

Come funziona la Posta Elettronica ?

Una breve spiegazione per capire come mai a volte le mail inviate non arrivano o sono considerate spam.

Un po' di Storia

La Posta Elettronica, E-Mail in inglese, è stata una delle primissime funzionalità che fu creata per l'allora rete di computer americani (all'inizio) delle università, centri di ricerca e installazioni militari, la famosa Arpanet.

Venne inventato un "modo di comunicare" (un "protocollo" in termini tecnici) per scambiarsi mail tra vari computer, e gli venne dato il nome SMTP, acronimo di Simple Mail Transfer Protocol.

La Rete di allora era un insieme chiuso, molto piccolo, solo pochissimi computer ben selezionati ed identificati potevano usarla e quindi scambiarsi mail, quindi non c'era bisogno di sicurezza, non c'erano estranei, niente spam (posta indesiderata) e tantomeno truffatori, venditori vari, ecc.

Un computer si connetteva ad un altro dicendo "eh io sono ABC, c'è posta per il tuo utente XYZ, eccola qua..". Nessuno metteva in dubbio che ABC non fosse ABC, non c'era motivo di dubitare e neanche che il contenuto non fosse più che legittimo.

Poi la Rete si ingrandì, sempre più computer venivano collegati, sempre più sistemi civili (la Rete militare venne separata) e nel corso del tempo l'evoluzione portò all'Internet che conosciamo adesso e come tutte le cose umane così grandi anche piena di cose "brutte", ladri, truffatori, spammers, ecc.

Ma il protocollo SMTP restò pressochè uguale.

Certo venne un po' migliorato, aggiunta un po' di sicurezza (es. le password) e un po' di controlli, ma sotto sotto il "cuore" e soprattutto il principio base restò lo stesso, principalmente per motivi di compatibilità.

Quindi non c'era davvero un modo per essere sicuri che ABC fosse davvero ABC !

Di conseguenza con la diffusione pubblica di grossi provider (fornitori) di accesso ad Internet e in generale di fornitori di caselle di posta, più o meno gratuitamente, il problema della sicurezza e qualità della email divenne un enorme problema.

Letteralmente chiunque poteva connettersi ad altri e dire "eh io sono presidente@casabianca, ho una mail per il tuo utente mariorossi@libero.it, eccola" e non c'era modo di impedirlo, di distinguere la vera Casa Bianca da un truffatore diffusore di virus informatici o venditore di pillole blu...

Quindi i grossi provider internazionali, quali ad esempio Google Mail (Gmail), Yahoo, Hotmail (Microsoft) e anche i nostrani Libero.it, Virgilio.it e infiniti altri per sopravvivere, per cercare di limitare i danni (costi, reputazione, ecc.) dovettero trovare nuovi sistemi per filtrare la mail buona, legittima dallo spam, la mail truffaldina e simili.

Adottarono quindi degli strumenti più o meno sofisticati ma, inevitabilmente, mai precisi al 100%.

E' un vero "microcosmo" il mondo dei filtri antispam, e ci vorrebbero ore per spiegare nel dettaglio tutte le tecniche utilizzate (a volte molto sofisticate, con sistemi di Intelligenza Artificiale per analizzare i contenuti, i tempi, le frequenze, i destinatari, ecc.),, ma i principi cardine sono:

1. una mail può arrivare SOLO dai server del provider della mail stessa, esempio, una mail di libero.it puo' SOLO arrivare dai server di libero.it, non dai server di Mario Rossi o dai server di gmail.com ecc.
2. la mail non può contenere certe "parole chiave" che potrebbero essere indice di spam (classico esempio: Viagra, ecc.) o scritte tutte in maiuscolo ecc.
3. la mail non può avere come allegato un programma eseguibile (un file .exe per Windows per esempio), potrebbe essere un virus o altro tipo di malware.

Ovviamente ogni provider è libero di scegliere quali filtri usare e soprattutto COSA fare quando si pensa di aver trovato una mail di spam: rifiutarla immediatamente o accettarla ma metterla nella cartella di SPAM del destinatario.

Inoltre questi filtri sono variabili nel tempo, la mail che oggi è considerata accettabile domani potrebbe essere bloccata, è una continua lotta tra provider e spammers e truffatori, in costante evoluzione.

