Edizione 2.0

Email Marketing e Antispam

Impariamo a conoscere i filtri e
le buone pratiche per evitarli

La biblioteca di VOXmail

Indice dei contenuti

1. UNO SPAM, DUE DEFINIZIONI

Parlando di email, con il termine **SPAM** si indica genericamente una **comunicazione massiva di tipo promozionale non richiesta dal proprietario della casella di posta**.

L'aumento esponenziale di questo tipo di traffico promozionale con il diffondersi della connettività internet ha portato sia i fornitori di servizio email, sia i governi a correre ai ripari per tutelare i propri clienti e i propri cittadini.

Chi invia comunicazioni commerciali ai propri clienti deve dunque stare attento a **due aspetti fondamentali**:

- per la normativa italiana è spam **una email non richiesta** (*quindi una email che non rispetta il* ***consenso*** *preventivamente fornito al mittente*).
- per i fornitori di servizi email e per i loro **filtri anti spam** è spam una email che **non genera interesse** nel destinatario, una email irrilevante.

Attenzione a non confondere le due cose!

Anche se per la **normativa italiana** (*che va rispettata in ogni sua parte*) è fondamentale **il consenso**, per essere sicuri che le email arrivino nella fatidica "posta in arrivo" è necessario che **i destinatari siano felici di riceverle**.

Consenso

La normativa prevede che il Consenso debba essere "informato, libero e specifico".
Informato: nel senso che deve essere presente una informativa che l'utente ha potuto visionare semplicemente
Libero: nel senso che deve essere fornito su base volontaria e non può essere "estorto" o "sottinteso".
Specifico: il consenso viene rilasciato ad uno specifico titolare, per un determinato argomento e per una determinata forma e frequenza di comunicazione.

2. FILTRI ANTISPAM. COSA, DOVE, COME, QUANDO E PERCHÉ

2.1 Aiuto, la mia mail finisce in Posta Indesiderata!

A parte casi estremi e molto rari, dire semplicemente "**la mia email finisce in posta indesiderata**", non ha molto senso.

Posta Indesiderata

Molti filtri AntiSpam sfruttano la presenza di una cartella appositamente creata per ospitare i messaggi di posta sospetti.
Tale cartella viene normalmente chiamata **"Posta Indesiderata"** o semplicemente **"Spam"**

I filtri AntiSpam sono molto eterogenei ed ogni provider usa sistemi personalizzati con risultati assai diversi.

È estremamente raro che tutti i provider classifichino una email come spam; quando succede è per **casi piuttosto eclatanti e normalmente semplici da individuare.**

È dunque sbagliato pensare che se una email arriva in una casella in spam, allora arrivi a tutti in spam: con alcuni provider, ad esempio Gmail, la classificazione come spam può dipendere anche dalle abitudini del singolo destinatario.

Per capire quale sia il problema che stiamo affrontando, e se di problema effettivamente si tratti, è necessario **analizzare il contenuto dell'email**, verificare **il sistema di spedizione**, **il mittente** e, soprattutto, **il destinatario**.

2.2 Come funzionano i filtri AntiSpam?

I filtri AntiSpam utilizzano **mix di differenti tecniche** per poter identificare le email indesiderate.

La tecnica del Blacklisting consiste nell'individuazione di liste di parole, domini o altre caratteristiche da utilizzare come **filtro diretto**: una mail passa o meno il controllo in base alla presenza di uno degli elementi della lista. Una tecnica più evoluta è quella di calcolare uno **"score"**, assegnando **un punteggio ad ogni aspetto dell'invio** e classificando come Spam le email che superano una certa soglia.

Molti sistemi usano un mix di queste due tecniche, **blacklisting** come primo filtro **"grossolano"** e **score** per identificare casistiche meno evidenti.

In passato la maggior parte di queste liste o di questi punteggi erano gestite manualmente, sia in fase di inserimento, sia di rimozione o modifica.

Oggi la maggior parte dei filtri fa uso di **calcoli automatici**, basati su ciò che hanno fatto i propri utenti quando hanno ricevuto in passato email che riportavano **caratteristiche simili** a quelle dell'email in analisi.

Indirizzo IP

Ciascun computer connesso ad Internet è identificato da un proprio indirizzo chiamato "IP address" o spesso semplicemente IP.
Gli indirizzi IP sono rappresentati da una sequenza di quattro numeri divisi da punti (e.g. 127.0.0.1)

Ad esempio, a seguito di un numero cospicuo di segnalazioni di Spam relative a messaggi contenenti un collegamento verso uno specifico sito, un filtro potrebbe automaticamente inserire tale sito in blacklist e conseguente identificare come spam le successive email contenenti collegamenti allo stesso sito. Lo stesso filtro, individuando che alcuni utenti hanno recuperato messaggi dallo Spam contenenti lo stesso collegamento, potrebbe decidere di rimuoverlo dalla blacklist.

Oltre agli indizi più evidenti, come le segnalazioni di Spam, il filtro terrà conto anche di operazioni meno "drastiche", come la cancellazione di un messaggio non letto, oppure, in senso contrario, l'interazione dell'utente con l'email (apertura, risposta, clic sui collegamenti).

Parallelamente, oltre all'analisi dei collegamenti citata nell'esempio, gli aspetti tenuti in considerazione dai filtri sono molteplici: **nome mittente, email mittente, dominio** dell'email mittente, parole dell'**oggetto**, caratteristiche del testo (**maiuscole/minuscole, uso di colori forti o di testi grandi**), rapporto tra testi ed immagini, siti web (o domini) nei quali sono **ospitate le immagini** (o altre risorse) incluse nel messaggio.

Ognuno di questi elementi ha una sua importanza ed è sempre bene tenerli in considerazione quando prepariamo le nostre comunicazioni.

L'insieme di tutti questi fattori viene identificato con il termine **reputazione**, per via dei meccanismi di "memoria dei comportamenti" che li caratterizzano.

2.3 La lunga strada verso la "Posta in Arrivo"

La strada che una email percorre dal momento in cui viene inviata a quello in cui viene letta dal destinatario **è piena di ostacoli**: i filtri AntiSpam, al contrario di quello che si potrebbe pensare, **possono essere molteplici**.

Un aspetto tecnico spesso sottovalutato è la **corretta identificazione** del momento in cui interviene il **blocco per spam**: la maggior parte dei server fornisce spesso **errori generici** che vanno adeguatamente interpretati e studiati, imparando a conoscere **i comportamenti e le abitudini** dei singoli server riceventi.

Di seguito analizziamo le tre fasi fondamentali dell'invio di una email: trasmissione, consegna e ricezione.

SMTP

Il protocollo SMTP (Simple Mail Transmission Protocol) è il protocollo di comunicazione utilizzato per la trasmissione di posta elettronica. Il protocollo, definito ufficialmente nel 1982, è rimasto pressoché invariato: si tratta di uno dei protocolli internet più longevi.

