

Modulo 4

Posta elettronica

Nelle attività aziendali, così come in quelle personali, le comunicazioni occupano un posto importantissimo. Negli ultimi anni al trasferimento fisico di lettere e cartoline si è progressivamente sostituito quello elettronico, chiamato posta elettronica.

Come tutti i grandi cambiamenti anche alla base di questo ci sono forti motivi economici. Non solo spedire un messaggio di posta elettronica non richiede la spesa del francobollo, ma nemmeno quella della busta. Anche gli aspetti organizzativi hanno un forte impatto economico dato che la posta elettronica è accessibile da casa o dall'ufficio direttamente, senza la necessità di recarsi ad un ufficio postale e, cosa ancora più importante, viene spedita immediatamente.

Tuttavia anche la posta elettronica ha dei limiti. A differenza delle telefonate non permette di stabilire un contatto diretto con il destinatario. A differenza degli SMS non consente di avvisare il destinatario del suo arrivo. Limite ancora peggiore, la posta elettronica non è *sicura* sia nell'invio, sia nell'identificazione del mittente.

La posta elettronica viene sempre più spesso utilizzata per consegnare ogni sorta di documenti, detti *allegati*. Questa grossa potenzialità porta con sé un grosso pericolo, dato che sono proprio gli allegati di posta elettronica la maggior causa della diffusione di virus.

Se la posta elettronica ha tutti questi problemi e viene comunque ancora utilizzata è perché, accanto ai problemi, vi sono delle potenzialità. Se è vero che manca il contatto di-

retto con il destinatario è anche vero che ciò permette di inviare messaggi ad interlocutori impegnati in altre attività senza disturbarli, cioè non è invasiva. Inoltre un messaggio può essere archiviato a futura memoria, e non costringe a grossi sforzi di sintesi come gli SMS.

Alcuni limiti non sono superabili e quindi per discutere con un interlocutore il telefono risulta insuperabile, se non da un videotelefono, così come gli adolescenti non smetteranno di utilizzare gli SMS nonostante i richiami accorati di politici filatelici.

Altri limiti sono superabili già da ora: all'insicurezza dell'invio e della lettura si ovvia con la richiesta di una *ricevuta di ritorno*. Per risolvere altri limiti sono invece state poste le basi, anche se non sono ancora molto diffuse: nel Modulo 10 verrà illustrato come rendere certa l'identità del mittente tramite l'uso delle applicazioni di firma elettronica.

Rimangono i limiti alla sicurezza. Spesso questi problemi non hanno limitato l'utilizzo della posta elettronica, più per un insieme di ignoranza e di fatalismo che per altro. In questo modulo verranno illustrati questi problemi e verranno insegnate alcune tecniche per ridurre i rischi conseguenti.

4.1 FUNZIONAMENTO

L'utilizzo della posta elettronica coinvolge quattro distinte apparecchiature: il PC del mittente, quello del destinatario, i server di posta elettronica a cui mittente e destinatario fanno capo. Può capitare che i server di posta elettronica a cui fanno riferimento il mittente e il destinatario coincidano, ma anche in questo caso la situazione non è concettualmente differente.

Ogni utente che voglia utilizzare la posta elettronica deve dotarsi di un programma che permetta di gestirla e di un indirizzo a cui farsela spedire. Il programma di posta deve essere istruito in modo da conoscere il server a cui spedire la posta in uscita e il server da cui ritirare la posta in arrivo.

Normalmente gli utenti, così come le piccole organizzazioni, si rivolgono a un *Internet Service Provider*, ovvero un'azienda che fornisce il modo per connettersi ad Internet. Sarà questa azienda a fornire i nomi dei server usati per l'inoltro

della posta in partenza e per lo scarico della posta arrivata. L'indirizzo di posta elettronica, in questo caso, viene fornito direttamente dal provider.

Quando un utente vuole inviare un messaggio a qualcuno, innanzitutto deve ottenerne l'indirizzo di posta elettronica. Questo normalmente non è un problema, in quanto la posta elettronica è ormai così diffusa che tale indirizzo viene normalmente indicato anche sui biglietti da visita. Il grosso limite di questa organizzazione è che non esiste un elenco degli indirizzi di posta elettronica, e quindi non è facile trovare un indirizzo ignoto, a meno di non contattare per telefono il corrispondente. Questo non viene normalmente recepito come un problema, perché questa scomodità corrisponde, di fatto, a un aumento della *privacy*, tant'è vero che anche per i telefoni cellulari la situazione non è molto differente.

Nel momento in cui il messaggio è stato composto, attraverso il programma di posta elettronica, il mittente lo può inviare. A questo scopo deve prima verificare di *essere connesso ad Internet*, ovvero al proprio *ISP*. A questo punto, usando il programma, può spedire la posta al server di posta elettronica e quindi disconnettersi. In questa fase l'unica certezza è che il messaggio è arrivato sul server di posta elettronica dell'*ISP*. Quando riceve il messaggio di posta inviato dall'utente, il programma che gestisce la posta elettronica sul server si attiva per capire a chi la deve inviare. Per farlo utilizza la parte di indirizzo che segue il simbolo @ e che corrisponde al dominio del gestore del destinatario. Se questo dominio coincide con il suo, allora il server normalmente non invia ulteriormente la posta, ma la inserisce nella casella del destinatario. Se invece il dominio del destinatario non corrisponde al proprio, il server di posta cerca di scoprire chi è il server di posta del destinatario. Per fare questo interroga un altro tipo di server, detto *DNS* (*Domain Name Server ovvero server dei nomi di dominio*). Questo tipo di richiesta ottiene come risultato una lista di nomi di server a cui inviare la posta, ordinati per priorità. La lista ottenuta potrebbe anche ridursi a un solo server, in quanto piccole organizzazioni potrebbero anche averne uno solo. Normalmente però vi sono almeno due server di posta e le grandi organizzazioni possono averne ben di più.

Il server che deve inviare il messaggio contatta il primo server della lista e tenta di effettuare la spedizione. Se tutto

funziona, conclude semplicemente le operazioni. Se invece non ci riesce, prova a utilizzare il secondo server della lista. Se nessuno dei server della lista riesce a ricevere la posta, allora il messaggio viene lasciato in una coda di uscita dove vengono accumulati i messaggi non inviati. Periodicamente il server verifica se vi sono messaggi in coda di uscita e cerca di inviarli. Se non vi riesce per un certo tempo allora invia un messaggio al mittente segnalando che per quel numero di ore non è riuscito a inviare la posta.

Può succedere che il server a cui viene inviata il messaggio rifiuti di riceverlo indicandone il motivo al server che cerca di spedirlo. Tale motivo può essere semplicemente un indirizzo errato nella parte che precede la @, oppure il fatto che la casella del destinatario è piena e quindi non vengono più accettati altri messaggi. In entrambi i casi viene data segnalazione al mittente.

