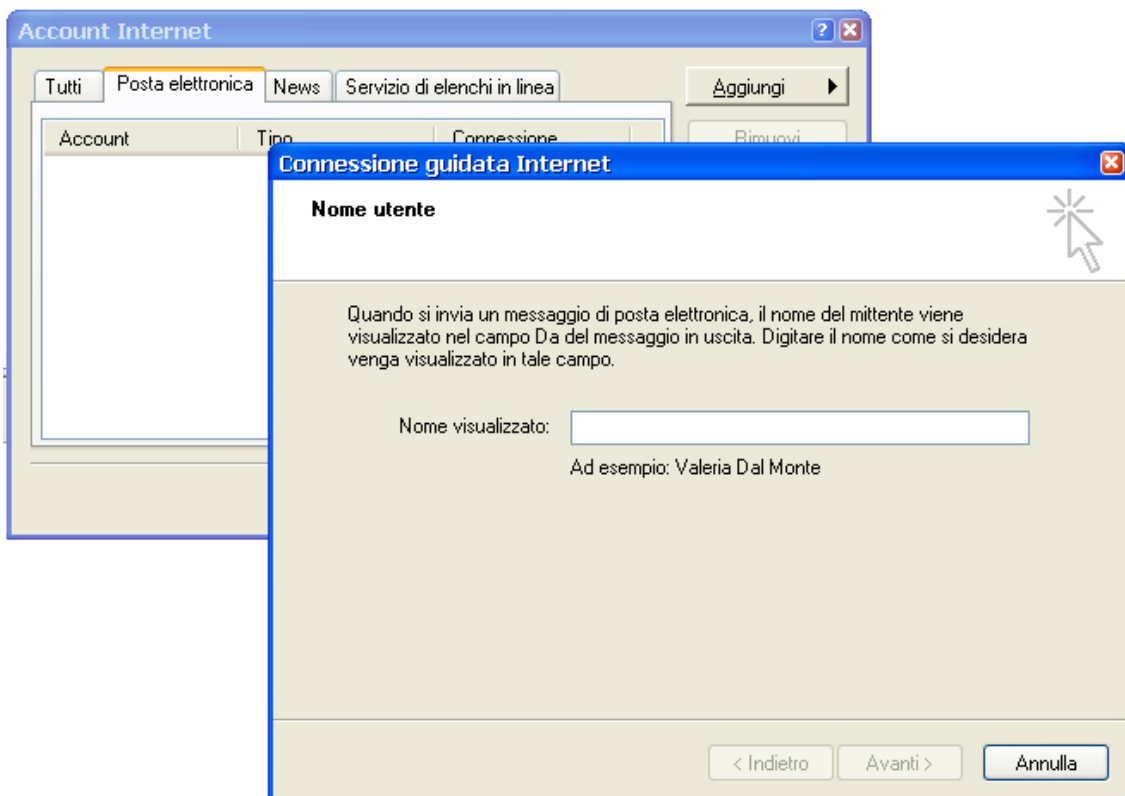


## NOZIONI AVANZATE: CONFIGURAZIONE DI OUTLOOK EXPRESS

Se si dispone di un computer collegato direttamente, via modem, a Internet, per far sì che un programma di posta elettronica come Outlook Express sia in grado di ricevere e inviare messaggi bisogna preventivamente configurare in maniera corretta l'**ACCOUNT** (la **CASELLA**) presso il **PROVIDER**, un'operazione distinta da quella della connessione a Internet. Outlook Express è dotato allo scopo di una procedura di **CONNESSIONE GUIDATA** che fornisce tutte le istruzioni necessarie. È sufficiente inserire le informazioni richieste nelle varie schermate successive per condurre in porto senza troppe difficoltà l'operazione. È necessario però, prima di iniziare, dotarsi dei **PARAMETRI DI CONFIGURAZIONE** richiesti, dati che deve fornire il **PROVIDER** stesso o che sono reperibili sul sito di quest'ultimo. I parametri che servono sono in genere quelli per la ricezione (**POP3**) e l'invio (**SMTP**), nonché **L'INDIRIZZO DI E-MAIL** fornito dall'**ISP** e la relativa **PASSWORD DI POSTA ELETTRONICA**.