Trasmissione

1. **Limiti di invio**

   Chi spedisce la nostra email (ovvero il nostro server SMTP) verifica **chi siamo, quanti messaggi abbiamo inviato** nelle ore/giorni precedenti, il **contenuto dell'email** e i **destinatari**. Potrebbe decidere di **bloccare la nostra email** senza nemmeno provare a recapitarla: quasi tutti i provider di **caselle gratuite o lowcost** operano questo tipo di "filtro in uscita".

2. **Nolisting**

   Se il nostro mail server decide di **provare a consegnare l'email**, tenterà di contattare il mail server (o uno dei mail server) del dominio di destinazione. In questa fase di connessione il sistema potrebbe cadere in trappole AntiSpam

come, ad esempio, il **"nolisting"**, tecnica nella quale il dominio destinatario dichiara come suo mail server principale **un server inesistente** e solamente come secondario il suo reale server ricevente, o altre tecniche similari (**fake mx, mx sandwich**).

3. **Blacklist IP**

   Superato l'eventuale **nolisting** e trovato il server ricevente "giusto", il sistema, prima di accettare la connessione, **verificherà che l'IP mittente** non sia in **blacklisting** (blacklist pubbliche o private). Alcuni server forniscono una spiegazione più o meno generica per il rifiuto, mentre altri si limitano a non accettare la connessione.

4. **Autenticazione**

   Accettata la connessione il server aspetterà che il mittente si "presenti" e a quel punto potrà fare nuove verifiche legate all'indirizzo email **"mittente della busta"** (*envelope sender*) e **IP mittente**, sulla validità del dominio del mittente ed eventualmente, se non li ritenesse validi, chiudere la connessione.

TARPIT

Tecnica che introduce una enorme lentezza nei vari passaggi del protocollo SMTP facendo si che il mittente perda svariati minuti per consegnare l'email.

5. **Greylisting**

   Dopo aver verificato il mittente, verrà richiesto l'elenco dei destinatari. In questa fase agisce solitamente un filtro AntiSpam, chiamato **"Greylisting",** che consiste nel **rifiutare il primo tentativo di invio** di una email da uno specifico mittente ad uno specifico destinatario.

Questa tecnica, costringendo il mittente a mantenere il messaggio in "coda di spedizione" e a ritentare l'invio successivamente, introduce un **costo operativo** per il server

mittente sperando che l'eventuale spammer **non sia disposto a sostenerlo**. Sullo stesso principio si basano anche altre tecniche, tra le quali la più diffusa è il **TARPIT**.

Consegna

6. **Analisi contenuto in tempo reale**

   Alcuni filtri effettuano un **controllo AntiSpam sul contenuto** appena lo ricevono e potrebbero quindi terminare la connessione **rifiutando il messaggio istantaneamente**. Altri, dopo averlo classificato come spam, decidono di rispondere *"OK! Ho ricevuto il tuo spam, il messaggio verrà cestinato"*: non essendo un avvertimento di errore, un mittente non attento **potrebbe limitarsi alla validità dell'OK** e considerare il messaggio consegnato, mentre il ricevente ha già comunicato di averlo cestinato.

7. **Analisi differita**

   Pur avendo terminato la connessione con successo, potremmo incappare nell'azione censoria di altri filtri AntiSpam. Non potendo più comunicare in tempo **reale l'avvenuta classificazione**, il mail server **crea un nuovo messaggio**, chiamato bounce, da recapitare al mittente nel quale gli verrà detto che **l'email è stata bloccata**.

8. **Posta indesiderata**

   Pur non avendo bloccato il messaggio nelle fasi precedenti, un filtro potrebbe stabilire che **il messaggio risulti sospetto.**

   In questo caso potrebbe inserire questa informazione modificando l'oggetto del messaggio o repitandolo nella casella "posta indesiderata".

Bounce

Identifica particolari messaggi generati da un server per avvisare che una precedente email non è stata consegnata. Il formato standard di questi messaggi è implementato solamente dal 50% dei server, complicandone la gestione automazzata.

Ricezione

9. AVAS

Acronimo per “AntiVirus AntiSpam”, definisce un software installato nel dispositivo di chi legge la posta e che si “intromette” nella procedura di scaricamento per verificare tutti i messaggi in arrivo.

Questo è possibile perché i client di posta (come Outlook o Thunderbird) utilizzano un protocollo di scaricamento della posta standard (POP3 o IMAP4).

10. Client di posta

Alcuni client operano filtri AntiSpam propri, normalmente basati sui contenuti o su regole di “posta in arrivo” impostate dai propri utilizzatori.

Filtri Bayesiani

Alcuni programmi di posta basano il filtraggio su filtri Bayesiani.
Analizzando le parole più frequentemente usate nei messaggi letti e quelle più frequentemente usate nei messaggi segnalati come spam, imparano a classificare le email successive.

Per superare alcuni di questi ostacoli (quelli relativi alla fase di Trasmissione) è sufficiente **usare un buon mail server** che sappia come si consegna una email, mentre per evitare gli altri sono necessari **buoni contenuti e buona reputazione** .

Per questo è fondamentale che dietro al **buon server SMTP** di invio ci sia anche **uno strumento in grado di analizzare**, tradurre e classificare i messaggi relativi ai problemi di consegna, sia che avvengano durante la connessione, sia che avvengano tramite invio di “bounce” successivi alla consegna.

L’abilità di superare tutti questi ostacoli viene definita **deliverability**.

2.4 Le blacklist pubbliche

Le grandi blacklist pubbliche oggi rappresentano il **filtro più grossolano:** identificano i **"grandi" problemi di spam**, lasciando poi ad altri meccanismi, come analisi del comportamento dell'utente, estrazioni di “impronte digitali” dall'email e **blacklisting collaborativo**, il compito di fare filtraggio in maniera più selettiva.

Molti provider dispongono di liste che hanno funzionamenti simili, ma che **non sono pubbliche**, per cui non è possibile in alcun modo verificare se si è o meno "blacklistati": occorre **controllare con costanza le statistiche** e prestare attenzione a cambiamenti improvvisi nelle percentuali di **apertura e di click** verso i singoli provider.

Ancora oggi è comunque importante assicurarsi di **non essere in una delle liste pubbliche**, almeno di quelle più importanti e utilizzate, ma è bene sapere che la questione non si esaurisce con questo controllo.

Le tipologie di blacklist sono due: **IP-based**, quindi liste di indirizzi IP di spedizione, oppure **Domain-based**, liste di domini citati nel corpo dell'email sotto forma di link, di indirizzi email, di indirizzi dai quali vengono recuperate le immagini o anche di semplice testo.

IP-Based:

Note con gli acronimi **RBL** (Real-time Black List) e **DNSBL** (DNS-based Blackhole List), sono liste di indirizzi IP aggiornate in tempo reale e usate dai provider per controllare se le email provengono da infrastrutture che consentono l'invio in open-relay (invio aperto liberamente a sender esterni all'infrastruttura stessa, cosa sempre più rara) o riferibili a spammer.