Quando il destinatario vuole leggere il messaggio, inizia attivando il programma di posta elettronica e collegandosi ad Internet. A questo punto può dare indicazione al programma di scaricare la posta elettronica giacente nella propria casella. Per farlo deve utilizzare una coppia di *nome utente e password che gli sono stati forniti dal suo ISP*. Una volta che si è qualificato, allora può scaricare la posta, sconnettersi da Internet, e leggere comodamente i suoi messaggi, magari preparando delle risposte che, a loro volta, verranno inviati secondo con le stesse modalità che abbiamo appena descritto.

Esaminando queste fasi, alcune anche non banali, si può osservare come le operazioni da parte di mittente e destinatario siano molto semplici, dato che consistono nell'attivare la connessione a Internet e poi nel premere il pulsante di invio e ricezione, fornendo, tutt'al più, un identificativo e una password. Le operazioni complesse sono svolte dai server, che sono mantenuti dagli ISP, e questo rende molto semplice tutta la gestione, quanto meno agli occhi dell'utente.

Ma non si deve guardare solo alla semplicità, si devono considerare anche i possibili limiti. Ad esempio, per scaricare la posta è stato chiesto un nome utente e una password, non così per spedire dei messaggi. Ciò significa che una persona potrebbe molto facilmente cambiare il proprio indirizzo e mascherarsi da qualcun altro. Per questo non è il caso di prendere per oro colato ciò che arriva per posta elettroni-

ca: piuttosto che niente, in caso di messaggi importanti, vale fare un controllo telefonico.

Il secondo problema è dovuto al fatto che non vi è conferma né dell'arrivo né della lettura del messaggio, ma solo alcune segnalazioni relative ad eventuali errori. Questo è dovuto al fatto che il protocollo utilizzato per lo scambio della posta elettronica era concepito, all'inizio, più come dimostrazione delle possibilità che non come prodotto vero e proprio. D'altra parte la semplicità lo ha reso interessante, utilizzabile e di conseguenza utilizzato su scala mondiale.

Qualcuno dotato di occhio clinico avrà notato, esaminando la descrizione, che il messaggio di posta elettronica viene inviato tramite Internet e come da nessuna parte si sia fatto cenno a sistemi di crittografia: ciò è esatto e implica che la posta elettronica non offre garanzie di riservatezza. Nulla che sia confidenziale dovrebbe mai passare per posta elettronica senza una precedente fase di crittografia. Nei Moduli 9 e 10 saranno illustrate tecniche per rendere sicuri i messaggi di posta elettronica per chi avesse tali esigenze.

4.2 RICEVUTA DI RITORNO

Come appena visto non esiste, nel normale protocollo di invio della posta elettronica, alcun modo per trasmettere la conferma dell'arrivo di un messaggio nella casella del destinatario e tanto meno per avere conferma della lettura dal messaggio da parte di quest'ultimo.

A questo problema hanno pensato i costruttori di programmi di gestione della posta elettronica, inserendo il concetto di *ricevuta di ritorno*. Questo è stato fatto non utilizzando il meccanismo di invio, ma a operando sul formato del messaggio di posta elettronica.

Il formato dei messaggi di posta elettronica, che segue lo standard RFC822, è molto semplice perché permette di spedire messaggi codificati in ASCII a 7 bit, e contiene tutte le informazioni necessarie alla gestione del messaggio in quelle che vengono chiamati *intestazioni* o *header*, poste all'inizio e separate dal messaggio da una riga vuota. Ogni intestazione consiste in una riga nel formato *intestazione: descrizione dell'intestazione*.

Tabella 4.1 Alcune intestazioni

Intestazione	Significato
Date	Data e ora di spedizione
From	Indirizzo di posta del mittente
To	Indirizzo di posta del destinatario
Subject	Oggetto
Reply to	Indirizzo a cui inviare la risposta
User-Agent	Programma utilizzato per comporre il messaggio

Nelle intestazioni la più nota è *Subject*, che definisce l'oggetto del messaggio, ma nella Tabella 4.1 sono riportate alcune tra le intestazioni più comuni e interessanti. Per stimolare l'emissione di una ricevuta di ritorno nel messaggio viene inclusa un'intestazione chiamata *Disposition-Notification-To*. Nel momento dell'apertura del messaggio il programma di gestione della posta vede questa intestazione e agisce di conseguenza.

Non sempre è buona norma inviare ricevute di ritorno. Di solito è meglio impostare il programma di posta in modo che richieda una conferma esplicita, in modo da lasciare all'utente la decisione finale.

IMPOSTARE LA RICHIESTA DI RICEVUTA DI RITORNO

Per poter inviare un messaggio che comprenda una richiesta di ricevuta di ritorno si deve naturalmente scrivere il messaggio e poi, prima di inviarlo, aggiungere tra le opzioni anche la richiesta della ricevuta.

Ovviamente ogni programma di posta opera in maniera differente, perciò verranno illustrate le operazioni per due programmi che si possono considerare buoni riferimenti: *MS Outlook Express* per la piattaforma Windows e *Mozilla* come riferimento per tutte le piattaforme.

Per configurare la richiesta di ricevuta quando si utilizza Outlook Express si operi secondo la seguente procedura.

1. Avviare il programma Outlook Express.
2. Aprire la finestra di composizione del messaggio facendo clic sul pulsante Crea messaggio.

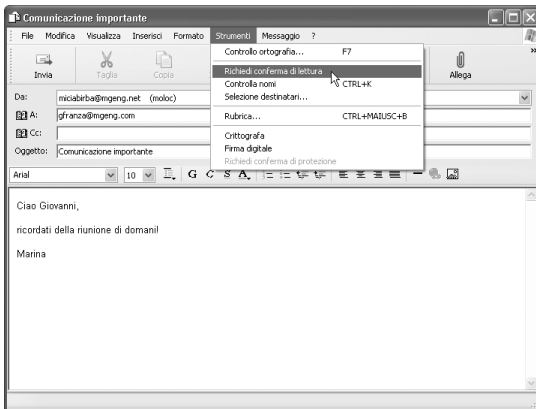


Figura 4.1 Richiesta di ricevuta di ritorno in Outlook express.

3. Completare il messaggio con il destinatario e l'oggetto.
4. Scrivere il testo del messaggio.
5. Fare clic sulla voce **Strumenti** nella barra dei menu (Figura 4.1).
6. Scegliere **Richiedi conferma di lettura**.
7. Fare clic sul pulsante **Invia**.

Per configurare la richiesta di ricevuta quando si utilizza il programma Mozilla si operi secondo la seguente procedura.

1. Avviare il gestore di posta del programma Mozilla.
2. Aprire la finestra di composizione del messaggio facendo clic sul pulsante **Componi**.
3. Completare il messaggio indicando il destinatario e l'oggetto.
4. Scrivere il testo del messaggio.
5. Fare clic sulla voce **Opzioni** sulla barra dei menu (Figura 4.2).
6. Scegliere **Ricevuta di ritorno**.
7. Fare clic sul pulsante **Spedisci**.

