

Spam, la posta spazzatura

(i tutorial di Alessandro de Simone)

Copyright Alessandro de Simone 2003 – 2004 – 2005 (www.alessandrodesimone.net) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore (spam@alessandrodesimone.net) per gli accordi del caso.

Copyright Alessandro de Simone 2003 – 2004 – 2005 (www.alessandrodesimone.net) – No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document – even if partially – without author's written authorization. Websites and publishing house who wish to employ this document must write the author (spam@alessandrodesimone.net).

Clicca sul collegamento specifico per consultare altri Tutorial attinenti al medesimo argomento:

"**Spam, la posta spazzatura**" (questo Tutorial) - Considerazioni generali sulle e-mail, non richieste, che riceviamo quotidianamente.

"**MailWasher**" - Primi passi sull'uso del programma MailWasher prendendo come riferimento la versione gratuita.

"**MailWasher Pro 3.3**" - Impostazione dei parametri più importanti della versione MailWasher Pro 3.3

"**MailWasher - Uso del programma**" - Caratteristiche più importanti di MailWasher prendendo come riferimento la versione Pro 3.3

"**MailWasher - I messaggi e gli avvisi**" - Descrizione dei messaggi che compaiono usando MailWasher

"**Benign**" - Il programma che previene i danni provocati da e-mail contenenti codici dannosi per il nostro PC.

Che cos'è lo spam

Per comprendere a fondo come agisca lo spam occorre anzitutto sapere che cosa sia. Come è noto, per **Spam** si intende generalmente la cosiddetta "posta-spazzatura", termine generico che ovviamente non possiamo qui accettare in un'accezione così semplicistica. In linea di massima ognuno di noi può ricevere, tramite il programma di posta elettronica abitualmente utilizzato (*Outlook Express* oppure *Eudora*, tanto per citare i più comuni), e-mail di ogni tipo, provenienti dalle fonti più disparate. Per quanto riguarda le sole e-mail, quelle da considerare realmente utili (ma soprattutto innocue per il nostro PC) sono le mail che riceviamo da amici fidati o da persone la cui competenza e prudenza sia considerata affidabile.

Questo spazio è disponibile per il tuo messaggio pubblicitario.

Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.

[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.

[Clic ici](#) pour détail ou [Contact](#)

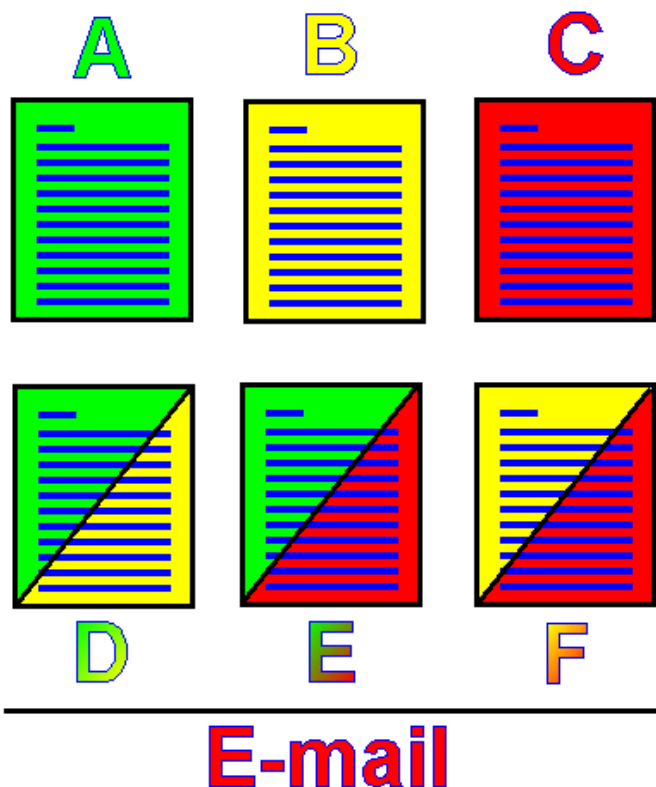


Figura 1. Le sei tipologie di e-mail.