- **sbl.spamhaus.org (SBL):** Spamhaus è probabilmente il fornitore di liste maggiormente conosciuto e utilizzato, Spamhaus Block List (SBL) è un database di IP dai quali Spamhaus sconsiglia di accettare email.
- **xbl.spamhaus.org (XBL):** La Exploits Bot List (XBL) è una lista di proxy aperti e indirizzi IP infettati da bot e virus e

utilizzati per la successiva ondata di infezione o di spam. Usando servizi professionali di un ESP è quasi impossibile avere problemi con questa lista.

- **cbl.abuseat.org (CBL):** Lista che utilizza spamtraps per identificare indirizzi IP fonte di malware, trojan, virus e spam. È disponibile uno strumento di autorimozione.
- **SpamCop (SCBL):** è un servizio di segnalazione di spam che consente ai destinatari di email massive non richieste (UBE - Unsolicited Bulk Email) e email commerciali non richieste (UCE - Unsolicited Commercial Email) di segnalare i relativi indirizzi IP di spedizione. Le informazioni raccolte contribuiscono al mantenimento della lista Spamcop Blocking List (SCBL). Come tutti i filtri collaborativi è soggetto all'errore dei segnalatori. Il delisting è automatico, dopo 24 ore dall'ultima segnalazione.

Domain Based:

In questo caso le liste raccolgono domini che appaiono all'interno dell'email (URI Real-time Blacklist).

- **dbl.spamhaus.org (DBL):** Database realtime di domini trovati in messaggi SPAM, molto spesso domini riferibili a gruppi di spammer, malware, phishing e altro.
- **black.uribl.com (URIBL):** Lista di domini usati in messaggi di SPAM. Uribl.com ha molte liste pubbliche, ma la più usata risulta essere black.uribl.com, che ha l'obiettivo dichiarato di zero falsi positivi. La lista si aggiorna automaticamente e anche il delisting è automatizzato. I proprietari di domini possono richiedere il delisting.
- **surbl.org (SURBL):** lista di domini apparsi in messaggi di posta non richiesti. I proprietari dei domini possono chiedere la rimozione.

Come già detto sopra, il **non apparire in queste liste** non vuol dire in automatico che i messaggi inviati arrivino a destinazione; viceversa, avere problemi con qualche blacklist significa avere **problemi di deliverability**.

Una volta verificata la presenza - in termini di indirizzo IP o dominio - in una delle liste è fondamentale **capire come mai si è finiti nella lista**, individuare quindi il problema scatenante (segnalazioni di abuso, invio a liste "sporche" e quindi con possibili spam trap...) e adottare le misure necessarie a risolvere la situazione.

Delisting

Molte blacklist, non tutte, consentono di inoltrare richieste per la rimozione del proprio ip/dominio dalla lista. È importante inoltrare la richiesta solo dopo aver compreso i motivi dell'inserimento e aver risolto il problema scatenante.

Solo dopo aver individuato il problema ed averlo risolto, sarà possibile rivolgersi al gestore della lista per ottenere **il delisting**: facendo il contrario - quindi chiedendo il delisting prima di aver risolto il problema – si **peggiorerebbe soltanto la situazione** e l'indirizzo IP o il dominio "incriminati" finirebbero in breve nuovamente nella lista.

Le liste hanno **"memoria" dei blocchi passati** e ottenere una successiva rimozione per uno stesso indirizzo IP o dominio sarà sempre più difficile.

2.5 I filtri AntiSpam collaborativi: Cloudmark

Fra i vari filtri antispam merita un posto di rilievo, per estensione d'uso e per le peculiarità di funzionamento, **Cloudmark**, utilizzato in **Italia** da fornitori di caselle email molto importanti, tra i quali **Libero, Virgilio, Tiscali, Aruba, Fastweb e Register.it**.

L'idea fondamentale del servizio Cloudmark è quella di un **filtro collaborativo**, che basa la classificazione delle email in relazione ai feedback inviati da chi ha ricevuto l'email; in questa maniera, evitando dunque qualsiasi tipo di automatismo, si demanda la decisione ai diretti interessati.

L'email arrivata è **spam** per un certo numero di destinatari? **Allora è spam.**

Fingerprint

Elementi distintivi di una email, come mittente, porzioni di testo, link e indirizzi email, codificati in modo da poter essere facilmente estraibili e confrontabili. Mantenendo una blacklist di Fingerprint è possibile riconoscere le email di spam e bloccarle.

Cloudmark Authority nasce come "versione commerciale" di un progetto open source chiamato **Vipul's Razor**, scritto da Vipul Ved Prakash, poi cofondatore della stessa Cloudmark.

Il primo problema che Vipul ha affrontato quando ha cominciato a pensare il suo filtro è stato quello del **costo dell'analisi integrale** di ogni messaggio in ingresso: la soluzione è stata quella di creare un software capace di individuare ed estrarre, in maniera rapida ed efficace, **parti significative dell'email** - indirizzi email, piccole porzioni di testo, mittente, link... - e codificarle in "**impronte digitali**" compatte (**Cloudmark's fingerprint**).

Una volta che il filtro ha estrapolato le impronte dell'email in ingresso, il sistema verifica che ognuna di queste **non sia contenuta nel database delle impronte "blacklistate"** come portatrici di spam: se anche solo una di queste impronte viene riconosciuta come

sospetta, l'email stessa viene trattata come email di spam - e quindi, a seconda delle politiche dell'ISP, consegnata con l'**oggetto cambiato**, relegata nella **cartella "posta indesiderata"**, oppure **direttamente rifiutata** in tempo reale o tramite successivo bounce.

Il processo di estrazione delle "impronte digitali" è uno dei meccanismi chiave di Cloudmark ed è, chiaramente, segreto: dai test effettuati si evidenzia che praticamente **tutti gli indirizzi web** - anche solo citati, non necessariamente linkati - vengono trasformati in **impronte digitali,** come anche le sequenze di testo che possano sembrare indirizzi fisici o numeri di telefono, oppure particolari parole, o ancora nomi o contenuti degli allegati o la struttura del messaggio.

Per ogni email vengono estratte **un numero variabile di impronte**, dalle poche unità a parecchie decine, anche centinaia, che insieme formano una vera e propria **carta d'identità della missiva**.

Questa carta di identità è una **collezione di chiavi** generate dagli elementi fondamentali dell'email – come detto sopra si va dagli **indirizzi web** alle **sequenze di testo**, dai **numeri telefonici** ai contenuti veri e propri - ed è su questi elementi che Cloudmark basa il riconoscimento dello Spam.

L'**IP** del **server mittente** o la firma DKIM o l'autenticazione SPF **perdono di importanza** in questo processo: tutto si riduce ad una serie di **impronte** e in quante occasioni e da chi tali impronte sono state indicate come "**da bloccare**" o come "**da non bloccare**".

Partendo dall'idea base che **solo chi riceve** l'email può decidere se questa sia **spam o meno**, Cloudmark Authority lavora sulle segnalazioni da parte di chi utilizza il filtro: tutte le volte che un utente Cloudmark **mette in spam una email**, il filtro estrae tutte le impronte digitali dell'email e le invia al server centrale identificandole come **"sospette"**.