MODULARE LA RISPOSTA ALLA RICHIESTA DI RICEVUTA DI RITORNO

Come già affermato non è del tutto sicuro inviare automaticamente le risposte alle richieste di ricevuta di ritorno. In

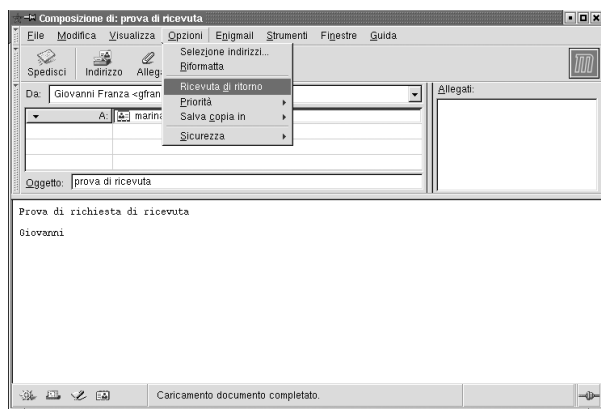


Figura 4.2 Richiesta di ricevuta di ritorno in Mozilla.

parte perché non tutte le mail aperte vengono lette con attenzione, in parte perché questo meccanismo potrebbe venire utilizzato in maniera truffaldina per capire se c'è qualcuno che legge i messaggi inviati a un determinato indirizzo di posta.

Ovviamente i programmi di gestione della posta permettono di scegliere tra varie opzioni, quali inviare sempre una ricevuta senza neppure chiedere conferma, evitare di inviare messaggi di conferma oppure sottomettere l'invio al consenso dell'operatore. L'attivazione dell'opzione "invia sempre la richiesta di ricevuta di ritorno" è caldamente sconsigliata dagli autori, che ricordano come tale pratica qualifichi il mittente in maniera non proprio carina: la ricevuta di ritorno va richiesta quando necessario e non in maniera estensiva. L'opzione è comunque illustrata in modo che chi ne abbia reale necessità possa utilizzarla.

Per configurare il programma Outlook Express si operi secondo la seguente procedura

1. Avviare il programma Outlook Express.
2. Scegliere Strumenti|Opzioni sulla barra dei menu.
3. Nella finestra visualizzata fare clic sull'etichetta Conferme in modo da attivare la corrispondente sezione (Figura 4.3).

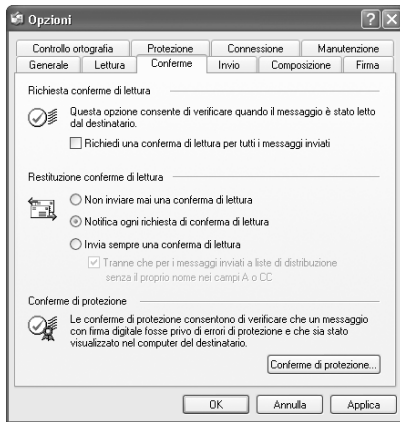


Figura 4.3 Le impostazioni relative alle ricevute di ritorno in Outlook Express.

4. Nel riquadro Richiesta conferme di lettura fare clic su Richiedi una conferma di lettura per tutti i messaggi inviati. Normalmente è bene che tale opzione non sia attiva, a meno che l'utente non ne abbia davvero bisogno.
5. Nel riquadro Restituzione conferme di lettura scegliere il livello voluto facendo clic sul pulsante di opzione Notifica ogni richiesta di conferma di lettura: le possibili alternative, poco consigliabili, sono rappresentate dai pulsanti di opzione Non inviare mai una conferma di lettura e Invia sempre una conferma di lettura.
6. Fare clic sul pulsante OK per confermare le scelte effettuate e chiudere la finestra.

Per configurare il programma Mozilla si operi secondo la seguente procedura.

1. Avviare il gestore di posta del programma Mozilla.
2. Scegliere Modifica|Preferenze... sulla barra dei menu.
3. Nella finestra visualizzata fare clic sulla croce a sinistra della voce Posta e Gruppi di discussione, in modo da espandere la lista (Figura 4.4).
4. Fare clic sulla voce Ricevute di ritorno in modo da visualizzare, sulla destra, le relative opzioni.

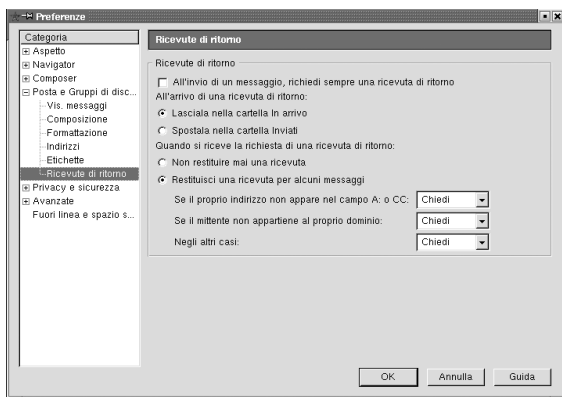


Figura 4.4 Le impostazioni relative alle ricevute di ritorno in Mozilla.

5. Fare clic sul pulsante di opzione **All'invio di un messaggio, richiedi sempre una ricevuta di ritorno** in modo da disattivare l'opzione. È consigliabile che solo gli utenti con una reale necessità attivino questa opzione, che di solito disturba i corrispondenti abituali.
6. Sotto l'indicazione **Quando si riceve la richiesta di una ricevuta di ritorno** fare clic sul pulsante di opzione **Restituisci una ricevuta per alcuni tipi di messaggi** in modo da attivare le scelte sottostanti. Per disattivare completamente l'invio di ricevute si attivi il pulsante di opzione **Non restituire mai una ricevuta**.
7. Le ultime tre righe permettono di selezionare l'invio delle ricevute a seconda di vari tipi di messaggi. Per l'utilizzo normale si utilizzino le stesse selezioni per tutti i casi. Le selezioni possibili sono **Chiedi** (suggerita), **Non spedire e Spedisci** (sconsigliata).
8. Fare clic sul pulsante **OK** per confermare le scelte fatte e chiudere la finestra.

4.3 MESSAGGI NON VOLUTI (SPAM O JUNKMAIL)

Chiunque abbia utilizzato la posta elettronica avrà scoperto molto rapidamente che, nel giro di pochi giorni, la sua casel-

la di posta inizia a riempirsi di messaggi che arrivano da mittenti più svariati e comunque non noti. Non che questa sia una novità, purtroppo, dato che anche le normali cassette postali tendono a riempirsi di pubblicità non voluta.