La connessione guidata di Outlook Express viene avviata dal menu **STRUMENTI**, selezionando il comando **ACCOUNT**; nella finestra di dialogo **ACCOUNT INTERNET** selezionate la scheda **POSTA ELETTRONICA**, quindi premete il pulsante **AGGIUNGI** per lanciare la procedura guidata. A questo punto è sufficiente sfogliare via via le schermate per completare la configurazione.



## ULTERIORI FUNZIONI AVANZATE DI OUTLOOK EXPRESS

Outlook Express presenta molte caratteristiche avanzate, che non verranno qui esaminate, ma che possono interessare l'utente:

- **LA GESTIONE DI PIÙ ACCOUNT E-MAIL**, che permette all'utente di raccogliere messaggi inviati a più indirizzi, nel caso disponga di più di una casella sul server di posta elettronica;
- **LA GESTIONE DI PIÙ IDENTITÀ**, che permette a più utenti, identificandosi all'avvio del programma, di utilizzare Outlook Express;
- **IL BLOCCO DEI MITTENTI**, che evita di scaricare dal server messaggi indesiderati provenienti da determinati soggetti;



- **LA CREAZIONE DI REGOLE PIÙ COMPLESSE E ARTICOLATE, PER UNA GESTIONE IN AUTOMATICO DEI MESSAGGI** (per esempio per rispondere in automatico ai messaggi durante la propria assenza);
- **LA CRITTOGRAFIA DEI MESSAGGI, SIA IN USCITA SIA IN ENTRATA**, che garantisce la privacy della posta elettronica;
- **L'UTILIZZO DI HTML PER MANDARE MESSAGGI GRAFICAMENTE AVANZATI**, come le pagine Web.



## LE MAILING LIST

Abbiamo già visto che i programmi di posta elettronica permettono di inviare lo stesso messaggio a più di un destinatario: per farlo è sufficiente inserire nel campo del destinatario un elenco di indirizzi separati dalla virgola. Quando si crea un gruppo nella propria rubrica, inoltre, si utilizza in pratica una lista personale cui corrisponde un elenco di più destinatari.

Si potrebbe dire che le mailing list rappresentano il passo successivo: si tratta di sistemi che permettono la diffusione di messaggi di posta elettronica, e perciò la condivisione di informazioni e conoscenze, all'interno di un gruppo di utenti Internet unito da un interesse in comune. Queste persone possono entrare in contatto reciproco e scambiarsi messaggi, in modo che ogni messaggio spedito da una di loro sia ricevuto da tutte le altre.

In pratica una lista è un elenco di indirizzi di posta elettronica, che si trova su un nodo della Rete - il server della lista - al quale chiunque è interessato può aggiungere automaticamente il proprio nome. Ogni lista dispone di un indirizzo di posta elettronica: i messaggi inviati a questo indirizzo saranno automaticamente spediti a tutti gli iscritti della lista. Un programma specifico, denominato **LISTSERVER**, situato sullo stesso computer che ospita la lista, si occupa di tutte le operazioni connesse alla gestione della lista e dell'aggiornamento dell'elenco degli iscritti.

Per iscriversi a una mailing list è necessario scrivere un messaggio al listserver (che ha un indirizzo diverso da quello della lista); di solito si tratta di un messaggio standard con il campo Oggetto vuoto e il cui testo è: **SUBSCRIBE NOMELISTA**.

La procedura per annullare la propria iscrizione è molto simile: bisogna scrivere un altro messaggio al listserver con il testo **UNSUBSCRIBE NOMELISTA** e il campo Oggetto vuoto.

Una volta ricevuta la richiesta di iscrizione, il listserver aggiunge automaticamente il nostro nome all'elenco degli iscritti alla lista. Ciò significa che ci arriverà una copia di tutti i messaggi inviati alla lista da uno qualunque dei suoi membri e che anche noi potremo mandare all'indirizzo della lista dei messaggi, che saranno letti da tutti gli iscritti.

È importante comprendere che il funzionamento delle liste si basa sull'uso di due diversi indirizzi di posta elettronica: l'**INDIRIZZO DEL LISTSERVER**, cui vanno inviati i messaggi per le operazioni "amministrative" (iscrizione, dimissioni...) e l'**INDIRIZZO DELLA LISTA**, cui devono essere spediti i messaggi indirizzati a tutti gli iscritti. Questa modalità permette di gestire in modo pratico le centinaia di iscrizioni che possono giungere a una mailing list, e di far funzionare la lista in modo automatico.