Le e-mail...

In figura 1 sono rappresentate sei tipologie di e-mail, indicate con lettere da "A" a "F" e caratterizzate da colori diversi, tradizionalmente rappresentativi del grado di pericolo: verde (nessun pericolo da segnalare), giallo (da considerare con attenzione), rosso (altamente pericolose).

Tipo A (figura 1, A). Sono le mail prive di trojan o virus e contenenti quindi informazioni che realmente abbiamo richiesto o che ci aspettiamo di ricevere. Sono le mail che ci vediamo recapitare da amici, conoscenti, colleghi di ufficio, newsletter esplicitamente richieste da una nostra precedente sottoscrizione e così via.

Tipo B (figura 1, B). Sono le mail che, pur se non esplicitamente richieste, ci vengono inviate perché, per esempio,

qualcuno ha ricevuto il nostro indirizzo e-mail da una persona nota a entrambi oppure perché qualcuno ha digitato il nostro indirizzo e-mail in modo erroneo (per esempio: *pippo34@libero.it*) ritenendo invece di inviarlo a un'altra persona (*pippo35@libero.it*). Molto più spesso sono messaggi pubblicitari provenienti da fonti che hanno avuto il nostro indirizzo nella maniera più disparata (amici di amici, scansioni sul web, agenzie di fornitura specializzate nella ricerca di indirizzi e così via). Sono potenzialmente pericolose perché virus e trojan si diffondono proprio grazie a persone che si comportano in modo superficiale quando ricevono – e aprono – e-mail non richieste.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.
[Clic ici](#) pour détail ou [Contact](#)

Tipo C (figura 1, C). Sono mail **realmente pericolose**, inviate in malafede da persone che intendono attaccare il nostro PC o diffondere un'epidemia. Queste mail contengono codice maligno che riesce a svilupparsi approfittando di alcune falle presenti nei client (programmi) di posta elettronica o nella superficialità con cui gli utenti sotto-utilizzano le pur sofisticate impostazioni di sicurezza che li caratterizzano. È noto, per esempio, che in una precedente versione di *Outlook Express* era sufficiente visualizzare l'anteprima di una mail contenente codice maligno per infettare il PC. Ciò era dovuto a una particolare procedura informatica, basata sui famigerati *ActiveX*, incorporata in *Outlook Express*. Un particolare *ActiveX*, nonostante fosse stato progettato dalla stessa Microsoft, presentava una falla di sicurezza che veniva abilmente sfruttata per diffondere virus. Si dice che il problema sia stato rimosso nelle versioni più recenti di *Outlook Express*, ma non è detto che nel futuro venga scoperta, e sfruttata, una nuova falla per la diffusione dei virus.

Tipo D (figura 1, D). Sono mail provenienti (in apparenza) da nostri conoscenti, ma molto più spesso arrivano alla nostra casella da parte di amici dei nostri amici. Spieghiamoci meglio: quante volte, entrando in possesso di una notizia che riteniamo particolarmente interessante (sia questa una semplice barzelletta, la data di una trasmissione TV da vedere "assolutamente", una documentazione politica, una conferenza, una manifestazione artistica o sportiva) abbiamo ritenuto di fare cosa gradita inviandola a tutti i nostri amici e conoscenti? E in che modo inviamo loro tali informazioni? Ovvio: inserendo tutti i rispettivi indirizzi di posta elettronica nel campo *A:* oppure *CC:* del nostro client di posta elettronica. In questo modo - senza saperlo e (spero) senza rendervene conto - create una delle famigerate catene di S. Antonio. Tra i conoscenti dei vostri conoscenti ai quali avete indirizzato la mail, con gli indirizzi bene in evidenza, ci sarà sicuramente qualcuno che, anche se in perfetta buona fede, aggiungerà tutti gli indirizzi nella propria rubrica, con l'intenzione di utilizzarli per la prossima - inconsapevole o no - catena di S. Antonio. Ed ecco che il vostro indirizzo, che all'inizio era conosciuto solo da un avvocato di tutto rispetto o da un medico particolarmente discreto, giungerà prima o poi a quanti spacciano cocaina su Internet. Esagero? Forse sì, ma è meglio pensare che forse no...

