Massimizzare la deliverability delle tue email

Panoramica

La configurazione corretta del tuo account MailUp è fondamentale per massimizzare la **deliverability**, cioè la capacità di recapitare le email nella casella di posta in arrivo dei tuoi destinatari. Prova a immaginare la deliverability come un'equazione: il risultato è dato dal recapito in inbox (avvenuto o mancato) delle tue email, con diverse variabili a influenzarne la consegna. Tra queste: la tua reputazione di mittente, il contenuto del messaggio inviato, il livello di coinvolgimento dei destinatari, la reputazione dell'infrastruttura di invio che stai utilizzando e altre ancora.

- Nel **glossario** ti guideremo tra le parole chiave
- Esamineremo i **metodi di autenticazione dell'email**, una parte importante dell'equazione deliverability
- Ti indicheremo alcuni **passi per configurare** al meglio il tuo account MailUp.

Glossario

- **Autenticazione**
  L'autenticazione è un insieme di tecniche volte a dotare i messaggi del sistema di trasferimento email con informazioni verificabili. Il suo scopo è quello di convalidare le identità delle parti che partecipano all'invio di un messaggio - in quanto possono modificarlo. I risultati di questa convalida possono quindi influenzare le decisioni di consegna, che non implicano alcun meccanismo di "filtraggio dei contenuti". Ci sono diversi metodi di autenticazione (FCrDNS, ADSP, SPF, DKIM, DMARC) e ciascuno di questi favorisce la reputazione e la valutazione della convalida del mittente.

- **Email commerciale**
  Si tratta di una comunicazione di natura commerciale; il suo obiettivo è la promozione di un prodotto o un servizio.

- **Email transazionali**
  Un'email transazionale viene solitamente inviata in seguito a una specifica azione dell'utente (per esempio un ordine online). Le email transazionali sono ricevute, conferme, promemoria o qualsiasi altra email di natura non commerciale i cui contenuti sono modellati su un preciso destinatario. Dal punto di vista normativo (CASL http://blog.mailup.it/2014/04/casl-canada-spam/), un'email che include contenuti commerciali è considerata un'email commerciale (vedi sopra).

- **Engagement (Coinvolgimento)**
  Misura come gli iscritti interagiscono con i tuoi messaggi. Il livello di coinvolgimento – determinato dai tassi di apertura del messaggio, il tempo speso nella visualizzazione, i clic e le risposte – migliora la reputazione del mittente e la deliverability. Un coinvolgimento molto basso – assenza di azioni da parte del destinatario o, peggio ancora, eliminazione del messaggio o sua segnalazione come spam – causa problemi di deliverability nel breve periodo.

- **Envelope Sender / Return Path**
  Un indirizzo email a cui sono recapitati i messaggi errati (bounce) asincroni. Dal momento che questo indirizzo email è incluso nell' header dell'email, il suo dominio prende parte al processo di valutazione della reputazione.

- **Filtraggio dei contenuti / Fingerprinting**
  Sono tecniche volte a valutare il contenuto di un'email (parole specifiche, URL o "chunk") per individuare i messaggi spam e i suoi modelli. Il filtraggio dei contenuti è più utilizzato nel mondo aziendale, dove gli amministratori di sistema possono impostare restrizioni sui contenuti che ricevono i dipendenti. A livello dei consumatori i principali ISP (ad esempio Google, Yahoo!), per bloccare lo spam, considerano i parametri di autenticazione, reputazione e coinvolgimento dell'utente (vedi "Engagement") più affidabili del filtraggio dei contenuti – anche se possono adottare entrambi gli strumenti.

- **IP condiviso**
  È un gruppo di indirizzi IP usati per più clienti, i quali condividono metriche di reputazione comuni e permettono –nel loro insieme– di mantenere una consistente frequenza di invio.

- **IP dedicato**
  È un indirizzo IP utilizzato esclusivamente per un mittente o per una parte del suo traffico email (per esempio le email transazionali). Quando si usa un IP dedicato, il traffico di email che parte da quell'indirizzo IP è isolato rispetto agli altri. Una consistente frequenza di invio – così come l'alta qualità dei messaggi inviati – sono fattori cruciali per costruire e mantenere una buona reputazione. La mancanza di volumi di invio e/o o di frequenza può causare una mancanza di reputazione per l'IP dedicato, che di conseguenza può portare a problemi di deliverability. Per questo motivo l'adozione di un indirizzo IP non è raccomandabile in assoluto, ma da valutare caso per caso.