Alcune liste sono caratterizzate dalla presenza di un **MODERATORE**, che decide di accettare o meno le richieste di iscrizione e si occupa di vigilare sul contenuto dei messaggi che circolano in lista. Un moderatore è spesso necessario nelle liste in cui si discutono temi delicati e controversi, per filtrare eventuali messaggi polemici, provocatori o addirittura oltraggiosi. Se la lista non ha un moderatore, tutte le lettere sono pubblicate automaticamente.

Il numero di mailing list attualmente disponibili in Rete è sterminato, e si accresce di giorno in giorno. Nell'avvicinarsi alle mailing list, la prima difficoltà potrebbe quindi essere reperire e selezionare le liste che potrebbero davvero interessare e fornire informazioni utili.

In Rete si possono trovare liste per discutere praticamente su ogni argomento, dalle piante grasse allo yoga, dall'Epatite C ai telefilm. Ci sono liste scientifiche, economiche, politiche, letterarie, che trattano argomenti più o meno specifici a vari livelli, liste dedicate agli amanti dei gatti o delle piante grasse, tanto per fare degli esempi casuali. Molto numerose sono le liste che trattano di informatica, e di argomenti di informatica molto specifici (per esempio, un determinato programma, o un particolare modello di computer). Molte liste sono pubbliche, altre sono riservate a gruppi di lavoro o di studio. Alcune liste sono definite a "forte traffico", perché contraddistinte dallo scambio di decine di messaggi al giorno, altre hanno ritmi più tranquilli (uno o due messaggi la settimana).

Lo strumento sicuramente più potente per trovare liste su qualsiasi argomento è il database **LISZT** ([WWW.LISZT.COM](http://WWW.LISZT.COM)), che contiene oltre 90.000 liste, di cui circa 3000 "selezionate" e inserite in un indice sistematico denominato "Liszt select", e consente di effettuare ricerche per parole chiave.



Per trovare mailing list di potenziale interesse si possono consultare anche siti che contengono elenchi di liste, come [WWW.CLEARINGHOUSE.NET](http://WWW.CLEARINGHOUSE.NET) e, per le liste italiane, [WWW.CILEA.IT/MAILLIST](http://WWW.CILEA.IT/MAILLIST).



## LA NETIQUETTE

Esiste un vero e proprio galateo che regola la comunicazione via posta elettronica e, in generale, attraverso Internet. Si tratta di norme che dovrebbero essere familiari a tutti e il cui rispetto è segno di correttezza e di cortesia.

In generale si suggerisce di essere concisi, evitare ambiguità ed esporre i concetti in modo chiaro e ordinato.

Nel campo Oggetto di un'e-mail è opportuno specificare sempre un titolo chiaro per i propri messaggi, in modo che gli interlocutori possano farsi subito un'idea di cosa si tratti.

Utilizzare le maiuscole è un po' come urlare: è bene ricorrervi, quindi, soltanto per sottolineare un punto che si ritiene realmente importante o per evidenziare un titolo o un sottotitolo.

Poiché il testo scritto non sempre permette di cogliere e valutare elementi quali il significato ironico di una frase, è sempre meglio cercare di essere espliciti. Proprio per ovviare all'impossibilità di rendere tutti quelli elementi "di relazione" che completano la comunicazione interpersonale e aiutano a interpretare i contenuti (come l'espressione del viso, l'intonazione della voce), gli utenti di Internet hanno sviluppato alcuni meccanismi di comunicazione che permettono di esprimere in forma codificata emozioni e stati d'animo: gli **EMOTICONS** o "**FACCINE**", icone costruite con simboli e caratteri della tastiera. Il simbolo più famoso è lo "**SMILE**", utilizzato per indicare il tono scherzoso di un'osservazione. Si costruisce con i due punti, il trattino orizzontale e la parentesi chiusa. Quando si digitano questi caratteri, alcuni programmi (tra questi Word, se non si modifica l'impostazione di default) riconoscono lo smile e creano in modo automatico una faccina rotonda sorridente.

Esistono moltissimi "emoticons" di questo tipo, ma anche in questo caso è consigliabile usarli solo se si è certi che i propri interlocutori siano in grado di comprenderne il significato.