Tuttavia anche tale fenomeno è una limitazione alla sicurezza, dato che consuma risorse quali il collegamento a Internet, lo spazio su disco e il tempo di chi deve leggere la posta. Agire contro questi fenomeni non è una cosa secondaria ma, anzi, un compito importante da non sottostimare.

La posta elettronica non voluta è, come quella ordinaria, solitamente di origine commerciale ed è costituita da messaggi generalmente pubblicitari. Tali messaggi sono solitamente indirizzati ad utenti il cui indirizzo postale è stato ricavato scandendo la rete.

I messaggi non voluti ma indirizzati specificamente e singolarmente sono magari fastidiosi, ma vengono recepiti come normali messaggi commerciali. Ben diverso è il caso di quelle entità che spediscono messaggi a raffica a tutto il mondo o, ancora peggio, il caso in cui messaggi molto simili continuano ad arrivare. Curiosamente gli autori stanno sperimentando una situazione del genere il cui argomento è *acquistate il nostro sistema antivirus se volete evitare problemi*: al di là del tono vagamente ricattatorio è ben logico che se una persona non è interessata a un prodotto, lo sarà sempre meno via via che riceve continue mail di offerta dello stesso prodotto.

In questo tipo di messaggi rientrano anche fenomeni già noti nel mondo della posta ordinaria. Il primo viene chiamato "catena di sant'antonio" ed è costituito da un messaggio contenente promesse di prosperità e minacce di disastri, a seconda che il destinatario rispedisca o meno un certo numero di copie del messaggio ad altri malcapitati. Un altro fenomeno, ispirato al marketing multilivello, è molto simile, ma il suo fascino è di tipo monetario: al destinatario viene chiesto di spedire una piccola cifra in denaro a una serie di persone indicate nel messaggio e di rispedire il messaggio ad ulteriori malcapitati modificandolo, eliminando il primo nome della lista contenuta nel messaggio e aggiungendo il proprio nome in fondo alla lista.

Questo tipo di posta non voluta è nota come *junkmail*, ovvero *posta di scarto*. Un altro termine utilizzato è *spam*. Tale

termine non ha un significato proprio, ma deriva da uno sketch dei comici inglesi Monty Python, Monty Python's Flying Circus nel quale la parola "spam" veniva ripetuta moltissime volte risultando l'ingrediente che si trovava in tutti i piatti di una tavola calda. ("Spam" è, tra le altre cose, un marchio di fabbrica relativo alla carne di maiale in scatola).

COME DIFENDERSI

Vi sono varie difese dallo spam: alcune sono tecniche, altre legali. Le difese tecniche sono basate sull'attivazione dei filtri messi a disposizione dai programmi di mail e verranno illustrate nei prossimi paragrafi, mentre le difese legali sono basate sull'applicazione della legge sulla privacy e della legge postale. Non sono semplici da utilizzare, ma possono risolvere i casi più gravi, anche se richiedono l'intervento di legali esperti con relativi costi. Dato che questo volume è prevalentemente a carattere tecnico, tali strade non verranno illustrate.

L'impostazione dei filtri

Praticamente tutti i programmi per la gestione della posta elettronica dispongono di filtri. Lo scopo di un filtro è normalmente quello di identificare i messaggi in arrivo in modo da archivarli automaticamente. I messaggi possono essere identificati utilizzando tutte le loro caratteristiche, a partire dal mittente e dall'oggetto per arrivare alla priorità e al contenuto.

Una volta identificato un tipo di messaggio vi si può abbinare un'azione. Le azioni possono essere le più varie, dall'archiviazione in una determinata cartella di posta, alla cancellazione, alla generazione di un messaggio automatico di risposta quando l'utente è fuori ufficio e vuole pregare i corrispondenti di pazientare e non attendersi una risposta immediata.

Di solito non si imposta un singolo filtro, ma più filtri. Quando sono stati impostati più filtri è necessario prestare attenzione all'ordine di applicazione. Per capire questo concetto si pensi ad un filtro, che chiameremo filtro *A*, che sposti tutti i messaggi provenienti da un certo mittente in una cartella dedicata, e ad un filtro, che chiameremo filtro *B*, che cancelli tutti i messaggi con un certo oggetto. Se arriva un messaggio con l'oggetto indicato dal mittente indicato, allora la sua sorte dipenderà dall'ordine di applicazione dei filtri: se si applicano

nell'ordine *A, B*, allora il messaggio verrà spostato nella cartella indicata dal filtro *A* e quindi, non essendo più nella cartella della posta in arrivo, non verrà più visto dal filtro *B*. Se invece si inverte l'ordine di applicazione, il filtro *B* cancellerà il messaggio, che non potrà quindi più essere spostato dal filtro *A*.

Un'ultima segnalazione di cautela: è bene non creare filtri che cancellano direttamente i messaggi, ma preferire uno spostamento in una cartella creata per contenere lo spam. Si tratta di un'utile precauzione per evitare di perdere dei messaggi a causa di un filtro scritto in maniera impropria.

Come in precedenza, anche qui verranno indicate le procedure per Outlook Express e per Mozilla, che vengono utilizzati come ambienti di riferimento. Per configurare i filtri in Outlook Express si operi secondo la seguente procedura:

1. Avviare il programma Outlook Express.
2. Fare clic su Strumenti nella barra dei menu.
3. Scegliere la voce Regole Messaggi.
4. Scegliere la voce Posta elettronica in modo da far apparire una finestra di dialogo.

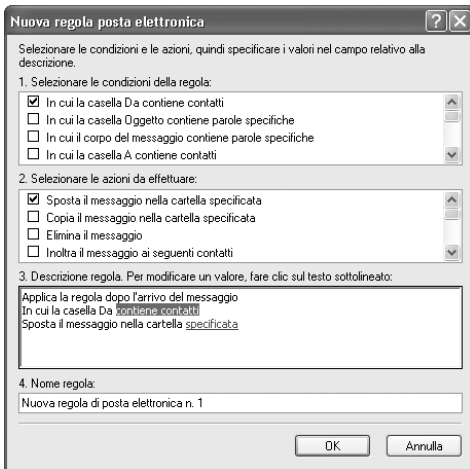


Figura 4.5 Le impostazioni relative ai filtri in Outlook Express.