Tipo E (figura 1, E). Questo tipo di mail è quello più insidioso perché apparentemente proviene da un amico (ecco perché è raffigurato per metà in verde) ma in realtà si tratta quasi sempre di un messaggio contenente codice maligno. Il messaggio quasi certamente è stato creato sul PC del nostro conoscente (infettato a sua insaputa) ed a noi inviato dallo stesso virus creato per utilizzare automaticamente la rubrica del programma di posta elettronica. Ovvio che, in questo caso, in realtà è il virus che ha inviato la mail; la responsabilità del vostro amico è limitata - si fa per dire - alla superficialità con cui apre le mail sconosciute (contenenti virus) o installa programmi di dubbia provenienza.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.
[Clic ici](#) pour détail ou [Contact](#)

Tipo F (figura 1, F). Si tratta di mail di provenienza non richiesta contenete intenzionalmente codice maligno. Viene distribuita da persone che, sperando di infettare milioni di PC, desiderano "semplicemente" passare agli onori(?) della cronaca. Alla categoria di "codice maligno" appartengono principalmente due tipi di e-mail. Del primo fanno parte le lettere che contengono script incorporati, vale a dire porzioni di programmi abilmente celati all'interno della stessa mail e, come tali, invisibili all'utente. Non si tratta di allegati (vedi dopo nel paragrafo specifico), ma di comandi che il PC è indotto ad eseguire non appena la mail viene aperta per la lettura (del tipo, tanto per semplificare: "cerca nel PC la parola *Bancomat*. Se questa è presente all'interno di un file di testo, cattura i successivi 200 caratteri e inviali all'indirizzo *CartaRubata@Ladro.com*). Alla seconda categoria appartengono i codici maligni inseriti all'interno dell'intestazione della mail, vale a dire in quella parte della lettera che contiene informazioni tecniche che l'utente di solito non legge mai. Il pericolo è duplice non solo per quest'ultimo motivo (a chi verrebbe in mente di controllare tutte le intestazioni delle mail che riceve?) ma anche perché il client di posta elettronica esegue alla lettera i comandi implicitamente presenti nell'intestazione stessa, ritenendo che siano affidabili. E' quindi sufficiente alterare la parte iniziale (in gergo definita "*MIME header*" per far eseguire – senza alcun controllo ulteriore – il file allegato alla mail che, presentandosi magari come un innocente file grafico o musicale, contiene in realtà un virus che si diffonde rapidamente grazie all'equivoco in cui è stato indotto il client.

...e gli allegati

Le mail singolarmente considerate, in realtà, non sono tanto pericolose come lo erano nel passato. Le falle più pericolose contenute nei programmi di posta elettronica sono ormai state corrette e non dovrebbero rappresentare un serio pericolo, almeno per gli utenti che aggiornano periodicamente i propri antivirus e firewall. Perché rappresentino un serio pericolo è però sufficiente che uno solo dei nostri amici (nel cui PC è memorizzato il nostro indirizzo di posta elettronica) sia superficiale o imprudente nelle normali operazioni di salvaguardia, affinché eventuali virus o trojan, benché obsoleti, riescano a raggiungere il nostro PC ed infettarlo (caso di figura 1 E).

Se, comunque, ci si può difendere con una certa semplicità dalle normali mail, non così è per gli allegati che a volte le corredano.

Anche in figura 2 ho indicato con il colore verde gli allegati "sicuri", in giallo quelli potenzialmente pericolosi e in rosso quelli sicuramente pericolosi. Nonostante la casistica sia molto simile a quella considerata nella descrizione delle semplici e-mail (figura 1) conviene approfondire il discorso.

