Da Wikipedia, l'enciclopedia libera

E-MAIL

La **E-Mail** (abbreviazione di *Electronic Mail*, in italiano: **posta elettronica**) è un servizio internet grazie al quale ogni utente può inviare o ricevere dei messaggi. È l'applicazione Internet più conosciuta e più utilizzata attualmente. La sua nascita risale al 1972. È la controparte digitale ed elettronica della posta ordinaria e cartacea. A differenza di quest'ultima, il ritardo con cui arriva dal mittente al destinatario è normalmente di pochi secondi/minuti. Lo scopo del servizio di e-mail è il trasferimento di messaggi da un utente ad un altro

Ciascun utente può possedere una o più *caselle e-mail*, su cui può ricevere messaggi, che vengono conservati per lui. Quando lo desidera, l'utente può consultare il contenuto della sua casella, organizzarlo, inviare messaggi a uno o più utenti.

L'accesso alla casella di posta elettronica è normalmente controllato da una password o da altre forme di autenticazione.

La modalità di accesso al servizio è quindi asincrona, ovvero per la trasmissione di un messaggio non è necessario che mittente e destinatario siano contemporaneamente attivi o collegati.

La consegna al destinatario dei messaggi inviati *non* è garantita. Nel caso un server SMTP non riesca a consegnare un messaggio che ha ricevuto, tenta normalmente di inviare una notifica al mittente per avvisarlo della mancata consegna, ma anche questa notifica è a sua volta un messaggio di e-mail (generato automaticamente dal server), e quindi la sua consegna non è garantita.

Il mittente può anche richiedere una *conferma di consegna* o *di lettura* dei messaggi inviati, ma il destinatario è normalmente in grado di decidere se vuole inviare o meno tale conferma. Il significato della conferma di lettura può essere ambiguo, in quanto aver visualizzato un messaggio per pochi secondi in un client non significa averlo letto, compreso o averne condiviso il contenuto.

- *Subject:* (*Oggetto:*) dovrebbe contenere una breve descrizione dell'oggetto del messaggio. È considerata buona educazione utilizzare questo campo per aiutare il destinatario a capire il contenuto del messaggio.
- *From:* (*Da:*): indirizzo e-mail del mittente
- *To:* (*A:*): indirizzi e-mail dei destinatari
- *Cc:* (Carbon Copy, *Copia Carbone:*): indirizzi e-mail dei destinatari in copia conoscenza.
- *Bcc:* (Blind Carbon Copy, *Copia Carbone Nascosta* (Ccn): indirizzi e-mail dei destinatari in copia conoscenza nascosta, ovvero destinatari che riceveranno il messaggio ma il cui indirizzo non apparirà. Questa è in realtà una *pseudo-intestazione*, in quanto è visibile solo al mittente del messaggio, e per definizione non viene riportata nei messaggi inviati ai destinatari. I destinatari in Bcc appaiono solamente nella busta. Questo campo è talvolta nascosto di default, ed in alcuni client e-mail in lingua italiana può assumere il nome "Ccn".

Visibilità dei destinatari

Gli indirizzi dei destinatari diretti (*To:*) e di quelli in copia conoscenza (*Cc:*) sono ugualmente visibili a tutti i destinatari.

La scelta di mettere un destinatario in uno dei due campi è legata al ruolo che le persone hanno riguardo all'argomento del messaggio. Ad esempio, se un messaggio richiede di eseguire un compito, si intende che si chiede a chi è destinatario diretto di eseguirlo, mentre i destinatari in copia conoscenza vengono informati che questa richiesta è stata fatta, ma non ci si aspetta che siano loro ad eseguire il compito.

Gli indirizzi dei destinatari in copia conoscenza nascosta non appaiono nel messaggio consegnato ai destinatari. Questo consente di fatto di far sapere a terzi che cosa si sta dicendo e a chi senza che i destinatari "ufficiali" ne siano a conoscenza. 'Mettere in CC' o 'in CCN' è locuzione diffusa negli ambienti lavorativi e nei gruppi sociali organizzati.

Quando l'e-mail viene utilizzata per diffondere messaggi a molte persone che non si conoscono tra loro (ad esempio comunicati pubblici, annunci, messaggi spiritosi più o meno utili), il fatto che ciascun destinatario possa sapere chi sono gli altri destinatari e i loro indirizzi non è in generale opportuno, per ragioni di privacy e di sicurezza.

In particolare, se si invia un messaggio ad un gran numero di persone che non necessariamente si conoscono tra di loro, costoro non necessariamente saranno d'accordo che il loro indirizzo, ed il fatto che hanno ricevuto quel messaggio, sia reso noto ad estranei.

Inoltre, molti worm si propagano per e-mail, e utilizzano gli indirizzi presenti nei messaggi per diffondersi. Inviare un messaggio con gli indirizzi dei destinatari in chiaro significa quindi esporre tutti i destinatari ad un ulteriore rischio di contagio se uno di loro viene contagiato.

Per ovviare a questo problema, è consigliabile utilizzare in questi casi il *Bcc:*, oppure una mailing list.

Abusi

Il protocollo SMTP è privo di strumenti per impedire abusi del sistema di posta elettronica, in particolare non esistono strumenti semplici ed efficaci per controllare quali messaggi vengono consegnati nella casella di un utente (autorizzazione), ed inoltre non esiste autenticazione del mittente riportato da un messaggio. Questo comporta la possibilità di diversi tipi di abusi.

Il principale utilizzo improprio dell'e-mail è lo spam, l'invio massiccio a molti utenti di messaggi indesiderati, in genere di natura pubblicitaria-commerciale. Secondo alcune fonti, l'incidenza di questi messaggi raggiungerebbe i due terzi del traffico totale di posta elettronica.

Un altro fenomeno negativo è costituito dalle catene di sant'Antonio, messaggi che contengono informazioni allarmanti, promesse di facili guadagni o vere e proprie bufale, ed invitano ad inoltrare il messaggio ai propri conoscenti, finendo talvolta per circolare per mesi o per anni.

Esiste inoltre la possibilità di falsificare il nome e l'indirizzo del mittente visualizzati nel programma client del destinatario, inducendo l'utente a ritenere attendibile un messaggio del tutto falso. Questa vulnerabilità viene usata per costruire vere e proprie truffe o scherzi che si basano sulla fiducia che la maggior parte degli utenti erroneamente ripone nel "mittente" di un messaggio di posta elettronica. Anche i worm che si replicano per posta elettronica usano questo meccanismo, allo scopo di indurre gli utenti a provare interesse o a prestare fiducia in un messaggio, in modo che lo aprano ed eventualmente installino allegati infetti.