Una volta raggiunto un certo limite di segnalazioni, **le impronte vengono giudicate**, non prima però di verificare l'affidabilità di chi le ha segnalate.

Essendo infatti un sistema basato su segnalazioni, è fondamentale che la rete di segnalatori **mantenga una reputazione alta**, altrimenti

l'intero filtro sarebbe messo sotto scacco dagli abusi.

Se gli agenti coinvolti nella segnalazione passano il check di fiducia, l'impronta digitale sospetta **diventa ufficialmente "cattiva"** e passa al server Catalogo, per essere poi distribuita in tutta la rete di installazioni Cloudmark.

Cloudmark ha un sistema per la gestione dei **"falsi positivi"**, quindi di quelle impronte digitali che, seppur indicate come "cattive", si rivelano alla prova dei fatti come "buone", quindi non portatrici di Spam.

Stando alle stesse dichiarazioni di Cloudmark, in questa categoria si ritrovano spesso gli **invii massivi, Newsletter e Dem**, che, per quanto ben gestiti e curati, **possono generare segnalazioni di abuso** e quindi blacklisting da parte del filtro.

Per gestire questo tipo di problematiche, Cloudmark **raccoglie anche feedback "positivi"**: se qualcuno "ripesca" dalla cartella spam un messaggio e **lo porta in posta in arrivo**, l'azione viene registrata dal filtro, che poi farà - in automatico - le valutazioni del caso.

Appare chiaro che l'azione di recupero di un messaggio dalla cartella spam **è oltremodo rara**, per cui è evidente che una impronta digitale "cattiva" difficilmente potrà sperare in un rivalutazione da parte del filtro.

2.6 È tutta questione di reputazione

Come spesso accade nelle questioni legate al web e all'email marketing, **il buon senso è l'arma migliore** che abbiamo a nostra disposizione. Pensare di poter utilizzare trucchi per trarre in inganno i filtri AntiSpam è inutile e spesso dannoso.

I moderni filtri AntiSpam lavorano sulla **reputazione**, analizzando le reazioni degli utenti agli invii, spesso in tempo reale; **catturare l'attenzione del proprio pubblico** diventa fondamentale, se vogliamo continuare a raggiungerlo. Inviare email **rilevanti** per l'interlocutore è l'arma principale.

Il basso costo dell'invio email porta a pensare sia meglio inviarne una in più piuttosto che una in meno: in realtà **ogni email ignorata** perché non rilevante, **diminuisce la reputazione** e aumenta quindi le probabilità che le email successive (*anche la stessa newsletter inviata ad altri destinatari dello stesso dominio pochi minuti dopo*) **possano essere classificata come spam**.

Per aumentare la rilevanza è necessario **segmentare la propria lista** e cercare di mandare email **solo a chi mostra interesse**: l'approccio all'invio email non deve essere quello del volantinaggio in buchetta. Abbiamo la possibilità di avere informazioni sul gradimento delle nostre comunicazioni e usandole riusciremo ad **ottimizzare i costi** e a **migliorare il rendimento delle spedizioni stesse**, oltre a minimizzare il rischio di incorrere nelle maglie dei filtri AntiSpam.

I filtri AntiSpam sono diffidenti e quindi considerano gli sconosciuti in maniera potenzialmente negativa.

La reputazione, come nel mondo "reale", **si costruisce a fatica e si distrugge molto velocemente**: farsi una buona reputazione richiede costanza e qualità, mentre basta un invio per vanificare il lavoro fatto fino a quel momento; e non tutti i provider, un po' come le persone, si comportano allo stesso modo... alcuni hanno memoria breve, altri ricordano a lungo gli "sgarbi", altri ancora reagiscono velocemente, mentre alcuni se la prendono con comodo.

2.7 Se finisco in SPAM, me ne accorgo?

Non è facile accorgersi di avere un **effettivo problema di spam**, poiché la maggior parte dei filtri AntiSpam, quando blocca un messaggio, non fornisce motivazioni al mittente, o ne fornisce di molto generiche o fuorvianti.

In alcuni casi la classificazione come Spam avviene senza che vi sia nessun tipo di comunicazione al mittente, il caso più frequente è la consegna in "posta indesiderata".

Le grandi **blacklist pubbliche** (*Spamhaus, Surbl, Uribl, Spamcop*) possono essere una fonte di dati, ma bisogna tenere presente che vengono attivate **solo su casi davvero eclatanti**.

È possibile anche ottenere informazioni circa **la reputazione degli indirizzi IP di spedizione** (*Senderbase, Senderscore*), ma anche in questo caso le segnalazioni scattano solo di fronte ad abusi conclamati.

Il semplice fatto di **non essere presenti in nessuna blacklist** pubblica e avere una buona reputazione secondo Senderbase e Senderscore **non assicura che le proprie email arrivino a destinazione.**

Deliverability

Il termine Deliverability identifica la capacità di consegna dei messaggi nella casella di posta in arrivo. Sulla deliverability influiscono numerosi aspetti, spesso difficilmente misurabili.

Al contrario, avere una bassa reputazione sui servizi pubblici o essere presenti in famose blacklist, rende molto probabili **problemi di deliverability**.

Esistono **indicatori affidabili** che mostrino dunque il livello di deliverability delle nostre email? La risposta a questo quesito si trova direttamente nell'**analisi dell'efficacia delle nostre comunicazioni**, tramite, ad esempio, le statistiche fornite da chi si occupa di consegnarle: è fondamentale rilevare **chi e quanti** siano i destinatari che **aprono le email**, chi e quanti **cliccano su ogni**

specifico link e, se possibile, chi e quanti, una volta arrivati sul sito, **generano "conversioni"** (e di quale valore).

Una diminuzione sensibile del tasso di apertura (*open rate*) senza una contemporanea diminuzione del tasso di **"click rate su open rate"**, ovvero il rapporto fra aperture e successivi click su link, può essere sintomo di un **problema di deliverability**.

Apertura

Con il termine apertura si intende il fatto che il messaggio sia stato visualizzato dal destinatario.
Tecnicamente le aperture vengono rilevate grazie alla richiesta da parte del client di posta di una particolare immagine inserita nel messaggio.

Su questi dati però non incide solamente l'eventuale problema di consegna delle email: mittente, oggetto della mail e contenuti **possono variare il comportamento del ricevente** in maniera drastica, spingendo l'utente a non aprire la mail o a non cliccare sul link per **semplice disinteresse** e non perché non ha ricevuto la mail in seguito ad una classificazione come Spam.

In particolare può essere utile **monitorare i tassi di apertura** suddivisi per ciascun dominio ricevente: se un determinato invio **peggiora il tasso di apertura** verso Libero.it ma mantiene invariato quello verso Gmail.com, si può ipotizzare di avere **un problema di spam** sul primo dominio.