- **Rate limiting / Throttling**
  Rate limiting è il processo con cui gli ISP ritardano la consegna delle email indesiderate (o sconosciute), filtrano lo spam e garantiscono che la posta desiderata (per esempio le email transazionali) raggiungano tempestivamente la casella di posta in arrivo. Ogni ISP ha i propri limiti di invio basati su condizioni temporali (ora e giorno), così da regolare e ridurre il volume di invio quando è troppo alto o troppo basso.

- **Dominio / Dominio Apex**
  La parte del dominio utilizzato da un mittente per inviare le email (per esempio mycompany.com). Si tratta della radice di tutti i meccanismi di reputazione e di autenticazione, e dovrebbe essere direttamente collegata al sito dell'azienda o alla sua brand identity.

- **Sotto-dominio**
  È un dominio di livello inferiore. Se mycompany.com (http://mycompany.com/) è il dominio di primo livello (apex), news.mycompany.com (http://news.mycompany.com/) è un suo sotto-dominio. Dal momento che solitamente il dominio apex è già configurato per servire adeguatamente il sito aziendale del mittente - ed eventuali modifiche potrebbero avere effetti collaterali indesiderati - è consigliabile che un mittente crei dei sottodomini per inviare email (domini di terzo livello come news.mycompanyname.com e di quarto livello come bounce.news.mycompanyname.com). La scelta del dominio, del sotto-dominio e delle denominazioni è fondamentale, perché può avere un effetto determinante su come gli ISP e le autorità anti-spam considerano il tuo flusso di email. Per maggiori informazioni consulta la sezione *Guida alla configurazione* che trovi più avanti.

- **Web interface domain**:
  Un sotto-dominio che sarà usato:
  - In tutti i link tracciati nelle tue email
  - Nell'URL della versione web del messaggio
  - Nell'URL di tutte le pagine web usate dal sistema (per esempio la landing page di conferma iscrizione)
  - Nell'URL della tua piattaforma MailUp

Metodi di autenticazione dell'email

1. **Sender Policy Framework (SPF):**
   L'SPF è uno dei metodi per autenticare le comunicazioni via email. Vengono aggiunte alcune informazioni alle impostazioni del tuo dominio web, indicando che certi sistemi sono autorizzati a inviare email per tuo conto. L'aggiunta dell'autenticazione con SPF può incrementare la tua deliverability, ossia la percentuale di messaggi recapitata nella posta in arrivo, anzichè nello spam. Nel dettaglio, l'SPF fornisce un meccanismo che consenta la ricezione di exchangers di posta elettronica per verificare che la posta in arrivo da un dominio sia stata inviata da un host autorizzato dagli amministratori di quel dominio. L'elenco degli indirizzi IP autorizzati per un dominio è pubblicato nei record del Domain Name System (DNS) per quel dominio nella forma di un record TXT appositamente formattato (vedi la nostra pagina *Implementare l'autenticazione Sender ID e Record SPF*).

2. **DomainKeys Identified Mail (DKIM)**
   Il DKIM è uno dei metodi per autenticare le comunicazioni via email. Funziona aggiungendo una firma criptata alle tue email. Nello specifico, la nostra chiave pubblica DKIM va aggiunta alle impostazioni del tuo dominio web e una specifica firma viene aggiunta a tutte le email che inviamo per te. Questa firma viene criptata sulla base di alcuni elementi di ogni email inviata e perciò è unica per ogni email. Quando il server di posta ricevente analizza la tua email, decritterà la firma usando la chiave pubblica menzionata in precedenza e genererà una nuova stringa di hash basata sugli stessi elementi. Se la firma decrittata combacia con la nuova stringa di hash, la mail verrà considerata autenticata con DKIM. Un esempio di firma DKIM è il seguente:

   ```
   DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=transactional; d=mailup.com;
   h=From:To:Date:Subject:MIME-Version:Content-Type:List-Id:List-Unsubscribe:Message-ID; i=news-it@mailup.com;
   bh=eFMbGLxi/7mcdDRUg+V0yHUTmA1F4EXExVBQxIxBr2I=;
   b=ra3pGFHHvCr9OZsm9vnOid........Yj00/+nTKs=
   ```

   Se il messaggio ha una firma valida (non manipolato) il dominio firmatario, identificato dal d=tag, comunicherà chi sei ai ricevitori, i quali gestiranno la posta di conseguenza. I sistemi di valutazione della reputazione esamineranno la reputazione del dominio firmatario per decidere se recapitare l'email nella casella di posta in arrivo o nella cartella spam.