Anzitutto c'è da dire che ad ogni e-mail può essere allegato un qualsiasi file, sia questo un semplice file di testo, una fotografia, un sofisticato documento (magari formattato con cura

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

Espace pour votre annonce.
[Clic ici](#) pour détail ou [Contact](#)

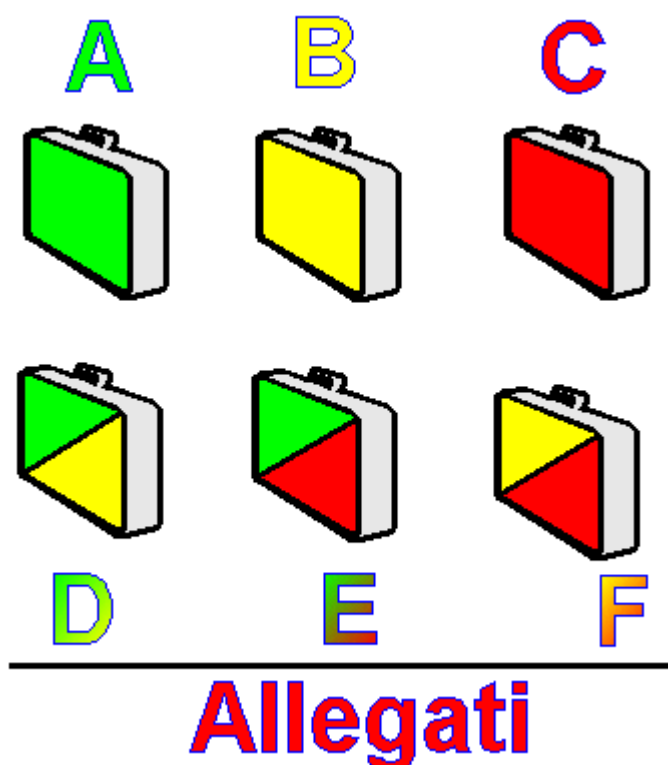


Figura 2. Le sei tipologie di allegati.

impossibile: esistono centinaia di programmi grafici che possono aver generato quella foto e non è possibile che sul nostro PC siano tutti presenti!). Grazie all'universalità del formato grafico, però, la software house che ha realizzato il programma di posta elettronica che noi usiamo abitualmente (come *Outlook Express*) lo correda del cosiddetto "visualizzatore". Si tratta di una parte del programma stesso, estremamente semplice e banale, che si limita esclusivamente a visualizzare la foto (o il disegno) senza consentire all'utente di elaborarlo ulteriormente. Tale opportunità, praticamente insignificante per ciò che riguarda i file di contenuto grafico (non esistono, almeno al momento, virus capaci di nascondersi in una fotografia e di attivarsi automaticamente non appena viene visualizzata) è invece di straordinaria importanza per ciò che riguarda i cosiddetti macro-virus. Sono, questi, programmi maligni che possono essere incorporati in normali documenti di *Word* o di *Excel* – in maniera del tutto invisibile all'utente finale (che si illude di consultare un normale documento) – ma che scatenano l'infezione non appena vengono aperti. Se, invece di *Word* o *Excel*, viene usato un programma diverso per esempio, un semplice "visualizzatore") le potenzialità infettive contenute nel file non possono essere attivate e l'infezione è quindi scongiurata.

Esaminiamo ora le casistiche possibili:

Caso A (figura 2, A). Si tratta di allegati innocui, inviati in allegato da amici fidati che controllano frequentemente il loro PC e si assicurano che non siano presenti virus o trojan.

Caso B (figura 2, B). Si tratta di semplici allegati non richiesti: quasi sempre sono messaggi pubblicitari ben formattati e colorati, contenenti grafici, fotografie e caratterizzati da un aspetto accattivante. Non rappresentano un pericolo nemmeno aprendoli con programmi potenzialmente pericolosi: è, semplicemente, "spazzatura" non richiesta.

e contenente figure o grafici) sia – ovviamente – virus e trojan più o meno abilmente nascosti.

Qualunque programma di posta elettronica, per nostra fortuna, può segnalarci la presenza di allegati e non esiste una procedura che li apra automaticamente non appena sono ricevuti: quest'ultima operazione è sempre affidata all'utente, che deve quindi responsabilmente decidere se aprire l'allegato oppure no.