2.8 I feedback loops, ovvero andare oltre all'evidenza

Per ovviare, almeno parzialmente, ai dubbi relativi allo status di "spam" delle nostre email, esistono meccanismi chiamati **Feedback loops (FBL)**: alcuni provider permettono di trasferire al mittente le informazioni su **chi marca l'email ricevuta come spam.**

Ottenere queste informazioni **non è semplice**: è necessario dimostrare di avere **titolarità sugli IP** dai quali partono le email e spesso è necessario utilizzare sistemi di autenticazione e dimostrare di essere **proprietari dei domini autenticati.**

Per i **professionisti dell'invio email**, come **VOXmail**, queste pratiche sono consolidate e fonte importante di **informazioni sullo stato effettivo della deliverability** e su eventuali abusi della propria piattaforma.

I provider principali, per il mercato italiano, che forniscono questo tipo di informazione sono **Yahoo, Outlook.com (Hotmail) e Libero**. **Gmail** offre uno strumento similare, ma non comunica la singola notifica, bensì riporta solamente dati aggregati.

Un basso numero di segnalazioni di abuso non significa automaticamente che si stia lavorando bene. **Una email già classificata come spam** dal provider molto probabilmente verrà ignorata dal destinatario e quindi **non provocherà nuove segnalazioni.** Per assurdo, l'assenza totale di segnalazioni potrebbe indicare che tutte le email siano state recapitate in spam.

Fra gli strumenti dedicati ai professionisti dell'invio email, spicca **SNDS**: Microsoft fornisce (ai possessori di indirizzi IP) dati relativi al monitoraggio delle email inviate da tali IP verso utenti Microsoft. **SNDS** fornisce informazioni su **blacklisting, numero di email ricevute e quante sono state classificate come spam** da ciascun IP per ogni giorno (*meno del 10%, tra il 10 e il 90%, più del 90%*).

2.9 Ma a me non era mai capitato!

Spesso si ha il dubbio o la sensazione che la ricezione delle nostre email da parte dei destinatari sia un fatto che **non ci compete direttamente**, oppure regolato da leggi misteriose e aggirabili unicamente tramite trucchi di vario genere.

In realtà, come spesso accade, **non esistono trucchi**, ma **"buone pratiche"** da seguire con costanza.

Se un messaggio viene bloccato da un filtro AntiSpam oggi non è assolutamente detto che verrà bloccato anche domani (o viceversa).

Il fatto che **non si facciano modifiche** ad una newsletter periodica che di solito arriva correttamente ai destinatari, non impedisce ai filtri di cambiare comportamenti e **prendere decisioni diverse**.

Fare analisi per capire il motivo della classificazione **è spesso molto difficile e costoso**, soprattutto in termini di tempo: è necessario procedere per tentativi successivi, facendo prove, a distanza di poco tempo l'una dall'altra, nelle quali **si cambia solo un aspetto dell'email** e si verifica se ci sono variazioni nella classificazione.

3. HO CAPITO. E ADESSO COME FACCIO?

3.1 Condizioni necessarie e sufficienti

Perché una email sia consegnata e venga inserita in posta in arrivo sono **necessarie due condizioni**:

1. Il server di invio deve **avere buona reputazione**, essere configurato correttamente e comportarsi "bene" nei confronti dei server di destinazione (*non bombardarli, rispettare le richieste dei singoli provider, rispettare i messaggi di errore*).

2. Il messaggio deve **essere rilevante** per i destinatari.

Se manca una delle due condizioni, l'email non verrà consegnata o finirà in spam. Questo significa che **un buon server**, ben configurato e manutenuto, **non riuscirà comunque a consegnare spam.**

Allo stesso tempo **una buona email**, potenzialmente gradita da chi la riceve, inviata da un buon mittente **non verrà consegnata** in posta in arrivo se spedita **da un server con cattiva reputazione**.

Entrambe le condizioni sono necessarie per la corretta consegna dell'email, ma **nessuna delle due è sufficiente da sola** a garantire il risultato cercato: **VOXmail** si occupa della **prima condizione**, a voi spetta la seconda.

3.2 Tecniche di autenticazione

Chi si è occupato a livello tecnico di inviare grossi quantitativi di email, si sarà sicuramente imbattuto in una serie di sigle piuttosto oscure, che identificano **varie tecnologie di firma.**

DKIM e SPF sono due sistemi per "autenticare" l'email, sotto due aspetti distinti:

- **DKIM (*DomainKeys Identified Mail*)** è un metodo tramite il quale il proprietario di un dominio "certifica" di prendersi **la responsabilità di quella specifica email**
- **SPF (*Sender Policy Framework*)** è un metodo per dichiarare quali indirizzi IP possono spedire email per un **determinato dominio**.

Entrambi permettono ai filtri AntiSpam di riconoscere con più precisione il mittente come una sorta di **"carta di identità"**: avercela può essere necessario per entrare in certe nazioni, ma **non garantisce di poterlo fare** (*anzi, proprio grazie alla carta di identità, tali stati possono decidere di respingere le persone indesiderate*).

Quindi **SPF e DKIM devono essere implementati**, ma devono anche corrispondere a **soggetti con una buona reputazione**, altrimenti è come non averli o persino peggio.

DMARC *(Domain-based Message Authentication, Reporting & Conformance*) "aumenta" le funzionalità di DKIM e SPF, rendendo note le **norme di comportamento** che un server deve tenere **quando una email non è firmata** con questi protocolli o quando è firmata con un particolare dominio.
DMARC può dire, ad esempio, **che le email con mittente @yahoo.com** possono **partire solo dagli IP di Yahoo** ed utilizzare obbligatoriamente la firma **DKIM**.

Al momento sconsigliamo l'adozione generalizzata di DMARC a chi spedisce email, poiché ci sono ancora meccanismi da oliare e un record DMARC potrebbe far sì che la vostra email **diventi inutilizzabile** su vari strumenti web.

3.3 Il mittente

Il mittente gioca un ruolo chiave nell'invio email: molti filtri antispam analizzano infatti il dominio del mittente, e **ne tracciano la "reputazione"**, in base all'interazione utenti, alle segnalazioni di abuso e agli errori generati dagli invii precedenti.

In molti casi, alle volte proprio per paura di "sporcare" il proprio dominio aziendale, si usa come mittente una **casella gratuita** (anche note come freemail, come @gmail.com, @libero.it, @alice.it, @yahoo.com, etc..), ma questa pratica è problematica sotto molti punti di vista, e lo sarà sempre di più.

I problemi di base riguardano **la riconoscibilità** – chi riceve l'email **deve potersi fidare del mittente** – e il fatto di **legare la propria reputazione** mittente al dominio della piattaforma freemail, che potrebbe portare con sé una storia complessa, **fatta di abusi e spam**.

Proprio per evitare questi abusi, molti fornitori di Freemail hanno già pubblicato **record DMARC** che richiedono di **considerare spam o cestinare** messaggi con mittenti appartenenti ai loro domini quando sono inviate da server che non siano sotto il loro controllo: questo significa che, al momento, non è possibile usare mittenti **Libero, Iol, Inwind, Aol, Yahoo** per inviare le proprie newsletter tramite servizi di invio massivo.

