gestisce dove l'hai comprato o dove l'hai puntato (il registrar, il tuo hosting, Cloudflare…), che non sempre è dove hai la posta. Entra in quel pannello e cerca la zona DNS: lì si aggiungono i record di questa guida.

Una modifica del DNS impiega da pochi minuti a qualche ora per vedersi. Poi torna su **Verifiche** in Secuenza.

SPF: chi può inviare per il tuo dominio

L'SPF è un record **TXT** nella radice del dominio che comincia con `v=spf1`, dice quali server possono inviare a suo nome e finisce con `~all` (gli altri sono sospetti) o `-all` (gli altri sono rifiutati).

Provider	Cosa deve includere il tuo SPF
Microsoft 365	`include:spf.protection.outlook.com`
Google Workspace	`include:_spf.google.com`
IONOS	`include:_spf-eu.ionos.com`
OVHcloud	`include:mx.ovh.com`
Hostinger	`include:_spf.mail.hostinger.com`
Aruba	`include:_spf.aruba.it`
Zoho Mail (UE)	`include:zoho.eu`

Per esempio, con Microsoft 365: `v=spf1 include:spf.protection.outlook.com ~all`.

Tre regole da conoscere:

- **Può esserci un solo SPF.** Se ne hai già uno (per il sito, per il programma di fatturazione), non aggiungerne un altro: riunisci gli `include` nello stesso record. Con due, nessuno dei due vale.
- **Al massimo 10 consultazioni.** Ogni `include` conta, e anche quelli che contiene. Se le superi, i server lo considerano rotto.
- **Mai** `+all`: permetterebbe a chiunque di inviare a tuo nome.

Se la tua casella è un indirizzo Gmail o Outlook.com (non del tuo dominio), non devi impostare nulla: SPF e firma sono quelli del provider. Queste caselle però hanno limiti bassi, che Secuenza rispetta.

DKIM: la firma delle tue email

Con DKIM, il tuo provider firma ogni email con una chiave privata e tu pubblichi la chiave pubblica nel DNS, con un nome come `selettore._domainkey.tuodominio.it`. Così chi riceve sa che l'email non è stata modificata per strada e che viene davvero dal tuo dominio.

- **Microsoft 365:** nel portale Microsoft Defender, nelle impostazioni di autenticazione della posta (DKIM), scegli il tuo dominio. Ti dà due record **CNAME** (`selector1` e `selector2`): aggiungili al DNS e torna nel portale per attivare la firma.
- **Google Workspace:** nella console di amministrazione, in Gmail → Autentica email, genera un record da **2048 bit**, aggiungilo come **TXT** su `google._domainkey` e premi «Avvia

autenticazione».

- **IONOS, OVHcloud, Hostinger, Aruba, Zoho e la maggior parte degli hosting:** cerca «DKIM» nel pannello della posta. Molti la attivano da soli se anche il DNS è da loro; altrimenti ti danno il record da copiare.

Secuenza cerca la firma con i nomi abituali di ogni provider. Se la tua ha un altro nome, il **test di invio reale** (Pro) la trova. Usa chiavi da **2048 bit**: quelle da 1024 sono ormai considerate deboli.

DMARC: cosa fare con ciò che non passa

DMARC è un record **TXT** su `_dmarc.tuodominio.it` che dice ai provider cosa fare con un'email che dice di venire dal tuo dominio ma non supera né SPF né DKIM, e dove mandarti i rapporti. Perché conti, il dominio del mittente deve coincidere con quello dell'SPF o della firma DKIM (l'«allineamento»).

Comincia osservando:

```
v=DMARC1; p=none; rua=mailto:dmarc@tuodominio.it
```

1. **Da due a quattro settimane su `p=none`**: non cambia nulla, ma ricevi rapporti su chi invia per il tuo dominio. Controlla che tutto ciò che è legittimo parta firmato (la tua casella, il tuo sito, le tue fatture).
2. **Passa a `p=quarantine`**: ciò che non passa finirà nello spam.
3. **E poi a `p=reject`**: ciò che non passa viene rifiutato. È ciò che protegge meglio il tuo dominio da chi vuole spacciarsi per te.

I rapporti arrivano in XML. Ci sono servizi gratuiti che li riassumono; basta guardarli ogni tanto.

Verificarlo con Secuenza

Nella scheda di ogni casella, **Verifiche** controlla SPF, DKIM e DMARC, e anche la ricezione della posta (MX), il nome inverso del server, MTA-STS, BIMI e la cifratura. Ogni verifica risulta verde, gialla o rossa, con cosa impostare e dove. Se hai già un SPF, ti propone il record completo con ciò che manca.

Con **Pro**, inoltre:

- **Test di invio reale:** Secuenza invia un'email vera dalla tua casella e ti dice cosa vede il server che la riceve: firma, SPF, allineamento DMARC, cifratura e controllo antispam.
- **Liste nere:** controlla se il tuo server o il tuo dominio compaiono nelle liste usate dai filtri.

E la sezione **Sicurezza** riunisce ciò che il freno ha fermato, i tuoi numeri di 30 giorni rispetto ai loro limiti e lo stato di ogni casella: lo spiega Sicurezza dell'invio.

La reputazione: cosa guardano i filtri

Con i record a posto, conta come ti comporti:

- **Comincia piano.** Una casella o un dominio nuovi che all'improvviso inviano centinaia di email sembrano spam. Il riscaldamento di Secuenza aumenta il limite giorno dopo giorno.
- **Rispetta i limiti.** Per ogni provider, Secuenza usa un limite giornaliero e orario prudente, sotto il suo massimo, e distribuisce gli invii nei tuoi orari.
- **Disiscriversi deve essere facile.** Ogni email ha il link di disiscrizione e l'intestazione che permette a Gmail e Outlook di mostrare il loro pulsante «Annulla iscrizione». Le disiscrizioni si applicano subito.
- **Liste pulite.** Non comprare mai liste. Le email non recapitate e i contatti inattivi vengono messi da parte, e il freno di sicurezza mette in pausa una campagna se ci sono troppe email non recapitate o disiscrizioni, e ferma gli invii verso un provider dove nessuno apre le tue email.
- **Pochi reclami.** Se più di 2 o 3 persone su mille segnalano le tue email come spam, i filtri ti penalizzano. Scrivi solo a chi si aspetta le tue email.
- **Email da persona.** Testo chiaro, pochi link, niente abbreviatori di URL, immagini con testo intorno. Carica le immagini dall'editor: quelle di Drive o Dropbox, o incollate dentro l'email, spesso finiscono nello spam. Il controllo antispam ti avvisa di ciò che di solito pesa.
- **Fatti rispondere.** Una risposta è il segnale migliore che la tua email è gradita. Scrivi perché la gente risponda.

Se le tue email finiscono nello spam

1. Apri **Verifiche**: i tre record sono verdi?
2. Con Pro, fai il **test di invio reale** e guarda cosa non va sul server che riceve.
3. Rivedi il **controllo antispam** delle email della campagna.
4. Guarda in **Sicurezza** se il freno ha fermato qualche provider, e in **Risultati** le disiscrizioni e le email non recapitate: se aumentano, fermati e pulisci la lista.
5. Abbassa il limite per qualche giorno e poi rialzalo piano.