E' un business miliardario quello dello spam, ci sono dietro interessi enormi delle bande criminali, non è diverso dal mondo dei documenti falsi, del contrabbando, traffico di droga ecc.

Si, ok ma in Psicogest?

Per offrire ai propri clienti la possibilità di inviare email direttamente da dentro il programma cercando di non inciampare nei filtri antispam Psicogest ha due funzionalità:

- A. la mail che viene inviata ha come mittente un indirizzo su "@mail.psicogest.it", in modo che il suddetto punto 1 non sia contravvenuto.
Infatti "mail.psicogest.it" è un dominio (uno "spazio") Internet di proprietà di Psicogest e qualsiasi mail con tale indirizzo può essere identificata correttamente.

B. la possibilità di scegliere di usare il servizio SMTP del proprio provider (funzionalità SMTP personalizzato in Psicogest, pagina Impostazioni Email)

In questo modo la mail non "esce" dai server di Psicogest bensì dai server del provider (es. libero.it) dell'utente, in modo del tutto identico alle mail che il cliente normalmente spedisce dal proprio computer, telefono, ecc.

La funzionalità A è quella attiva di default, perché non comporta alcun settaggio da parte del cliente. In genere offre una buona "reputazione" della mail in uscita, ma ovviamente si è sempre soggetti alle regole di cui sopra.

La funzionalità B è la migliore, l'UNICA vera "soluzione" al problema, essa replica lo stesso modo usato dal cliente quando manda una mail dal proprio computer, telefono, tablet o altro. È il modo più corretto, più "legale", più "sicuro" di inviare una mail.

Ma allora perché non si fa così sempre e per tutti?

Bella domanda: i motivi sono principalmente due:

1. bisogna configurare in Psicogest le giuste impostazioni per usare tale funzionalità, a volte per il cliente poco pratico di questione informatiche non è così semplice
2. talvolta i provider stessi sono ultra paranoici e bloccano gli invii pure in questo modo! Perché? Perché "vedono" che la connessione al loro server di posta arriva da un indirizzo IP (indirizzo internet, i 4 numeretti separati da punti) che NON è l'abituale indirizzo dal quale arriva quel loro utente.
Esempio: mariorossi@libero.it si connette da casa sua ai server di Libero.it per spedire la sua posta, casa sua ha un indirizzo IP 1.2.3.4, tutto ok fin qui.
Ma negli stessi momenti Libero.it vede che una connessione che dice di essere mariorossi arriva ANCHE dall'indirizzo IP 4.5.6.7 (uno dei sistemi di Psicogest), e considera sospetta la cosa!
(Un po' come le società delle carte di credito quando vedono che c'è una transazione dalla Russia mentre 5 minuti fa ne avete fatta una a Milano.. cosa sospetta!).

Ma quindi come se ne esce?

Non se ne esce; o meglio non vi è certezza assoluta con nessuna modalità che la propria mail giunga al destinatario.

Si possono adottare una serie di accorgimenti, funzioni, suggerire ai provider "ehi, guarda che PsicoGest recapita fatture di prestazioni sanitarie, non vende bitcoin!" (non con queste parole, ma il senso è quello di "ri-nobilitare" i server di PsicoGest agli occhi dei provider), ma non vi è comunque mai la certezza.

Diciamo che il tasso di “fallimenti” con l’invio Standard di mail da PsicoGest (quindi non con Configurazione SMTP correttamente attivato) è piuttosto basso, inferiore al 10%; tuttavia, se immaginiamo un traffico medio giornaliero delle mail che escono da PsicoGest (centinaia di migliaia), il numero assoluto di fallimenti appare più consistente.

Di qui la realizzazione di un sistema “estremo”, che bypassa la questione mail: il link diretto. Ovvero la possibilità di generare un codice unico, un link, che può essere copiato ed incollato in un SMS, un Whatsapp, Telegram, ecc... che fornisce al cliente/ paziente accesso diretto alla propria fattura.

Ci auguriamo che questi chiarimenti possano essere stati d’aiuto e che, soprattutto, possano essere stati per i nostri utenti un “piccolo apprendimento” di meccanismi che stanno dietro a PsicoGest. Un sistema tutt’altro che semplice (nel suo “dietro le quinte”), soprattutto nel momento in cui deve interfacciarsi con il mondo esterno: STS, SDI, ma anche le “semplici” mail.

La Divisione Tecnica di PsicoGest