Alla fine del 2015 **Gmail** ha annunciato che a metà del 2016 avrebbe attivato una **policy DMARC altrettanto restrittiva** sui propri domini. Al momento – **settembre 2016** – risultano unicamente dei test sulle email del dominio **@googlemail.com**.

Ci si attende la pubblicazione definitiva dei record DMARC sul dominio @gmail.com **fra la fine del 2016 e l'inizio del 2017**: il passaggio di Gmail a queste politiche molto probabilmente trainerà anche altri fornitori, andando ad assottigliare ulteriormente la gamma delle caselle free utilizzabili per invii massivi.

È dunque molto importante passare quanto prima a **mittenti su domini di proprietà**, di cui si abbia controllo diretto.

3.4 Gli indirizzi IP di spedizione

Nel **complicato processo** di consegna delle email, i compiti a carico del fornitore di servizio di invio sono numerosi.

Alcuni fornitori permettono di ottenere, specie per database di invio cospicui, **IP dedicati al singolo servizio**.

È davvero un vantaggio?

Avere un **indirizzo IP dedicato** alle proprie spedizioni permette di isolare la reputazione, che non viene "inquinata" (ma neppure in positivo) da altri.

Mantenere la reputazione di un IP vuole dire anche assicurare un volume di invio costante e continuo, altrimenti c'è il serio rischio che questa scelta comporti più danni che vantaggi: come già accennato, i sistemi AntiSpam valutano con attenzione questi parametri.

Warm-Up

Si parla di **"warm-up" degli indirizzi IP** come tecnica per abituare i filtri AntiSpam alla nostra "presenza": quando si comincia ad inviare email da un nuovo indirizzo IP è opportuno partire con **poche email al giorno**, aumentando il volume di settimana in settimana fino a portarlo a regime, in caso contrario si rischia che i filtri rifiutino tutto fin da subito.

Un indirizzo IP shared (condiviso) avrà una **reputazione generata dalla media** delle singole reputazioni di chi lo utilizza: di norma è la soluzione più stabile, anche grazie agli accorgimenti del fornitore di servizio, che si occuperà di mantenere il più possibile costante il traffico in uscita.

Chi si occupa, per mestiere, di inviare email, avrà a disposizione **un parco di indirizzi IP costantemente utilizzati**, con un volume di invio il più possibile costante, **attivi da anni**.

Oggigiorno la reputazione degli indirizzi IP è solamente uno dei molti fattori presi in considerazione dai filtri AntiSpam, ma ha ancora peso, soprattutto in relazione ai fenomeni di spam più eclatanti.

La **tentazione di cambiare IP** in seguito ad una classificazione

negativa, o in seguito alle evidenze di un decadimento della reputazione, è sempre molto forte.

È necessario però riflettere sul fatto che la reputazione dell'indirizzo IP **non è un fattore casuale**, ma viene generata in seguito a segnalazioni, comportamenti anomali e via dicendo: se non si interviene alla radice, **analizzando e cambiando i comportamenti** che hanno portato alla classificazione, cambiare IP (o dominio) è una soluzione che **può funzionare solo a brevissimo tempo**.

I moderni filtri AntiSpam sono **"diffidenti"**: se improvvisamente cominciano a ricevere email da un IP o un dominio che non conoscono, **di base avranno scarsa fiducia** e assegneranno una bassa reputazione.

È importante quindi capire quale sia **il problema di fondo** (*perché gli utenti non interagiscono? perché ci sono segnalazioni di abuso? le mie newsletter sono interessanti? le invio al giusto segmento di utenti?*) e cominciare a **comportarsi meglio**, in attesa che i filtri ne prendano atto.

Purtroppo, come nei rapporti umani, è sicuramente più difficile riconquistare la fiducia dopo averla persa, che guadagnarla la prima volta.

VOXmail utilizza centinaia di propri IP, condividendoli tra i clienti. L'autenticazione avviene utilizzando **chiavi DKIM e record SPF di VOXmail**, che si assume l'onere e la responsabilità di monitorare i propri clienti, prevenendo abusi e mantenendo **un'ottima base reputazionale**.

3.5 Le liste di invio

Il database degli iscritti rappresenta una ricchezza fondamentale, che è bene curare con costanza ed attenzione.

Innanzitutto è fondamentale che la lista dei destinatari sia stata creata utilizzando **strategie di database corrette** e che quindi gli utenti **siano effettivamente interessati** alle comunicazioni che si invieranno.

Una costruzione poco accorta - o **l'acquisto incauto di liste altrui** - può portare ad una serie di problemi piuttosto seri, dovuti alla presenza di numerosi indirizzi non più validi o peggio spamtraps.

Caselle inesistenti

Tentare di inviare un numero elevato di email a indirizzi non esistenti (*errati, non più attivi*) è un fattore **molto penalizzante**, che quasi tutti i filtri AntiSpam prendono in considerazione per calcolare la vostra reputazione.

Obsolescenza della lista

Nel mercato consumer esiste un **ricambio di indirizzi email** molto elevato, poiché molti utenti passano facilmente da un operatore ad un altro, in base allo spazio offerto, alle funzionalità disponibili, o semplicemente perché la vecchia casella **è ormai saturata dalla spam.**

Nel mercato business **c'è un ricambio più lento**, dovuto al normale avvicendamento di ruoli all'interno di aziende, ad eventuali cambi di lavoro, o in seguito a chiusura di attività, **evidente soprattutto in periodi di crisi**.

È del tutto normale aspettarsi, nell'arco di 12 mesi, una **contrazione valutabile fra il 2% e il 6% degli indirizzi effettivamente funzionanti.**

La contrazione media di una lista, a partire da queste valutazioni, **a distanza di 5 anni** diventa quindi tra il **10% e il 30%.**

SpamTrap

Un altro valido motivo per mantenere pulita e "in ordine" la propria lista è quello di evitare di incappare nelle spamtrap, **vere e proprie trappole**, che consentono ai filtri di individuare, con ragionevole certezza, chi fa uso poco accorto **di indirizzari non acquisiti correttamente**.

La Spamtrap può avere diverse nature: può essere, ad esempio, un **indirizzo inesistente** inserito ad arte in alcune pagine web, in modo che **programmi automatizzati lo trovino** e lo inseriscano nelle liste generate a puro scopo di spam o destinate alla vendita a terzi.

La ricezione di email a questi indirizzi è in automatico **segnalata al gestore della spamtrap**, che prenderà le opportune misure, spesso molto drastiche.

In altri casi la SpamTrap è una casella realmente esistente, ma **abbandonata e dismessa** da vari anni. Il gestore provvede per un periodo ragionevolmente lungo ad **informare chi invia email a questo indirizzo della sua dismissione**; passato questo periodo, la casella viene trasformata in **"trappola"**.

3.6 Manutenzione delle liste di indirizzi

Per evitare che la propria lista sia colpita dai pericoli identificati nel capitolo precedente, è sufficiente seguire alcuni accorgimenti.