In realtà alcuni allegati vengono visualizzati nella finestra di anteprima; per svolgere tale operazione di visualizzazione il programma deve necessariamente utilizzare un codice adatto allo scopo. Per visualizzare una fotografia ricevuta come allegato, tanto per essere più chiari, non necessariamente il programma di posta elettronica utilizza il medesimo programma che ha generato quella foto (del resto sarebbe praticamente

Caso C (figura 2, C). È il caso dei virus. Di solito sono programmi che nascondono la loro reale nocività grazie a una denominazione accattivante, del tipo *Guardami_Nuda.Exe* oppure *TiStoCercando.Com*. La gente comune, che è molto più imprudente o ingenua di quanto non si creda, si affretta a cliccare due volte sul nome del file, scatenando inevitabilmente l'infezione. La principale causa della diffusione dei virus è da attribuire infatti alla curiosità, alla superficialità e all'ignoranza, non necessariamente in quest'ordine. L'impazienza può tuttavia avere una sua parte: quando si hanno decine di mail da controllare, non si ha sempre la prudenza di attivare tutte le procedure che il caso richiede per verificare il contenuto dei file allegati. Spesso si preme un doppio clic perché si è stanchi o soprappensiero, ma in ogni caso il danno è fatto.

Caso D (figura 2, D). Sono le catene di S. Antonio realizzate dai nostri conoscenti più o meno disinvolti. Si tratta di messaggi sinceri, magari scritti di proprio pugno, ai quali viene allegato un documento (ricevuto chissà come) che invita a raccogliere fondi per le "Orfanelle Trovatelle del Sacro Ordine delle Carmelitane Senza Calze e Senza Baffi" o altre organizzazioni umanitarie di origine non sempre limpida.

Caso E (figura 2, E). Idem come il caso C, solo che in questo caso è il PC del nostro amico, in modo più o meno inconsapevole, a diffondere mail con allegati maligni.

Caso F (figura 2, F). Come il caso B, ma la mail proviene da utenti, inconsapevoli, i cui PC sono stati infettati con uno dei mille sistemi possibili.

I vari casi della vita

In conclusione è possibile affermare che nella nostra casella di posta elettronica possono capitare ben 42 tipi di e-mail diverse: anzitutto le sei considerate singolarmente nella figura 1; a ciascuna di queste mail, inoltre, potrebbe essere allegato uno dei sei tipi di file considerati in figura 2 (sei per sei = 36). L'invio di un semplice allegato, privo di e-mail, non è infatti possibile: è necessario almeno un messaggio "vuoto", che funga da contenitore, anche se caratterizzato soltanto dall'indirizzo del destinatario e da quello di provenienza. In realtà la casistica possibile si riduce notevolmente, ma si tratta solo di percentuali: alcune sono più frequenti (soprattutto l'accoppiata A di figura 1 con la E di figura 2, oltre alle singole mail di tipo B). Ma, basandosi sulla ben nota legge di Murphy, "Se una cosa può andar male, lo farà". E meglio quindi prestare la massima prudenza.

Clicca sul collegamento specifico per consultare altri Tutorial attinenti al medesimo argomento:

"**Spam, la posta spazzatura**" (questo Tutorial) - Considerazioni generali sulle e-mail, non richieste, che riceviamo quotidianamente.

"**MailWasher**" - Primi passi sull'uso del programma MailWasher prendendo come riferimento la versione gratuita.

"**MailWasher Pro 3.3**" - Impostazione dei parametri più importanti della versione MailWasher Pro 3.3

"**MailWasher - Uso del programma**" - Caratteristiche più importanti di MailWasher prendendo come riferimento la versione Pro 3.3

"**MailWasher - I messaggi e gli avvisi**" - Descrizione dei messaggi che compaiono usando MailWasher

"**Benign**" - Il programma che previene i danni provocati da e-mail contenenti codici dannosi per il nostro PC.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

Il presente Tutorial è stato modificato il giorno 22 settembre 2005
Per ulteriori aggiornamenti consultare il sito www.alessandrodesimone.net