3. **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
   Il DMARC consente al proprietario di un dominio, che è anche il mittente di messaggi email, di chiedere ai provider di posta elettronica di non consegnare messaggi non autorizzati che sembrano provenire dal proprio dominio. Questo meccanismo è utile per prevenire attacchi di phishing e spoofing.

   Da un punto di vista tecnico, il DMARC (Domain-based Message Authentication, Reporting & Conformance) è un sistema basato sulle autenticaticazioni DKIM e SPF che aiuta i server di ricezione (ad es. Gmail, Yahoo, Libero) a sapere cosa fare quando un messaggio non può essere autenticato. Per farlo, consente al mittente di un'email di pubblicare una "policy" su quale meccanismo (SPF, DKIM o entrambi) viene utilizzato per inviare email e di dare istruzioni ai server di ricezione su come gestire eventuali problemi di autenticazione (monitora, metti in spam o rifiuta i messaggi). Inoltre, il DMARC fornisce un meccanismo di reporting per le azioni fatte, basate sulla policy. In questo modo coordina i risultati del DKIM e dell'SPF e specifica in quali circostanze l'indirizzo email mittente, che spesso è visibile al destinatario finale, può essere considerato legittimo.

4. **Forward-confirmed reverse DNS (FCrDNS)**:
   Conosciuto anche come full-circle reverse DNS, double-reverse DNS, o iprev, FCrDNS è un parametro di configurazione del network in cui un determinato indirizzo IP ha sia le voci Domain Name System (DNS) forward (name-to-address) sia quelle reverse (address-to-name), che si corrispondono a vicenda. Questa è la configurazione standard prevista dalle norme di Internet che supportano molti protocolli DNS-reliant e che è raccomandata come best practice. La verifica FCrDNS può creare un modulo di verifica autenticazione debole in quanto esiste una relazione valida tra il proprietario di un nome di dominio e il proprietario della rete a cui è stato dato un indirizzo IP.

5. **Author Domain Signing Practices (ADSP)**:
   ADSP è un'estensione facoltativa per lo schema di autenticazione email DKIM, per cui un dominio può pubblicare le pratiche di firma che adotta al momento dell'inoltro per conto degli autori associati. È un modo per legare il dominio firma DKIM con il dominio di posta elettronica nel campo From: l'header di un messaggio (noto anche come "dominio dell'autore"). Per creare quella connessione un proprietario di dominio pubblica un record ADSP nel DNS, che contiene un'informativa sulla posta inviata da quel dominio. Un'

informativa di "tutti" ha l'obiettivo di trasmettere ai sistemi di ricezione che tutta la loro posta è stata firmata con DKIM, senza fare alcuna richiesta su cosa fare con i messaggi non firmati. Una norma stabilisce che i messaggi non firmati siano scartati. ADSP non è mai riuscito a diffondersi e nel 2013 è stato retrocesso a "storico". È stato sostituito da DMARC.

Autenticazione su domini personalizzati

Ogni account MailUp è autenticato di default (FCrDNS, SPF, DKIM) sui domini di nostra proprietà, direttamente connessi con la nostra infrastruttura di invio. Questi domini - per definizione - non sono correlati con la brand identity del mittente. Anche se le impostazioni predefinite sono sufficienti in termini di autenticazione dell'email, alcuni mittenti potrebbero aver bisogno di configurazioni aggiuntive (per esempio DMARC) e di brandizzare utilizzando un dominio personalizzato.

Alcune note:

- Le email sembreranno provenire direttamente dal tuo dominio, invece che dai nostri server.
- L'uso di un dominio personalizzato è obbligatorio per le impostazioni di autenticazione avanzate come DMARC.
- Sono necessarie le firme personalizzate DKIM e le impostazioni DNS, che richiedono che il mittente abbia pieno accesso ai record DNS del proprio dominio.

Per necessità di autenticazione è possibile avvalersi del servizio Deliverability Suite.