5. Nel primo riquadro in alto, Selezionare le condizioni della regola, fare clic sulla casella di controllo che corrisponde all'analisi voluta. Si vedrà apparire la scelta nella casella di testo Descrizione regola.
6. Nel riquadro in centro, Selezionare le azioni da effettuare, fare clic sulla casella di controllo che corrisponde all'azione voluta. Si vedrà apparire la scelta nella casella di testo Descrizione regola.
7. Nella casella di testo Descrizione regola fare clic sulla parte della condizione che è ancora generica e che appare sottolineata, in modo da aprire una finestra di dialogo con cui impostarla.
8. Nella finestra di dialogo inserire i termini voluti nella casella di testo in alto in modo da attivare il tasto Aggiungi....
9. Fare clic sul tasto Aggiungi....
10. Fare clic sul pulsante OK per chiudere la finestra.
11. Operare in modo simile per personalizzare l'azione da effettuare, se necessario.
12. Fare clic sul pulsante OK per confermare la regola e chiudere la finestra di dialogo.
13. Nella finestra Regole messaggi, nella scheda Regole posta elettronica si può decidere di inserire una nuova regola facendo clic sul pulsante Nuova..., oppure cancellare una regola selezionandola e quindi facendo clic sul pulsante Rimuovi..., oppure ancora modificare una regola selezionandola e poi facendo clic sul pulsante Modifica....
14. Nel caso ci siano più regole si può modificare il loro ordine selezionandone una e poi facendo clic sul pulsante Sposta su oppure Sposta giù.
15. Al termine delle operazioni fare clic su OK per confermare e chiudere la finestra di dialogo.

Nell'inserimento dei filtri successivi l'azione sui menu fa aprire direttamente la finestra Regole messaggi ed è necessario fare clic sul pulsante Nuova... per iniziare a definire la regola.

Per configurare i filtri in Mozilla si operi secondo la seguente procedura.

1. Avviare il gestore di posta del programma Mozilla.
2. Fare clic sulla voce Strumenti posta sulla barra dei menu.
3. Scegliere la voce Filtri messaggi... in modo da visualizzare la finestra di gestione.

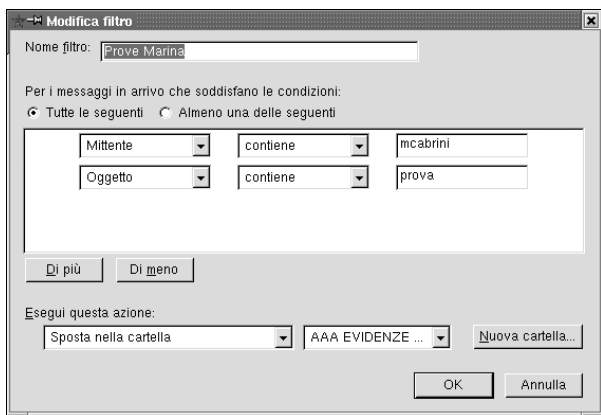


Figura 4.6 Le impostazioni di un filtro in Mozilla.

4. Nella finestra *Filtri messaggi* apparirà la lista dei filtri con l'indicazione della loro attivazione o meno. Al primo utilizzo tale finestra è vuota.
5. Per inserire un nuovo filtro fare clic sul pulsante *Nuovo...*
6. Nella nuova finestra *Modifica filtro* usare la casella di testo *Nome filtro* per dare un nome al filtro. È bene che tale nome sia descrittivo dell'azione del filtro.
7. Dato che possono essere impostate più condizioni si può scegliere, cliccando sull'apposito pulsante di opzione, se il filtro seleziona i messaggi che soddisfano tutte le regole contemporaneamente (pulsante di opzione *Tutte le seguenti*), oppure se il filtro seleziona i messaggi che ne soddisfano almeno una (pulsante di opzione *Almeno una delle seguenti*). La prima scelta va fatta quando, ad esempio, si vogliono selezionare i messaggi con un certo *oggetto* che arrivano da un determinato *mittente*, la seconda quando si vogliono selezionare messaggi che provengono da un *mittente* oppure da un altro.
8. Nel riquadro vi sono delle caselle di riepilogo. Quella di sinistra permette di scegliere l'elemento del messaggio, ad esempio *Oggetto* oppure *Mittente* o una qualunque delle intestazioni. Gli utenti veramente esperti possono addirittura indicare intestazioni non previste nella lista.

Tabella 4.2 Le possibili analisi sugli elementi del messaggio.

Analisi	Significato
contiene	Vero se il testo specificato è compreso nell'elemento selezionato
non contiene	Vero se il testo specificato non è compreso nell'elemento selezionato
è	Vero se l'elemento selezionato è uguale al testo specificato
non è	Vero se l'elemento selezionato è differente al testo specificato
inizia con	Vero se l'elemento selezionato comincia con il testo specificato
finisce con	Vero se l'elemento selezionato termina con il testo specificato

9. Nella seconda casella di riepilogo, posta alla destra della prima, si può scegliere il tipo di analisi da compiere tra quelle illustrate nella Tabella 4.2.
10. A destra delle due caselle di riepilogo c'è una casella di testo nella quale introdurre il riferimento, quale, ad esempio, l'indirizzo di un mittente da cui provengono messaggi da filtrare.
11. Facendo clic sul pulsante *Di più* si possono aggiungere delle condizioni, da impostare come nei tre punti precedenti. Facendo clic sul pulsante *Di meno* si può cancellare l'ultima condizione inserita.
12. Sotto la voce *Esegui questa azione*: è presente una casella di riepilogo che consente di scegliere tra le azioni illustrate nella Tabella 4.3. A lato di questa casella di riepilogo

Tabella 4.3 Le possibili azioni sugli elementi del messaggio.

Azione	Significato
Sposta nella cartella	Inserisce il messaggio in una cartella che viene scelta da una casella di riepilogo
Cambia la priorità a	Permette di cambiare la priorità del messaggio. La priorità da assegnare è selezionabile da una casella di riepilogo
Elimina il messaggio	Elimina il messaggio. Questa sarebbe la corretta fine dei messaggi di spam
Contrassegna il messaggio come letto	Fa apparire come letto il messaggio anche se, di fatto, non è stato letto.
Spunta il messaggio	Mette in evidenza il messaggio
Etichetta il messaggio	Permette di assegnare un'etichetta al messaggio. L'etichetta da applicare è selezionabile da una casella di riepilogo

logo può apparire una seconda casella che permette di completare l'azione: ad esempio quando si seleziona l'azione Sposta nella cartella viene visualizzata una seconda casella di riepilogo che permette di scegliere tra le cartelle gestite dal programma di posta.