1. In **fase di acquisizione** di un nuovo iscritto, verificare l'indirizzo email, utilizzando il **Confirmed Opt-in**.
   Questo metodo, consigliato dal Garante della Privacy, impedisce che **spamtrap** finiscano nel vostro database.

2. La pulizia della lista è fondamentale: continuare a **scrivere a caselle inesistenti** può essere poco costoso in termini economici ma **costosissimo in termini di reputazione**.

3. **Mantenere viva la lista**: mandate almeno una email ogni 6 mesi a tutti, in maniera da ricordare ai vostri iscritti e ai filtri AntiSpam la vostra esistenza. **Se inviate troppo di rado**, aumentano drasticamente le possibilità che qualcuno dei vostri vecchi iscritti, non ricordandosi più di voi, **vi segnali come spammer**, anche se in origine vi aveva dato il consenso ad essere contattato.

Confirmed Opt-in

Sistema che prevede l'invio di una email all'indirizzo che chiede l'iscrizione, confermandola solo quando viene cliccato il link presente nel testo del messaggio, verificandone così correttezza e proprietà.

Ricordate che non è possibile individuare una spamtrap, dal momento che chi gestisce questi indirizzi fa di tutto per mantenerli segreti. **Prevenire, in questo caso, è molto meglio che curare.**

VOXmail implementa il **Confirmed Opt-in** come unico metodo di acquisizione degli indirizzi e **pulisce in automatico** le vostre liste ad ogni invio.

3.7 Stanchezza della lista

La corretta acquisizione e il successivo mantenimento della lista sono i primi passi fondamentali per evitare di attirare l'**attenzione dei filtri antispam**. A lungo andare però anche il database costruito più correttamente può mostrare **segni di stanchezza**, che se sottovalutati possono avere ripercussioni importanti.

La **"stanchezza"** di un contatto è, in sostanza, il grado di **mancata interazione con i nostri invii**, valutata sul medio periodo.

Se un destinatario **non apre e non clicca** nostre newsletter da **oltre dieci invii**, è molto facile che **non sia interessato** a quello che scriviamo, oppure che, semplicemente, non siamo stati in grado di raccogliere e capitalizzare **l'interesse mostrato al momento dell'iscrizione**.

Il perdurare e l'accumularsi di situazioni di stanchezza può ripercuotersi sulla reputazione, andando quindi ad avere **effetto negativo sulla deliverability**: come già detto, ogni email ignorata può influire sui rating calcolati dai filtri antispam, fino a decretare una classificazione negativa delle nostre missive.

Il vero rischio è quello che le ripercussioni di tale classificazione negativa vadano ad impedire la corretta ricezione da parte di chi invece sarebbe molto interessato a leggere le nostre newsletter.

È bene tenere d'occhio questi segnali, **filtrare e raccogliere** in gruppi i **destinatari "stanchi"**, cominciare a **spedire loro meno spesso**, oppure fare **invii mirati**, tentando di risvegliare l'interesse, per poi andare ad estrarre dal gruppo gli utenti che, interagendo, **sono usciti dallo stato di sonnolenza**.

VOXmail sta sperimentando **automatismi e strumenti** in grado di aiutare nell'individuazione e nella gestione dei **contatti stanchi**.

3.8 Le newsletter

Abbiamo già detto che, per garantire la deliverability, è fondamentale che le comunicazioni generino interesse in chi le riceve. Esistono però alcuni accorgimenti "tecnici" che vanno osservati per evitare di attirare l'attenzione dei filtri AntiSpam:

Peso della email

Alcuni filtri AntiSpam considerano anche il peso (*le dimensioni*) dell'email ai fini del filtraggio. In particolare dimensioni **superiori ai 100KB** portano ad un **calo percepibile del tasso di consegna** in posta in arrivo.

Formato "multipart"

Quando si inviano email in formato **HTML** è sempre bene utilizzare il formato **multipart/alternative** che prevede l'inserimento sia della versione HTML, sia di una versione **completamente testuale** della stessa email.

Oggi praticamente tutti i client di posta sono in grado di leggere una email HTML, ma la versione testuale continua ad avere un **certo peso per alcuni filtri**. L'inserimento della versione alternativa in testo semplice è una buona prassi che **molti software automatizzano**.

Link

Ogni indirizzo inserito in una newsletter è **attentamente esaminato dai filtri**. È buona norma evitare di inserire collegamenti a molti siti diversi nella stessa email. Sono da evitare collegamenti (e indirizzi sorgenti di immagini) **ai siti di affiliazione o che possano avere reputazione discutibile**. Sconsigliabile anche l'utilizzo di url-shortener.

Url Shortener

I servizi di Url-shortening consentono di creare indirizzi web brevi per pagine che avrebbero altrimenti uni indirizzo molto lungo.
Nati prevalentemente per l'uso nei Social Network, hanno il difetto di nascondere il reale sito di destinazione.

Immagini e testo

Evitare di inviare email composte di **una sola grande immagine**. I filtri AntiSpam raramente analizzano i contenuti delle immagini, di conseguenza, se hanno pochi elementi per valutare una email, tendono a dare giudizi negativi.

Inoltre, gli utenti che usano client che **bloccano le immagini** in questo caso si troverebbero di fronte ad una email vuota, che quindi avrà **maggiori probabilità di venir cestinata**.

È importante non usare **caratteri troppo grandi e colorati**, troppe maiuscole o troppi simboli di punteggiatura (*sequenze di punti esclamativi*).
Questi espedienti eccessivamente "promozionali" attirano le attenzioni di alcuni filtri AntiSpam.

Mittente

Il destinatario deve essere in grado di **riconoscerci**: utilizzare un nome mittente costante e significativo agevola la riconoscibilità.

Stesso discorso vale per **l'indirizzo email mittente**: utilizzate lo stesso usato per la **conferma di iscrizione** o comunque quello che più probabilmente pensiate **compaia nella rubrica del destinatario**. Se l'email proviene da un contatto in rubrica è molto meno probabile che sia classificata come spam.

No Reply

Alcuni filtri AntiSpam hanno regole apposite per penalizzare la sequenza "noreply" o "no-reply" negli indirizzi mittente e, fattore ancora più importante, per migliorare la propria reputazione è bene incentivare le risposte, non impedirle.

Il fatto che una persona risponda ad una vostra email potrebbe essere la garanzia che le vostre future email non arriveranno più in spam alla sua casella.

Se volete comunicare senza che chi ascolta possa rispondere, fate web advertising, comprate spot in TV o alla radio. L'email marketing è **marketing relazionale**, e per sua natura apre un canale diretto uno ad uno, che è **indispensabile e utile gestire**.

Link di disiscrizione

Un contatto che non riesce a disiscriversi facilmente dalla newsletter sarà un contatto che, con tutta probabilità, la segnalerà come spam, incidendo in maniera pesante sulla **reputazione del mittente.**

Per questo è importante mettere **bene in evidenza il link di disiscrizione**: mai cercare di impedire ad un utente di disiscriversi o complicargli la vita per farlo. È molto meglio avere un destinatario in meno che un destinatario inattivo o, peggio, arrabbiato.