Guida alla configurazione

1. **Scegli il dominio FROM**
   Quale dominio utilizzerai per inviare con MailUp? Il tuo dominio di primo livello (cioè il dominio apex di cui abbiamo parlato sopra) o un sottodominio (ad esempio news.mydomain.com)? Nel primo caso il FROM EMAIL figurerebbe più o meno come updates@mydomain.com, nel secondo come updates@news.mydomain.com. La decisione si basa sulla tua possibilità di accedere e modificare i record DNS di quel dominio. Puoi verificare con la persona addetta all'accesso al sistema di gestione del dominio.
   Negli esempi a seguire abbiamo assunto che il dominio di invio corrisponda al dominio apex (mydomain.com). Se non puoi modificare i record DNS del tuo dominio apex, allora dovrai configurare un sotto-dominio (ad esempio news.mydomain.com) e fare riferimento a quello (al posto di mydomain.com) nei passaggi descritti di seguito.

2. **Verifica il tuo FROM EMAIL**
   Ora che hai scelto il dominio FROM, devi creare un FROM EMAIL sotto quel dominio e verificarlo nel tuo account MailUp. Per prevenire eventuali abusi, MailUp richiede che il FROM EMAIL sia verificato prima di essere utilizzato. La verifica è molto semplice: MailUp invierà un messaggio di verifica all'indirizzo FROM EMAIL fornito, e avrai bisogno di cliccare nel link contenuto nel messaggio. Puoi verificare il FROM EMAIL quando configuri una lista nel tuo account MailUp, quando imposti un nuovo invio o aggiungendo una nuova email mittente dalla pagina di Autenticazione mittenti.

3. **Configura il record SPF per il dominio di invio**
   Aggiungere l'autenticazione SPF è facile. Ecco quello che devi fare.
   - Contatta la tua società di web hosting, o la società con cui hai registrato il dominio, oppure l'amministratore di rete che gestisce il tuo dominio.
   - Digli che hai bisogno di una modifica ai record DNS (Domain Name System)
   - Se non hai ancora pubblicato un record SPF, digli di aggiungere questo record TXT:

     v=spf1 include:musvc.com ~all

   - Se hai già attivo un record SPF (ossia, hai un record TXT che inizia con v=spf1), allora digli di aggiungere la stringa "include:musvc.com" prima della keyword finale "all".

     esempio: v=spf1 include:mydomain1.com include:mydomain2.com include:musvc.com ~all

   - Attendi 24-48 ore: ci vuole un pò di tempo affinché le modifiche al DNS si propaghino sulla rete.
   - Verifica nella pagina Autenticazione mittenti che le email mittente con il tuo dominio superino il test SPF.

4. **Abilita l'autenticazione DKIM**
   Aggiungere l'autenticazione DKIM è semplice. Ecco cosa devi fare.
   - Contatta la tua società di web hosting, o la società con cui hai registrato il dominio, oppure l'amministratore di rete che gestisce il tuo dominio.
   - Digli che hai bisogno di una modifica ai record DNS (Domain Name System)
   - Chiedigli di creare questi due CNAME (ricordati di sostituire mydomain.com con il tuo dominio)

     `(1) ml01._domainkey.mydomain.com`

   - ... e fallo puntare a

     `ml01.dkim.musvc.com.`

     `(2) ml02._domainkey.mydomain.com`

   - ... e fallo puntare a

     `ml02.dkim.musvc.com.`

- Se non è possible creare un CNAME, puoi anche implementare l'autenticazione DKIM facendo delle modifiche ad alcuni record TXT delle impostazioni DNS. In tal caso, contattaci per maggiori dettagli.
- Attendi 24-48 ore: ci vuole un po' di tempo affinché le modifiche si propaghino sulla rete.
- Verifica nella pagina Autenticazione mittenti che le email mittente con il tuo dominio superino il test DKIM.

Ti ricordiamo che per utilizzare la firma DKIM personalizzata, i seguenti indirizzi email (role account) abuse@mydomain.com e postmaster@mydomain.com devono essere attivi, poter ricevere la posta ed essere monitorati.
Se utilizzi un sottodominio come dominio di invio (per esempio s m.mydomain.com) devi anche inoltrare quelle email (abuse@m.mydomain.com e postmaster@..) a abuse@mailup.com

5. **Configura l'interfaccia di dominio (opzionale)**
Se desideri usare un'interfaccia di dominio personalizzata (vedi la voce nel Glossario), puoi creare un C-NAME nel tuo sistema di gestione di dominio (per esempio news.mydomain.com) e puntare a c.mailup.com
Per poter utilizzare un'interfaccia di dominio personalizzata, è necessario avere attiva una piattaforma Edizione PRO oppure ENTERPRISE.