13. Per confermare la regola fare clic sul pulsante OK, che chiuderà anche la finestra Modifica filtro.
14. Una volta inserito un filtro si possono utilizzare, nella finestra Filtri messaggi, anche i pulsanti Modifica ed Elimina, dopo aver selezionato il filtro con un clic.
15. Una volta inseriti due o più filtri si possono utilizzare, nella finestra Filtri messaggi, i pulsanti Muovi su e Muovi giù. Questi pulsanti agiscono sul filtro selezionato e lo spostano, cambiando l'ordine della lista dei filtri. Questo ordine può essere importante quando due filtri hanno delle regole comuni, come abbiamo già visto in precedenza.
16. Facendo un clic sul filtro, in corrispondenza della colonna Abilitato, si può abilitare o disabilitare un filtro. In questo modo si possono mantenere dei filtri che non devono essere applicati, disabilitandoli temporaneamente senza do-

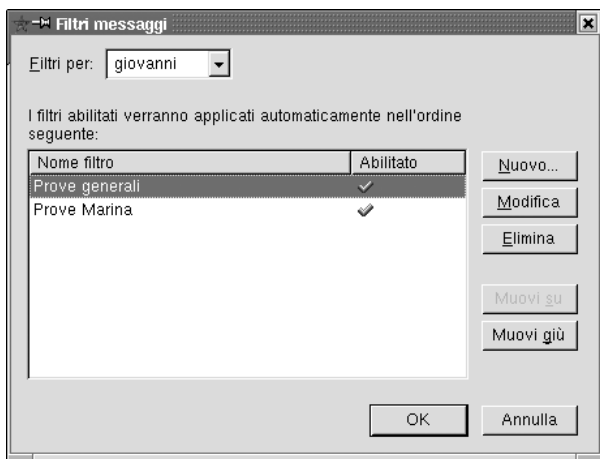


Figura 4.7 Le impostazioni dei filtri in Mozilla.

verli cancellare. Questo è particolarmente comodo in quanto la fase di impostazione delle condizioni di un filtro potrebbe richiedere del lavoro che è spiacevole sprecare.

17. Facendo clic sul pulsante OK si conferma il lavoro fatto e si chiude la finestra Filtri messaggi.

4.4 ALLEGATI

All'origine la posta elettronica veniva utilizzata esclusivamente per comunicazioni di tipo testuale, esattamente come la normale posta. Questo, però, limitava le possibilità, per cui vennero studiati dei modi per includere nella posta dei documenti non testuali. Il meccanismo utilizzato si basa sul fatto che tutti i documenti elettronici sono comunque dei file e quindi potrebbero essere legati al testo di un messaggio. Però per farlo bisogna superare due scogli: il primo è costituito dal fatto che i documenti sono normalmente in formato binario, il secondo che occorre differenziarli dal testo e, magari, gestirli in maniera automatica.

La soluzione a questi due problemi si chiama *MIME*, ovvero *Multi-purpose Internet Mail Extensions* (estensioni polivalenti alla posta in Internet). Con questa tecnica vengono previste delle intestazioni aggiuntive che individuano:

- l'inizio di un messaggio contenente varie parti;
- la composizione della riga di separazione delle varie parti;
- il nome, eventuale, di un file di documento per memorizzare una parte;
- il modo con cui una parte binaria viene trasformata in una parte di testo.

Con questa soluzione i documenti vengono *allegati* al messaggio di posta e prendono proprio questo nome. In realtà è tutto il messaggio a risultare differente, in quanto sin dall'inizio, tra le intestazioni, appare un'intestazione che avvisa della sua particolarità. Questa intestazione è del tipo: `Content-Type: multipart/mixed; boundary="——060903040709060005090909"`. Il nome *Content-Type* indica il tipo del contenuto del messaggio. Si noti come venga specificata, con il termine *boundary* (ovvero confine, limite), la riga di delimitazione tra le varie parti del messaggio.

Ogni parte del messaggio (*allegato*) inizia con righe del tipo: Content-Type: application/msword; name="cap03.doc", che specificano sia il tipo di utilizzo della parte, sia il nome di un eventuale file in cui memorizzarla. In questo caso il nome application/msword, detto *tipo MIME*, indica il tipo di documento memorizzato e, quindi, il tipo di applicativo che lo ha generato o che lo può gestire.

Per finire vi è un'intestazione del tipo Content-Transfer-Encoding: base64 che specifica il modo con cui il documento, in formato binario, è stato trasformato in un documento di testo. In questo caso vengono usate solo 64 delle 256 combinazioni di bit possibili per ogni byte e quindi il documento viene spezzato in sequenze consecutive di 6 bit, ciascuna delle quali viene trascritta in un singolo byte. Questa operazione allunga il documento ad almeno 4/3, dato che per scrivere 6 bit se ne impiegano 8 e poi ci sono i capo riga aggiuntivi. Questo allungamento, però, garantisce che tutte le 64 combinazioni siano simboli alfanumerici inseribili comodamente nel messaggio.

Al termine di queste intestazioni c'è il documento, ridotto a testo e diviso, per comodità, in righe, che si conclude con una riga uguale al valore della boundary appena illustrata. Un messaggio di posta elettronica può contenere quanti allegati vuole, senza limiti, dato che il programma che legge il messaggio è in grado di dividerlo in parti e di gestirle automaticamente.

C'è un tipo particolare di allegato che viene gestito quando si spediscono messaggi in formato HTML in modo da avere la possibilità di renderlo esteticamente più gradevole. I programmi di posta sono stati istruiti per sapere che non tutti vogliono ricevere messaggi preparati in questo modo, quindi creano due versioni del messaggio stesso. In una versione viene scritto solamente il testo, mentre l'altra versione contiene il codice HTML con tutte le informazioni inserite dall'utente. Questi due messaggi vengono trattati come se fossero entrambi degli allegati, ma l'intestazione Content-Type non viene impostata a multipart/mixed, bensì a multipart/alternative. In questo modo, all'atto della visualizzazione del messaggio il programma di gestione mostrerà la parte ritenuta più idonea dall'utente, scartando automaticamente l'altra.

Non tutti i programmi di posta elettronica sono sempre stati in grado di gestire gli allegati, ma tutti i moderni pro-

grammi di posta elettronica sono in grado di gestirli. Per poterlo fare ogni programma dispone, al suo interno, di una tabella di configurazione che abbina il tipo dell'allegato (detto anche *tipo MIME*) con un programma in grado di visualizzarlo. All'atto della ricezione di un messaggio di posta contenente un allegato, il programma ne verifica il tipo e, scandendo la tabella, decide come trattare l'allegato stesso.

A seconda della configurazione gli allegati possono:

- apparire come un simbolo grafico cliccabile;
- essere salvati su disco usando il nome indicato nell'intestazione;
- essere visualizzati direttamente dal programma di posta elettronica;
- essere aperti con un programma di visualizzazione ridotto (anteprima);
- essere aperti con un programma completo;
- essere avviati in esecuzione (solo se sono programmi, naturalmente).

Ovviamente ciò dipende dalla configurazione del programma di posta: l'elenco è stato proposto in ordine decrescente di sicurezza, con la prima alternativa più sicura dell'ultima. Osservando l'elenco ci si rende anche conto che è in ordine crescente di potenzialità. Ancora una volta la sicurezza e la comodità d'uso costringono a compromessi.