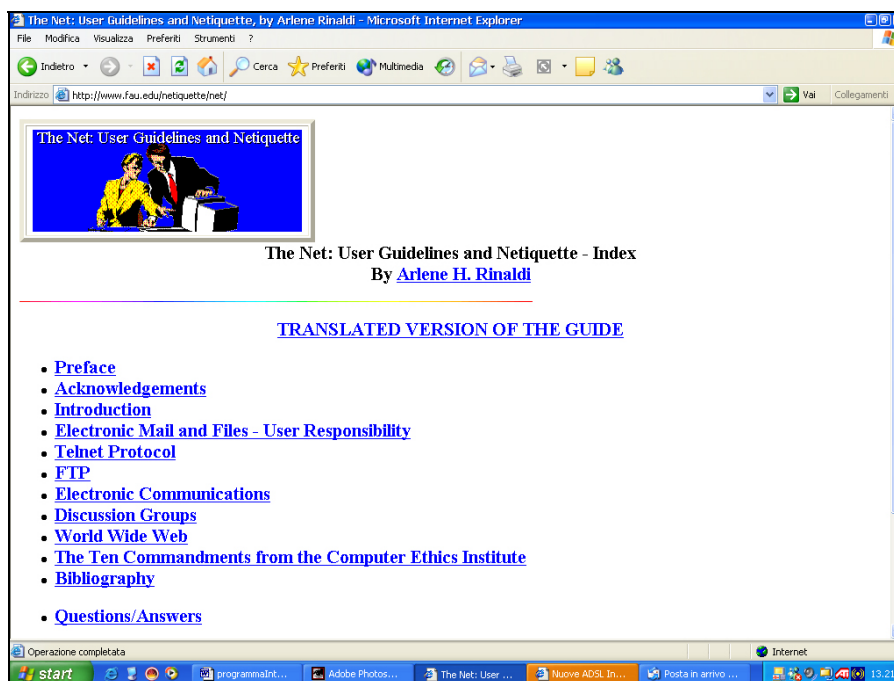
Ecco alcune delle "faccine" più utilizzate:

:~)	Contentezza
:-(	Tristezza
:~o	Sorpresa
:~@	Urlo
:~l	Indifferente
:~e	Delusione
>:~<	Matto da legare
:~D	Risata
;~)	Occhiolino
@}~>---	Invio una rosa

Il rispetto della netiquette diventa particolarmente importante per chi scrive a una mailing list, e si rivolge quindi a una molteplicità di destinatari contemporaneamente. Per essere davvero efficaci i messaggi inviati a una lista dovrebbero essere sintetici, chiari e limitarsi a trattare un argomento per volta (da specificare sempre nell'oggetto del messaggio). La mailing list è fatta per discutere un argomento ben definito. Se si vuole comunicare qualcosa di non attinente a qualche iscritto (in gergo si dice **OFF-TOPIC**) è sempre meglio farlo sotto forma di messaggio personale.

Nelle liste, inoltre, è importante evitare i messaggi polemici o, peggio, gli insulti personali (in gergo si chiamano **FLAMES**): poiché i messaggi sono letti da più persone, e perciò sono pubblici, capita facilmente che anche lievi accenni polemici o sottolineature ironiche, che passerebbero inosservati in una comunicazione personale, possano creare irritazione e suscitare reazioni indispettite.

Quando si partecipa a una mailing list (ma quanto detto vale in generale), infine, vanno rispettate alcune indicazioni di carattere tecnico: **EVITATE DI FORMATTARE I MESSAGGI IN HTML** (è una funzionalità avanzata consentita da programmi come Outlook Express), **UTILIZZATE LA LETTERA SEGUITA DA UN APOSTROFO AL POSTO DELLE LETTERE ACCENTATE**, che potrebbero non essere riconosciute come tali dagli utenti che leggono la posta con programmi diversi dal vostro, **USATE LE CITAZIONI IN MODO OPPORTUNO E INCLUDETE UNA FIRMA IN FONDO AL MESSAGGIO**, così da essere identificati con certezza dai vostri destinatari. Una guida alla netiquette si può consultare presso la **NETIQUETTE HOME PAGE**, all'indirizzo [WWW.FAU.EDU/NETIQUETTE/NETIQUET-TE.HTM1](http://WWW.FAU.EDU/NETIQUETTE/NETIQUET-TE.HTM1). In questo sito sono disponibili anche i link alle copie tradotte della guida.



## POSTA ELETTRONICA E VIRUS

La più diffusa preoccupazione riguardo all'uso della posta elettronica è la possibilità di ricevere via email **VIRUS INFORMATICI** in grado di distruggere i dati memorizzati sul nostro computer (tale mezzo di diffusione è attualmente il più comune).