Frequenza di invio

Trovare la **giusta cadenza** di invio è fondamentale: il vostro lettore più appassionato potrebbe essere felicissimo di leggere una vostra **newsletter promozionale alla settimana** ed invece arrabbiarsi se ne riceve **dieci al giorno**.

Tenete sempre presente che più email vengono ignorate (o peggio cestinate) più è facile che quelle successive finiscano in spam.

Tassi di apertura e clic

Nel corso del tempo, su un database consolidato, è normale che questi due indicatori **tendano a calare** (*le passioni e gli interessi cambiano*), ma non devono avere crolli o variazioni incontrollate ed eccessive.

Buona norma è quella di fare un gruppo dei vecchi destinatari inattivi e cercare di riattivarli mandando loro una offerta particolarmente significativa. Nel caso non reagissero, smettete di mandare loro email, oppure dilazionate maggiormente nel tempo le email.

VOXmail automatizza sia la generazione dei messaggi in **formato multipart**, sia la procedura di **disiscrizione facilitata** inserita in ciascuna email inviata.

4. VERIFICHE E CONTROLLI

4.1 Posso verificare la mia lista?

Esistono programmi e servizi che fanno una verifica delle liste email per "pulirle" prima di effettuare un invio. Questi programmi possono fare alcuni controlli:

1. **Verifica sintattica dell'indirizzo email.**
   Esistono delle regole precise di formattazione degli indirizzi email, per cui è piuttosto semplice effettuare questo tipo di controllo già in fase di acquisizione del contatto.

2. **Verifica dell'esistenza del dominio e verifica che sia configurato per ricevere email.**

3. **Contattare il mail server e chiedere le "verifica" dell'indirizzo email.**
   Nonostante questo tipo di verifica sia previsto dalla specifica, la maggior parte dei mail server non lo implementa, proprio per evitare un abuso da parte degli spammer.

4. **Contattare il mail server e provare ad inviare una email reale, salvo poi rinunciare all'invio poco prima della conferma.**
   Questo controllo non si differenzia sostanzialmente da un invio effettivo, anzi, alcuni provider puniscono i tentativi di invio email non completati, considerandoli un indicatore di "spamminess".

VOXmail si occupa automaticamente della **verifica sintattica** in fase di caricamento di una lista o iscrizione del singolo contatto. Le rimanenti verifiche vengono effettuate **contestualmente al primo invio**.

4.2 Posso sapere in anticipo se la mia newsletter è corretta?

È sicuramente possibile e consigliabile **fare dei test** prima degli invii reali, ma è importante **comprenderne i limiti.**

Uno degli **"spam test"** più comuni è il check effettuato dando in pasto l'email ad un popolare software AntiSpam, chiamato **SpamAssassin**.

Questo tipo di approccio ha **diversi problemi**:

1. l'email analizzata da SpamAssassin in questo modo **non viene realmente spedita** e quindi non è possibile controllare alcune informazioni fondamentali (*come, ad esempio, l'IP che la spedisce*).

2. Yahoo, Gmail, Libero, Alice, Outlook.com e **la maggior parte dei grossi provider di posta** non usa SpamAssassin, ma altri sistemi che forniranno, nei fatti, **risultati molto diversi**.

3. Anche chi usa SpamAssassin non è assolutamente detto che lo utilizzi con **la stessa configurazione** (*la configurazione incide in maniera fondamentale sul risultato*) e, comunque, anche a parità di configurazione, i risultati possono variare di molto a causa dei database interni che SpamAssassin costruisce man a mano che riceve email e tramite i quali **può cambiare il suo comportamento**.

Un altro metodo "empirico" di test è **l'invio diretto della newsletter ad un indirizzo email reale**. Anche in questo caso ci sono diversi limiti:

1. Ogni provider utilizza sistemi AntiSpam differenti, per cui bisognerebbe **avere una casella di posta per ogni provider**, cosa fattibile per quelli gratuiti, più **complicata o impossibile** per quelli a pagamento o aziendali.

2. Alcuni provider **modificano il comportamento da casella a casella**, quindi anche provando ad inviare l'email ad una loro casella non avremo la certezza che il comportamento sarà lo stesso per le altre loro caselle (*Gmail ne è il classico esempio*).

3. L'invio dell'email di test, **almeno in termini di "volume"**, è molto diverso dall'invio della email reale.
   Il filtro AntiSpam farà quindi considerazioni basate **solamente su quella email specifica**, mentre nell'invio effettivo potrà fare considerazioni basate sul **comportamento dei primi destinatari** che la riceveranno: la sua decisione relativamente all'email massiva potrebbe essere differente da quella relativa all'email di test.

L'operazione di test preventivo è **quindi molto dispendiosa** e non completamente affidabile.

Vi consigliamo di investire il vostro tempo per implementare le **"best practice"** indicate nei capitoli precedenti, partendo dalla **corretta raccolta del consenso**, proseguendo con la **costante pulizia della lista**, senza perdere di vista il **monitoraggio dei risultati**.

5. IN CONCLUSIONE

Speriamo che questo excursus piuttosto esteso nel mondo dei **filtri Antispam** sia servito a farvi un'idea un po' più precisa del percorso ad ostacoli che ogni email affronta prima di arrivare alla **casella del destinatario**.

In questa edizione aggiornata abbiamo voluto approfondire alcuni aspetti tecnici: parlando di email marketing è davvero utile poter comprendere i meccanismi che stanno dietro ai filtri, proprio per **evitare errori** che potrebbero avere strascichi molto lunghi.

Riassumendo in maniera brutale, **a prescindere dalle tecnologie**, sempre in evoluzione, per riuscire ad inviare email massive **senza aver paura dei filtri** è necessario:

- **Acquisire gli indirizzi** destinatari in maniera corretta
- Inviare **comunicazioni interessanti** per il nostro target
- Rispettare la volontà dei destinatari (**link di disiscrizione**)
- **Analizzare** i risultati, correggere, segmentare, rianalizzare
- Selezionare **un partner tecnologico affidabile** (ESP)

Come spesso accade, **il buon senso è sempre il miglior alleato** che si possa avere: diffidate delle scorciatoie a buon prezzo, per ottenere gli ottimi risultati che l'email marketing può dare sono sempre necessari **impegno e perseveranza**.

Email Marketing e Filtri Antispam
Revisione: 2.0
Data: 15 Settembre 2016
Autori: Stefano Bagnara e Alessandro Grazioli
Collana: La biblioteca di VOXmail
www.voxmail.it
biblioteca@voxmail.it

VOX mail

INVIO NEWSLETTER FACILE & VELOCE

Come funzionano i filtri AntiSpam?
Quando intervengono e per quali motivi?
Che ruolo hanno l'autenticazione e la reputazione?

Impara a gestire la tua lista contatti e pianifica le tue comunicazioni massimizzandone rilevanza ed efficacia.

Email Marketing e Antispam

Edizione 2.0

www.voxmail.it - biblioteca@voxmail.it