USO MALIGNO DEGLI ALLEGATI

I rischi per la sicurezza creati dalla gestione degli allegati di posta elettronica non sono affatto teorici: la quasi totalità dei nuovi virus hanno utilizzato questo meccanismo per introdursi nei PC. C'è da osservare tuttavia come questi meccanismi funzionino praticamente solo sulla piattaforma Windows/Outlook e non su quella Linux/Mozilla. Questo si verifica non solo per la diversa diffusione dei differenti sistemi, quanto per i differenti scopi dei progettisti: sempre tesi a dare nuove funzionalità gli uni, più conservativi e attenti alla sicurezza gli altri. Non è una questione di bravura, quanto una questione di ambiente di riferimento e di scelte: è chiaro che in un libro sulla sicurezza le scelte pendano poi da quel lato.

Vari sono i meccanismi utilizzati dai virus, ma tutti sono basati su una distonia, e due ingenuità. La distonia è dovuta al fatto che Outlook indica il tipo dell'allegato usando, correttamente, il tipo MIME, ma poi, all'atto dell'apertura del file, utilizza i meccanismi di Windows basati sull'estensione. La prima ingenuità è non bloccare l'esecuzione di file eseguibili, senza considerare che questa è una porta spalancata a comportamenti pericolosi.

La seconda ingenuità è lasciare che la visualizzazione del nome del file corrispondente all'allegato possa avvenire secondo le regole impostate per il desktop. Il guaio è che l'impostazione standard nasconde proprio l'estensione del file. Merita comunque segnalare che questo problema è stato risolto nelle ultime versioni di Outlook Express, per le quali non valgono alcune delle seguenti osservazioni.

Il tipico meccanismo di contagio è il seguente: qualcuno costruisce un programma, contenente un virus, e lo salva in un file chiamandolo, ad esempio, *belgatto.jpg.exe*. Nel testo del messaggio scrive qualcosa del tipo: *guarda che bel gatto e che cosa strana che fa*. In un secondo tempo questo programma viene allegato a un messaggio di posta elettronica che viene salvato sul disco del PC. Questo messaggio viene modificato, con un semplice editor di testo, cambiando l'intestazione dell'allegato da *application/octet-stream* usata per i programmi a *image/jpeg* che identifica le immagini, e quindi inviato.

Quando il programma di posta elettronica riceve il messaggio, lo visualizza insieme a un'icona standard che rappresenta un'immagine e il nome *belgatto.jpg*. L'utente che riceve questo messaggio legge il testo, vede l'icona, legge il nome e ci fa sopra un doppio clic per vedere l'immagine, scatenando il virus e creandosi una bella serie di problemi. Va ancora peggio a chi ha selezionato l'opzione relativa alla visualizzazione delle anteprime, dove esiste: il guaio succede all'apertura del messaggio senza nemmeno l'intervento umano. Il problema è che Outlook Express non permette che minime deroghe a questa modalità di anteprima. Tutto questo problema è creato non solo dalla perversità di chi confeziona simili oggetti vandalici, ma anche dalla dabbenaggine di chi, per abbellire l'aspetto del desktop, nasconde quelle estensioni sulle quali si basa l'esecuzione dei programmi. Vale poi indicare al pubblico ludibrio l'assoluta stupidità del-

l'utilizzare due differenti meccanismi: uno per specificare cosa contenga l'allegato e l'altro per decidere che farne. Non sarebbe da stupirsi se qualcuno chiedesse i danni per un tale leggerezza.

DIMINUIRE I RISCHI

Per ridurre il rischio di contrarre un virus tramite la posta elettronica le misure sono semplici, anche se riducono, ma non di molto, le potenzialità dello strumento. Le misure che verranno descritte non sono relative al sistema operativo Linux né al programma Mozilla, in quanto il loro modo di operare li rende immuni dagli attacchi basati sulla contraffazione del tipo MIME. Dato poi che i programmi di produttività aziendale installabili sotto Linux non gestiscono le macro dei formati Microsoft, anche questo tipo di attacco è molto improbabile.

La prima cosa da fare è configurare il desktop di Windows in modo da rendere sempre visibili le estensioni: sicuramente vedere Documento di bilancio 2002.doc è meno bello di vedere Documento di bilancio 2002, ma almeno si sa quale sarà il suo utilizzo. La seconda cosa da fare è imporre che tutti gli allegati siano gestiti da Outlook Express evitando l'esecuzione di allegati pericolosi in quanto programmi.

La terza cosa da fare è comunque impostare un antivirus, secondo le modalità illustrate nel prossimo modulo, in modo da ridurre il problema costituito dai virus delle macro.

Configurazione del desktop

Questa configurazione è tipica del desktop di Windows che, a partire da Windows 95, permette di nascondere le estensioni e, anzi, presenta questa opzione come valore predefinito. Questa impostazione non è buona, perché non permette di capire esattamente con che tipo di file si ha a che fare. Inoltre alcune vecchie versioni di Outlook Express impiegavano questa impostazione per visualizzare il nome degli eventuali allegati, perciò la visualizzazione delle estensioni dei file è di particolare importanza soprattutto per quei computer su cui non è possibile installare una versione recente di Outlook Express. Per effettuare questa configurazione si proceda secondo la seguente procedura.

1. Fare doppio clic sull'icona Risorse del computer del desktop.
2. Scegliere Strumenti|Opzioni cartella... dalla barra dei menu.
3. Nella finestra Opzioni cartella fare clic sull'etichetta Visualizzazione in modo da raggiungere la relativa sezione (Figura 4.8).
4. Nella casella Opzioni avanzate fare clic sulla casella di controllo Nascondi le estensioni per i tipi di file conosciuti in modo da disattivarla.
5. Fare clic sul pulsante Applica a tutte le cartelle posto nella parte superiore della finestra.
6. Fare clic sul pulsante OK per confermare le operazioni e chiudere la finestra.

Configurazione del programma di posta elettronica

Innanzitutto si verifichi di disporre dell'ultima versione di Outlook Express e quindi, per metterlo in condizioni di minima

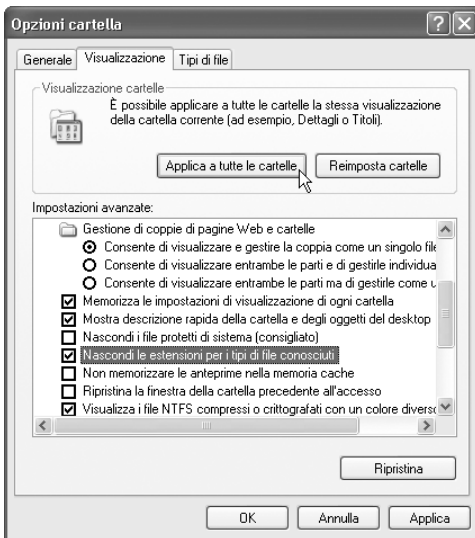


Figura 4.8 L'impostazione del desktop di Windows XP.

sicurezza, lo si configuri in modo che non permetta di aprire gli allegati che considera pericolosi operando secondo la seguente procedura.