Per capire quanto sia fondata questa preoccupazione, può essere utile comprendere il funzionamento dei virus. I virus informatici sono programmi in grado di introdursi in altri programmi e di modificarne il comportamento. Alcuni sono innocui e si limitano a creare effetti di disturbo, per esempio facendo apparire scritte stravaganti sullo schermo, altri possono essere molto pericolosi e causare danni di vario tipo: possono cancellare file, rallentare il funzionamento del computer, ridurre lo spazio disponibile nella memoria principale, segnalare falsi malfunzionamenti; nei casi più gravi riescono a distruggere la **FILE ALLOCATION TABLE (FAT)** e a rendere il disco rigido inutilizzabile. La perdita di tutte le informazioni archiviate sul computer è il danno peggiore che i virus possono compiere; essi non sono però in grado di danneggiare le componenti fisiche del computer.

Essendo programmi, i virus non possono diffondersi attraverso semplici messaggi "testuali" di posta elettronica. I messaggi di solo testo sono sempre sicuri. Un potenziale rischio sono i file allegati ai messaggi. Attraverso gli **ATTACHMENT**, infatti, possono diffondersi due tipi di virus: programmi eseguibili, in genere caratterizzati dall'estensione **.EXE** e **MACROVIRUS**, inseriti per esempio in documenti Word o Excel. Per difendersi dal primo tipo di virus di solito basta fare un po' di attenzione: i programmi eseguibili allegati a messaggi provenienti da persone che non si conoscono non devono mai essere avviati, se non dopo aver ottenuto garanzie sulla loro provenienza e sul loro contenuto. Allo stesso modo, è sempre bene diffidare dei messaggi che arrivano da persone conosciute ma che hanno qualcosa di strano.

La peculiarità di molti virus, infatti, è proprio la capacità di autoinviarsi agli indirizzi contenuti nella rubrica di posta elettronica del computer infettato, trasformando il proprietario in un ignaro autore.

Di tanto in tanto, comunque, capita di ricevere messaggi di posta elettronica che avvertono della diffusione di nuovi pericolosissimi virus e mettono in guardia contro messaggi dal titolo sospetto (del genere: "Attenzione: se ricevete un messaggio che ha come titolo Win a holiday non apritelo... cancellerà ogni cosa contenuta nel vostro hard disk..."). In questi casi ci sono buone probabilità che si tratti di uno scherzo: in gergo si chiamano **VIRUS HOAX** ("**BUFALE**", si potrebbe dire), falsi avvertimenti riguardo a un virus. Se vi arriva un messaggio di questo tipo, potete verificare di cosa si tratta consultando una pagina specifica del sito Symantec, **[HTTP://WWW.SYMANTEC.COM/AVCENTER](http://www.symantec.com/avcenter)**, che è sempre aggiornata sugli ultimi virus e virus hoax in circolazione.



Alcuni virus che si diffondono abbastanza frequentemente attraverso la posta elettronica, ma non solo, sono i **MACROVIRUS**, o **VIRUS DI MACRO**. Come abbiamo visto a proposito di Word ed Excel, le macro sono sequenze di operazioni che vengono "impacchettate" in un unico comando. Attraverso le macro è possibile associare ad alcuni documenti particolari comandi, in modo che all'apertura del documento si producano determinate azioni. Il rischio è che le macro in questione siano utilizzate per fare danni invece che per svolgere compiti utili, per esempio interferiscano con il contenuto o l'impaginazione dei documenti e si propaghino ad altri file dello stesso tipo, rinominandoli o addirittura cancellandoli.

Poiché le istruzioni macro sono salvate all'interno di normali documenti Word o Excel, chi apre i file può trovarsi a eseguirle automaticamente e quindi essere infettato. I macrovirus non sono facili da riconoscere. Le ultime versioni di Microsoft Office offrono una discreta protezione, avvisando sempre della presenza di macro nei documenti che si stanno aprendo e permettendo di disabilitare l'esecuzione di macro "insicure".

La difesa più affidabile, comunque, è l'utilizzo di un software antivirus, che permetta di individuare i macrovirus e di eliminarli.