6. **Configura un Envelope Sender personalizzato (opzionale)**
Usando un Envelope Sender personalizzato (vedi la voce nel Glossario) puoi "allinearlo" con l'indirizzo FROM EMAIL, che permette maggiori configurazioni avanzate per l'invio. Questo indirizzo può essere qualsiasi account email a tua scelta di un sotto-dominio di quello utilizzato per il FROM EMAIL (per esempio se il FROM EMAIL è news@mydomain.com, l'Envelope Sender potrebbe essere bounce@bounce.mydomain.com). Affinché il sistema MailUp possa essere in grado di elaborare le email errate (bounce), sarà necessario l'accesso inviato a quell'indirizzo.
Creare due record DNS così composti:

1) Tipo: MX
Nome: bounce.mydomain.com
Valore: mx01.musvc.com
Priorità: 10

2) Tipo: TXT
Nome: bounce.mydomain.com
Valore: "v=spf1 include:musvc.com ~all"

Per maggiori informazioni riguardo il secondo record (SPF) potete far riferimento a questa pagina.

Modificando il record MX, la gestione delle email di quel dominio passerà sotto il controllo di MailUp e verrà gestita automaticamente dalla piattaforma. Gli account precedentemente configurati non riceveranno e non potranno più inviare le email.

7. **PTR dei server SMTP (per IP dedicati)**

Se il tuo flusso di email è inviato attraverso SMTP dedicati, ognuno di questi dovrebbe avere un PTR allineato con la base dell'host domain. Un esempio:

mx67202.mydomain.com A 93.174.67.202

mx67203.mydomain.com A 93.174.67.203

Ogni PTR dovrebbe avere lo stesso SPF / Sender ID records come il dominio di invio:

mx67202.newsletter.mydomain.com TXT v=spf1 include:musvc.com ~all

mx67202.newsletter.mydomain.com TXT spf2.0/pra include:musvc.com ~all

8. **Abilita il DMARC**

Poiché il DMARC è basato sul SPF e DKIM tutti gli step precedenti devono essere completati prima di poter abilitare il DMARC, anche su eventuali flussi **esterni** a MailUp. Quindi è molto importante verificare che **tutti i flussi** email che coinvolgono il dominio rispettino le condizioni necessarie.

Il seguente record di tipo TXT deve essere aggiunto ai record DNS del dominio di invio: _dmarc.mydomain.com
Il valore del campo TXT può cambiare a seconda della policy scelta, quello di seguito è solo un esempio:

Un record DMARC semplice è il seguente: *v=DMARC1; p=none; rua=mailto:dmarc.rua@mycompany.com; ruf=mailto:auth-reports@mycompany.com.*

dove:
* **v** è la versione (DMARC1 è l'unica disponibile)
* **p** è la policy. Valori accettabili sono *none* (non fare nessuna azione, raccogli solo i dati e manda gli avvisi) *quarantine* (considera sospetta la mail che non passa il DMARC) *reject* (blocca tutte le email sospette)
* **pct** è la % di messaggi non allineati che devono essere rifiutati (da 1 a 100 dove 100 significa tutti i messaggi)
* **rua:** Invia i report aggregati a questo indirizzo (deve essere monitorato)
* **ruf:** Invia i report dettagliati (Forensic) a questo indirizzo

Gli indirizzi email che ricevono i report possono essere su qualsiasi dominio, non necessariamente quello usato per l'autenticazione.

Noi consigliamo caldamente di abilitare progressivamente il DMARC utilizzando la policy *p=none* all'inizio. Controllate il traffico per intercettare anomalie nei report (ad esempio messaggi non correttamente firmati / allineati).
Una volta verificato che tutti i messaggi legittimi sono autenticati potete cambiare la policy in *p=quarantine*.
Rivedete i risultati ancora una volta (guardate anche nello spam) e quando siete assolutamente sicuri che tutti i messaggi sono firmati e autenticati potete cambiare la policy in *p=reject* per utilizzare in pieno il DMARC

Potete anche sfruttare il parametro **pct** per evitare di avere subito un impatto su tutte le vostre email. In ottica molto conservativa, dopo aver abilitato la policy "quarantine" potete iniziare con *pct=1* e poi aumentare progressivamente a 10, 25, 50, 100