1. Avviare il programma Outlook Express.
2. Scegliere Strumenti|Opzioni... dalla barra dei menu.
3. Sulla finestra che viene aperta fare clic sull'etichetta Protezione in modo da visualizzare la sezione relativa (Figura 4.9).
4. Fare clic sulla casella di controllo Non consentire salvataggio o apertura di allegati che potrebbero contenere virus in modo da attivarla.
5. Fare clic sul pulsante OK in modo da confermare le scelte fatte e chiudere la finestra.

Una volta eseguita questa configurazione gli allegati che potrebbero essere degli eseguibili non saranno gestibili. Nell'intestazione del riquadro di anteprima apparirà un'icona con il simbolo della graffetta in presenza di uno o più allegati. Facendo clic su questa icona si potrà vedere l'elenco degli allegati, ma gli allegati considerati pericolosi non potranno essere manipolati in alcun modo.



Figura 4.9 L'impostazione della protezione di Outlook Express.

Per quanto queste configurazioni siano buone, esse non coprono i *virus delle macro* dato che la protezione che abbiamo appena visto opera esaminando le estensioni dei file. Tutto ciò che si riesce ad ottenere è un generico messaggio che invita alla prudenza. In questo caso l'unica possibilità è data dall'utilizzo di un sistema antivirus, così come illustrato nel prossimo modulo.

Cambio del programma di posta elettronica

Per migliorare la sicurezza è comunque meglio non utilizzare Outlook Express ma, al suo posto, impiegare Mozilla, che si limita a visualizzare in anteprima i file per i quali dispone di un visualizzatore interno e a chiedere all'utente quale programma utilizzare per gli altri tipi di file.

Chi avesse dubbi si ricordi che Mozilla è comunque un prodotto libero, installabile sia in ambiente Windows che Linux che Macintosh (MacOS X) senza dover sostenere ulteriori costi che non siano quelli di scaricamento dalla rete. Inoltre Mozilla ha la buona abitudine di mantenere gli archivi della posta in una serie di file di testo contenuti in una cartella comune, e ciò permette controlli e salvataggi della posta ben più semplici e immediati rispetto ad Outlook Express.

L'installazione di Mozilla permette inoltre di installare in seguito un altro prodotto, Enigmail, che consente una veloce gestione delle firme elettroniche per aumentare ulteriormente i livelli di sicurezza collegati allo scambio di messaggi di posta elettronica.

Per installare Mozilla è sufficiente collegarsi al sito www.mozilla.org e seguire le istruzioni date, prima scegliendo la versione, quindi il tipo di processore (ovvero se si utilizza un PC, un Macintosh, o ancora altri computer) e alla fine il sistema operativo. A questo punto si scarica il software e lo si installa fornendo solo alcune informazioni al programma automatico di installazione.

4.5 UN VIRUS PARTICOLARE

A questo punto merita introdurre il primo tipo di virus di cui viene fornito il nome. Questo tipo di virus viene chiamato *hoax* (letteralmente inganno o tiro scherzoso). Viene citato

qui in quanto il rimedio per questo virus non può essere costituito dalle misure appena viste e nemmeno da quanto verrà affrontato nei prossimi capitoli.

Questi virus sono in realtà dei normali messaggi di posta elettronica, che vengono inviati a una lunga lista di persone e che avvisano della presenza di un determinato virus. Nel messaggio vi sono istruzioni dettagliate su come individuare e eliminare il virus. Insieme a tali istruzioni viene segnalato che il virus si propaga utilizzando la rubrica e si richiede di inoltrare la segnalazione a tutte le persone contenute nella rubrica. In realtà la segnalazione è fasulla, dato che il cosiddetto "virus" è semplicemente un programma poco noto e ancora meno utilizzato, per cui la cura non sortisce normalmente alcun effetto. Ovviamente il fatto di poter individuare il virus accentua la credibilità del messaggio e il fatto che le manovre eseguite non creino problemi completa la sensazione di aver risolto un possibile grave problema. Come conseguenza l'utente inoltra il messaggio a tutte le persone note.

A questo punto il virus ha ottenuto il suo scopo: essendosi propagato grazie alla buona fede dell'utente, è riuscito a fargli perdere tempo e a far sì che altre persone lo sprechino grazie all'inoltro del messaggio. Si tratta, in sostanza, di una versione elettronica della catena di sant'antonio, dove, al posto delle minacce di malocchio, viene utilizzata la montante paura del virus.

I rimedi a questo tipo di virus non sono semplici, in quanto potrebbe anche trattarsi di segnalazioni corrette. La prima cosa da fare è cercare di avere informazioni. Queste si possono avere contattando un consulente informatico (e le aziende dovrebbero davvero averne uno) oppure facendo una rapida ricerca sui siti dei vari produttori di antivirus, oppure su Google (www.google.it). Per la ricerca su Google si utilizzi il nome del virus che viene riportato nel messaggio aggiungendolo magari al nome di un antivirus come: *+nomevirus +nomeantivirus*. Questo tipo di ricerca di solito porta alle pagine del sito degli antivirus, dove sono fornite notizie sul virus e qui si deve verificare se il virus viene indicato come hoax.

Che si sia sicuri o meno della natura di hoax del virus, non è mai buona norma inoltrare il messaggio ad altri, tanto meno a tutti gli indirizzi della rubrica. Fino ad ora questi virus sono stati benigni, ma non è detto che sia così e non è

mai buona norma suggerire manovre di cui non si ha conoscenza, dato che si avrebbe la responsabilità di eventuali danni provocati.

Per terminare tale illustrazione possiamo citare un messaggio scherzoso che girava in rete tempo fa: in questo messaggio, che si qualificava come proveniente da un paese molto povero, si avvisava dell'impossibilità degli autori di accedere a tecniche avanzate. In virtù di questo si chiedeva comprensione all'utente e gli si chiedeva di eseguire una serie di operazioni atte a danneggiare il computer. Ovviamente tutti i destinatari ridevano di un simile virus che così scopertamente chiedeva di danneggiare il PC, pensando che solo un matto avrebbe potuto eseguire tali operazioni. Ma quanti di questi utenti hanno inoltrato un hoax credendo, oltretutto, di aver aiutato i loro corrispondenti ?

4.6 CONCLUSIONI

La posta elettronica è uno strumento molto potente e molto utilizzato, la cui importanza è destinata a crescere ancora. Tuttavia è uno strumento pericoloso, in quanto viene ampiamente sfruttato per l'invio di virus, di cui costituisce uno dei principali strumenti di distribuzione, e per l'invio di messaggi non voluti, prevalentemente a carattere commerciale.

L'uso di un buon sistema operativo, di un buon programma di gestione della posta e di corrette impostazioni permette di ridurre sensibilmente questi rischi e di operare con tranquillità. È comunque buona norma adottare un antivirus per abbassare ulteriormente i livelli di rischio, ma questo è argomento del prossimo modulo.