## COME SONO FATTI I VIRUS

Il virus è composto da una serie di istruzioni che vengono inserite all'interno delle istruzioni di un altro programma, il programma portatore, confondendosi con esso. Il numero limitato di istruzioni contenute in un virus fa sì che esso sia leggero e facilmente trasportabile: in questo modo può avere maggiore probabilità di diffondersi senza essere riconosciuto dai sistemi ospite. Al momento dell'esecuzione del programma portatore, viene subito eseguito il codice del virus, che inizia a diffondersi cercando altri programmi cui attaccarsi, in modo da contagiare tutto il sistema. Da questo procedimento di infezione, che assomiglia a quello dei virus veri, deriva anche il nome dato a questo tipo di programmi.

Di solito i virus sono scritti con linguaggi di programmazione definiti "di basso livello" (come l'Assembler), ovvero linguaggi in grado di lavorare a diretto contatto con le istruzioni in linguaggio macchina del computer. In questo modo, infatti, i virus sono in grado di interferire con funzioni base del computer, come la scrittura sui registri di memoria, la creazione o cancellazione di file e cartelle, senza essere intercettati dai filtri di controllo del sistema operativo.

Molto spesso, per esempio, i virus agiscono sulla tabella di allocazione dei file, lo schedario dove sono registrate le posizioni dei file sul disco rigido, oppure sul settore di boot, ovvero la parte del disco che contiene il programma per il caricamento del sistema operativo nella memoria RAM (in questo caso si parla di una particolare categoria di virus, i **VIRUS DI BOOT**: essi risiedono nel settore di avvio del disco rigido e si attivano nello stesso momento in cui il computer viene acceso).

Alcuni, infine, distinguono tra virus e **WORMS**. Un worm è un tipo particolare di virus, in grado di replicare se stesso e di utilizzare la memoria, ma senza attaccarsi ad altri programmi. Un worm può arrivare a occupare tutta la memoria RAM, o tutto il disco rigido, e "soffocare" in questo modo il PC.

## GLI ANTIVIRUS

Lo strumento più sicuro per difendersi dai virus sono i programmi antivirus, software specifici che sono in grado di riconoscere eventuali virus presenti sul computer e di rimuoverli.

Gli antivirus controllano continuamente i dischi e la memoria del computer, per individuare la stringa di comandi che compone un virus e, in caso positivo, ripuliscono i file infetti. Ogni antivirus possiede un archivio delle tracce virali dei virus di cui è in grado di riconoscere i comandi, ma deve essere aggiornato con frequenza per poter individuare i nuovi "ceppi virali" che vengono via via scoperti dai ricercatori.

Tra gli antivirus più famosi si possono citare il **McAFEE VIRUSSCAN** ([WWW.MCAFEE.COM](http://www.mcafee.com)), il **NORTON ANTIVIRUS** ([WWW.NORTON.COM](http://www.norton.com)), **F-SECURE** ([WWW.DATAFELLOWS.COM](http://www.datafellows.com)), **DR. SOLOMON** ([WWW.DRSOLOMON.COM](http://www.drsoolomon.com)), **PC-CILLIN** ([WWW.ANTIVIRUS.COM](http://www.antivirus.com)). Dopo avere installato un antivirus, ricordatevi di aggiornarlo regolarmente (si possono prelevare i nuovi file di descrizione dei virus direttamente dal sito del produttore), così da avere gli "anticorpi" del vostro computer sempre agguerriti contro i nuovi virus che vengono continuamente sviluppati. Se non viene mantenuto aggiornato, infatti, l'antivirus diventa presto inutile.

Infine, sottolineiamo che i virus possono essere trasmessi anche scaricando programmi infetti da un sito, oppure attraverso lo scambio di dischetti. Per difendersi con sicurezza dai virus è quindi importante prendere anche altre precauzioni, come prelevare file soltanto da server sicuri e non scaricare programmi di dubbia provenienza, proteggere contro la scrittura tutti i dischetti su cui non occorre scrivere, evitare il passaggio di floppy da un computer all'altro a meno che non si sia certi della "salute" dell'altro computer, e avere un **SISTEMA DI BACKUP** e ripristino di programmi e dati.

Infine è molto utile tenere sempre **AGGIORNATO IL SISTEMA OPERATIVO** installato sull'elaboratore. In tal senso la Microsoft ha messo a punto negli ultimi anni un apposito sito internet dove è possibile effettuare l'aggiornamento on-line ([HTTP://V4.WINDOWSUPDATE.MICROSOFT.COM/IT/DEFAULT.ASP](http://v4.windowsupdate.microsoft.com/it/default.asp)).

